FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESTRATEGIAS DE CIBERSEGURIDAD PARA MEJORAR LA ROBUSTEZ DE LA CONTINUIDAD DEL NEGOCIO OPERATIVO EN LOS ENTORNOS CLOUD DE ITIPERU, LIMA 2023

Línea de investigación:

Ingeniería de software, simulación y desarrollo de TICs

Tesis para optar el título profesional de Ingeniero de Sistemas

Autor:

Estrada Torres, Carlos Gilmer

Asesor:

Alfaro Bernedo, Juan Oswaldo

ORCID: 0000-0002-9803-5986

Jurado:

López Juárez, Bertha Beatriz

Zevallos León, Máximo

Aparicio Montenegro, Pablo Roberto

Lima - Perú

2024

ESTRATEGIAS DE CIBERSEGURIDAD PARA MEJORAR LA ROBUSTEZ DE LA CONTINUIDAD DEL NEGOCIO OPERATIVO EN LOS ENTORNOS CLOUD DE ITIPERU, LIMA 2023.

INFORME DE ORIGINALIDAD

26%	25%	7%	13%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	4%
2	hdl.handle.net Fuente de Internet	3%
3	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	1%
4	repositorio.unfv.edu.pe Fuente de Internet	1%
5	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
6	www.incibe.es Fuente de Internet	1%
7	repositorio.usmp.edu.pe Fuente de Internet	<1%
8	www.ibm.com Fuente de Internet	<1%

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESTRATEGIAS DE CIBERSEGURIDAD PARA MEJORAR LA ROBUSTEZ DE LA CONTINUIDAD DEL NEGOCIO OPERATIVO EN LOS ENTORNOS CLOUD DE ITIPERU, LIMA 2023.

Línea de investigación:

Ingeniería de Software, simulación y desarrollo de TIC's

Tesis para optar el Título Profesional de Ingeniero de Sistemas

Autor:

Estrada Torres, Carlos Gilmer

Asesor:

Alfaro Bernedo, Juan Oswaldo

ORCID: 0000-0002-9803-5986

Jurado:

López Juárez, Bertha Beatriz

Zevallos León, Máximo

Aparicio Montenegro, Pablo Roberto

Lima - Perú

2024

Agradecimiento

Expreso mi profunda gratitud hacia Dios, quien ha sido mi constante fuente de fuerza e inspiración a lo largo de este recorrido. Mis padres merecen un especial reconocimiento por su amor y apoyo incansable, que han sido fundamentales en mi viaje. A mi hermano, le agradezco por estar siempre a mi lado y brindarme su apoyo y consejos. Un agradecimiento especial a mis profesores, cuya guía ha sido esencial en mi desarrollo profesional como ingeniero de sistemas. Y, por supuesto, no puedo dejar de agradecer a mis amigos por su inestimable amistad y apoyo, que han sido vitales en los momentos más desafiantes de mi carrera académica. Todos ustedes han jugado un papel crucial en alcanzar este importante hito.

Dedicatoria

Dedico este logro a mis padres, cuyo amor y apoyo incondicional han sido mi mayor motivación. A mi hermano, por su compañía y aliento, que han sido esenciales en mi camino. También, extiendo esta dedicación a mi Universidad, por brindarme un entorno académico enriquecedor y oportunidades cruciales para mi desarrollo profesional. Todos ustedes han sido pilares fundamentales en esta importante etapa de mi vida.

ÍNDICE

Pág.

RESUMEN……vii

ABSTRACT……viii

I. INTRODUCCIÓN……1

1.1. Descripción y formulación del problema……1

1.2. Antecedentes……6

1.3. Objetivos……13

-Objetivo general……13

-Objetivos específicos……14

1.4. Justificación……14

1.5. Hipótesis……16

II. MARCO TEÓRICO……17

2.1. Bases teóricas sobre el tema de investigación……17

III. MÉTODO……31

3.1. Tipo de Investigación……31

3.2. Ámbito temporal y espacial……32

3.3. Variables……32

3.4. Población y muestra……36

3.5. Instrumentos……37

3.6. Procedimientos……43

3.7. Análisis de datos……44

3.8. Consideraciones éticas……45

IV. RESULTADOS……46

V. DISCUSIÓN DE RESULTADOS……..……..……..82

VI. CONCLUSIONES……..……..…….…85

VII. RECOMENDACIONES……..……..…..86

VIII. REFERENCIAS…….87

IX. ANEXOS…….96

ÍNDICE DE TABLAS

Tabla 1. Validación de expertos……..42

Tabla 2. Prueba de Alfa De Cronbach – fiabilidad ……43

Tabla 3. Análisis descriptivo del pre test y post test……...46

Tabla 4. Prueba de la normalidad……...47

Tabla 5. Comparación de la autentificación multifactor Pre Test vs. Post Test…….48

Tabla 6. Comparación de los derechos de acceso en el Pre Test vs. Post Test……...49

Tabla 7. Comparación del monitoreo de acceso al usuario en el Pre Test vs. Post Test……50

Tabla 8. Comparación del control de acceso en el Pre Test vs. Post Test…….….51

Tabla 9. Comparación seguridad de accesos en el Pre Test vs. Post Test…….….53

Tabla 10. Comparación protección de datos sensibles en el Pre Test vs. Post Test……..….54

Tabla 11. Comparación criptografía en el Pre Test vs. Post Test……...55

Tabla 12. Comparación protocolos seguros en el Pre Test vs. Post Test……56

Tabla 13. Comparación del plan de acción de Pre Test vs. Post Test…….57

Tabla 14. Comparación de las políticas para el manejo seguro de los certificados digitales de Pre Test vs. Post Test…….58

Tabla 15. Comparación el impacto en la continuidad del negocio Pre Test vs. Post Test…….59

Tabla 16. Comparación el impacto de una brecha de seguridad Pre Test vs. Post Test…….60

Tabla 17. Comparación del impacto ante un ataque de seguridad Pre Test vs. Post Test……..61

Tabla 18. Comparación del impacto financiero Pre Test vs. Post Test……..63

Tabla 19. Comparación del impacto por fallas en el alojamiento web Pre Test vs. Post Test…...64

Tabla 20. Comparación de la frecuencia de vulnerabilidades de seguridad Pre Test vs. Post Test……..65

Tabla 21. Comparación de la frecuencia de vulnerabilidades de seguridad Pre Test vs. Post Test……..67

Tabla 22. Comparación del aprovechamiento de las vulnerabilidades Pre Test vs. Post Test…...68

Tabla 23. Comparación de la probabilidad de que fallas humanas Pre Test vs. Post Test…….69

Tabla 24. Comparación de la probabilidad de ataques a los servidores de alojamiento web Pre Test vs. Post Test…….71

Tabla 25. Comparación de la identificación de mecanismos de seguridad en los servicios alojados Pre Test vs. Post Test……...72

Tabla 26. Comparación de las políticas de seguridad Pre Test vs. Post Test…….73

Tabla 27. Comparación de los procedimientos ante incidentes de seguridad Pre Test vs. Post Test……..75

Tabla 28. Comparación de configuraciones de la red Pre Test vs. Post Test…….76

Tabla 29. Comparación de acuerdos de confiabilidad Pre Test vs. Post Test……77

Tabla 30. Comprobación de la hipótesis general……79

Tabla 31. Comprobación de la hipótesis específica 1…….79

Tabla 32. Comprobación de la hipótesis específica 2…….80

Tabla 33. Comprobación de la hipótesis específica 3…….81

ÍNDICE DE FIGURAS

Figura 1. Ciberataques en el país Perú 2023……3

Figura 2. Etapas de la ciberseguridad……17

Figura 3. Principales tendencias de ciberseguridad……19

Figura 4. Interacción entre nubes cloud……21

Figura 5. Niveles de Cloud Computing……22

Figura 6. Máquinas virtuales……23

Figura 7. Portal Web……24

Figura 8. Estructura de la ISO 27001……27

Figura 9. Zero Trust Security……28

Figura 10. Máquinas virtuales……30

Figura 11. Relación de variables……32

Figura 12. Población de máquinas virtuales……36

Figura 13. Población de páginas web……36

Figura 14. Sección del cuestionario para control de accesos……38

Figura 15. Sección del cuestionario de criptografía……39

Figura 16. Cuestionario de seguridad de las operaciones……40

Figura 17. Sección del cuestionario de seguridad de las comunicaciones……41

Figura 18. Formula de Alfa de Cronbach……43

Figura 19. Diagrama de comparación de autentificación multifactor……48

Figura 20. Diagrama de comparación de derechos de acceso……50

Figura 21. Diagrama de comparación de monitoreo de acceso al usuario……51

Figura 22. Diagrama de comparación de control de acceso……52

Figura 23. Diagrama de comparación seguridad de accesos……..……..53

Figura 24. Diagrama de comparación protección de datos sensibles…….……..…54

Figura 25. Diagrama de comparación de criptografía…….……55

Figura 26. Diagrama de comparación de protocolos seguros…….…….56

Figura 27. Diagrama de comparación de plan de acción…….……57

Figura 28. Diagrama de comparación políticas para el manejo seguro de los certificados digitales……....58

Figura 29. Diagrama de comparación del impacto en la continuidad del negocio……..60

Figura 30. Diagrama de comparación del impacto de una brecha de seguridad…….61

Figura 31. Diagrama de comparación del impacto ante un ataque de seguridad……62

Figura 32. Diagrama de comparación del impacto financiero……63

Figura 33. Diagrama de comparación del impacto por fallas en el alojamiento web…….……65

Figura 34. Diagrama de comparación de la frecuencia de vulnerabilidades de seguridad…….66

Figura 35. Diagrama de comparación de la frecuencia de vulnerabilidades de seguridad…….67

Figura 36. Diagrama de comparación del aprovechamiento de las vulnerabilidades……..…69

Figura 37. Diagrama de comparación de la probabilidad de que fallas humanas……...70

Figura 38. Diagrama de comparación de probabilidad de ataques a los servidores de alojamiento web……...71

Figura 39. Diagrama de comparación de la identificación de mecanismos de seguridad en los servicios alojados……73

Figura 40. Diagrama de comparación de las políticas de seguridad……...74

Figura 41. Diagrama de comparación de los procedimientos ante incidentes de seguridad……76

Figura 42. Diagrama de comparación de configuraciones de la red……77

Figura 43. Diagrama de comparación de acuerdos de confiabilidad……...78

RESUMEN

El propósito de la siguiente investigación fue determinar el grado de influencia que se produce al implementar estrategias de ciberseguridad sobre la robustez de la continuidad del negocio operativo en los entornos cloud de ITIPERU, Lima-Perú 2023. Según ello, la población de estudio abarcó la infraestructura tecnológica: hosting, cloud microsoft Azure, portales web, sistemas web y máquinas virtuales. El muestreo fue no probabilístico por conveniencia, asimismo la técnica de recolección de datos fue a través de la observación de campo y la encuesta, empleándose un diseño cuasiexperimental, donde se realizó una prueba pre-test y post-test con un instrumento validado más la prueba Alfa de Cronbach de 0,885. Para el análisis de las hipótesis de empleó la prueba no paramétrica de Wilcoxon. La implementación consistió en adaptar la normativa ISO 27001 y la herramienta Zero trust según las necesidades de la infraestructura cloud de ITIPERU. Según ello, se halló que la estrategia de ciberseguridad mejoró la robustez de la continuidad del negocio operativo con un nivel de significancia de 0,005. Además, el análisis de los tres indicadores de la variable continuidad de negocio demostraron mejoras significativas luego de la implementación de estrategias de ciberseguridad; disponibilidad de servicio cloud (p=0,005), tiempo de recuperación de la integridad (p=0.003), y gestión de incidencias (p=0.005). Concluyendo que la adopción de estrategias de ciberseguridad mejora la continuidad de negocio operativo de ITIPERU.

Palabras clave: ISO 27001, ciberseguridad, Zero trust, continuidad de negocio.

ABSTRACT

The purpose of the following research was to determine the degree of influence that occurs when implementing cybersecurity strategies on the robustness of operational business continuity in the cloud environments of ITIPERU, Lima-Peru 2023. Accordingly, the study population covered the technological infrastructure: hosting, Microsoft azure cloud, web portals, web systems and virtual machines. The sampling was non-probabilistic by convenience, likewise the data collection technique was through field observation and survey, using a quasi-experimental design, where a pre-test and post-test was performed with a validated instrument plus Cronbach's Alpha test of 0.885. The Wilcoxon non-parametric test was used to analyze the hypotheses. The implementation consisted of adapting the ISO 27001 standard and the Zero trust tool according to the needs of ITIPERU's cloud infrastructure. Accordingly, it was found that the cybersecurity strategy improved the robustness of operational business continuity with a significance level of 0.005. In addition, the analysis of the three indicators of the business continuity variable showed significant improvements after the implementation of cybersecurity strategies; cloud service availability (p=0.005), integrity recovery time (p=0.003), and incident management (p=0.005). Concluding that the adoption of cybersecurity strategies improves ITIPERU's operational business continuity.

Key words: ISO 27001, cybersecurity, zero trust, business continuity.

I. INTRODUCCIÓN

Los beneficios de los entornos digitales y sucesos como la COVID-19, fortaleció la perspectiva de tener un medio virtual para iniciar el intercambio de un servicio y/o bien por un costo monetario. Con lo cual la experiencia física o tradicional, ha sido trasladado a los medios digitales por las empresas y/o organizaciones, para facilitar el desarrollo de diferentes actividades comerciales, educativas o de índole social (Chiriboga, Tapia, Fuentes, & Sánchez,2022).

Ante este fenómeno, la transformación digital de las empresas es un hecho, por lo que, el control de la seguridad de la información se traslada a los entornos cloud. Siendo así, que a lo largo del tiempo de han planteado diferentes estrategias de ciberseguridad, para asegurar la protección de datos, aumentar la resiliencia de la infraestructura cloud, y gestionar eficazmente los incidentes de seguridad (Rojas et al., 2023).

1.1. Descripción y formulación del problema

De acuerdo al Foro Económico Mundial (FEM, 2022), reportó que los entornos digitales han revolucionado la comunicación empresarial de manera significativa, transformando la forma en que las empresas se comunican, operan y se relacionan con sus clientes, socios comerciales y empleados. Permitiendo una comunicación instantánea y sin límites, es decir, las empresas logran comunicarse de forma rápida y eficiente a través de correos electrónicos, videoconferencias, chats en línea y otras herramientas de comunicación digital.

Sin embargo, la interconexión a nivel global ha incrementado las vulnerabilidades informáticas de las organizaciones, por lo tanto, las Pequeñas y Medianas Empresas (PYMES) como las grandes empresas enfrentan retos similares en ciberseguridad. La principal insuficiencia que surge dentro de las PYMES es la limitación en recursos, equipos y presupuestos de seguridad, con lo cual, son posicionados desfavorablemente frente a las amenazas cibernéticas. Al ser

frecuentemente proveedores o socios de entidades más grandes y al estar conectadas digitalmente; las PYMES pueden ser vistas por los ciberdelincuentes como accesos indirectos para comprometer sistemas de organizaciones de mayor envergadura o robustez (Sánchez et al., 2021).

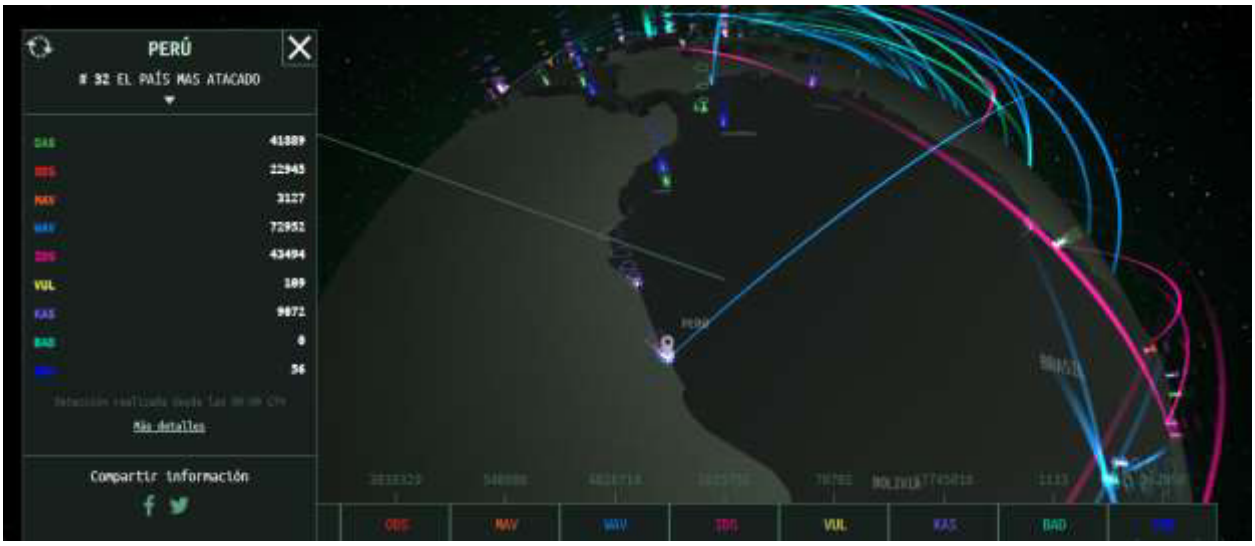
Ante la dependencia tecnológica en todas las áreas de una organización externa e internamente, la Comisión Económica para América Latina y el Caribe (CEPAL) en el 2021 mencionó que la regularización de los riesgos tecnológicos como la privacidad de los datos y las amenazas de ciberseguridad deben promoverse para el desarrollo digital (CEPAL, 2022). Debido a ello, la propuesta de emplear un medio de protección para el sistema de información con estrategias de seguridad ha demostrado que tiene una enorme influencia para aumentar los niveles de competitividad (Medeiros et al., 2019).

De esta manera, al poseer un protocolo básico de ciberseguridad en las PYMES es imperativo que permita asegurar la continuidad del negocio a través de la defensa virtual contra los ciberataques (Bustillos y Rojas, 2022). Por ejemplo, un reporte realizado por Kaspersky en el 2022 mencionó que las PYMES de américa latina han presentado amenazas a través del virus troyano, los ataques de internet, y los ataques al Protocolo de Escritorio Remoto; lo cual ha involucrado una pérdida económica en promedio de 155 mil dólares, y una disminución de su reputación (Kaspersky, 2022).

Por ello, la compañía de Kaspersky Lab desarrolló una plataforma virtual para visualizar las diferentes amenazas cibernéticas como malware, virus, entre otros ataques en tiempo real como se observa en la Figura 1.

Figura 1

Ciberataques en el país Perú 2023



Nota. Captura de imagen realizado de la página web de Kaspersky Ciberamenaza-Mapa en tiempo real en Perú.

En consecuencia, la continuidad de negocio de una empresa podría verse afectada por la falta de gestión en la protección de datos y la vulnerabilidad de las operaciones en los entornos cloud. Además, los informes sobre la continuidad de negocio y los ciberataques son limitados, ya que, no se ha estipulado por alguna institución manera formal que se encargue de contabilizar las pérdidas económicas respecto a los ciberataques a las empresas (Calvillo, 2020).

Para ello, la Organización Mundial de Trabajo (OIT, por su sigla en inglés) mencionó que la continuidad de negocio debe presentar tres categorías: medidas preventivas, arreglos de preparación y opciones de respuesta (Rodríguez, 2021). Una encuesta realizada por CEPAL, mencionó que los ataques a la seguridad fueron a través del phishing fue de 31%, vulnerabilidades asociado a productos de hardware y software en 30%, y robo de credenciales de 29%, fueron algunas de las causas más frecuentes de las empresas. Asimismo, las empresas que tienen un

tamaño entre uno a nueve empleados dentro de la organización supera más del 80% de ciberataques anualmente (Díaz, 2022).

Los entornos cloud computing han permitido que las empresas mejoren los servicios y los sistemas de información, sin embargo, las PYMES presentan dificultades para la adaptación en este ámbito informático, ya que a un mantienen una nube privada mientras que las grandes empresas han implementado un servicio público y/o hibrido permitiendo afrontar con más facilidad los retos tecnológicos, debido al incremento de la competitividad electrónica (Guevara y Domingo, 2022).

Con lo cual, la Organización Internacional de Normalización (ISO, sigla en inglés), han desarrollado diferentes documentos, que son un marco de referencia internacional para ser aplicado en cualquier organización, ya sea privada o pública (ISO, s.f.). Para este proyecto de investigación se abordará la ISO/IEC 27001 y el modelo de Zero Trush (confianza cero) que abarca la seguridad de la información para implementar estrategias de ciberseguridad y medir la repercusión en la continuidad de negocio operativo en entornos cloud.

1.1.1. Situación problemática

ITIPERU SAC, es una empresa ubicada en el distrito de Independencia en Lima-Perú. Se dedica desde hace 4 años a proveer servicios de tecnologías de la información a diversas empresas y negocios. Su oferta incluye alojamiento web, desarrollo de portales web, soluciones Cloud y outsourcing de gestión de servicios de TI; proyectos que son llevados a cabo tanto en sus propias instalaciones de la empresa como también en las oficinas de los clientes.

A pesar de su crecimiento y consolidación en el mercado, ITIPERU SAC enfrenta desafíos significativos relacionados con la seguridad en la administración de sus páginas web y máquinas virtuales hospedadas en Microsoft Azure de sus clientes. La situación problemática identificada

revela carencias como la falta de autenticación multifactor en la administración; derechos de acceso desactualizados; ausencia de un monitoreo efectivo de los accesos de usuarios; controles de acceso insuficientes basados en roles; y una deficiente configuración de sistemas de alerta de seguridad.

Ante esta realidad, se plantea implementar estrategias de ciberseguridad empleando normativas internacionales como la ISO 27001 y una herramienta de ciberseguridad como Zero Trust que permita ayudar a mitigar los riesgos asociados, y garantizar la protección de la información, tanto de la empresa como de sus clientes. La implementación de autenticación multifactor, la revisión periódica de los derechos de acceso, el establecimiento de controles de acceso por roles, la instalación de sistemas de monitoreo y alertas proactivas son medidas esenciales que el presente estudio plantea para solucionar la problemática de ITIPERU. Este enfoque no solo está dirigido a resolver las vulnerabilidades actuales, sino también a establecer un marco de seguridad brindando una continuidad sostenible que pueda adaptarse a los desafíos emergentes, en el dinámico entorno de la ciberseguridad y la continuidad de negocio operativo.

1.1.2. Formulación del problema

Redactar adecuadamente el enunciado para la formulación del problema de investigación, constituye un gran reto, porque influirá en el enfoque y desarrollo del estudio; es decir, permitirá orientar el concepto central de la investigación y se expondrá la razón que impulsa al investigador a explorar un tema específico (Arias, 2022).

1.1.3. Problema General

¿En qué medida la implementación de estrategias de ciberseguridad, contribuyó a mejorar la robustez de la continuidad del negocio operativo en los entornos cloud de ITIPERU, Lima-2023?

1.1.4. Problemas Específicos

¿De qué manera la implementación de estrategias de ciberseguridad, mejoró la disponibilidad de servicios cloud en ITIPERU?

¿De qué manera la implementación de estrategias de ciberseguridad, mejoró el tiempo de recuperación de la integridad en entornos cloud en ITIPERU?

¿De qué manera la implementación de estrategias de ciberseguridad, mejoró las incidencias en los entornos cloud en ITIPERU?

1.2. Antecedentes

La presentación de los antecedentes de una investigación se determina en función de las variables involucradas en el estudio y del grupo demográfico considerado. En cada uno de los antecedentes, es esencial incluir el nombre del autor, la fecha en que se realizó el estudio, el asunto central de la investigación y el hallazgo más significativo (Arias, 2022).

1.2.1. A nivel Internacional

Mora (2020), presentó la metodológica para la gestión de la seguridad de la información alineada a la norma ISO 27001 y ciberseguridad con la ISO/IEC 27032. Se enfocó en los activos físicos e intangibles de la organización, como servidores, equipos de red, aplicaciones informáticas, sistemas operativos y gestores de bases de datos. Se empleó metodologías de evaluación de activos como CID (Confidencialidad, integridad, disponibilidad). y MAGERIT para determinar la importancia y criticidad de la información que contienen. En cuanto a la planificación y análisis de riesgos, la metodología integra herramientas establecidas por ISO 27001 y ISO/IEC 27032 para una gestión de riesgos orientada a la seguridad de la información. Se documentan los parámetros de especificación de los planes de acción en función del nivel o prioridad determinado. Finalmente, implemento un Sistema de Gestión de Seguridad de la

Información (SGSI) eficiente, que se centra en la reducción de la probabilidad de incidentes de seguridad de la información y en la mejora continua a través de procesos de aprendizaje.

Amancha (2020), implementó en la Cooperativa de Ahorro y Crédito Sierra Centro mediadas de seguridad; por lo que la metodología fue multifacética, es decir que incluyó investigación bibliográfica, de campo y aplicada. La fase de investigación bibliográfica consistió en revisar libros, investigaciones previas y normas internacionales relevantes para fundamentar el marco teórico en seguridad informática y de la información, así como la continuidad del negocio. En la investigación de campo, se utilizaron encuestas y entrevistas dirigidas a usuarios, técnicos de sistemas y al gerente general para obtener una comprensión detallada de la situación actual y las necesidades específicas de la cooperativa. Esto se complementó con un análisis de los resultados obtenidos para entender las vulnerabilidades y amenazas existentes. La metodología aplicada resultó en la elaboración del Plan Director de Seguridad, basándose en la información recopilada y los análisis realizados. Este plan incluyó la definición de políticas de seguridad informática, y políticas de la información adicionales para proteger los activos tecnológicos de la cooperativa. Concluyó que el plan de seguridad es una herramienta esencial para mejorar la seguridad informática y asegurar la continuidad operativa de la Cooperativa de Ahorro y Crédito Sierra Centro Ltda., mitigando así los riesgos asociados con la ciberseguridad y aumentando la confianza en sus capacidades tecnológicas.

Cifre (2020), verificó el cumplimiento de las cláusulas de la norma ISO 2230 para determinar el nivel de madurez de la empresa en relación con la gestión de la continuidad del negocio. Este estándar proporciono una guía detallada sobre las fases necesarias para el diseño de un plan de continuidad del negocio. Para el análisis de impacto en el negocio, se llevó a cabo un Business Impact Analysis que permitió identificar los procesos prioritarios de la empresa y evaluar

su nivel de criticidad, para determinar el impacto que causaría su interrupción. En lo que respecta al análisis de riesgos, se utilizó la metodología MAGERIT, la cual es un estándar para la gestión de riesgos de los sistemas de información que considera la disponibilidad, integridad y confidencialidad de la información como dimensiones de valoración. Con estos procedimientos, el estudio buscó ofrecer una estructura sólida para la creación de un plan que permitiera a la empresa afrontar incidentes y minimizar el tiempo de inactividad de los servicios.

Díaz-Parco (2022), tuvieron como objetivo principal desarrollar un Plan de Continuidad del Negocio para el departamento de TI de la empresa TELECOMSEC, con el propósito de mantener la operatividad durante interrupciones no planificadas. La metodología aplicada incluyó la recopilación de datos sobre la infraestructura tecnológica y los servicios de la empresa, el análisis de impacto del negocio para determinar procesos y servicios críticos, y el análisis de riesgos utilizando la metodología MAGERIT para evaluar las amenazas y vulnerabilidades. El resultado principal fue la creación de un plan estructurado con estrategias de recuperación alineadas a la norma internacional ISO 22301:2019, considerando diferentes escenarios de riesgo. Este plan incluyó la definición de pruebas, mantenimiento y revisión, así como la capacitación relevante para el personal técnico. La conclusión del autor resalta la importancia de contar con un plan como un componente esencial para la resiliencia empresarial. Esto refuerza positivamente la imagen y reputación de la empresa frente a sus clientes y partes interesadas.

Gutiérrez (2022), realizó una investigación de campo con un enfoque cualitativo y descriptivo para proponer estrategias de recuperación para los servicios críticos y establecer tiempos de recuperación necesarios frente a eventos de vulnerabilidad. La unidad de análisis se basó en entrevistas a miembros de la empresa intervisión y a encargados de soluciones tecnológicas con cargos gerenciales que participan en procesos clave de la organización. Se utilizó

un enfoque inductivo, partiendo de observaciones específicas para obtener conocimientos generales, y la recolección de datos se apoyó en guías del Instituto de Ciberseguridad de España (INCIBE), encuestas electrónicas, y metodologías como NIST y COBIT 5 para identificar riesgos y las medidas necesarias para mitigarlos. Los resultados del estudio permitieron identificar los servicios críticos de la PYME Intervisión que podrían verse afectados por vulnerabilidades, tales como servidores de aplicaciones, web, equipos de computación y dispositivos de comunicación. Se establecieron políticas de respaldo y se analizó la situación actual de la empresa para elaborar una matriz de riesgos que identifica amenazas y su probabilidad. En conclusión, la investigación buscó mejorar la seguridad de la información y la continuidad del negocio en Intervisión mediante el análisis de procesos y políticas de ciberseguridad, utilizando una metodología apoyada en estándares reconocidos y datos recogidos directamente de la empresa.

1.2.2. A nivel Nacional

Mendoza y Vega (2019), se llevó a cabo una evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad en la empresa "SISC". El propósito de esta investigación consistió en identificar posibles deficiencias en el ámbito de ciberseguridad relacionadas con la detección y respuesta a eventos de ciberseguridad en dicha empresa. Se procuró, de esta manera, determinar los controles necesarios para subsanar las deficiencias identificadas y proponer un plan de implementación para dichos controles. Como marco de referencia, se adoptó la versión 1.1 del marco elaborado por el National Institute of Standards and Technology de Estados Unidos (NIST). Como resultado de este proyecto de investigación, se espera que las empresas orientadas a implementar soluciones tecnológicas para la protección contra ciberataques desarrollen un enfoque basado en procesos que les permita mejorar sus capacidades de detección y respuesta frente a eventos de ciberseguridad. En el ámbito específico de la empresa evaluada, este trabajo ha

contribuido a que la gerencia aumente su comprensión sobre los aspectos de ciberseguridad, identifique los tipos de riesgos a los que está expuesto, y adopte una gestión más efectiva en el ámbito de la ciberseguridad.

Vilcarromero (2019), desarrolló un sistema de gestión de ciberseguridad destinado al centro de operaciones de seguridad de una empresa de telecomunicaciones, con el propósito de mejorar un marco existente de ciberseguridad. La finalidad era crear una solución que facilitara la implementación, operación, monitoreo, revisión y mejora continua. La metodología de adopción empleada para llevar a cabo este marco, se centra en una gobernanza coherente, buscando tomar decisiones informadas de manera efectiva. En resumen, el marco del NIST propuesto en esta iniciativa contribuye a la formulación de estrategias de ciberseguridad específicamente diseñadas para una empresa del sector de las telecomunicaciones. Este enfoque se basa en el análisis de experiencias y publicaciones reconocidas en la materia, priorizando la ciberseguridad como un tema de alta relevancia y ayudando a identificar los servicios críticos para la organización.

Cabezas (2020), desarrolló un marco de trabajo de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima. Esto incluyó la identificación, evaluación y armonización de las normas y controles relacionados con la ciberseguridad, y la demostración del modelo sugerido aplicándolo en una empresa real. La metodología fue la PDCA (Plan-Do-Check-Act), que es un ciclo iterativo de cuatro fases que promueve la mejora continua en todos los procesos. La investigación se basó en controles de seguridad de la ISO/IEC 27001 y 27002, así como en los controles críticos de seguridad CIS y los lineamientos del marco de trabajo de ciberseguridad NIST CSF. Se elaboró un inventario de activos de hardware y software, y se diseñó una matriz de roles y responsabilidades. Además, se implementó un plan de gestión de riesgos, se gestionaron cuentas de usuario y contraseñas, se

protegió la red empresarial, se desarrolló un plan de concientización y capacitación, se estableció una gestión de copias de seguridad. Concluyendo con una implementación exitosa del marco de trabajo de ciberseguridad, generando mayor responsabilidad y conciencia en función de la seguridad cibernética. Se destacó la importancia de la mejora continua y la adaptación de los controles de ciberseguridad a las necesidades específicas de cada empresa.

Salinas (2020), elaboró una propuesta para un modelo de ciberseguridad con un nuevo enfoque para cajas municipales durante la transformación digital. Este modelo incluyó características de integridad, confidencialidad y disponibilidad, buscando adaptarse a las exigencias de la transformación digital, responder a amenazas y ataques informáticos que evolucionan constantemente. Incluyó la identificación y comparación de distintos modelos de ciberseguridad, además de proponer características aplicables para un modelo nuevo. Los métodos se centraron en el análisis de la población y muestra de cajas municipales, aplicando técnicas e instrumentos adecuados para la recolección. Los resultados del estudio incluyeron el desarrollo de una propuesta basada en el modelo de ciberseguridad "Zero Trust", siguiendo el marco de gestión de ciberseguridad NIST. Se diseñó un modelo organizacional basado en niveles estratégicos, operacionales y tácticos en forma de pirámide, para mejorar la gestión de la ciberseguridad y facilitar la comunicación entre departamentos. Además, se modificó el organigrama del departamento de seguridad de la información, creándose una nueva sección dentro del departamento de Tecnologías de la Información llamada "Seguridad informática", y se diseñó una arquitectura de seguridad para proteger el perímetro y lo que se encuentra fuera de él (internet). Se implementó una matriz de soporte de 20 controles de seguridad CIS y se desarrollaron acciones para fortalecer la cultura de ciberseguridad en la organización. La propuesta se validó mediante un juicio de expertos con usuarios potenciales. Concluyó con la identificación y evaluación de

modelos de ciberseguridad existentes, como "Defensa en Profundidad", "Modelo Perimetral", "Modelo Zero Trust" y "Modelo Think Security". Las características necesarias del modelo se determinaron y validaron a través de una lista de cotejo por parte de usuarios potenciales. La propuesta final integró el modelo "Zero Trust", un diseño organizacional renovado, la matriz de controles CIS, y estrategias para crear una cultura organizacional de ciberseguridad, todo lo cual fue validado por expertos en ciberseguridad.

Murga (2022), aplicó la Metodología Zero Trust para mejorar la seguridad en la infraestructura de red de una empresa. Tuvo un enfoque cuantitativo de tipo cuasi experimental, caracterizado por la no selección aleatoria de sujetos y centrado en el análisis de datos numéricos para validar los objetivos planteados en la investigación. Se utilizaron entrevistas para recolectar datos y software estadístico para el análisis, con un enfoque particular en la seguridad de la infraestructura de red y la implementación de la Metodología Zero Trust como variable independiente. Los resultados del pre-test mostraron que la mayoría de los usuarios no tenían dificultades para acceder a los recursos compartidos y que no era necesario ingresar credenciales para conectarse a dichos recursos. No se utilizaban filtros de seguridad para el inicio de sesión en el sistema ERP, y la navegación en internet no era consistentemente fluida. Además, se encontró que una proporción significativa de usuarios experimentaba desconexiones con el sistema ERP o los módulos utilizados para su trabajo diario. El análisis de las entrevistas reveló que no todos los perfiles de usuario de Windows requerían contraseña para el acceso y que muchos no contaban con un grupo de trabajo local o un dominio de red local. Estos hallazgos sugieren áreas de vulnerabilidad y oportunidades para mejorar la seguridad de la infraestructura de red mediante la implementación de la Metodología Zero Trust. Concluyó que la infraestructura de red era vulnerable y presentaba varias áreas de riesgo, lo que justifica la necesidad de implementar mejoras

en la seguridad. La Metodología Zero Trust se identificó como una solución potencial para proteger los recursos dentro y fuera de la infraestructura de red, garantizando la seguridad de la información.

Castillo (2022), presentó un plan para detectar amenazas involuntarias de ciberseguridad en entidades gubernamentales originadas por el personal interno, a partir de su conducta en la infraestructura de tecnologías de la información. Vinculó una serie de patrones de comportamiento en el personal interno de las instituciones públicas con las posibles amenazas no intencionales de ciberseguridad. El proceso inicial se inició con la definición de los elementos, seguido por una fase de diseño individual para cada uno, centrándose principalmente en la lista de patrones de comportamiento y la matriz de gestión de riesgos. Estos elementos marcan la diferencia con otras investigaciones y tienen la capacidad de adaptarse a nuevas situaciones que puedan surgir como parte de los procesos de TI en una o varias organizaciones.

1.3. Objetivos

Los objetivos de investigación son acciones que indican las metas que se plantean. Una vez que se logra el objetivo de la investigación, se alcanzan las metas propuestas. Es importante tener en cuenta que los objetivos indican lo que se hará en la investigación, pero no señalan cómo se hará o cuál es la importancia de hacerla (Coronel, 2023).

1.3.1. Objetivo general

Determinar el grado de influencia que ejerce la implementación de estrategias de ciberseguridad, en la robustez de la continuidad del negocio operativo en los entornos cloud ITIPERU, Lima 2023.

1.3.2. Objetivos específicos

Determinar el grado de influencia que ejerce la implementación de estrategias de ciberseguridad en la disponibilidad de servicios cloud en ITIPERU.

Determinar el grado de influencia que ejerce la implementación de estrategias de ciberseguridad en el tiempo de recuperación de la integridad en entornos cloud en ITIPERU.

Determinar el grado de influencia que ejerce la implementación de estrategias de ciberseguridad en las incidencias en los entornos cloud en ITIPERU.

1.4. Justificación

Involucra la identificación y descripción de las brechas en el conocimiento que la investigación se propone a disminuir. Se presentan diversos razonamientos para respaldar la relevancia de la investigación desde una perspectiva teórica, metodológica y práctica (Bonet et al., 2023).

1.4.1. Teórica

En el contexto de transformación digital y la creciente adopción de tecnologías en la nube, las empresas se enfrentan a un panorama de amenazas cibernéticas de manera dinámica y compleja. ITIPERU, integrando activamente soluciones basadas en la nube como portales web y máquinas virtuales, se expone a riesgos inherentes que podrían comprometer la integridad, disponibilidad y confidencialidad de sus operaciones. Este proyecto busca no solo identificar y analizar las vulnerabilidades y amenazas en estos entornos digitales, sino también diseñar y proponer estrategias de mitigación y prevención que sean efectivas y escalables. Al hacerlo, no solo protegeremos los activos de información de la empresa, sino que también preservaremos su valor y reputación en el mercado, asegurando la confianza de clientes y socios. La implementación de estas medidas es crucial para el cumplimiento de las regulaciones vigentes y representa una

inversión estratégica que reducirá costos a largo plazo al evitar incidentes de seguridad, minimizando interrupciones y maximizando la resiliencia operativa.

1.4.2. Metodológica

Para el desarrollo de la tesis, es primordial la selección de un marco metodológico que no solo se alinee con las mejores prácticas internacionales, sino que también se adapte a las particularidades de ITIPERU. La normativa ISO/IEC 27001 proporciona un sistema de gestión de seguridad de la información (SGSI) que garantiza la protección de los datos a través de un enfoque sistemático y constante. Adicionalmente, el modelo Zero Trust se enfoca en la premisa de 'nunca confiar, siempre verificar', lo cual es esencial en un entorno donde las amenazas internas y externas son cada vez más sofisticadas. La integración de estos dos pilares metodológicos permitirá a ITIPERU no solo fortalecer su postura de seguridad sino también promover una cultura de ciberseguridad consciente y proactiva. La adopción de estas estrategias resultará en la minimización de riesgos y en la optimización de la continuidad del negocio, asegurando la integridad y disponibilidad de los servicios críticos de la empresa.

1.4.3. Práctica

La adopción práctica de la norma ISO/IEC 27001 junto con el modelo Zero Trust en ITIPERU es crucial para anticiparse y fortalecer las defensas frente a la naturaleza cambiante de las amenazas digitales. El SGSI establecido por la ISO/IEC 27001 no solo sistematiza la identificación y gestión de riesgos de seguridad, sino que también asegura la conformidad con las regulaciones vigentes, fortaleciendo la confianza entre clientes y socios. Zero Trust añade una capa adicional de seguridad al no presuponer confianza alguna, exigiendo constante verificación en todos los accesos a recursos de la empresa, una práctica especialmente pertinente en la protección de infraestructuras en la nube. La integración de estos enfoques no es meramente una mejora de la

seguridad; representa una evolución hacia una gestión más inteligente y una cultura de seguridad proactiva. Así, ITIPERU no solo elevará su postura de seguridad, sino que también se diferenciará en el mercado, incrementará su eficiencia operativa y disminuirá los costos resultantes de incidentes de seguridad.

1.5. Hipótesis

Es una proposición que puede ser tanto aceptada como rechazada; para ello, se recopila información previa, con el fin de establecer conexiones entre los hechos y ofrecer una explicación sobre sus causas. Por lo general, se exponen inicialmente las razones evidentes que respaldan la creencia en la viabilidad de algo, concluyendo finalmente con una afirmación (Espinoza, 2018).

1.5.1. Hipótesis general

La implementación de estrategias de ciberseguridad mejora la robustez de la Continuidad del Negocio operativo en los entornos cloud en ITIPERU, Lima 2023.

1.5.2. Hipótesis especificas

La implementación de estrategias de ciberseguridad mejora la disponibilidad de servicios cloud en ITIPERU.

La implementación de estrategias de ciberseguridad mejora el tiempo de recuperación de la integridad en entornos cloud en ITIPERU.

La implementación de estrategias de ciberseguridad mejora las incidencias en los entornos cloud en ITIPERU.

II. MARCO TEÓRICO

2.1. Bases teóricas sobre el tema de investigación

2.1.1. Ciberseguridad

La ciberseguridad implica salvaguardar dispositivos, redes, aplicaciones de software, sistemas esenciales y datos ante posibles amenazas digitales. Las organizaciones tienen la responsabilidad de resguardar la integridad de los datos, asegurando la confianza del cliente y cumpliendo con las normativas establecidas. Para ello, emplean medidas y herramientas específicas de ciberseguridad destinadas a prevenir el acceso no autorizado a datos confidenciales y evitar interrupciones en las operaciones empresariales causadas por actividades de red indeseadas. La implementación de la ciberseguridad se lleva a cabo mediante la optimización de la defensa digital en la interacción entre personas, procesos y tecnologías. (Mendivil et al., 2022).

De manera, que se ha establecido criterios universales para garantizar la seguridad de los entornos cloud, como, por ejemplo, el ciclo de ciberseguridad, que describe cinco aspectos importantes, con el fin de garantizar la persistencia de las operaciones comerciales, tal como se evidencia en la Figura 2.

Figura 2

Etapas de la ciberseguridad

Nota. Adaptado del grafico de la página web de Ontek (2018), Las 5 etapas del ciclo de ciberseguridad.

2.1.2. Importancia de la ciberseguridad

En diversas industrias como la energética, el transporte, el comercio minorista y la manufactura, la implementación de sistemas digitales y conectividad de alta velocidad desempeña

un papel crucial al ofrecer servicios eficientes a los clientes y facilitar operaciones comerciales rentables. Así como se protegen los activos físicos, es imperativo salvaguardar los recursos digitales y los sistemas contra accesos no deseados. La ocurrencia involuntaria de violaciones y accesos no autorizados a sistemas informáticos, redes o recursos interconectados se denomina ciberataque (Orozco, 2021).

2.1.3. Tipos de ciberseguridad

2.1.3.1. Protección de infraestructuras esenciales. Esto se centra en sistemas vitales como la energía y el transporte, donde una falla o pérdida de datos podría desestabilizar a la sociedad. Un abordaje metódico para su ciberseguridad es imperativo.

2.1.3.2. Seguridad de red. Refiere a las defensas para dispositivos conectados en una red, utilizando herramientas como firewalls y sistemas de control de acceso, para gestionar permisos y acceso a recursos digitales.

2.1.3.3. Ciberseguridad en la nube. Enfatiza en la protección de datos y aplicaciones en entornos de nube, crucial para mantener la confianza del cliente y la resiliencia operativa, a la vez que se cumple con las regulaciones de privacidad.

2.1.3.4. Seguridad en el Internet de las Cosas (IoT). Apunta a la protección de dispositivos que se operan a través de internet, los cuales, debido a su conectividad constante y posibles fallos de software, representan un riesgo adicional.

2.1.3.5. Seguridad de datos. Protege los datos tanto en tránsito como almacenados, usando métodos como cifrado y copias de seguridad seguras para prevenir brechas de datos.

2.1.3.6. Seguridad en aplicaciones. Se enfoca en reforzar la seguridad de las aplicaciones desde su diseño hasta su implementación, promoviendo el desarrollo de código seguro.

2.1.3.7. Seguridad de punto final. Trata los riesgos asociados con el acceso remoto a la red corporativa, analizando archivos en dispositivos individuales para detectar y mitigar amenazas.

Para aplicar algún tipo de método de ciberseguridad en las organizaciones, More (2022) mencionó que debe considerar diferentes aspectos en la práctica para ampliar la capacidad de protección, señaló siete principios (Figura 3).

Figura 3

Principales tendencias de ciberseguridad

Nota. Fuente: More (2022)

2.1.4. Tipos de ataques informáticos

A continuación, se proporcionan algunos casos típicos de amenazas cibernéticas.

2.1.4.1. Malware. Es un término colectivo para programas diseñados para infiltrarse o dañar sistemas sin consentimiento. Incluye varios tipos de software perjudicial que buscan acceder a información privada o perturbar infraestructuras esenciales, como virus y spyware.

2.1.4.2. Ransomware. Es una estrategia comercial y conjunto de tecnologías que criminales utilizan para chantajear a organizaciones por dinero. Recursos especializados están disponibles para proteger contra amenazas de ransomware, especialmente en plataformas como Amazon Web Services (AWS, 2023).

2.1.4.3. Ataque de intermediario. Ocurre cuando un agente no autorizado intenta interceptar comunicaciones de datos, aumentando la vulnerabilidad de información delicada como detalles financieros.

2.1.4.4. Phishing. Es un tipo de amenaza cibernética que se vale del engaño para obtener datos personales. Los atacantes suelen usar correos que engañan a usuarios para que entreguen información sensible o descarguen archivos dañinos que pueden introducir malware.

2.1.4.5. Ataques DDoS. Son esfuerzos coordinados para inutilizar un servidor con una avalancha de peticiones falsas, lo que impide el acceso legítimo al servidor afectado.

2.1.4.6. Amenaza interna. Es un peligro para la seguridad que proviene de empleados maliciosos dentro de una empresa, quienes tienen acceso privilegiado y pueden comprometer la seguridad de los sistemas internos.

2.1.5. Cloud

El concepto de computación en la nube surge de un cambio de paradigma tecnológico que integra elementos como la computación distribuida, los centros de procesamiento de datos, la virtualización y el escalado de recursos informáticos; todo ello disponible según las necesidades del cliente a través de internet. Este enfoque, originado en la visión de Sun Microsystems de que "la red es el computador", se desmarca significativamente de la era anterior de la informática centrada en el PC. La computación en la nube amplía este enfoque al permitir el acceso a múltiples ordenadores interconectados a través de una red, proporcionando así recursos de procesamiento y

almacenamiento con una finalidad específica y con mayor facilidad de acceso y gestión de datos (Tenorio, 2017).

2.1.5.1. Tipos de Clouds. Se describen tres categorías.

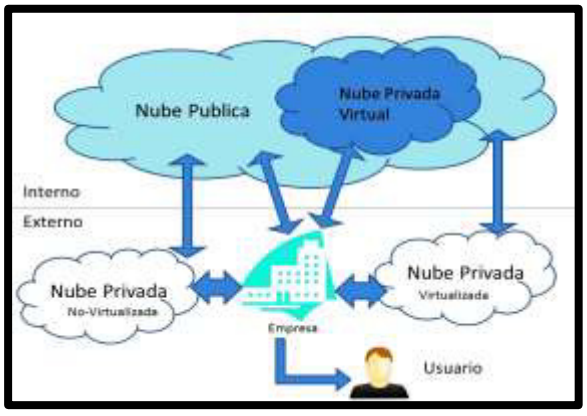
A. ***Nube pública.*** Esta modalidad utiliza una infraestructura que se comparte con otras organizaciones, incluyendo hardware, almacenamiento y recursos de red. Ejemplos prominentes incluyen servicios de Amazon, Google y Microsoft Azure, donde los costes se distribuyen entre todos los usuarios.

B. ***Nube privada.*** Se caracteriza por ofrecer software como servicio que se aloja internamente en una organización. Los servicios se restringen a la organización, y es una opción preferida para empresas financieras que manejan información sensible. Sus beneficios principales son una mayor flexibilidad, control y capacidad de escalabilidad.

C. ***Nube híbrida.*** Integra componentes de nubes públicas y privadas. Permite a las organizaciones seleccionar qué información crítica y confidencial se mantiene en una nube privada, mientras se aprovecha la nube pública para recursos adicionales cuando es necesario, como en la Figura 4.

Figura 4

Interacción entre nubes cloud



Nota. Visualización de la integración de los diferentes tipos de cloud.

2.1.6. Principales Cloud Computing (Figura 5)

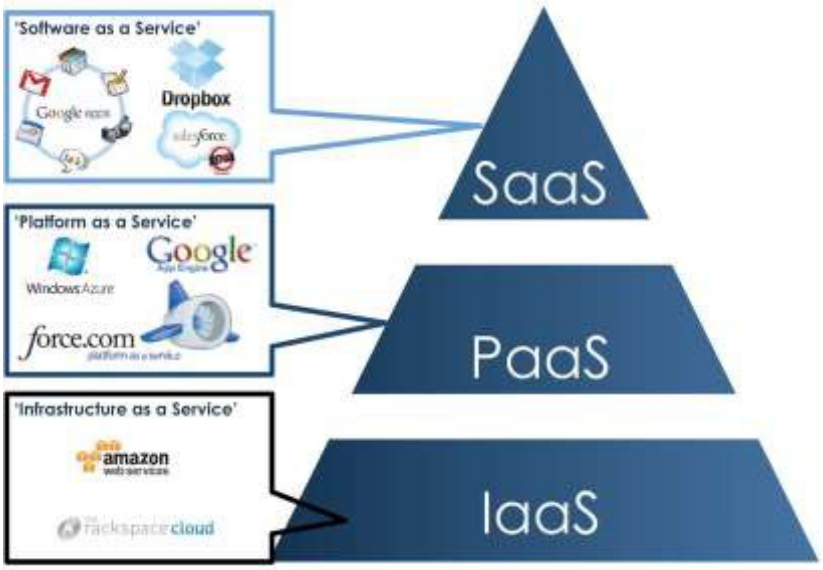
2.1.6.1. PaaS (Plataforma como Servicio): Este modelo ofrece un entorno virtual donde los usuarios pueden alojar datos y desarrollar sus aplicaciones personalizadas. Facilita la gestión del ciclo de vida de las aplicaciones, desde el desarrollo hasta la implementación, sin la complejidad de mantener la infraestructura.

2.1.6.2. SaaS (Software como Servicio): Proporciona aplicaciones listas para usar, alojadas en la nube del proveedor, eliminando la necesidad de instalaciones locales. Los usuarios acceden a estas aplicaciones a través de Internet, generalmente bajo un modelo de suscripción.

2.1.6.3. IaaS (Infraestructura como Servicio): Ofrece recursos de computación virtualizados como espacio de disco, potencia de procesamiento, bases de datos y transferencia de datos. Este servicio permite a los usuarios escalar y reducir recursos técnicos sobre demanda, pagando solo por lo que utilizan.

Figura 5

Niveles de Cloud Computing



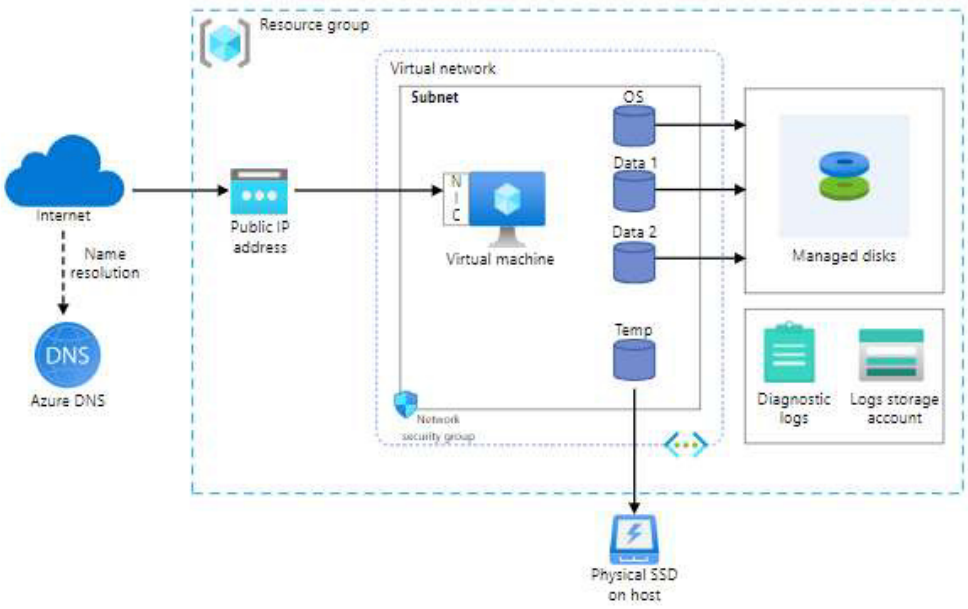
Nota. Fuente: Condor y segura (2017).

2.1.7. Maquina virtuales

Una máquina virtual es una representación virtual, o emulación, de una computadora física. A menudo se refieren a ellas como "huésped" mientras la máquina física en la que se ejecutan se conoce como el "host". La virtualización permite crear varias máquinas virtuales, cada una con su propio sistema operativo (SO) y aplicaciones como si fuera una máquina física. Una máquina virtual no puede interactuar directamente con un sistema físico. En cambio, necesita una capa de software ligera, llamada hipervisor, para coordinarse con el hardware físico subyacente. El hipervisor asigna recursos informáticos físicos, como procesadores, memoria y almacenamiento, a cada máquina virtual. Mantiene cada máquina virtual separada de las otras para que no interfieran entre sí (Cajicá, 2020).

Figura 6

Máquinas virtuales



Nota. Fuente: Microsoft (s.f).

2.1.8. Portales Web

El propósito esencial de un portal web es facilitar a los usuarios la búsqueda y el acceso a la información requerida sin necesidad de abandonar el sitio, promoviendo así el uso continuo del portal como se muestra en la Figura 7. Los pilares que sustentan los portales web son:

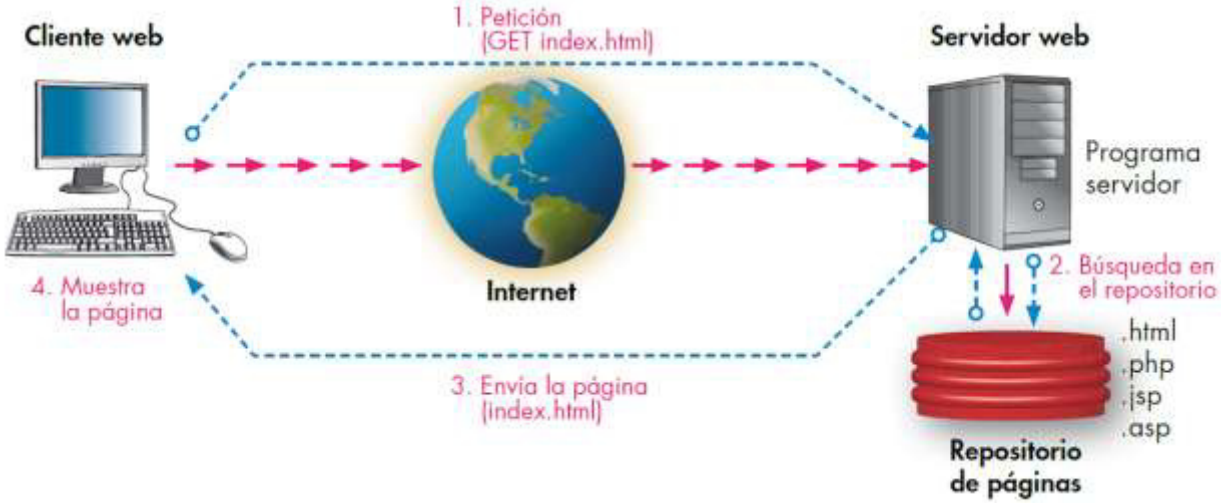
2.1.8.1. Contenido. Integran elementos como motores de búsqueda, directorios y noticias, ofreciendo una amplia gama de servicios.

2.1.8.2. Interacción. Proporcionan plataformas para la participación del usuario, incluyendo aplicaciones interactivas, foros, correo electrónico y espacios de chat.

2.1.8.3. Conveniencia. Ofrecen un punto de acceso unificado para obtener una amplia variedad de información en un solo lugar.

Figura 7

Portal Web



Nota. Fuente: Blogs servidores tutoriales (2015)

2.1.9. Estándares y marcos de trabajo

La ISO describe la normalización como proceso de establecer y aplicar directrices para sistematizar una actividad particular, buscando beneficios y eficiencia colectiva. Este proceso se fundamenta en conocimientos científicos y técnicos acumulados, así como en experiencia práctica,

y está orientado tanto a satisfacer necesidades actuales como a permitir avances futuros, manteniéndose alineado con el progreso continuo. En cuanto a los estándares, la ISO los considera como el conocimiento concentrado y refinado de expertos en el área, que entienden las exigencias de las partes interesadas que representan, incluyendo productores, comerciantes, consumidores, organizaciones de comercio, usuarios finales o entidades reguladoras (ISO, s,f).

2.1.10. Organización Internacional de Normalización

La ISO se dedica principalmente a la creación de estándares técnicos a nivel internacional. Estos estándares de ISO juegan un papel fundamental en mejorar la eficiencia, seguridad y transparencia en el desarrollo, producción y suministro de bienes y servicios. Facilitan el comercio internacional al hacer que las interacciones entre países sean más sencillas y equitativas. Además, ofrecen a los gobiernos un fundamento técnico para la legislación en áreas como salud, seguridad y medio ambiente (ISO, 2022).

2.1.10.1 Norma ISO 27001. Es una normativa establecida por la Organización Internacional de Normalización para asegurar eficazmente la información en distintas entidades. Originariamente lanzada en 2005 como ISO/IEC 27001 - 2005, la siguiente versión fue lanzada en la edición del año 2013 (ISO27001, 2013). Conforme a las directrices de la ISO, se debe realizar una evaluación completa de cualquier norma relacionada cada cinco años para propiciar mejoras continuas y actualizar las secciones necesarias. La versión más actual de la ISO 27001 fue actualizada en 2022, presentando modificaciones importantes en su estructura, particularmente las que se alinean con el "Anexo SL". Las empresas y organizaciones manejan información crítica y es esencial que esta sea manejada con diligencia en todas las operaciones pertinentes al tipo de negocio. Se debe tomar en cuenta que la protección ineficaz de datos conlleva serias repercusiones

que pueden ser de contexto legal, operativo, financiero y estructural, llegando al extremo de causar la clausura de la empresa. (Russell, 2022).

La creciente relevancia de la ISO 27001 y la seguridad de la información es innegable en el panorama actual, donde las organizaciones son cada vez más conscientes de los riesgos y vulnerabilidades que a menudo son explotados. Se está convirtiendo en una verdad inminente que, tarde o temprano, todas las empresas se enfrentarán a desafíos relacionados con la seguridad de sus datos. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) y obtener la certificación ISO 27001 se está volviendo crítico para la mayoría. Esto es especialmente cierto para las empresas encargadas de manejar datos sensibles y de gran valor, ya que la ISO 27001 ofrece beneficios significativos en varias áreas clave (Russell, 2022).

A. Estructura de la ISO27001. Su enfoque en la creciente necesidad de proteger la información dentro de las organizaciones. Su implementación se ha vuelto más común ya que las empresas son cada vez más conscientes de la inevitabilidad de las brechas de seguridad. Un Sistema de Gestión de Seguridad de la Información (SGSI) según la ISO 27001 tiene como objetivo salvaguardar información crítica, como datos personales de empleados, clientes y proveedores, así como información comercial de alto valor, que incluye propiedad intelectual, registros financieros y legales, y datos operativos. En la figura 8 se muestra las categorías de la estructura de la ISO27001.

Figura 8

Estructura de la ISO 27001

CONTROLES DE LA ISO 27001	a.5 Políticas de seguridad
	a.6 Organizacion de la información
	a.7 Seguridad en recursos
	a.8 Gestión de activos
	a.9 Control de accesos
	a.10 Criptografía
	a.11 Seguridad física y ambiental
	a.12 Seguridad de las operaciones
	a.13 Transferencia de la información
	a.14 Adquisición de sistemas, desarrollo y mantenimiento.
	a.15 Relación de los proveedores
	a.16 Gestión de los incidentes de seguridad
	a.17 Continuidad de negocio
	a.18 Cumplimiento con requerimientos legales y contractuales

Nota. Elaboración propia basado en NQA, rescatado de: https://www.nqa.com/es-es/certification/standards/ISO-27001/implementation

2.1.10.2. Norma ISO 22301. La ISO 22301, establecida por la Organización Internacional de Normalización, representa la norma internacional para la Gestión de la Continuidad de Negocio (SGCN). Su propósito es asistir a las organizaciones en la prevención, preparación, respuesta y recuperación ante incidentes imprevistos. Para lograr esto, la norma ofrece un marco práctico que facilita el establecimiento y la administración de un sistema de gestión de continuidad de negocio efectivo. El objetivo principal de la ISO 22301 es salvaguardar a la organización frente a una amplia variedad de amenazas e interrupciones potenciales. (NQA, s.f.).

A. Continuidad de negocio. La gestión de la continuidad empresarial es un proceso crítico que identifica y evalúa las amenazas potenciales a una empresa y el impacto operacional que podrían tener si se concretan. Este proceso es fundamental para construir y mantener la resiliencia organizativa, asegurando que la empresa pueda responder adecuadamente a tales

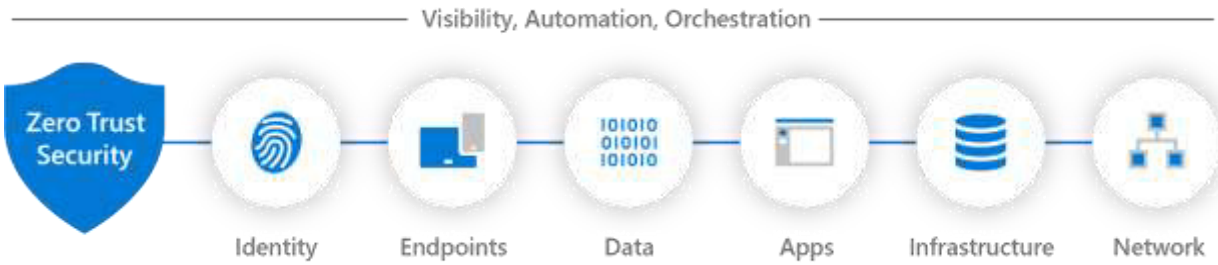
amenazas, adaptarse y continuar sus operaciones. Los planes de continuidad del negocio son esenciales para mitigar interrupciones y asegurar que los productos y servicios se mantengan dentro de plazos aceptables tras incidentes disruptivos, manteniendo así la entrega y operatividad de la empresa (Castro, et al., 2020).

2.1.11. Zero Trust (confianza cero)

El modelo de Zero Trust es una estrategia de seguridad informática que opera bajo el principio de no confiar automáticamente en ningún usuario o sistema, ya sea dentro o fuera de la red corporativa, sin una verificación adecuada. A diferencia de los métodos de seguridad tradicionales que presuponen la seguridad de todo lo que reside dentro de la red, Zero Trust insiste en una comprobación exhaustiva de la identidad y los permisos de acceso para cualquiera que intente acceder a los recursos de la red, siguiendo la norma de "nunca confiar, siempre verificar" para asegurar que ni los sistemas ni los usuarios internos son considerados seguros por defecto (Microsoft, 2023).

Figura 9

Zero Trust Security



Nota. Fuente: Microsoft (2023), rescatado de: https://learn.microsoft.com/es-es/security/zero-trust/zero-trust-overview

Hasta el momento, muchas empresas han adoptado un modelo de trabajo híbrido que brinda a los empleados la flexibilidad de acceder a aplicaciones y datos desde cualquier ubicación, pero

esta transición también ha planteado nuevos desafíos en términos de seguridad. Para abordar estos desafíos y asegurar la integridad de la red, se ha implementado la metodología de Zero Trust (INCIBE, 2023).

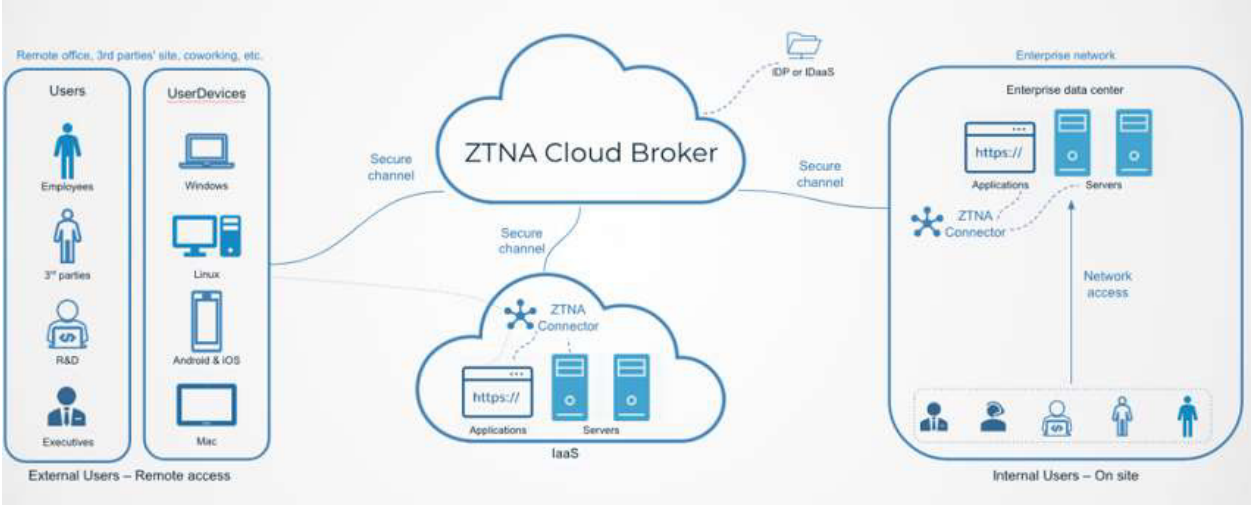
La implementación de un único punto de autenticación tiene como resultado una reducción en la superficie de exposición y centraliza el control de acceso a los servicios esenciales para las tareas laborales. Por medio del uso de Network Access Control (NAC), se logra restringir el acceso únicamente a aquellos dispositivos que demuestren no tener vulnerabilidades, facilitando un acceso seguro a aplicaciones en la nube y protegiendo la red contra posibles amenazas (NVIDIA, 2022).

La microsegmentación amplía el alcance del control de acceso a cualquier aplicación o información, limitándolo de manera precisa a aquellos usuarios que verdaderamente necesitan acceso y solo durante el tiempo necesario. La adopción de la Autenticación Multifactor (MFA) reduce el riesgo de exposición de credenciales, permitiendo a las empresas verificar la identidad de los usuarios y garantizar que solo los autorizados tengan acceso a aplicaciones y datos (Murga, 2022).

La verificación continua de la identidad y la autorización es igualmente esencial para asegurar que solo los usuarios y dispositivos autorizados puedan acceder a recursos protegidos. Cuando se combina con MFA, esta verificación continua se vuelve especialmente efectiva, como se evidencia al verificar la identidad de forma constante mediante diversos factores de autenticación en momentos específicos (INCIBE, 2023).

Figura 10

Máquinas virtuales



Nota. Fuente: CISET (s.f.), rescatado de: https://www.ciset.es/glosario/829-zero-trust-network-access-ztna

III. MÉTODO

3.1. Tipo de Investigación

3.1.1. Tipo de investigación

En este análisis, se determinó que el tipo de investigación es aplicada. De acuerdo con Arias y Covinos (2021), este enfoque busca resolver problemas y encontrar respuestas a preguntas específicas, aplicando conocimientos en la práctica y llevando a cabo estudios científicos con el fin de identificar posibles mejoras en situaciones de la vida cotidiana.

3.1.2. Nivel de investigación

Este estudio, de acuerdo con García y Sánchez (2020), se clasifica como explicativo, ya que implica la caracterización de un hecho, fenómeno, individuo o grupo con el propósito de comprender y establecer su estructura o comportamiento. Los resultados de este tipo de investigación se sitúan en un nivel intermedio en términos de la profundidad del conocimiento alcanzado.

3.1.3. Diseño de investigación

De acuerdo con Ramos-Galarza (2021), el diseño cuasiexperimental es un método de investigación que se utilizará pre-test y pos-test para estudiar los efectos de una intervención en situaciones donde no es posible realizar experimentos controlados aleatorios. Este diseño implica medir un grupo de sujetos en una línea de base (pretest), aplicar la intervención, y luego se evalúa a los mismos sujetos nuevamente después de la intervención (postest). La comparación de las medidas pretest y postest se utilizaron para inferir los efectos de la intervención

Es decir, la presente investigación realizó un análisis situacional inicial de la infraestructura de TI de ITIPERU, el cual fue equivalente al pre-test; para luego aplicar estrategias de ciberseguridad mediante la ISO 27001 y Zero Trush. Seguido de ello, se procedió a aplicar el post-

test, siendo así que se logró analizar el efecto sobre la robustez de la continuidad de negocio operativo en los entornos cloud.

Figura 11

Relación de variables

Nota: Elaboración propia.

Donde:

G = Población de estudio

O1= Pre-test

O2= Pos-test

X= Intervención estrategias de ciberseguridad

3.2. Ámbito temporal y espacial

3.2.1. Ámbito Espacial

La investigación fue llevada a cabo tomando como base la ciudad de Lima-Perú, en el distrito de Independencia, en la empresa ITIPERU SAC.

3.2.2. Ámbito Temporal

Debido a la estructura de la investigación, su desarrollo fue ejecutado durante el mes de setiembre 2023 al mes de diciembre 2023.

3.3. Variables

Una variable representa una cualidad que se mide, controla o manipula en un estudio. Se puede expresar de dos maneras: conceptual y operacional. La conceptualización es la definición teórica de la variable, por lo cual se debe extraer de los antecedentes del estudio; mientras, que la

definición operacional consiste en especificar el proceso propio de la variable según el criterio del investigador basado en los antecedentes (Arias y Covinos, 2022).

3.3.1. Variable independiente

Es la cualidad causal, que se caracteriza por facilitar al investigador su observación y manipulación según sea el caso del estudio (Oyola, 2021).

3.3.1.1. Estrategias de Ciberseguridad. Las estrategias de ciberseguridad afirman la importancia de dar responsabilidades a todas las partes interesadas y preserva la necesidad de proteger la privacidad en los procesos de seguridad con un marco de protección adecuado (Robayo,2022).

3.3.2. ***Variable dependiente***

Es la cualidad que representa el efecto inducido por la variable independiente, permitiendo analizar los cambios favorables o desfavorables de la hipótesis de estudio (Oyola, 2021).

3.3.2.1. Continuidad del Negocio operativo. La continuidad de negocio es la documentación de procesos que sirve de guía a la empresa para responder ante una interrupción y de esta manera recuperar, reanudar y reestablecer la entrega de productos o servicios a un nivel predefinido (Flores,2023).

3.3.1 Operacionalización de variables

Tabla 1.

Matriz de operacionalización de variables

VARIABLE	DEFINICION CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓNES	INDICADORES	FORMULA	ESCALA DE MEDICION	INSTRUMENTO
Estrategias de Ciberseguridad	Son medidas de seguridad cibernética que permitan el sustento y supervivencia de las PYMES en el entorno digital (Bustillos y Rojas,2022).	Se aplicó la norma internacional ISO 27001 asociado a la metodología Zero Trush, para la protección de datos y riesgos de ataques cibernéticos en entornos Cloud de la empresa ITIPERU.	Protección de datos	Control de accesos	TRP-∑respuestas "SI" TRN-∑respuestas "NO"	Ordinal	Ficha de recolección de datos .
				Criptografía	TCA=∑controles aplicados	Ordinal	
			Vulnerabilidades	Seguridad de las operaciones	Indicador de Nivel de Riesgo (NR): Nivel de Impacto (NI) Probabilidad de Ocurrencia de Riesgo (POR) NR=NI×POR	Ordinal	
				Seguridad de las comunicaciones	TRP=∑respuestas "SI" TRN=∑respuestas "NO"	Ordinal	

Continuidad del Negocio operativo	Implica la planificación, preparación y las acciones necesarias para garantizar que una empresa pueda sobrevivir y recuperarse de situaciones que podrían afectar negativamente su capacidad de operar (Olis et al.,2021).	Se medirá a través de indicadores clave (KPIs) para medir de manera efectiva el desempeño de la empresa ITIPERU SAC	Resiliencia en la Infraestructura Cloud	Disponibilidad de Servicios Cloud (%)	Disponibilidad (%) = (Tiempo total - Tiempo de inactividad) / Tiempo total * 100	Razón	Ficha de recolección de datos
				Tiempo de Recuperación de integridad	Tiempo de recuperación= Tiempo de detección + Tiempo de recuperación	Razón	
			Gestión de Incidentes de seguridad de la información	Incidencias	Cantidad de Incidentes Reportados = Número total de incidentes de seguridad reportados en el período de tiempo especificado	Razón	
					Tasa de Éxito en la Resolución de Incidentes (%) = (Número de incidentes resueltos con éxito / Número total de incidentes) x 100	Razón	

3.4. Población y muestra

3.4.1. Población

La población según Neill y Cortez (2018) es definida como un conjunto infinito o finito de sujetos, tanto como personas u objetos, que presentan características similares o comunes entre sí, requeridas para dicha investigación.

En esta investigación, la población que participó estuvo conformado por la infraestructura tecnológica hosting, cloud Microsoft Azure, portales web, máquinas virtuales. A continuación, se muestra las siguientes imágenes que describen la población de estudio.

Figura 12

Población de máquinas virtuales

CARACTERISTICAS MAQUINAS VIRTUALES		N° DE MAQUINAS VIRTUALES
Caracteristicas	**Especificaciones**	
Sistema Operativo	Windows Server 2022	
vCPU	4	**4**
RAM	8 GB	
Generación de VM	V2	
Arquitectura de VM	x64	

Figura 13

Población de páginas web

CARACTERISTICAS HOSTING		PAGINAS WEB ALOJADAS
Caracteristicas	**Especificaciones**	
CPU	2 Nudeos CPU	**6**
RAM	4 GB	
Almacenamiento	90 GB	

3.4.2. Muestra

Es un grupo de elementos elegidos de una población siguiendo un plan predefinido (muestreo), con el propósito de obtener conclusiones que puedan aplicarse a toda la población. (Del Castillo y Pinto, 2018).

Ante ello, la muestra será igual que la población de estudio, ya que, la empresa ITIPERU es una PYME que está en crecimiento, pero presenta algunas limitaciones en recursos, equipos y presupuestos de seguridad, con lo cual, son posicionados desfavorablemente frente a las amenazas cibernéticas.

3.4.3. Muestreo

El muestreo según Ventura (2017) es definida como un pequeño grupo de la población de la cual se está estudiando, representa la mayor población y se usa para sacar conclusiones de la población que se investiga. La muestra en esta investigación fue de tipo no probalístico por conveniencia debido a que este método permitió seleccionar a los participantes idóneos para el proyecto de investigación.

3.5. Instrumentos

3.5.1. Técnicas de recolección de datos

La técnica de recolección de datos según Hernández, Fernández y Baptista. (2014) pueden ser múltiples como: cuestionarios cerrados, registros de datos estadísticos, pruebas estandarizadas, sistemas de mediciones fisiológicas, aparatos de precisión, etc. Para el caso de la presente tesis, se tomó la ficha de recolección.

Por ello, la técnica de recolección de datos que se realizó fue observación de campo y cuasiexperimental, ya que, en la primera fase del proyecto se recolectará información sobre el estado de seguridad virtual de la empresa ITIPERU SAC. Luego, se empleó estrategias de ciberseguridad; para después aplicar el post-test, calculando el grado de influencia de las medidas de ciberseguridad en relación a la continuidad de negocio en entornos cloud.

3.5.2. Instrumentos de recolección de datos

Como instrumento de recolección de datos se empleó la ficha de registros de datos (Anexo B), ya que permitió registrar de manera estructurada y detallada las observaciones directas de la elaboración de estrategias de ciberseguridad para mejorar la robustez en la continuidad de negocio operativo en los entornos cloud, incluyendo control de accesos, criptografía, seguridad de las operaciones, seguridad de las comunicaciones, disponibilidad de los servicios cloud, tiempo de recuperación de integridad, e incidencias.

El instrumento que se realizó en el proyecto de investigación se tomó como referencia de la tesis implementación de controles y cumplimiento de requisitos de la ISO/IEC 27001:2013 para la seguridad de información en una PYME consultora de los autores Sota y Mechan (2018).

La presente investigación tiene dos variables: medidas de estrategia de ciberseguridad y continuidad de negocio operativo; cada una asumió un proceso para medir que se realizó a través de sus dimensiones, indicadores y formulas.

Para la variable de estrategias de ciberseguridad se contempló dos aspectos la protección de datos y las vulnerabilidades, cada una de ellas presenta dos indicadores.

La medición de la protección de datos consistió a través del control de accesos y la criptografía. Para el control de accesos se realizó las siguientes preguntas que serán respondidas con sí y no.

Figura 14

Sección del cuestionario para control de accesos

1.1)Control de accesos	SI	NO	Observaciones
¿Existen procedimientos de autenticación multifactor para el acceso a los recursos críticos?			
¿Se revisan y actualizan periódicamente los derechos de acceso ?			
¿Se registra y monitorea el acceso de usuarios a entornos cloud?			
¿Se utiliza control de acceso basado en roles para limitar el acceso a recursos según la necesidad del usuario?			
¿ Se tiene monitoreo y alertas de seguridad de accesos ?			

Nota. Elaboración propia.

Una vez obtenido el conteo de las preguntas se aplicó la siguiente formula: Total de Respuestas Positivas (TRP) y Total de Respuestas Negativas(TRN), según ello se aplicará la siguiente escala:

- Excelente: TRP igual a 80-100% del total de preguntas.
- Bueno: TRP igual a 60-79% del total de preguntas.
- Aceptable: TRP igual a 40-59% del total de preguntas.
- Insuficiente: TRP menor al 40% del total de preguntas.

Para criptografía se realizó un breve cuestionario con respuestas de si y no, para evaluar la seguridad de las contraseñas administradas por el servidor.

Figura 15

Sección del cuestionario de criptografía

2.1)Criptografía	SI	NO	Observaciones
¿Se utiliza cifrado para proteger los datos sensibles de los entornos cloud?			
¿Se cuenta con politica de controles criptograficos?			
¿Se emplean protocolos seguros (como TLS)?			
¿se cuenta con un plan de acción en caso de fallo o compromiso en los sistemas de cifrado			
¿Se han implementado políticas para el manejo seguro de los certificados digitales?			
TOTAL			

Nota. Elaboración propia.

Cada una de estas preguntas corresponde a un control de criptografía específico. Si se da una respuesta afirmativa, significa que dicho control está aplicado.

Fórmula de TCA=Número de controles de criptografía aplicados (respuestas "Sí").

Según ello, se procederá a registrarlo como porcentaje de acuerdo al siguiente rango:

- Madurez alta: 80-100% de los controles implementados.
- Madurez media: 60-79% de los controles implementados.
- Madurez baja: 40-59% de los controles implementados.
- Madurez muy baja: 0-39% de los controles implementados.

En la sección de vulnerabilidades se analizó la seguridad de las operaciones y la seguridad de las comunicaciones de acuerdo a la normativa ISO 27001.

La seguridad de las operaciones se realizó respondiendo el cuestionario que clasificó la respuesta en tres niveles: riesgo bajo, medio y alto.

Figura 16

Cuestionario de seguridad de las operaciones

2.1) Seguridad de las Operaciones				
Evaluación del Nivel de Impacto (NI)	**BAJO**	**MEDIO**	**ALTO**	**OBSERVACIONES**
En caso de un incidente de seguridad, ¿cuál sería el impacto en la continuidad del negocio?				
¿Cuál sería el impacto de una brecha de seguridad en la reputación de la empresa?				
¿Qué impacto tendría un ataque de seguridad en la integridad de los datos críticos?				
¿Cuál sería el impacto financiero de un incidente de seguridad?				
¿ cual seria el impacto por fallas en el alojamiento web ?				
Evaluación de la Probabilidad de Ocurrencia de Riesgo (POR)	**BAJO**	**MEDIO**	**ALTO**	**OBSERVACIONES**
¿Con qué frecuencia se han detectado vulnerabilidades de seguridad en las paginas web y maquinas virtuales?				
¿Cuál es la frecuencia de ataques de seguridad experimentados en el pasado?				
¿Qué tan probable es el aprovechamiento de las vulnerabilidades conocidas por los atacantes?				
¿Cuál es la probabilidad de que fallas humanas provoquen incidentes de seguridad?				
¿Cuál es la probalidad de ataques al los servidores de alojamiento web ?				

Fuente: elaboración propia.

Para calcular el Nivel de Riesgo (NR), primero se asignó un valor a las respuestas de cada pregunta según la escala ordinal (por ejemplo, Bajo = 1, Medio = 2, Alto = 3). Luego, se realizaron los siguientes pasos: Calcular el promedio del Nivel de Impacto (NI) y Probabilidad de Ocurrencia de Riesgo (POR): Sumar los valores asignados a cada respuesta y dividirlos por el número total de preguntas para obtener el promedio del NI y el POR.

Determinar el NR: Multiplicar el promedio del NI por el promedio del POR para obtener el NR. Siendo los rangos lo siguiente:

- NR Bajo: 1-2 (Riesgo Bajo)
- NR Medio: 3-6 (Riesgo Moderado)
- NR Alto: 7-9 (Riesgo Alto)

Para la seguridad de las comunicaciones se realizó un breve cuestionario, que se responderá con sí o no.

Figura 17

Sección del cuestionario de seguridad de las comunicaciones

2.2)Seguridad de las Comunicaciones	BAJO	MEDIO	ALTO	OBSERVACIONES
¿Se realizan identfican mecanismos de seguridad en los servicios alojados (paginas web,maquinas virtuales)				
¿Se cuenta con políticas de seguridad para el uso del correo electrónico y otros medios de comunicación				
¿Existen procedimientos para responder a incidentes de seguridad que afecten a las comunicaciones de la				
¿ Se realiza configuraciones de red adecuadas en las maquinas virtuales ?				
¿ Existe acuerdos de confidencialidad de divulgacion de informacion entre los clientes y la empresa ?				

Nota. Elaboración propia

Su análisis se realizó en relación al conteo de TRP=∑respuestas "SI" y TRN=∑respuestas "NO".

- Excelente: TRP = 3; 100% Respuestas Positivas
- Bueno: TRP = 2; aproximadamente 67% Respuestas Positivas
- Aceptable: TRP = 1; aproximadamente 33% Respuestas Positivas
- Insuficiente: TRP = 0; 0% Respuestas Positivas

Para la segunda variable, continuidad del negocio operativo, se calculó a través KPI, tanto para resiliencia en la infraestructura cloud, como gestión de incidentes de seguridad de la información.

Según la dimensión resiliencia en la infraestructura cloud, su primer indicador fue a través de la disponibilidad de servicios cloud. La fórmula es:

$$Disponibilidad\ (\%) = \frac{(Tiempo\ total - Tiempo\ de\ inactividad)}{Tiempo\ total} * 100\%$$

El segundo indicador será tiempo de recuperación de integridad, para lo cual se utilizará la siguiente formula:

Tiempo de Recuperación = Tiempo de Detección + Tiempo de Recuperación

El siguiente análisis se realizó en base a la gestión de incidentes de seguridad de la información, la cual empleó dos indicadores: Cantidad de incidentes y Tasa de éxito en la resolución.

La cantidad de incidentes= Número total de incidentes de seguridad reportados en un período de tiempo.

$$Tasa\ de\ éxito\ (\%) = \frac{Número\ de\ incidente\ resueltos}{Número\ total\ de\ incidentes} * 100\%$$

3.5.3. Validación y confiabilidad del instrumento

3.5.3.1. Validez. Según Villasis-Keever et al. (2018), afirmaron que la validez es una herramienta que nos ayuda a medir de manera más precisa la variable. En la presente investigación, la ficha de recolección de datos fue evaluado mediante el método de juicio de expertos, que consistió en analizar el contenido, ya que el investigador elaboró las preguntas de dicho cuestionario siguiendo las relaciones que existen entre los objetivos y el contenido del tema para luego hacer uso del muestreo, e identificar las preguntas más resaltantes de tal forma que estas sean representativas a la información y obtengan validez (Anexo C).

Tabla 1

Validación de expertos

Validadores	Puntaje
Lezama Gonzales, Pedro Martín	20
Vales Carrillo, Jorge Alberto	20
Román Concha, Norberto Ulises	18

Nota. Fueron tres validadores por juicio de experto.

3.5.3.2. Confiabilidad. Según Peraza et al (2017), afirma que la confiabilidad es el grado que se basa en producir resultados firmes y coherentes, es decir es el grado donde se producen los mismos resultados y hacen uso de métodos y medidas de consistencia. En el presente estudio, la ficha de recolección de datos fue procesada con el método de Alfa de Cronbach (Figura

16) para probar la confianza del instrumento. Su valoración fue mayor a 0.80 para aprobar el instrumento.

Figura 18

Formula de Alfa de Cronbach

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

α : Alfa de Cronbach
k : Número de ítems
V_i: Varianza de cada ítem
V_t: Varianza del total

Nota. Elaboración propia

Tabla 2

Prueba de Alfa De Cronbach – fiabilidad

Alfa de Cronbach	N de elementos
0,885	25

Nota. Elaboración propia.

El análisis de la confiabilidad del instrumento de medición utilizado en esta investigación, mediante el coeficiente Alfa de Cronbach, reveló un valor de 0.885 basado en 25 elementos. Este resultado indica una alta consistencia interna del cuestionario, lo que sugiere que los ítems están midiendo de manera efectiva y coherente el mismo concepto o constructo.

3.6. Procedimientos

El proyecto de tesis inició con una fase meticulosa de preparación, donde se desarrolló un proyecto detallado que especificó claramente la problemática, los objetivos y la justificación del estudio en ITIPERU. Este proyecto inicial también incluyó una revisión de la literatura pertinente, la formulación de un marco teórico y metodológico, con especial atención en la elaboración de un instrumento efectivo para la recolección de datos. Una vez que el proyecto estuvo debidamente constituido, se presentó ante el comité de tesis de la Universidad Nacional Federico Villarreal para su evaluación y aprobación.

Tras la aprobación del comité, la siguiente etapa consistió en la ejecución del proyecto dentro de ITIPERU. En esta etapa, se estableció las coordinaciones necesarias con la empresa para garantizar el acceso a la información y los recursos necesarios para la investigación. Se llevarán a cabo las actividades de investigación propuestas, tales como observaciones, entrevistas y, de ser necesario, visitas a la infraestructura de la empresa, siempre en concordancia con la metodología establecida.

Una vez en marcha el proyecto, se procedió a la recolección de datos. Esta fase crucial implicará el registro de los datos. Solo el investigador realizó el llenado de la ficha para asegurar la coherencia y calidad de la información recopilada. Al concluir la semana de evaluación, se recopilarán las fichas completadas y se verificarán para asegurarse de que los datos sean integrales y fidedignos.

La recolección de datos fue un proceso dinámico que requirió seguimiento y ajustes para adaptarse a cualquier eventualidad o hallazgo emergente. La información recabada fue luego procesada y preparada para el análisis, el cual fue el pilar para la siguiente fase de la tesis que incluirá la interpretación y discusión de los resultados.

3.7. Análisis de datos

En el procesamiento de datos se utilizó el software estadístico denominado SPSS en su versión número 25, según el autor Bernal (2010) “debe realizarse mediante el uso de herramientas estadísticas con el apoyo del computador, utilizando alguno de los programas estadísticos que hoy fácilmente se encuentran en el mercado”.

Los métodos que se emplearon en la presente investigación fueron el análisis descriptivo e inferencial. A través del análisis descriptivo se desarrolló tablas estadísticas básicas y gráficos para obtener una visión clara de la situación inicial de la empresa y de los cambios resultantes de las

intervenciones. Con especial interés en la comparación de los estados pre y post implementación. Para la aprobación o rechazo de las hipótesis de empleó el análisis inferencial, para lo cual se aplicó previamente la prueba de distribución de datos basado en Kolmogorov-Smirnov y Shapiro-Wilk. Se empleó ambas pruebas, porque el grupo de estudio era pequeño y se necesitó comparar si existía discrepancia en los datos obtenidos. Ambas pruebas indicaron el empleo de la prueba estadística no paramétrica de Wilcoxon, para evaluar la significancia de los cambios observados en variables como la disponibilidad de servicios en la nube y la efectividad de la gestión de incidentes. Todo ello, considerando un nivel de confianza al 95% y un nivel de significancia al 0,05%.

3.8. Consideraciones éticas

En el marco de este estudio de investigación, la recopilación de información se llevó a cabo de manera imparcial y objetiva, garantizando la integridad y evitando cualquier forma de alteración o manipulación de los datos; con el objetivo de asegurar la confiabilidad de los resultados obtenidos. Para asegurar una estructura sólida en el trabajo de investigación, se consideró la adhesión a las Normas APA 7ª Edición. Además, se aplicarán principios éticos profesionales, asegurando que todos los participantes sean informados de manera clara y precisa sobre la investigación, lo que garantiza la protección y confidencialidad de acuerdo con la Ley Número 29733, conocida como la Ley de Protección de Datos Personales, y el reglamento aprobado por el Decreto Supremo N°003-2013-JUS.

IV. RESULTADOS

Según la metodología aplicada, se analizó el entorno cloud de la empresa ITIPERU, mediante las 4 máquinas virtuales, y las 6 páginas web alojadas. Para ello, se empleó diferentes pruebas estadísticas de tipo descriptivo e inferencial, que se muestra en el presente capitulo.

4.1. Análisis, interpretación de resultados

Tabla 3

Análisis descriptivo del pre test y post test

			Estadístico	Desv. Error
Pre test	Media		26,6000	,61824
	95% de intervalo de confianza para la media	Límite inferior	25,2014	
		Límite superior	27,9986	
	Media recortada al 5%		26,5556	
	Mediana		26,5000	
	Varianza		3,822	
	Desv. Desviación		1,95505	
	Mínimo		24,00	
	Máximo		30,00	
	Rango		6,00	
	Rango intercuartil		3,25	
	Asimetría		,482	,687
	Curtosis		-,811	1,334
Post test	Media		39,8000	,67987
	95% de intervalo de confianza para la media	Límite inferior	38,2620	
		Límite superior	41,3380	
	Media recortada al 5%		39,7222	
	Mediana		39,0000	
	Varianza		4,622	
	Desv. Desviación		2,14994	
	Mínimo		37,00	
	Máximo		44,00	
	Rango		7,00	
	Rango intercuartil		3,25	
	Asimetría		,741	,687
	Curtosis		-,024	1,334

Nota. El análisis inicial al comparar los diferentes valores de medida central del pre test y post test muestra una mejora notable, es decir que la implementación de las estrategias de ciberseguridad tuvo un impacto positivo en el entorno cloud de la empresa ITIPERU.

Para la prueba de normalidad (Tabla 4) se necesitó plantear la hipótesis nula (H0) y la hipótesis alternativa (H1).

H0: Los datos presentan una distribución normal.

H1: Los datos no presentan una distribución normal.

Tabla 4

Prueba de la normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pre test	,193	10	,200*	,940	10	,555
Post test	,245	10	,030	,930	10	,044

Nota. El análisis de distribución de datos presentó las siguientes condiciones: *. Esto es un límite inferior de la significación verdadera, y a. Corrección de significación de Lilliefors.

Según el análisis de la **Tabla 4** se evidencia que las pruebas de la normalidad durante el pre test, tanto de Kolmogorov-Smirnov y Shapiro-Wilk, obtuvieron un nivel de significancia mayor a 0,05; con lo cual se infiere que no se rechaza la hipótesis nula, es decir, presenta una distribución normal de los datos. Respecto al post test, el nivel de significancia es lo contrario, en otras palabras, no presenta una distribución normal después de aplicar las estrategias de ciberseguridad para mejorar la robustez de la continuidad de negocio. Entonces, al no demostrarse en su totalidad la distribución normal de los datos, se debe seleccionar una prueba no paramétrica, como la prueba de Wilcoxon para la verificación de las hipótesis de este estudio, que permite comparar los rangos medios de cada prueba y determinar si existen diferencias significativas.

Tabla 5

Comparación de la autentificación multifactor Pre Test vs. Post Test

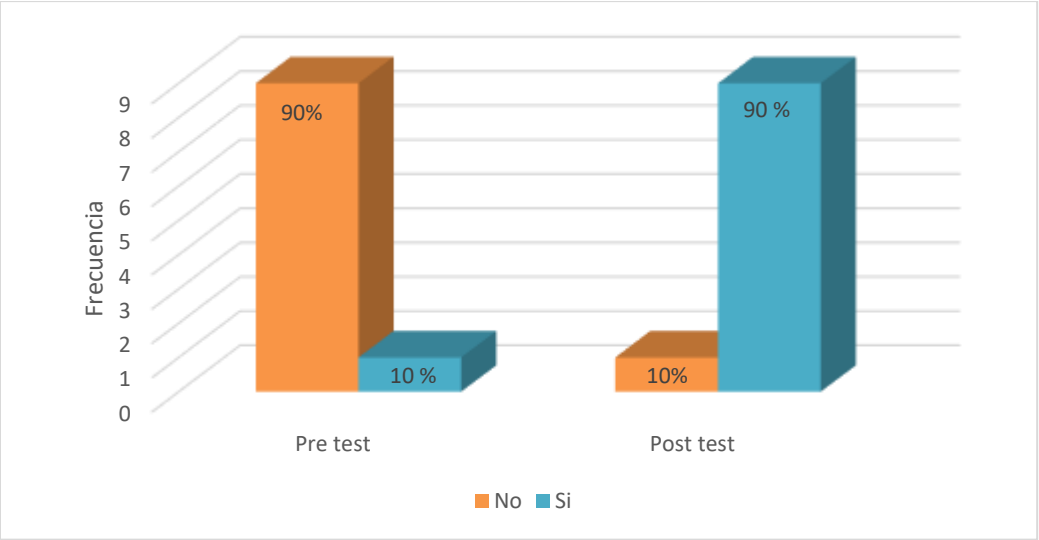
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	9	90,0	1	10,0
	Si	1	10,0	9	90,0
	Total	10	100,0	10	100,0

Nota. La primera pregunta fue ¿Existen procedimientos de autenticación multifactor para el acceso a los recursos críticos?

En la **Tabla 5** se observa que la autentificación multifactor en el pre test resultó con una respuesta negativa de 90%, evidenciando que la empresa ITIPERU no empleó validaciones para el acceso de los recursos tecnológicos de la administración de la infraestructura tecnológica de las páginas web y máquinas virtuales. En referencia al post test, cuando se aplicó estrategias de ciberseguridad, se halló una mejora del 90%; permitiendo mejorar el control de accesos y seguridad de la administración de las páginas web y máquinas virtuales.

Figura 19

Diagrama de comparación de autentificación multifactor



Nota. Visualización gráfica de los datos de la Tabla 5.

En la **Figura 19** se muestra los datos de la Tabla 3 en un diagrama de barras, evidenciando la gran diferencia del antes (90% de 10 componentes cloud, con respuesta negativa), y después (90% de 10 componentes cloud, con respuesta favorable) al aplicar el modelo de estrategias de ciberseguridad implementadas en la empresa ITIPERU.

Tabla 6

Comparación de los derechos de acceso en el Pre Test vs. Post Test

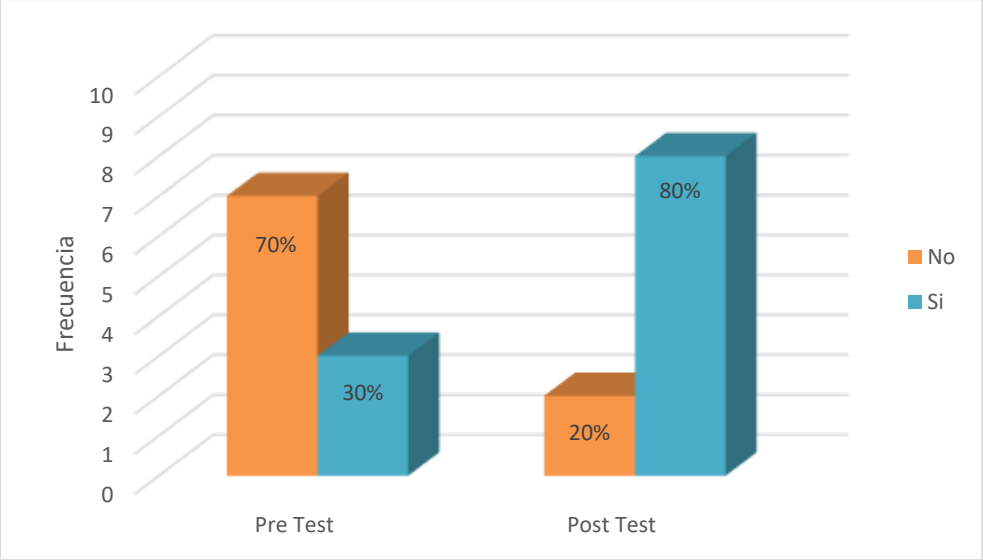
		Pre-Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	7	70,0	2	20,0
	Si	3	30,0	8	80,0
	Total	10	100,0	10	100,0

Nota. La segunda pregunta que se realizó fue ¿Se revisan y actualizan periódicamente los derechos de acceso?

Según la **Tabla 6,** la evaluación del pre test indica que el derecho de acceso no estaba determinado en un 70%, por lo que los niveles de acceso para la administración de las páginas web y las máquinas virtuales de ITIPERU se encontraban sin permisos, con información sensible a libre disposición de cualquier individuo. Posteriormente, al aplicar el modelo de estrategias de ciberseguridad para el procedimiento de permisos de acceso a la administración de la infraestructura cloud, se observa que mejoro en un 80%. Lo que a la empresa ITIPERU permitirá tener un mejor filtro para el control de accesos a personas no autorizadas de la organización.

Figura 20

Diagrama de comparación de derechos de acceso



Nota. Visualización gráfica de los datos de la Tabla 6.

La **Figura 20** facilita la distribución de la información respecto a la tabulación de la Tabla 6, lo cual permite visualizar que el 70% de la infraestructura cloud de ITIPERU estaba muy vulnerable, facilitando la extracción de datos sensibles. Sin embargo, ello disminuyo en un 80%, asegurando la protección de sus datos.

Tabla 7

Comparación del monitoreo de acceso al usuario en el Pre Test vs. Post Test

		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	10	100,0	1	10,0
	Si	0	0	9	90,0
	Total	10	100	10	100,0

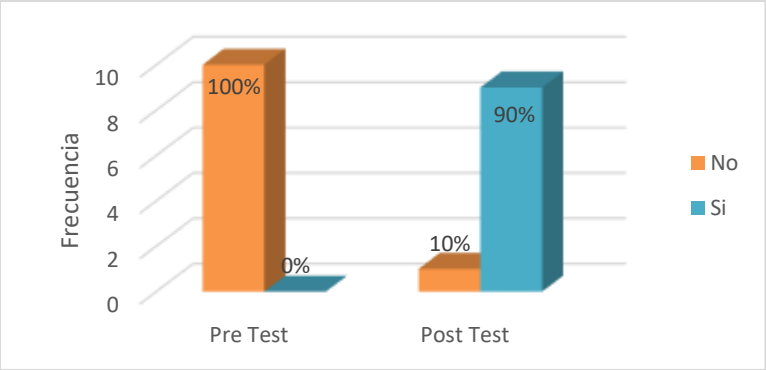
Nota. La tercera pregunta fue ¿Se registra y monitorea el acceso de usuarios a entornos cloud?

El análisis de la **Tabla 7** expone que previamente a la implementación de las medidas de ciberseguridad en un 100% no presentaron ningún tipo de monitoreo del acceso al usuario. Por lo

que luego de la implementación, el registro y monitoreo del acceso al usuario fue positivo en un 90%. Este cambio permite que haya una mejor gestión de administración constante de los usuarios internos y externos para prevenir el fraude o filtración de datos.

Figura 21

Diagrama de comparación de monitoreo de acceso al usuario



Nota. Visualización gráfica de los datos de la Tabla 7.

En la **Figura 21** se muestra que el pre test obtuvo un resultado de 100% en la respuesta no, lo cual pone de manifiesto la falta de registro y monitoreo del ingreso o salida de los usuarios dentro de las páginas web y máquinas virtuales. Empero, luego de la implementación de estrategias de ciberseguridad, el post test reveló el cambio positivo en un 90%, aumentando la confianza para la protección de los datos de la empresa, servicios cloud y clientes.

Tabla 8

Comparación del control de acceso en el Pre Test vs. Post Test

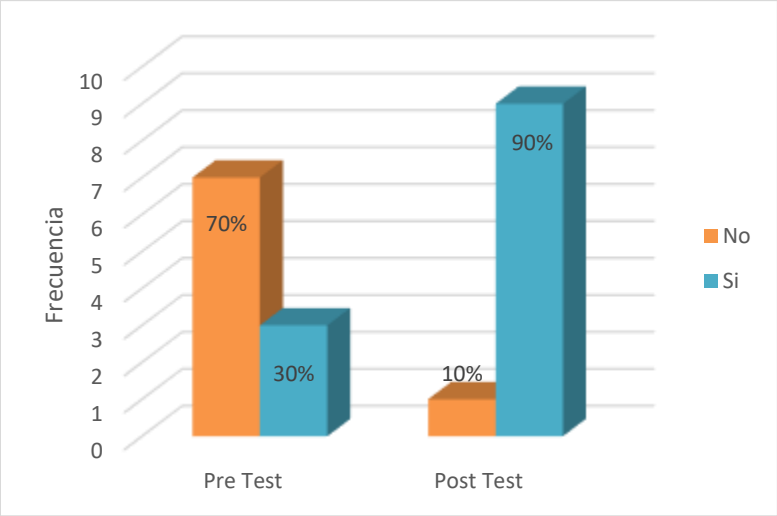
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	7	70,0	1	10,0
	Si	3	30,0	9	90,0
	Total	10	100,0	10	100,0

Nota. El cuarto enunciado fue ¿Se utiliza control de acceso basado en roles para limitar el acceso a recursos según la necesidad del usuario?

Para la **Tabla 8**, los resultados del pre test mencionan que el 70% del entorno virtual cloud no presentaba controles de acceso, y solo había en un 30%. Más al aplicar las estrategias de ciberseguridad, aumento en un 90%; proporcionando que la información confidencial tenga la opción de monitorear el ingreso no autorizados para ITIPERU en la administración de páginas webs y máquinas virtuales.

Figura 22

Diagrama de comparación de control de acceso



Nota. Visualización gráfica de los datos de la Tabla 8.

La visualización de la **Figura 22** presenta el cambio beneficioso de la implementación de las estrategias de ciberseguridad, ya que al inicio del estudio la empresa ITIPERU no contaba con un protocolo de control de accesos para monitorear y limitar el ingreso a secciones de la infraestructura que contuviera datos importantes; mejorando luego de la aplicación de métodos para su gestión de páginas webs y máquinas virtuales.

Tabla 9

Comparación seguridad de accesos en el Pre Test vs. Post Test

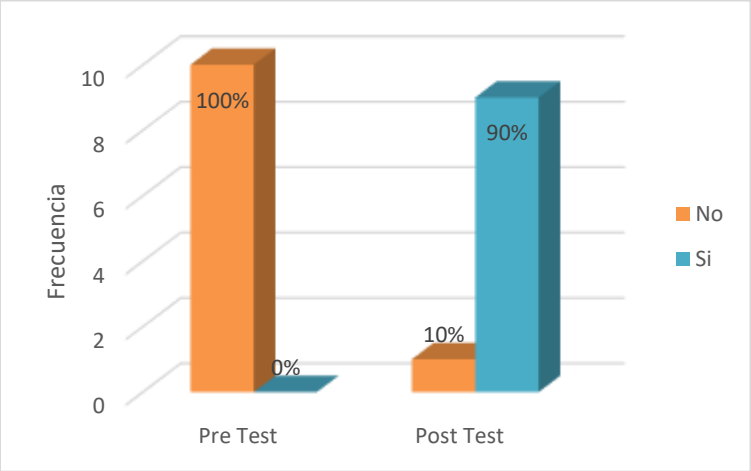
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	10	100,0	1	10,0
	Si	0	0,0	9	90,0
	Total	10	100,0	10	100,0

Nota. El quinto ítem fue ¿Se tiene monitoreo y alertas de seguridad de accesos?

La **Tabla 9** señala que ITIPERU al inicio del estudio presentó un 100% sin seguridad de accesos, es decir, que no tenía ninguna alerta de seguridad ante situaciones de intentos de acceso no autorizados; por lo cual los parámetros de seguridad aplicados mejoraron en un 90%. Consiguiendo que todo usuario siempre cumpla un proceso de seguridad para acceder adecuadamente a la infraestructura cloud.

Figura 23

Diagrama de comparación seguridad de accesos



Nota. Visualización gráfica de los datos de la Tabla 9.

El diagrama de barras de la **Figura 23** muestra el avance positivo que se obtuvo luego de la aplicación de métodos y parámetros de seguridad para el acceso en un 90% (post test) en la empresa ITIPERU para su administración de páginas webs y máquinas virtuales.

Tabla 10

Comparación protección de datos sensibles en el Pre Test vs. Post Test

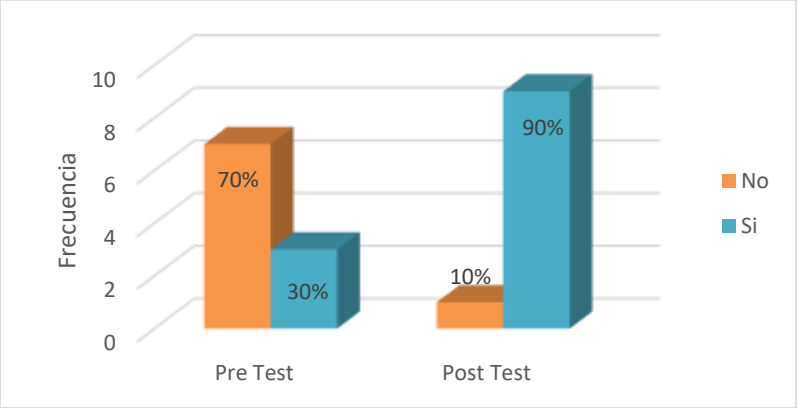
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	7	70,0	1	10,0
	Si	3	30,0	9	90,0
	Total	10	100,0	10	100,0

Nota. La sexta pregunta fue ¿Se utiliza cifrado para proteger los datos sensibles de los entornos cloud?

Al analizar la **Tabla 10** el entorno cloud de ITIPERU el 70% no presentaba protección de datos, y al realizar la implementación, el post test muestra que el 90% de su información crítica de los servicios cloud fueron cifrados. Este proceso tiene relevancia, ya que permite crear códigos para proteger a la organización, servidores y clientes, de ataques fraudulentos o extracción de datos confidenciales

Figura 24

Diagrama de comparación protección de datos sensibles



Nota. Visualización gráfica de los datos de la Tabla 10.

La **Figura 24** presenta los datos de manera gráfica, demostrando el cambio del pre test al post test; en donde los entornos cloud de ITIPERU fueron fortalecidos sus procesos mediante los cifrados y encriptación de la información sensible en un 90%.

Tabla 11

Comparación criptografía en el Pre Test vs. Post Test

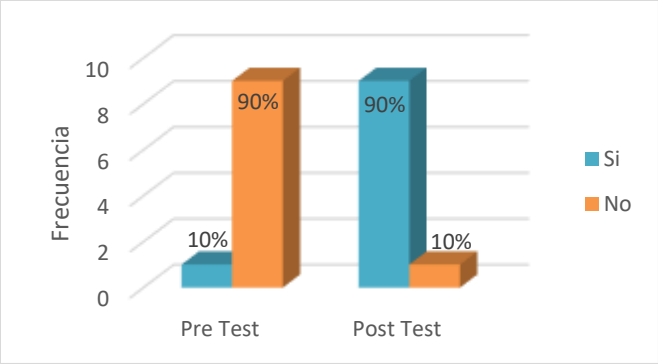
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	9	90,0	1	10,0
	Si	1	10,0	9	90,0
	Total	10	100,0	10	100,0

Nota. La séptima pregunta ¿Se cuenta con política de controles criptográficos?

Según la **Tabla 11**, ITIPERU mejoró en el desarrollo de políticas para la administración criptográfica en las máquinas virtuales y páginas web luego de la implementación de estrategias de ciberseguridad en un 90%; ya que inicialmente, en el pre test, solo obtuvo un 10% de controles adecuados. Permitiendo así, que los datos resguardados tengan un código para evitar que receptores no autorizados obtengan fácilmente la lectura de la información.

Figura 25

Diagrama de comparación de criptografía



Nota. Visualización gráfica de los datos de la Tabla 11.

En la **Figura 25** el análisis de la criptografía en ITIPERU expone que el 90% de la población estudiada no presentó ninguna política de seguridad basado en códigos para los accesos e información sensible; y que luego de la implementación en la evaluación del post test se reveló

que mejoró en un 90%. Dificultando la extracción de información confidencial a usuarios no autorizados.

Tabla 12

Comparación protocolos seguros en el Pre Test vs. Post Test

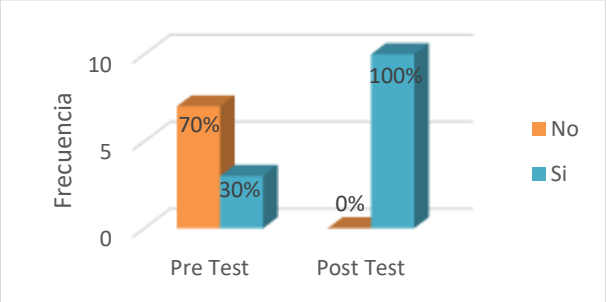
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	7	70,0	0	0
	Si	3	30,0	10	100,0
	Total	10	100,0	10	100,0

Nota. Se preguntó ¿Se emplean protocolos seguros (como TLS)?

En la **Tabla 12** se identificó que el 70% de los servicios cloud no tenía implementado TLS en las páginas webs y máquinas virtuales, lo cual permitía que no haya conexiones seguras en la administración de la infraestructura cloud de ITIPERU, pero luego se desarrolló los protocolos de seguridad completando al 100%, que permitió tener mejoras significativas para la organización.

Figura 26

Diagrama de comparación de protocolos seguros



Nota. Visualización gráfica de los datos de la Tabla 12.

Las barras verticales de la **Figura 26** muestran la comparación del pre test y post test; exponiendo la evolución favorable de un 30% hasta completar el 100% de los protocolos de seguridad, con el objetivo de mantener la integridad de las páginas webs y máquinas virtuales durante las comunicaciones de ITIPERU.

Tabla 13

Comparación del plan de acción de Pre Test vs. Post Test

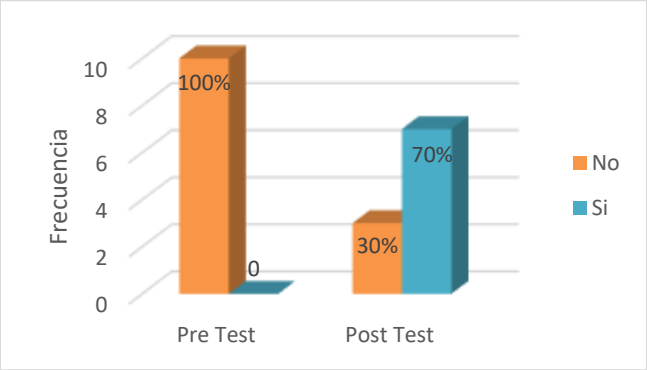
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	10	100,0	3	30,0
	Si	0	0	7	70,0
	Total	10	100,0	10	100,0

Nota. La siguiente pregunta fue ¿Se cuenta con un plan de acción en caso de fallo o compromiso en los sistemas de cifrado?

Para el plan de acción, la **Tabla 13** expone que ITIPERU al momento del pre test no presentaba protocolos de respaldo ante fallas del sistema de cifrado; por lo que, para el post test se desarrolló un plan de contingencia para respaldar la información de cada servicio ofrecido; así mantener la continuidad del negocio.

Figura 27

Diagrama de comparación de plan de acción



Nota. Visualización gráfica de los datos de la Tabla 13.

El diagrama de la **Figura 27** representa los valores porcentuales obtenidos durante el pre test y post test del plan de acción, con lo cual se observa una mejoría del 70% para el respaldo de información ante situaciones de falla de los sistemas de encriptación o que vulneren la integridad de los datos.

Tabla 14

Comparación de las políticas para el manejo seguro de los certificados digitales de Pre Test vs. Post Test

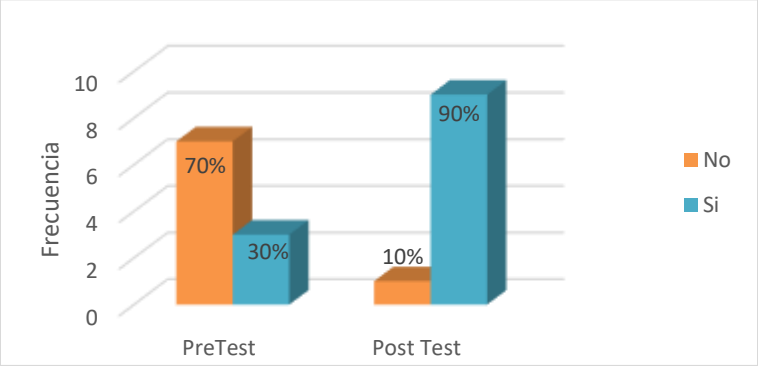
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	No	7	70,0	1	10,0
	Si	3	30,0	9	90,0
	Total	10	100,0	10	100,0

Nota. La siguiente pregunta fue ¿Se han implementado políticas para el manejo seguro de los certificados digitales?

La **Tabla 14** demuestra la comparación de políticas para el manejo seguro de los certificados digitales. En el pre test se identificó que el 70% no cuenta con un manejo adecuado de certificados digitales, y solo el 30 % si lo tenía. Posteriormente, el post test confirma el cambio significativo al 100 %, indicando el desarrollo de implementación de políticas para un manejo adecuado de certificados digitales.

Figura 28

Diagrama de comparación políticas para el manejo seguro de los certificados digitales



Nota. Visualización gráfica de los datos de la Tabla 14.

La **Figura 28** representa los valores porcentuales obtenidos durante el pre test y post test sobre políticas para el manejo seguro de los certificados digitales, donde se verifica la aplicación

de las estrategias de ciberseguridad hasta un 90 % en el post test, mejorando en un 70%, como se observa en el pre test. Esta medida beneficia a que las páginas webs y las máquinas virtuales se encuentren en un entorno seguro durante la navegación de los usuarios.

Tabla 15

Comparación el impacto en la continuidad del negocio Pre Test vs. Post Test

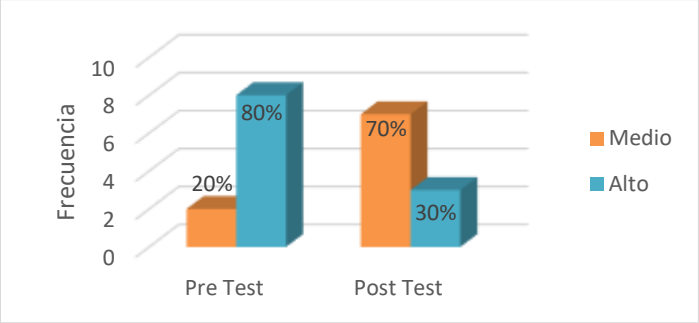
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	0	0	0	0
	Medio	2	20,0	7	70,0
	Alto	8	80,0	3	30,0
	Total	10	100,0	10	100,0

Nota. La siguiente interrogante fue: En caso de un incidente de seguridad, ¿cuál sería el impacto en la continuidad del negocio?

Según la **Tabla 15** se muestra una comparación del impacto en la continuidad del negocio, en donde el pre test indica que el 80% tendrían un impacto alto y un 20% un impacto medio en la continuidad del negocio, es decir, que la empresa ITIPERU presenta deficiencias en varias categorías como el control de accesos, roles de administración, caídas de servicios, entre otras asociadas a la falta de estrategias de ciberseguridad. Después, en el post test, los niveles del impacto en la continuidad del negocio cambió significativamente, ya que ahora se observó que un 70% como impacto medio y una disminución del impacto alto del 30%.

Figura 29

Diagrama de comparación del impacto en la continuidad del negocio



Nota. Visualización gráfica de los datos de la Tabla 15.

El diagrama de la **Figura 29** representa los cambios obtenidos durante el análisis del impacto en la continuidad del negocio; demostrando que el proceso fue favorable con las medidas adoptadas, mejorando la capacidad de la empresa ITIPERU para afrontar vulnerabilidades en las páginas webs y máquinas virtuales.

Tabla 16

Comparación el impacto de una brecha de seguridad Pre Test vs. Post Test

		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	0	0	0	0
	Medio	0	0	10	100,0
	Alto	10	100,0	0	0
	Total	10	100,0	10	100,0

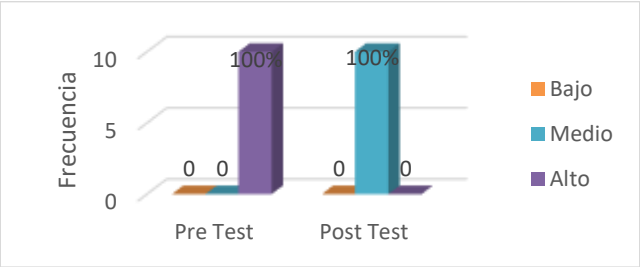
Nota. La pregunta fue ¿Cuál sería el impacto de una brecha de seguridad en la reputación de la empresa?

Los datos de la **Tabla 16** refleja el impacto de una brecha de seguridad en ITIPERU en dos evaluaciones. La evaluación del pre test midió un impacto alto de 100%, siendo un indicador negativo, ya que, permite que los usuarios no autorizados filtren información confidencial. Por ello, a través de la ISO 27001 y Zero Trust se aplicó procedimientos para disminuir incidentes de

ciberseguridad que se podrían presentar en las páginas webs y máquinas virtuales de los clientes; con lo cual se obtuvo un nivel medio al 100%.

Figura 30

Diagrama de comparación del impacto de una brecha de seguridad



Nota. Visualización gráfica de los datos de la Tabla 16.

Las diferencias del pre test y post test de la **Figura 30** confirma el avance que se realizó al aplicar las estrategias de ciberseguridad para disminuir la brecha de filtración o modificaciones no autorizadas, por lo que de un nivel alto de 100% en el pre test, minimizó a un nivel medio de 100%.

Tabla 17

Comparación del impacto ante un ataque de seguridad Pre Test vs. Post Test

		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	2	20,0	1	10,0
	Medio	1	10,0	7	70,0
	Alto	7	70,0	2	20,0
	Total	10	100,0	10	100,0

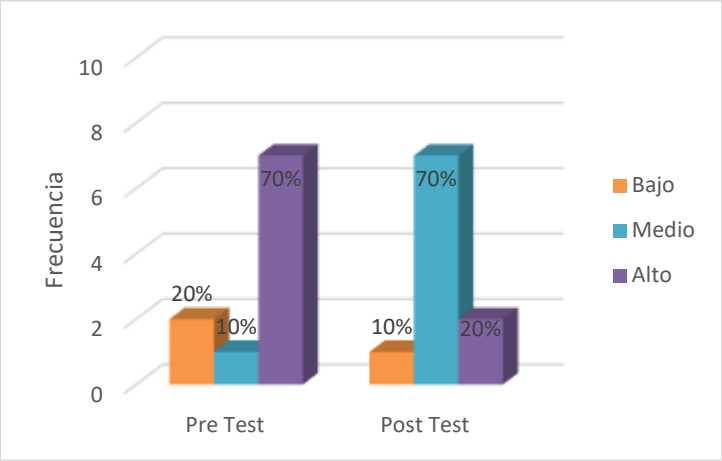
Nota. La pregunta abarcó ¿Qué impacto tendría un ataque de seguridad en la integridad de los datos críticos?

Como se visualiza en la **Tabla 17**, la empresa ITIPERU obtuvo en el pre test sobre la categoría de nivel de impacto ante un ataque de seguridad, un nivel alto de 70%, bajo de 20% y medio al 10%. Lo cual significa que las medidas adoptadas inicialmente por la empresa en los entornos cloud no controlaba, no solicitaba reportes de acceso, no presentaba políticas de

seguridad; aumentando riesgos que afecten la integridad de los datos críticos en la infraestructura administrada por ITIPERU. Ante esta problemática, al implementarse las medidas de ciberseguridad como las políticas de mitigación de riesgos se logró se reducir el nivel alto a un 20%, nivel medio al 70%, y 10% en el nivel bajo.

Figura 31

Diagrama de comparación del impacto ante un ataque de seguridad



Nota. Visualización gráfica de los datos de la Tabla 17.

Las barras verticales expuestas en la **Figura 31** expone la evolución del impacto que tendría un ataque de seguridad en la empresa, comparando los resultados obtenidos en dos momentos distintos: antes y después de implementar medidas de seguridad. En el pre test, la respuesta más alta es el nivel alto con un 70% de 10 componentes del servicio cloud (páginas web y máquinas virtuales); lo cual genera una preocupación por la alta vulnerabilidad ante ataques cibernéticos. Sin embargo, esta realidad cambio al aplicarse medidas de protección, generando un nivel de impacto medio de 70% y un nivel alto de solo 20%.

Tabla 18

Comparación del impacto financiero Pre Test vs. Post Test

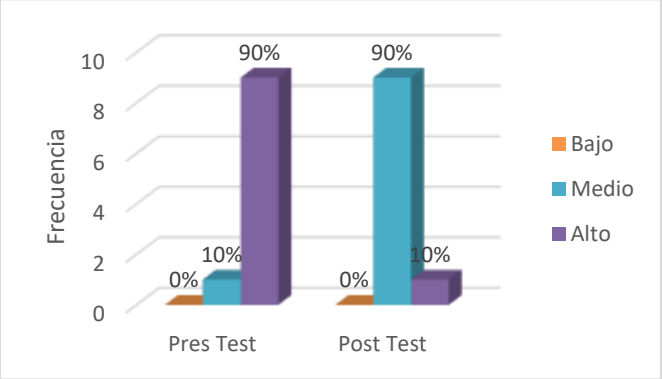
		Pres Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	0	0	0	0
	Medio	1	10,0	9	90,0
	Alto	9	90,0	1	10,0
	Total	10	100,0	10	100,0

Nota. La siguiente pregunta fue ¿Cuál sería el impacto financiero de un incidente de seguridad?,

El análisis de la **Tabla 18** ejemplifica la situación de la empresa ITIPERU, en la que el pre test indicó que el impacto financiero fue alto en 90%, reflejando una gran preocupación por las posibles consecuencias económicas severas que podría presentarse sí mantuviera la misma metodología de trabajo. Durante el proceso de implementación, se generó estrategias de seguridad de la información, con lo cual la finalización del proyecto generó confianza, siendo así que el post test, muestra un cambio significativo en la percepción del impacto financiero medio del 90%, y solo el 10% un impacto alto.

Figura 32

Diagrama de comparación del impacto financiero



Nota. Visualización gráfica de los datos de la Tabla 18.

Mediante la **Figura 32** se proyecta aclarar el impacto financiero de la empresa ITIPERU, demostrando la importancia de crear políticas de ciberseguridad para mantener la confianza de los clientes y/o usuarios; y así obtener nuevos clientes para el crecimiento gradual de la organización.

Tabla 19

Comparación del impacto por fallas en el alojamiento web Pre Test vs. Post Test

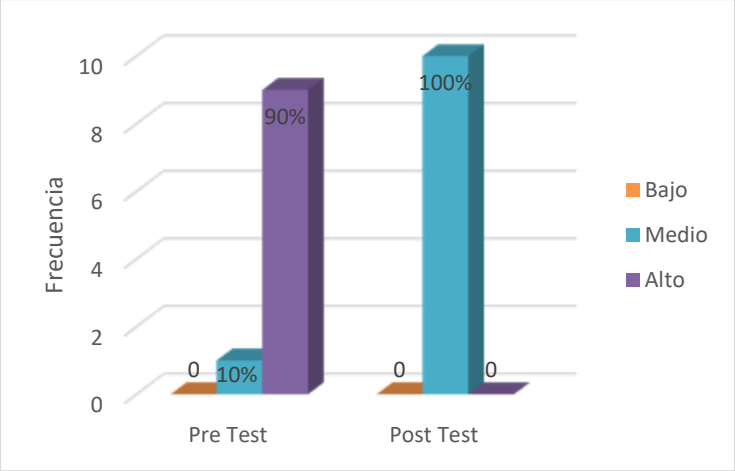
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	0	0	0	0
	Medio	1	10,0	10	100,0
	Alto	9	90,0	0	0
	Total	10	100,0	10	100,0

Nota. La pregunta fue ¿Cuál sería el impacto por fallas en el alojamiento web?

Por medio de la **Tabla 19** se muestra la evaluación del impacto por fallas en el alojamiento web que tenía ITIPERU; durante el pre test, se halló un impacto alto al 90%, lo que indica una gran preocupación por las posibles consecuencias negativas en el alojamiento web. Después de implementar cambios y mejoras, el post test, señaló la disminución a un nivel de impacto medio de 100%, logrando aumentar la confianza en la capacidad de ITIPERU para gestionar y mitigar las fallas del alojamiento web, para que no tengan consecuencias graves para la organización.

Figura 33

Diagrama de comparación del impacto por fallas en el alojamiento web



Nota. Visualización gráfica de los datos de la Tabla 19.

La **Figura 33** organiza gráficamente los datos del impacto por fallas en el alojamiento web en ITIPERU, antes y después de implementar mejoras. Entonces, al inicio el 90% presentó un impacto alto y un nivel medio de 10%; mientras que después, el post test indicó un valor de 100% en el impacto medio. Con lo cual, se reconoce que las medidas de ciberseguridad influyen en la capacidad de controlar las fallas y reducir el tiempo de acción para mantener la continuidad de negocio operativo.

Tabla 20

Comparación de la frecuencia de vulnerabilidades de seguridad Pre Test vs. Post Test

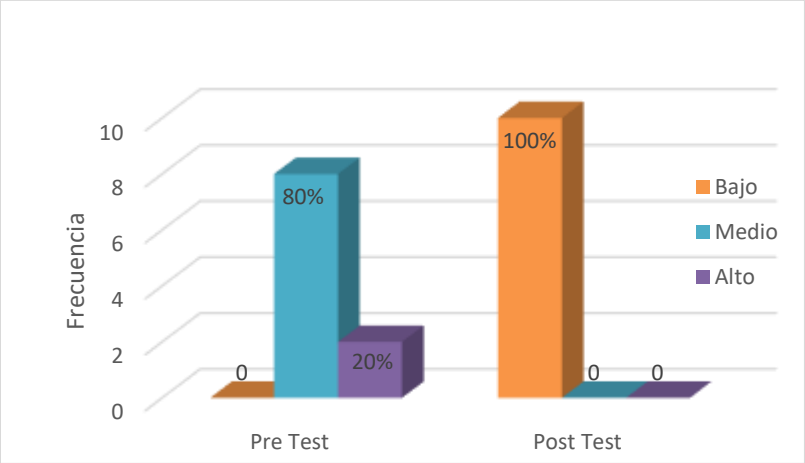
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	0	0	10	100,0
	Medio	8	80,0	0	0
	Alto	2	20,0	0	0
	Total	10	100,0	10	100,0

Nota. Se analizó la cantidad incidencias a través de la siguiente pregunta ¿Con qué frecuencia se han detectado vulnerabilidades de seguridad en las páginas web y máquinas virtuales?

Según la **Tabla 20** se observa la frecuencia con la que se detectaron vulnerabilidades de seguridad en las páginas web y máquinas virtuales de ITIPERU antes y después de realizar acciones de mejora (Pre Test vs. Post Test). En el pre test, el 80%, de los casos reportaron una frecuencia media de detección de vulnerabilidades, mientras que un menor porcentaje fue de nivel alto en un 20%. Tras aplicar las medidas correspondientes, los resultados del post test muestran un cambio favorable: todas las respuestas al 100% indican una frecuencia baja en la detección de vulnerabilidades. Esto significa que, después de las intervenciones, ITIPERU no percibió incidencias medias o altas de vulnerabilidades.

Figura 34

Diagrama de comparación de la frecuencia de vulnerabilidades de seguridad



Nota. Visualización gráfica de los datos de la Tabla 20.

El diagrama de la **Figura 34** presenta los valores porcentuales obtenidos durante la tesis; con lo cual se observa una reducción de las reiteraciones de las vulnerabilidades presentadas en las páginas webs y las máquinas virtuales, logrando obtener 100% luego de la implementación de estrategias de ciberseguridad, basado en la ISO 27001 y el modelo Zero Trust.

Tabla 21

Comparación de la frecuencia de vulnerabilidades de seguridad Pre Test vs. Post Test

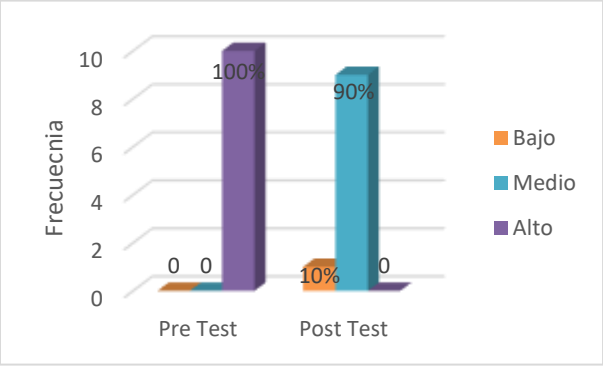
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	0	0	1	10,0
	Medio	0	0	9	90,0
	Alto	10	100,0	0	0
	Total	10	100,0	10	100,0

Nota. Se consultó lo siguiente ¿Cuál es la frecuencia de ataques de seguridad experimentados en el pasado?

Con la **Tabla 21** se obtiene el contraste de la frecuencia de vulnerabilidades de seguridad experimentadas por ITIPERU en dos periodos distintos, pre test y post test. En el pre test, todas las respuestas 100%, indicaron que la frecuencia de ataques de seguridad era alta, lo que refleja una situación crítica en cuanto a seguridad informática. Después de realizar mejoras y reevaluar en el post test, hay un cambio notable. La mayoría de las respuestas indican que el 90% de la frecuencia de vulnerabilidades de seguridad es media, y una pequeña proporción del 10% es de frecuencia baja. Con las medidas tomadas por ITIPERU han sido efectivas en disminuir la frecuencia de vulnerabilidades de seguridad.

Figura 35

Diagrama de comparación de la frecuencia de vulnerabilidades de seguridad



Nota. Visualización gráfica de los datos de la Tabla 21.

La representación de la **Figura 35** ayuda a apreciar el cambio de distribución en el nivel de frecuencia durante el pre test y post test en la empresa ITIPERU, consignado en las fichas de evaluación, al evaluar las páginas webs y las máquinas virtuales.

Tabla 22

Comparación del aprovechamiento de las vulnerabilidades Pre Test vs. Post Test

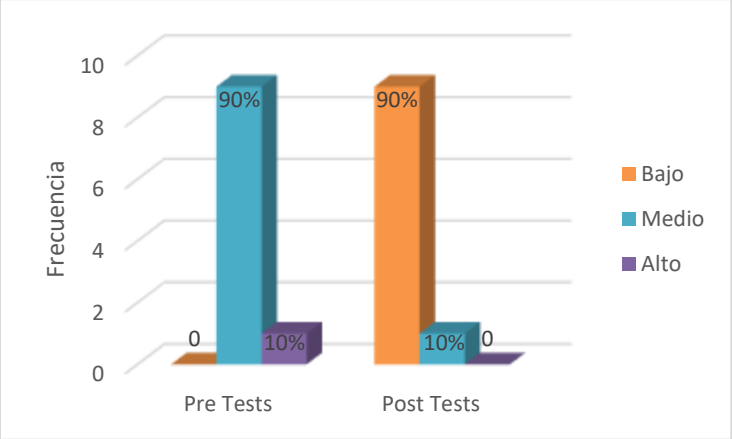
		Pre Tests		Post Tests	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	0	0	9	90,0
	Medio	9	90,0	1	10,0
	Alto	1	10,0	0	0
	Total	10	100,0	10	100,0

Nota. La pregunta fue ¿Qué tan probable es el aprovechamiento de las vulnerabilidades conocidas por los atacantes?

La **Tabla 22** evidencia cómo ITIPERU percibe la probabilidad de que los atacantes aprovechen las vulnerabilidades conocidas antes y después de implementar estrategias de ciberseguridad. En el pre test, el 90% consideró que era probable a un nivel medio que los atacantes aprovecharan las vulnerabilidades, y un pequeño porcentaje del 10% se consideraba altamente probable. Tras las medidas de perfeccionamiento, se ve reflejado en el post test, que el 90% ahora ve una baja probabilidad de que las vulnerabilidades sean aprovechadas, y solo un 10% se verifica que hay una probabilidad media.

Figura 36

Diagrama de comparación del aprovechamiento de las vulnerabilidades



Nota. Visualización gráfica de los datos de la Tabla 22.

El gráfico de la **Figura 36** contempla la distribución de los datos a través de las evaluaciones aplicadas a las páginas webs y máquinas virtuales de ITIPERU. Como se observa, inicialmente se consideró que existía una probabilidad alta de aprovechamiento de 90%, pero luego de la ejecución de las estrategias de seguridad se redujo al 90%, encontrándose en un nivel bajo de aprovechamiento.

Tabla 23

Comparación de la probabilidad de que fallas humanas Pre Test vs. Post Test

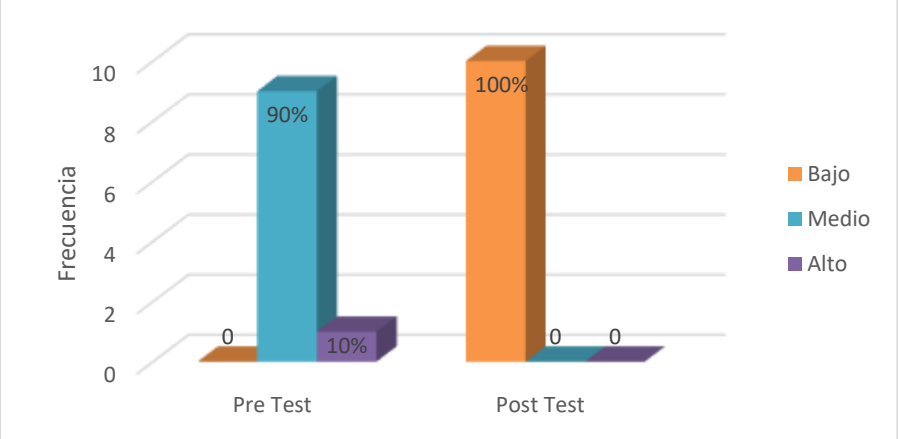
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	0	0	10	100,0
	Medio	9	90,0	0	0
	Alto	1	10,0	0	0
	Total	10	100,0	10	100

Nota. Se planteó el siguiente ítem ¿Cuál es la probabilidad de que fallas humanas provoquen incidentes de seguridad?

Siguiendo el análisis, la **tabla 23** compara la probabilidad de que las fallas humanas provoquen incidentes de seguridad en ITIPERU antes y después de implementar las correcciones adecuadas para mantener la seguridad de la infraestructura cloud. En el pre test, se detectó una probabilidad media del 90% de que las fallas humanas causaran incidentes de seguridad, y solo un 10% que la probabilidad era alta. Después de las intervenciones reflejadas en el post test, se consideró un 100% que la probabilidad de que las fallas humanas causen incidentes de seguridad fuera baja. Esto indica que las acciones tomadas han sido efectivas en reducir significativamente la posibilidad de que errores o negligencias humanas, y resulten en problemas de seguridad, disminuyendo la confianza de los servicios de brindados, y afectando la continuidad de negocio operativo.

Figura 37

Diagrama de comparación de la probabilidad de que fallas humanas



Nota. Visualización gráfica de los datos de la Tabla 23.

Por intermedio de la **Figura 37** se expresa el desarrollo favorable de reducir las fallas humanas que afecten la seguridad de los datos almacenados en las páginas webs y las máquinas virtuales.

Tabla 24

Comparación de la probabilidad de ataques a los servidores de alojamiento web Pre Test vs. Post Test

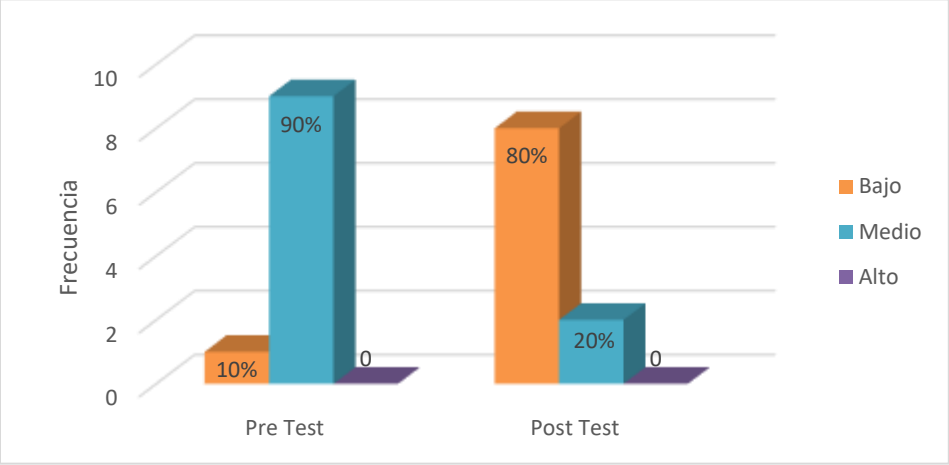
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	1	10,0	8	80,0
	Medio	9	90,0	2	20,0
	Alto	0	0	0	0
	Total	10	100,0	10	100,0

Nota. La pregunta fue ¿Cuál es la probabilidad de ataques a los servidores de alojamiento web?

La **Tabla 24** proporciona la probabilidad de que los servidores de alojamiento web de ITIPERU sufran ataques, comparando las respuestas obtenidas en dos evaluaciones diferentes: Pre Test y Post Test. En la evaluación inicial, el pre test, el 90% obtuvo una probabilidad alta, seguida de 10% con un nivel bajo. Luego, de aplicar la implementación, el post test señaló que el 80% de las páginas webs y las máquinas virtuales administradas por ITIPERU obtuvieron una asistencia de seguridad más robusto, y el 20% se mantuvo en una probabilidad media.

Figura 38

Diagrama de comparación de probabilidad de ataques a los servidores de alojamiento web



Nota. Visualización gráfica de los datos de la Tabla 24.

Según lo establecido en la **Figura 38,** el proceso de implementación de seguridad refleja como de un nivel medio de 90% en probabilidad de ataque a los servidores (pre test) disminuye a un nivel de probabilidad bajo de 80%, favoreciendo a mantener la confianza de los clientes de ITIPERU en sus sistemas de alojamiento web.

Tabla 25

Comparación de la identificación de mecanismos de seguridad en los servicios alojados Pre Test vs. Post Test

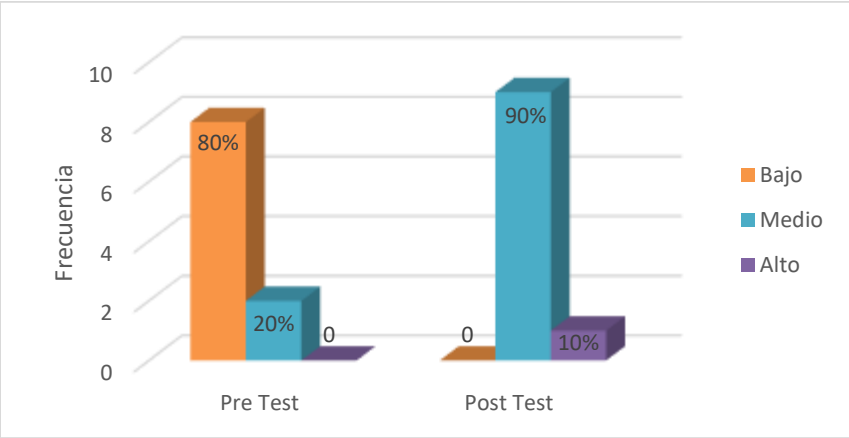
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	8	80,0	0	0
	Medio	2	20,0	9	90,0
	Alto	0	0	1	10,0
	Total	10	100,0	10	100,0

Nota. Se realizó la pregunta ¿Se realiza identificación de mecanismos de seguridad en los servicios alojados (páginas web, máquinas virtuales)?

La **Tabla 25** compara la identificación de mecanismos de seguridad en los servicios alojados por ITIPERU (como páginas web y máquinas virtuales) antes y después de realizar mejoras (Pre Test vs. Post Test). En el pre test, el 80% presentó mecanismos de seguridad bajos, y un 20% fue medio. Tras las mejoras indicadas en el post test, hay un cambio significativo, ya que el 90% fue calificado con un nivel medio para la identificación de mecanismos de seguridad, y un 10% fue alta. Este cambio sugiere que ITIPERU implemente medidas efectivas para mejorar la identificación de los mecanismos de seguridad en sus servicios alojados, reflejando una mejora en la postura de seguridad con una mayor conciencia y capacidad para detectar y gestionar las amenazas de seguridad en los entornos cloud .

Figura 39

Diagrama de comparación de la identificación de mecanismos de seguridad en los servicios alojados



Nota. Visualización gráfica de los datos de la Tabla 25.

De acuerdo a la **Figura 39**, se observa la representación en barras verticales de la Tabla 25, con el objetivo de señalar el cambio favorable de nivel bajo de 80% a un nivel medio de 90% para identificar los mecanismos de seguridad en los servicios alojados que brinda los entornos cloud de la empresa ITIPERU.

Tabla 26

Comparación de las políticas de seguridad Pre Test vs. Post Test

		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	10	100,0	1	10,0
	Medio	0	0	8	80,0
	Alto	0	0	1	10,0
	Total	10	100,0	10	100,0

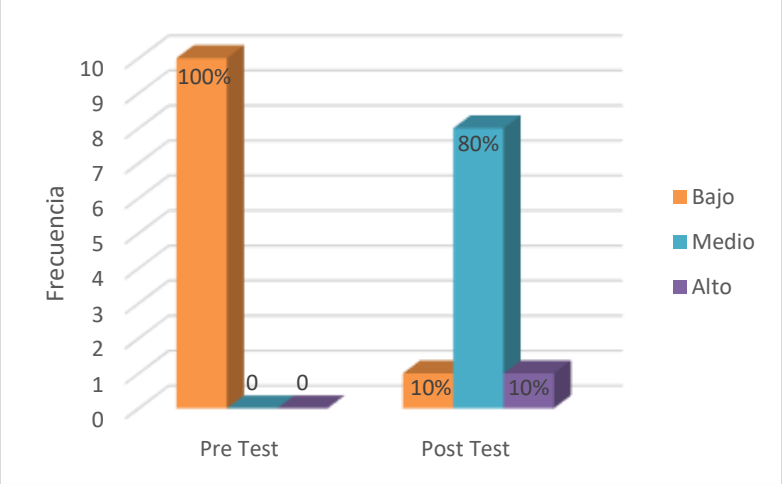
Nota. Se presentó el siguiente ítem ¿Se cuenta con políticas de seguridad para el uso del correo electrónico y otros medios de comunicación electrónica?

En la **Tabla 26** muestra la evaluación de las políticas de seguridad relacionadas con el uso del correo electrónico y otros medios de comunicación electrónica en ITIPERU, comparando los

resultados antes y después de realizar mejora de ciberseguridad. El pre test indicó que la totalidad del estudio en un 100% tenía un nivel bajo de políticas de seguridad; revelando una ausencia o deficiencia significativa en las políticas de seguridad para la comunicación electrónica. Sin embargo, el post test, mostró un cambio esencial. En su mayoría, el 80% califico de un nivel medio, un 10% fue nivel alto, y el resto del 10% fue bajo. Este cambio refleja una mejora sustancial en las políticas de seguridad para la comunicación electrónica en ITIPERU, indicando que las acciones tomadas han sido efectivas para aumentar la seguridad en este aspecto vital de las operaciones de la empresa.

Figura 40

Diagrama de comparación de las políticas de seguridad



Nota. Visualización gráfica de los datos de la Tabla 26.

Con la **Figura 40** se resalta el cambio positivo que se dio en las políticas de comunicación electrónica dentro de ITIPERU, al iniciar el estudio presentó un nivel bajo de 100% como lo muestra la barra naranja, pero luego de la implementación, su estadio cambia a un nivel medio de 80%. Contribuyendo a la mejora continua que debe desarrollar la empresa para asegurar la continuidad de negocio operativo.

Tabla 27

Comparación de los procedimientos ante incidentes de seguridad Pre Test vs. Post Test

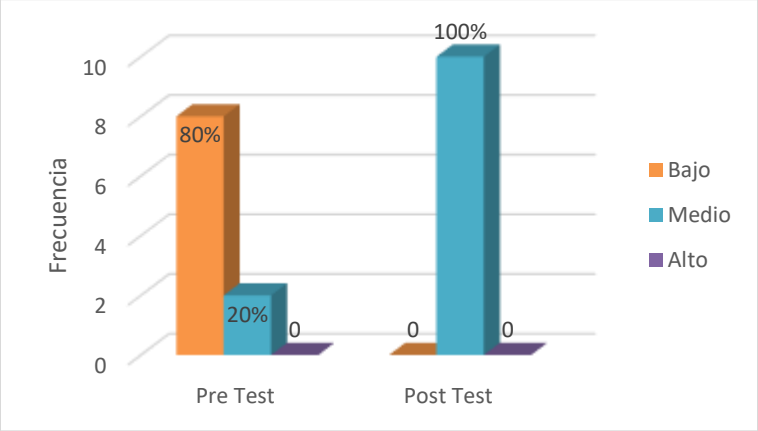
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	8	80,0	0	0
	Medio	2	20,0	10	100,0
	Alto	0	0	0	0
	Total	10	100,0	10	100,0

Nota. Se preguntó ¿Existen procedimientos para responder a incidentes de seguridad que afecten a las comunicaciones de la empresa?

La **Tabla 27** expresa la frecuencia y el porcentaje que resultó de la evaluación de los procedimientos de respuesta ante incidentes de seguridad. El pre test, halló que el 80% de las páginas virtuales y máquinas virtuales no tenían un procedimiento claro y adecuado ante algún incidente de seguridad en la infraestructura cloud de ITIPERU al momento de comunicarse; considerándolo en un nivel bajo. Asimismo, el 20% se en encontró en un nivel medio. Evidenciando, la falta de protocolos para certificar una comunicación segura entre los usuarios externos e internos de la empresa. Después de la implementación, el post test reveló una mejora de nivel medio del 100%. Aun así, se debe considerar una evaluación continua para identificar las amenazas o riesgos que pudieran perjudicar la ciberseguridad de las comunicaciones y la continuidad de negocio operativo en ITIPERU.

Figura 41

Diagrama de comparación de los procedimientos ante incidentes de seguridad



Nota. Visualización gráfica de los datos de la Tabla 27.

El gráfico **Figura 41** se ilustra la evolución del antes y después de ejecutar el proyecto de ciberseguridad en ITIPERU. Al inicio se obtuvo un nivel bajo de 80%, pero la implementación de protocolos más adecuados a las necesidades de ITIPERU lo llevo a un nivel medio al 100%.

Tabla 28

Comparación de configuraciones de la red Pre Test vs. Post Test

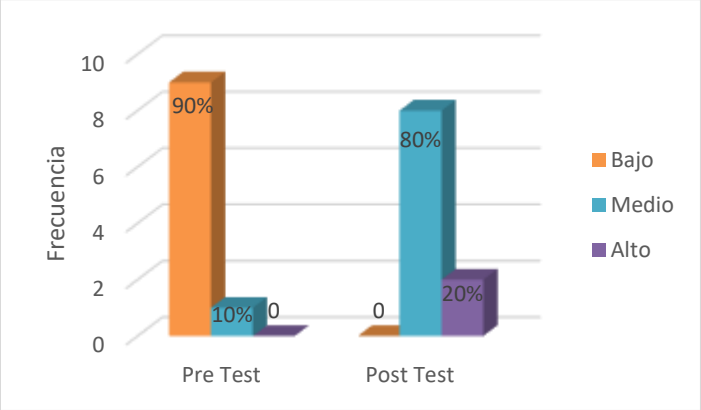
		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	9	90,0	0	0
	Medio	1	10,0	8	80,0
	Alto	0	0	2	20,0
	Total	10	100,0	10	100,0

Nota. El siguiente ítem fue ¿Se realiza configuraciones de red adecuadas en las máquinas virtuales?

Con la **Tabla 28** se demuestra la comparación de las configuraciones de las máquinas virtuales de ITIPERU, evaluadas antes y después de la implementación de mejoras. En el pre test, se identificaron que las máquinas virtuales tenían un nivel bajo del 90% de las configuraciones, y el 10% fue de nivel medio. Pero al establecer las nuevas estrategias de ciberseguridad, se halló un cambio en el post test, un 80% en el nivel medio y 20% en el nivel alto.

Figura 42

Diagrama de comparación de configuraciones de la red



Nota. Visualización gráfica de los datos de la Tabla 28.

El diagrama de la **Figura 42** presenta las barras verticales basado en los porcentajes obtenidos del pre test y post test sobre la configuración de red en las máquinas virtuales de ITIPERU. Con lo cual se observa un avance favorable, ya que al inicio se obtuvo una condición baja de 90%, pero después se obtuvo un nivel medio de 80%.

Tabla 29

Comparación de acuerdos de confiabilidad Pre Test vs. Post Test

		Pre Test		Post Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Bajo	10	100,0	0	0
	Medio	0	0	10	100,0
	Alto	0	0	0	0
	Total	10	100,0	10	100,0

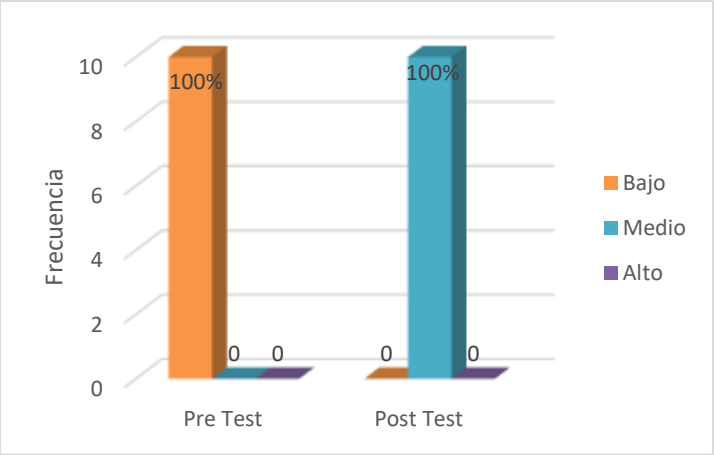
Nota. La última pregunta fue ¿Existe acuerdos de confidencialidad de divulgación de información entre los clientes y la empresa?

Según la **Tabla 29,** se observa que los acuerdos de confiabilidad se clasifican en tres niveles, por lo que durante el pre test el nivel bajo obtuvo una predominancia de 100%; luego en el post test, se obtuvo un resultado mejor consiguiendo un nivel medio de 100% para los acuerdos

de confiabilidad Esto implica que, aunque ha habido una mejora sustancial en la implementación de los acuerdos de confidencialidad, todavía no se alcanza el nivel más alto posible de seguridad en la protección de la información confidencial.

Figura 43

Diagrama de comparación de acuerdos de confiabilidad



Nota. Visualización gráfica de los datos de la Tabla 29.

Los datos de la **Figura 43** refleja el avance que se obtuvo en los acuerdos de confiabilidad, en un inicio se observó un nivel bajo de 100%, sin embargo, se logró conseguir un nivel medio del 100% luego de la implementación; por lo que se debe considerar que siempre se debe actualizar los acuerdos según las actualizaciones de la infraestructura cloud de ITIPERU.

4.2. Prueba de hipótesis

4.2.1. Hipótesis general

H1. La implementación de estrategias de ciberseguridad mejorará la robustez de la Continuidad del Negocio operativo en los entornos cloud en ITIPERU, Lima 2023.

H0. La implementación de estrategias de ciberseguridad no mejorará la robustez de la Continuidad del Negocio operativo en los entornos cloud en ITIPERU, Lima 2023.

Tabla 30

Comprobación de la hipótesis general

	Pre_test - Post_test
Z	-2,809[b]
Sig. asintótica(bilateral)	,005

Nota. Se consideró las siguientes condiciones: a. Prueba de rangos con signo de Wilcoxon, y b. Se basa en rangos negativos.

Según la **Tabla 30** el resultado de la hipótesis general empleando la prueba de Wilcoxon reveló que existe diferencia significativa entre el pre test y post test; esto debido al valor de significancia menor al 0.05, es decir, que hubo una mejora significativa después de la aplicación del test.

4.2.2. Hipótesis especificas

H1$_1$. La implementación de estrategias de ciberseguridad mejorará la disponibilidad de servicios cloud en ITIPERU.

H0. La implementación de estrategias de ciberseguridad no mejorará la disponibilidad de servicios cloud en la empresa ITIPERU.

Tabla 31

Comprobación de la hipótesis específica 1

Disponibilidad de servicios cloud	pre test - post test
Z	-2,823[b]
Sig. asintótica(bilateral)	,005

Nota. La primera comprobación manejo las siguientes condiciones estadísticas: a. Prueba de rangos con signo de Wilcoxon, y b. Se basa en rangos negativos.

La hipótesis específica 1 analizada en la **Tabla 31,** mediante la prueba de Wilcoxon indicó que existe diferencia significativa entre el pre test y post test, esto debido a su valor sig. menor al 0.05, es decir que hubo una mejora significativa después de la implementación de estrategias de ciberseguridad en cuanto a la disponibilidad de servicios cloud. Esto implica que las estrategias o

cambios aplicados han tenido un efecto positivo y han mejorado la disponibilidad de estos servicios.

H1$_2$. La implementación de estrategias de ciberseguridad mejorará el tiempo de recuperación de la integridad en entornos cloud en ITIPERU.

H0. La implementación de estrategias de ciberseguridad no mejorará el tiempo de recuperación de la integridad en entornos cloud en ITIPERU.

Tabla 32

Comprobación de la hipótesis específica 2

Tiempo de recuperación	pre test - post test
Z	-2,937[b]
Sig. asintótica(bilateral)	,003

Nota. Se consideró a. Prueba de rangos con signo de Wilcoxon, y b. Se basa en rangos positivos.

En la **Tabla 32** se analiza la hipótesis específica 2, con lo cual, la prueba de Wilcoxon halló que existe diferencia significativa entre el pre test y post test, esto debido a su valor sig. menor al 0.05, es decir que hubo una mejora significativa después de la aplicación de la implementación de estrategias de ciberseguridad en cuanto al tiempo de recuperación; repercutiendo en la reducción de tiempo para la recuperación de incidentes o fallas de los sistemas cloud en la administración de las páginas webs y máquinas virtuales.

H1$_3$. La implementación de estrategias de ciberseguridad mejorará las incidencias en los entornos cloud en la empresa ITIPERU.

H0. La implementación de estrategias de ciberseguridad no mejorará las incidencias en los entornos cloud en ITIPERU.

Tabla 33

Comprobación de la hipótesis específica 3

Gestión de incidencias	pre test – post test
Z	-2,805[b]
Sig. asintótica(bilateral)	,005

Nota. Se aplicó a. Prueba de rangos con signo de Wilcoxon, y b. Se basa en rangos positivos.

Con la **Tabla 33** se evalúa la hipótesis específica 3, en donde la prueba de Wilcoxon indica que existe diferencia significativa entre el pre test y post test, esto debido a su valor sig. menor al 0.05, es decir que hubo una mejora significativa después de la aplicación de métodos de ciberseguridad para gestionar adecuadamente las incidencias en entornos cloud

V. DISCUSIÓN DE RESULTADOS

La presente investigación halló durante la prueba de Pre Test que la empresa ITIPERU no presentaba estrategias de ciberseguridad en las máquinas virtuales y páginas web, por lo que se realizó un análisis situacional para aplicar herramientas basado en la norma ISO 27001 y la metodología de Zero Trust. Siendo así, que se volvió a medir en el Post-Test observándose un resultado favorable para asegurar la continuidad de negocio operativo y minimizar los riesgos de vulnerabilidad que pueda afectar la infraestructura tecnológica de la empresa.

La hipótesis general del estudio reveló que la implementación de estrategias de ciberseguridad mejoró la robustez de continuidad de negocio (p=0,005). Este hallazgo concuerda con el resultado de Avalos (2023) que menciono que la implementación de seguridad de la información basado en la norma ISO 27001 presentó un impacto positivo en la continuidad del negocio. Otros autores como Amancha (2020) y Gutiérrez (2022) identificaron que las empresas deben tener estrategias de ciberseguridad para asegurar y minimizar el riesgo de filtración de información crítica de una empresa, además de mejorar la continuidad de negocio.

También, Salinas (2020) refiere que el modelo Zero Trust confiere una arquitectura de acceso seguro, política de acceso estricta, control de entradas y salidas, segmentación y análisis del comportamiento del usuario. Sin embargo, durante la búsqueda bibliográfica no se halló estudios que analicen la asociación entre la norma ISO 27001 y el Zero Trust, pero diferentes foros como el “Blog sobre gobernanza de TI en Estados Unidos” (Irwin, 2019) menciona que ambas herramientas se complementan brindando a las empresas una seguridad mejorada con menor riesgo de filtración de datos, por lo que se espera que las empresas adapten estos modelos para seguir siendo competitivos en el mercado (Edwards, 2023).

La primera hipótesis está enfocada en el indicador de disponibilidad de servicios cloud, la cual mostró una diferencia significativa entre pre y post test con un valor menor a 0,005; es decir, que la implementación de estrategias de ciberseguridad influyó en la mejora de la resiliencia en la infraestructura cloud. Este resultado es similar para Barrios y Esteban (2021) que mencionaron que la disponibilidad e integridad de la información se ve reforzada por el uso de estrategias de ciberseguridad como la encriptación asimétrica. Asimismo, Bueno (2022) también confirma que la implementación de buenas prácticas de ciberseguridad basado en la normativa de ISO 27001 es beneficioso para asegurar la integridad, disponibilidad y confidencialidad de los sistemas informáticos.

La segunda hipótesis específica demostró que se mejoró el indicador tiempo de recuperación de la integridad en entornos cloud (p=0,003). Según la literatura consultada se halló resultados similares, Gómez y Doménech (2022) incorporó la normativo ISO 27001 asociado a un aplicativo de backup, con lo cual los tiempos de respuesta se minimiza y se facilita la accesibilidad de la información. El FEM (2022) recomendó a las PYMES tener protocolos de respuesta y recuperación rápida ante incidentes de seguridad, ya que son las que presentan mayor cantidad de ataques cibernéticos, las cuales pueden afectar su reputación e involucrar gastos económicos para la empresa y sus clientes (Bustillos y Rojas, 2022).

La tercera hipótesis específica halló una mejora significativa en la gestión de incidencias (p=0.005), este hallazgo similar se observa en la implementación de gestión de seguridad que realizó Medina (2023) ya que obtuvo un valor significativo menor a 0,05; al igual que Mallqui (2022) que mencionó que la variable ciberseguridad tiene una incidencia significativa sobre la gestión de TI de 0,00.

Con este análisis realizado, se observa que la implementación de estrategias de ciberseguridad basado en normativa internacionales y estandarizadas como la ISO 27001 junto con nuevas herramientas como Zero trust aumentan la robustez de la continuidad de negocio operativo en entornos cloud. Por otro lado, la literatura menciona que el uso de infraestructura en la nube permite que las empresas ahorren recursos y sea más barato administrar (Mokrani, 2021); y que se debe considerar que las diferentes normativas o programas de gestión de seguridad se deben adaptar en función del tamaño y necesidades requeridas por la empresa (Couce, 2021).

VI. CONCLUSIONES

a. La investigación confirmó que la implementación de estrategias de ciberseguridad basadas en la norma ISO 27001 y el modelo Zero Trust resultó en una mejora significativa en la robustez de la continuidad del negocio operativo y la seguridad en los entornos cloud en la empresa ITIPERU. Este resultado, es evidenciado por nivel de significativa entre el pre y post test (p=0.005), de manera que una estrategia de ciberseguridad bien estructurada es crucial para fortalecer la infraestructura tecnológica.

b. La disponibilidad de servicio cloud dentro de las estrategias de ciberseguridad basado en la normativa ISO 27001 y la herramienta de Zero trust obtuvo un hallazgo significativo (p=0,005); con lo cual, se demuestra que las combinaciones de ambos elementos se complementan para proteger los activos informáticos de una organización como en el caso de ITIPERU, mediante la autentificación y verificación continua de los usuarios, disminuyendo los riesgos de fuga de información, o suplantación de usuarios.

c. El indicador de tiempo de recuperación de la integridad presentó un grado de significancia alto (p=0.003) en la empresa ITIPERU, siendo así que se resalta la importancia de dar una repuesta rápida y efectiva ante situaciones de vulnerabilidad, y realizar un monitoreo constante para identificar y actuar ante amenazas que podrían interrumpir la disponibilidad del servicio cloud.

d. La investigación también demostró mejoras significativas en la gestión de incidencias, con un valor de p=0.005. Este hallazgo permite concluir que la gestión de incidencias es un aspecto crucial en la seguridad de la información, ya que permite responder rápidamente y eficientemente a situaciones de vulnerabilidad y minimizar el impacto de carácter adverso que estas incidencias puedan tener sobre el funcionamiento normal del servicio.

VII. RECOMENDACIONES

a. Se recomienda a la empresa ITIPERU crear un área o delegar la función a un colaborador de gestionar, mejorar y monitorear las estrategias de implementación de la normativa ISO 27001 y Zero Trust; con el objetivo de mantener una reputación intacta dentro del mercado de infraestructura TI; por ende, mantener y mejorar la robustez de la continuidad de negocio operativo a largo plazo.

b. Se invita a otras empresas similares a ITIPERU consideren adoptar un enfoque similar, especialmente en entornos cloud. Esta adaptación debe contemplar los distintos contextos operativos y tecnológicos, así como las amenazas específicas a las que cada organización podría estar expuesta, para lograr una estrategia de ciberseguridad verdaderamente eficaz.

c. Se aconseja a las empresas adoptar una política de evaluación y actualización constante de las estrategias de ciberseguridad para preservar y fortalecer su robustez en materia de seguridad. Este enfoque proactivo no solo ayuda a identificar y mitigar riesgos emergentes, sino que también asegura una protección más efectiva y actualizada frente a las vulnerabilidades dinámicas del mundo digital.

d. Se sugiere a futuros investigadores interesados en el presente tema, realizar más investigaciones para explorar en profundidad cómo estas dos metodologías propuestas en el estudio, normativa ISO 27001 y Zero Trust, pueden integrarse para optimizar la seguridad de la información en diferentes ámbitos de las empresas.

VIII. REFERENCIAS

Aguilar, L., y Otuyemi, E. (2020). Análisis documental: importancia de los entornos virtuales en los procesos educativos en el nivel superior. *Revista Tecnología, Ciencia y Educación*, (17), 57–77. https://doi.org/10.51302/tce.2020.485

Amancha, W. (2020). *Plan de ciberseguridad para asegurar la continuidad del negocio en la cooperativa de ahorro y crédito sierra centro Ltdo.* [Tesis de pregrado, Universidad Regional Autónoma de los Andes]. Repositorio Institucional URAA. https://dspace.uniandes.edu.ec/handle/123456789/11692

Amazon. (18 de octubre de 2023). *¿Qué es la ciberseguridad?* Amazon Web Services. https://aws.amazon.com/es/what-is/cybersecurity/

Arias, J. y Covinos S. (2022). *Metodología de la investigación: El método ARIAS para realizar un proyecto de tesis*. Repositorio Concytec. https://repositorio.concytec.gob.pe/bitstream/20.500.12390/3109/1/2022_Metodologia_de_la_investigacion_El_metodo_%20ARIAS.pdf

Avalos, V. (2023). *ISO 27001: Seguridad de la información y su impacto en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.* [Tesis de pregrado, Universidad Peruana de Ciencias Aplicadas]. Repositorio Institucional UPC. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/661432/Avalos_AS.pdf?sequence=3&isAllowed=y

Barrios, M., y Esteban, M. (2021). *Desarrollo de técnica de ciberseguridad para la encriptación de datos y detección de anomalías en la comunicación de un PLC con la nube en la*

industria 4.0. [Tesis de pregrado, Universidad Santo Tomás]. Repositorio Universidad Santo Tomás. https://repository.usta.edu.co/handle/11634/35662

Bernal, C. (2010). Propuesta de un proceso de investigación cuantitativa. Aplicación en la caracterización de las MYPES productoras de software. *Revista de Ciencias Humanas y Sociales*, 26(62), 58–76. https://dialnet.unirioja.es/descarga/articulo/6043099.pdf

Bonet, O., Mazot, A., Casanova, M., y Cruz, N. (2023). Proyecto de investigación y tesis. Guía para su elaboración. *MediSur*, 21 (1), 274-288. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1727-897X2023000100274&lng=es&tlng=es.

Bueno, G. (2022) *Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador*. [Tesis de maestría, Universidad Estatal Península de Santa Elena]. Repositorio UPSE. https://repositorio.upse.edu.ec/handle/46000/8979

Bustillos, O., y Rojas, J. (2022). Protocolo básico de ciberseguridad para pymes. *Interfases*, (016), 166–184. https://revistas.ulima.edu.pe/index.php/Interfases/article/view/6021

Cabezas, I. (2020). *Implementación de un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima.* [Tesis de pregrado, Universidad de San Martín de Porres]. Repositorio USMP. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/7059/cabezas_jic.pdf?sequence=1&isAllowed=y

Cajicá, A. 2020. *Máquinas virtuales sobre un clúster para laboratorio virtual.* [Tesis de pregrado, Benemérita Universidad Autónoma de Puebla]. Repositorio BUAP. *https://repositorioinstitucional.buap.mx/items/5c4847eb-45b0-4268-9c3d-094a2bf3c821*

Calvillo, S. (23 de Setiembre de 2020). *Continuidad de negocio ante un ciberataque*. Disaster Recovery Journal. https://drjenespanol.com/articulos/continuidad-de-negocio-ante-un-ciberataque/

Castillo, A. (2022). *Diseño de un modelo para identificar amenazas no intencionales de ciberseguridad en instituciones públicas generadas por personal interno a partir de su comportamiento sobre la infraestructura de TI.* [Tesis de pregrado, Pontificia Universidad Católica del Perú]. Repositorio Institucional PUCP. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/23059/CASTILLO_LOPEZ_ANDERSON_DISEÑO_MODELO_IDENTIFICAR.pdf?sequence=1&isAllowed=y

Castro, L. (2013). Gestión de la continuidad del negocio: caso Ravmar Freight del sector logístico. *Revista de Ciencias de la Gestión*, 6(1), 1–15. https://revistas.pucp.edu.pe/index.php/360gestion/article/download/24544/23298/

Chiriboga, P., Tapia, L., Fuentes, L., y Sánchez, J. (2022). Estrategias digitales de ampliación de mercados y la competitividad de la empresa importadora S. T. Rio Import. *Dominio De Las Ciencias*, *8*(3), 682–699. https://doi.org/10.23857/dc.v8i3.2834

Cifre, S. (2020). *Modelo de seguridad para la gestión de vulnerabilidades de servidores en nubes privadas.* [Tesis de maestría, Universidad Tecnológica de Santa Fe]. https://ria.utn.edu.ar/bitstream/handle/20.500.12272/6050/Tesis%20de%20Maestría%20-%20Cifre%20Simón.pdf?sequence=1&isAllowed=y

CISET (s,f). *Máquinas virtuales*. https://www.ciset.es/glosario/829-zero-trust-network-access-ztna

Comisión Económica para América Latina y el Caribe. (2022). Tecnologías digitales para el nuevo futuro. *Educitec - Revista de Estudios y Pesquisas sobre Ensino Tecnológico*. https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b41a4fd9/content

Cóndor, J., & Segura, K. (2017). *Propuesta de una Arquitectura Cloud Computing como soporte a la estrategia de Transformación Digital en empresas de ingeniería y construcción. Caso de Estudio: Universidad Peruana de Ciencias Aplicadas (UPC).* [Tesis de Maestría, UPC]. Repositorio UPC. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/622740/CondorU_Judith.pdf

Coronel, C. (2023). Los objetivos de la investigación. *Revista Archivo Médico de Camagüey*, 27, e9591. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1025-02552023000100048&lng=es&tlng=es.

Couce, J. (2021). *Implementación y aplicación de la ISO 27001:2013 en una consultora de TI de tamaño mediano*. [Tesis de maestría, Universidad San Jorge]. Repositorio USJ. https://repositorio.usj.es/handle/123456789/723

Del Castillo, E., y Pinto, M. (2018). Importancia de la muestra en una investigación científica. *Revista Ciencia Latina*, 6(2), 4375 - 4397 https://www.ciencialatina.org/index.php/cienciala/article/download/1805/2571

Díaz, R. (2022). *Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe.* Santiago. Documentos de Proyectos (LC/TS.2022/70) para la Comisión

Económica para América Latina y el Caribe. https://repositorio.cepal.org/bitstream/handle/11362/48065/1/S2200203_es.pdf

Díaz-Parco, P. (2022). *Plan de continuidad del negocio (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC.* [Tesis de pregrado, Universidad Técnica de Ambato]. Repositorio Institucional UTA. https://repositorio.uta.edu.ec/handle/123456789/36852

Edwards, M. (10 de octubre de 2023). *How ISO 27001 Can Help Organisations Implement a Zero Trust Security Model.* ISMS.online. https://www.isms.online/knowledge/iso-27001-and-implementing-a-zero-trust-security-model/

Espinoza, E. (2018). La hipótesis en la investigación. Mendive. *Revista de Educación*, 16(1), 122–139. http://scielo.sld.cu/scielo.php?script=sci_arttext&

Foro Económico Mundial. (2022). *Annual Report 2021-2022*. https://es.weforum.org/publications/annual-report-2021-2022

Flores, E. (2023). *Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC orientado a PYMES.* [Tesis, Pontificia Universidad Católica del Perú]. Repositorio institucional PUCP. http://hdl.handle.net/20.500.12404/25097

ISO. (15 de noviembre de 2023). *Normas mundiales para bienes y servicios de confianza.* https://www.iso.org/es/home.

More, S. (13 de abril de 2022). Principales tendencias de ciberseguridad. Gartner. https://www.gartner.es/es/articulos/las-7-principales-tendencias-en-ciberseguridad-para-2022

García, D., & Sánchez, C. (2020). Diseño teórico de la investigación: instrucciones metodológicas para el desarrollo de propuestas y proyectos de investigación científica. *Información tecnológica*, 31(6), 159–168. https://doi.org/10.4067/S0718-07642020000600159

Guevara, R., y Cortez, R. (2018). Importancia de la población y muestra en la investigación científica. *CIENCIA UNEMI*, 11(28), 118–127. https://dialnet.unirioja.es/descarga/articulo/8728928.pdf

Guevara, V., y Domingo, S. (2022). La nube en Pymes mediante las normas ISO 27005. *Revista Ingeniería*, 6(15), 169–182. https://doi.org/10.33996/revistaingenieria.v6i15.98

Gómez, C., y Doménech, G. (2022). *Análisis e implementación para la integración del sistema de información (SGSI) ISO 27001 con aplicación Uranium Backup para protección de servidores virtuales en plataforma VMware ESXi, replicación y recuperación en la Empresa Comercial e Industrial Sucre Comsucre S.A.* [Tesis de licenciatura, Universidad de Guayaquil]. Red de Investigadores. https://redi.cedia.edu.ec/document/45011

Gutiérrez, A. (2022). *Diseño del Plan de Continuidad de negocio aplicado a Seguridad de Información en PYME Intervision de Guayaquil.* [Tesis de pregrado, Universidad Politécnica Salesiana]. Repositorio Institucional UPS. https://dspace.ups.edu.ec/bitstream/123456789/22136/1/UPS-GT003667.pdf

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación.* (6.ª ed.). McGraw-Hill. https://www.esup.edu.pe/wp-

content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

INCIBE. (09 de octubre de 2023). *Metodología zero trust: Fundamentos y beneficios*. https://www.incibe.es/incibe-cert/blog/metodologia-zero-trust-fundamentos-y-beneficios

Irwin, L. (10 de diciembre de 2019). *Implementing zero trust with ISO 27001.* IT Governance USA Blog. https://www.itgovernanceusa.com/blog/implementing-zero-trust-with-iso-27001

ISO. (s.f). *Organización Internacional de Normalización*. https://www.iso.org/home.html

Kaspersky. (27 de junio de 2022). *Las PYMEs de América Latina enfrentan un creciente número de ciberataques.* https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/

Kaspersky. (s.f). *Ciberseguridad.* https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Microsoft. (s.f.). *Máquinas virtuales*. https://learn.microsoft.com/es-es/azure/architecture/reference-architectures/n-tier/windows-vm

Mallqui, A. (2022). *Ciberseguridad y su incidencia en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.* [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/96925?show=full

Medeiros, V., Godoi, L., y Teixeira, E. (2019). La competitividad y sus factores determinantes: Un análisis sistémico para países en desarrollo. *Revista de CEPAL*, 129. https://repositorio.cepal.org/handle/11362/44910

Medina, J. (2023). *ISO 27001 para la gestión de seguridad de la información en el área TI de una empresa industrial, Lima 2023.* [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional – UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/121182?show=full

Mendivil, J., Sanz, B., y Gutierrez, M. (2022). Formación y concienciación en ciberseguridad, basada en competencias: una revisión sistemática de literatura. PIXEL-BIT. *Revista de Medios y Educación*, 63. https://revistapixelbit.com/index.php/pixelbit/article/view/3006

Mendoza, F., y Vega, G. (2019). *Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC.* [Tesis de maestría, Universidad del Pacífico]. Repositorio de UP. https://repositorio.up.edu.pe/handle/11354/2250

Microsoft. (10 de diciembre de 2023). *Zero Trust Security*. https://learn.microsoft.com/es-es/security/zero-trust/zero-trust-overview

Mokrani, O. (2021). *Diseño y manejo de infraestructuras de red cumpliendo con los estándares de ciberseguridad*. [Tesis de pregrado, Universidad Politécnica de Madrid]. Biblioteca Facultad de Informática. https://oa.upm.es/66341/

Mora, J. (2020). *Propuesta metodológica para la gestión de la seguridad de la información alineada a la norma ISO 27001 y ciberseguridad.* [Tesis de maestría, Universidad Católica del Ecuador]. Repositorio Institucional UCE. https://repositorio.puce.edu.ec/handle/22000/21011

Murga, A. (2022). *Diseño de un modelo de seguridad basado en la metodología zero trust, para salvaguardar, proteger los accesos a los recursos compartidos en red, en la empresa Resead*. [Tesis de pregrado, Universidad Peruana de las Américas]. Repositorio de la

Universidad Peruana de las Américas. http://repositorio.ulasamericas.edu.pe/bitstream/handle/123456789/2969/1.Tesis%20Murga%20Robles.pdf?sequence=1&isAllowed=y

NQA. (s. f.). *ISO 22301*. https://www.nqa.com/es-pe/certification/standards/iso-22301

NVIDIA. (28 de octubre de 2022). *Zero Trust*. https://la.blogs.nvidia.com/2022/10/28/que-es-zero-trust/

Neill, D., y Cortez, L. (2018). *Procesos y fundamentos de la investigación científica.* [Trabajo de titulación, Universidad Técnica de Machala]. Repositorio Institucional UTMACH. https://repositorio.utmachala.edu.ec/handle/48000/12498

Orozco, C. (2021). *Estrategias algorítmicas orientadas a la ciberseguridad: Un mapeo sistemático.* [Tesis de maestría, Universidad Politécnica Salesiana]. Repositorio Institucional UPS. https://revistapixelbit.com/index.php/pixelbit/article/view/3245

Oyola, A. (2021) La variable. *Revista Del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo*, 14(1), 90–93. https://doi.org/10.35434/rcmhnaaa.2021.141.905

Ontek. (13 de abril de 2018). *Las 5 etapas del ciclo de ciberseguridad*. https://www.ontek.net/etapas-ciberseguridad/

Olis, J., López, M., y Méndez, K. (2021). Planificación de la continuidad del negocio en las organizaciones. *Revista Venezolana de Gerencia (RVG)*, 26(95), 344–361. https://www.redalyc.org/journal/280/28069360008/html/

Peraza, S., Uzcátegui, B., Guerrero, D., Medina, D., Ramírez, A., y Lezama, L. (2017). Diseño, confiabilidad, validez y normas de la escala de resiliencia para estudiantes universitarios.

Revista de Pedagogía, 38(103), 158–176. https://www.redalyc.org/articulo.oa?id=65954978008

Ley Nº 29733. Ley de Protección de Datos Personales. Perú. (22 de marzo de 2013). https://www.gob.pe/institucion/egesg/normas-legales/1941246-003-2013-jus

Rodríguez, Y. (2021). Continuidad del negocio: conceptualización y metodologías de evaluación. *SIGNOS - Investigación en Sistemas de Gestión*, 13(1), 10–24. https://doi.org/10.15332/24631140.6337

Rojas, J., Ajuría, J., y Arambarri, J. (2023). Metodología de transformación digital para incrementar la competitividad de las pymes de logística ligera en el Perú. *Industrial Data*, *26*(1), 63-90.https://dx.doi.org/10.15381/idata.v26i1.23745

Russell, J. (2022). *ISO 27001*: *Guía sobre la Norma internacional para la gestión de la seguridad de la información*. [*Guía en PDF*]. NQA. https://www.nqa.com/medialibraries/NQA/NQA-Media Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Robayo, H. (2022). *Estrategias de ciberseguridad.* [Libro electrónico]. https://dialnet.unirioja.es/descarga/libro/924425.pdf

Ramos-Galarza, C. (2021). Diseño de investigación experimental. Revista CienciAmérica, 10(1), 1-7. https://dialnet.unirioja.es/descarga/articulo/7890336.pdf

Salinas, A. (2020). *Modelo de ciberseguridad para cajas municipales en tiempos de transformación digital.* [Tesis de maestría, Universidad Privada del Norte]. Repositorio UPN. https://repositorio.upn.edu.pe/handle/11537/29733

Sánchez, J., Díaz, P., y Vargas, C. (2021). Evaluación de la ciberseguridad en pequeñas y medianas empresas en el contexto de la industria 4.0. *Información Tecnológica*, 32(5), 111–120. https://doi.org/10.4067/S0718-07642021000500121

Servidores y Tutoriales (28 de octubre de 2015). Esquema de la petición web. https://servidoresstutoriales.blogspot.com/2015/10/esquema-de-la-peticion-web-servidor-web.html

Sota, M., y Mechan, D. (2018). *Implementación de controles y cumplimiento de requisitos de la ISO/IEC 27001: 2013 para la seguridad.* [Tesis de pregrado, Universidad San Martín de Porres]. Repositorio Institucional USMP. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/4326/sota_mechan.pdf?sequence=1&isAllowed=y

Tenorio, A. (2017). *Optimización de una IaaS en Cloud Computing haciendo uso de una Nube Privada.* [Tesis de pregrado, Universidad Peruana Cayetano Heredia]. Repositorio Institucional UPCH. http://repositorio.upch.edu.pe/handle/upch/1396

Vilcarromero, M. (2019). *Propuesta de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones.* [Tesis de pregrado, Universidad Peruana de Ciencias Aplicadas]. Repositorio Institucional UPCH. https://repositorioacademico.upc.edu.pe/handle/10757/624832

Ventura, M. (2017). Importancia del muestreo en la investigación científica. *Revista Cubana Salud Pública*, 43(4). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662017000400014

Villasis-Keever, M., Reyes-Morales, H., y Rojas-Russell, M. (2018). El protocolo de investigación VII. Validez y confiabilidad de las mediciones. *Revista Médica del Instituto Mexicano del Seguro Social*, 56(4), 414–419. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-91902018000400414

IX. ANEXOS

ANEXO A: Matriz de Consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES
A. Problema general ¿En qué medida la implementación de estrategias de ciberseguridad, contribuirá a mejorar la robustez de la continuidad del negocio operativo en los entornos cloud de ITIPERU, Lima 2023? B. Problemas específicos 1. ¿De qué manera la implementación de estrategias de ciberseguridad, mejorará la disponibilidad de servicios cloud en ITIPERU?	A. Objetivo general Determinar el grado de influencia que ejercerá la implementación de estrategias de ciberseguridad en la robustez de la continuidad del negocio operativo en los entornos cloud en ITIPERU, Lima 2023. B. Objetivos específicos 1. Determinar el grado de influencia que ejercerá la implementación de estrategias de ciberseguridad en la disponibilidad de servicios cloud en ITIPERU.	A. Hipótesis general La implementación de estrategias de ciberseguridad mejorará la robustez de la Continuidad del Negocio operativo en los entornos cloud en ITIPERU, Lima 2023. B. Hipótesis específicas 1. La implementación de estrategias de ciberseguridad mejorará la disponibilidad de servicios cloud en ITIPERU. 2. La implementación de estrategias de ciberseguridad	Variable independiente Estrategias de Ciberseguridad Variable dependiente Continuidad del Negocio operativo

2. ¿De qué manera la implementación de estrategias de ciberseguridad, mejorará el tiempo de recuperación de la integridad en entornos cloud en ITIPERU? 3. ¿De qué manera la implementación de estrategias de ciberseguridad, mejorará las incidencias en los entornos cloud en ITIPERU?	2. Determinar el grado de influencia que ejercerá la implementación de estrategias de ciberseguridad en el tiempo de recuperación de la integridad en entornos cloud en ITIPERU. 3. Determinar el grado de influencia que ejercerá la implementación de estrategias de ciberseguridad en las incidencias en los entornos cloud en ITIPERU.	mejorará el tiempo de recuperación de la integridad en entornos cloud en ITIPERU. 3. La implementación de estrategias de ciberseguridad mejorará las incidencias en los entornos cloud en ITIPERU.	

ANEXO B: Ficha de recolección de datos

FICHA DE RECOLECCION DE DATOS: MODELO DE ESTRATEGIAS DE CIBERSEGURIDAD PARA MEJORAR LA ROBUSTEZ DE LA CONTINUIDAD DEL NEGOCIO OPERATIVO EN LOS ENTORNOS CLOUD EN LA EMPRESA ITIPERU SAC, LIMA PERÚ 2023.

VARIABLE 1: MODELO DE ESTRATEGIAS DE CIBERSEGURIDAD

1) PROTECCION DE DATOS

Control de accesos		SI	NO	OBSERVACIONES
1	¿Existen procedimientos de autenticación multifactor para el acceso a los recursos críticos?			
2	¿Se revisan y actualizan periódicamente los derechos de acceso ?			
3	¿Se registra y monitorea el acceso de usuarios a entornos cloud?			
4	¿Se utiliza control de acceso basado en roles para limitar el acceso a recursos según la necesidad del usuario?			
5	¿ Se tiene monitoreo y alertas de seguridad de accesos ?			
	TOTAL			
	RESULTADO DEL TRP %			

2)Criptografía		SI	NO	OBSERVACIONES
1	¿Se utiliza cifrado para proteger los datos sensibles de los entornos cloud?			
2	¿Se cuenta con política de controles criptográficos?			
3	¿Se emplean protocolos seguros (como TLS)?			
4	¿se cuenta con un plan de acción en caso de fallo o compromiso en los sistemas de cifrado			
5	¿Se han implementado políticas para el manejo seguro de los certificados digitales?			
	TOTAL			
	RESULTADO DEL TCA %			

3)SEGURIDAD DE LAS OPERACIONES

Vulnerabilidades

Evaluación del Nivel de Impacto (NI)		BAJO	MEDIO	ALTO	OBSERVACIONES
1	En caso de un incidente de seguridad, ¿cuál sería el impacto en la continuidad del negocio?				
2	¿Cuál sería el impacto de una brecha de seguridad en la reputación de la empresa?				
3	¿Qué impacto tendría un ataque de seguridad en la integridad de los datos críticos?				
4	¿Cuál sería el impacto financiero de un incidente de seguridad?				
5	¿ cual sería el impacto por fallas en el alojamiento web ?				
Evaluación de la Probabilidad de Ocurrencia de Riesgo (POR)		**BAJO**	**MEDIO**	**ALTO**	**OBSERVACIONES**
1	¿Con qué frecuencia se han detectado vulnerabilidades de seguridad en las paginas web y maquinas virtu				
2	¿Cuál es la frecuencia de ataques de seguridad experimentados en el pasado?				
3	¿Qué tan probable es el aprovechamiento de las vulnerabilidades conocidas por los atacantes?				
4	¿Cuál es la probabilidad de que fallas humanas provoquen incidentes de seguridad?				
5	¿Cuál es la probalidad de ataques al los servidores de alojamiento web ?				
Seguridad de las comunicaciones		**BAJO**	**MEDIO**	**ALTO**	**OBSERVACIONES**
1	¿Se realizan identifican mecanismos de seguridad en los servicios alojados (paginas web,maquinas virtual				
2	¿Se cuenta con políticas de seguridad para el uso del correo electrónico y otros medios de comunicación				
3	¿Existen procedimientos para responder a incidentes de seguridad que afecten a las comunicaciones de la				
4	¿ Se realiza configuraciones de red adecuadas en las maquinas virtuales ?				
5	¿ Existe acuerdos de confidencialidad de divulgacion de informacion entre los clientes y la empresa ?				

VARIABLE 2: CONTINUIDAD DE NEGOCIO OPERATIVO

Periodo de Evaluación: [Fecha de inicio _____/xx/xx/2023_____] - [Fecha de fin:__ xx/xx/2023_____]

Sección 1: Disponibilidad de Servicios Cloud

Fecha	Tiempo Programado (horas)		Tiempo de Inactividad (horas)	Causa de la Inactividad	Acciones Tomadas	Observaciones	Disponibilidad

Instrucciones: Registre diariamente el tiempo programado de operación y cualquier tiempo de inactividad que ocurra, especificando la causa y las acciones tomadas para resolverlo.

Sección 2: Tiempo de Recuperación de Integridad

Fecha	Hora del Incidente	Hora de Detección	Hora de Resolución	Tiempo de	Impacto en el Servicio	Observaciones

Instrucciones: En caso de un incidente, registre el momento en que ocurre, el momento en que se detecta y cuando se resuelve completamente.

Sección 3: Gestión de Incidentes de Seguridad de la Información

Fecha	Incidentes	Incidentes Resueltos	Tiempo Medio de Respuesta	Eficacia de la	Observaciones

Instrucciones: Registre todos los incidentes de seguridad que se reporten, los que se resuelvan y el tiempo medio que se toma para responder a estos incidentes.

ANEXO C: Ficha de validación por juicio de expertos

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
FACULTAD DE INGENIERIAINDUSTRIAL Y DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

1.1. Apellidos y Nombres: PEDRO MARTÍN LEZAMA GONZALES
1.2. Grado académico: DOCTOR EN INGENIERÍA
1.3. Cargo e institución donde labora: DOCENTE DE LA ESCUELA UNIVERSITARIA DE POSGRADO-UNFV
1.4. Nombre del instrumento motivo de evaluación: CUESTIONARIO
1.5. Autor(A) de Instrumento: ESTRADA TORRES, CARLOS GILMER
1.6. Criterios de aplicabilidad:

a. De 01 a 09: (No válido, reformular)
b. De 10 a 12: (No válido, modificar)
c. De 13 a 15: (Válido, mejorar)
d. De 16 a 17: (Válido, precisar)
e. De 19 a 20: (Válido aplicar)

II. ASPECTOS DE VALIDACIÓN

INDICADORES DE EVALUCION DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (13-15)	Muy Bueno (16-18)	Excelente (19-20)
		1	2	3	4	5
1. CLARIDAD	Esta formulado con lenguaje comprensible.					x
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.					x
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.					x
4. ORGANIZACIÓN	Existe una organización lógica.					x
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales					x
6. INTENCIONALIDAD	Esta adecuado para valorar las variables de la Hipótesis.					x
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.					x
8. COHERENCIA	Existe coherencia entre los problemas objetivos, hipótesis, variables e indicadores.					x
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis.					x
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.					x

VALORACIÓN CUANTITATIVA (TOTAL X 0.4): **20.**

VALORACIÓN CUALITATIVA: **VÁLIDO**

OPINIÓN DE APLICABILIDAD: **APLICAR**

Lima, 29 de noviembre del 2023

DNI No __09656793___ Telf.: _945473135

FIRMA DEL EXPERTO INFORMANTE

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
FACULTAD DE INGENIERIAINDUSTRIAL Y DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

1.1. Apellidos y Nombres: ROMAN CONCHA NORBERTO ULISES
1.2. Grado académico: MAGISTER
1.3. Cargo e institución donde labora: JEFE DE LA OFICINA DE EDUCACIÓN VIRTUAL UNMS
1.4. Nombre del instrumento motivo de evaluación: CUESTIONARIO
1.5. Autor(A) de Instrumento: ESTRADA TORRES, CARLOS GILMER
1.6. Criterios de aplicabilidad:

a. De 01 a 09: (No válido, reformular)
b. De 10 a 12: (No válido, modificar)
c. De 13 a 15: (Válido, mejorar)
d. De 16 a 17: (Válido, precisar)
e. De 19 a 20: (Válido aplicar)

II. ASPECTOS DE VALIDACIÓN

INDICADORES DE EVALUCION DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (13-15)	Muy Bueno (16-18)	Excelente (19-20)
		1	2	3	4	5
1. CLARIDAD	Esta formulado con lenguaje comprensible.					X
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.					X
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.					X
4. ORGANIZACIÓN	Existe una organización lógica.				X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales					X
6. INTENCIONALIDAD	Esta adecuado para valorar las variables de la Hipótesis.					X
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.				X	
8. COHERENCIA	Existe coherencia entre los problemas objetivos, hipótesis, variables e indicadores.					X
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis.					X
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.				X	

VALORACIÓN CUANTITATIVA (TOTAL X 0.4): **18.**

VALORACIÓN CUALITATIVA: **VÁLIDO**

OPINIÓN DE APLICABILIDAD: **APLICAR**

Lima, 24 de noviembre del 2023

DNI No __08510560____ Telf.: _938345776_

FIRMA DEL EXPERTO INFORMANTE

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
FACULTAD DE INGENIERIAINDUSTRIAL Y DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTOS

I. DATOS GENERALES

1.1. Apellidos y Nombres: JORGE ALBERTO VALES CARRILLO
1.2. Grado académico: DOCTOR EN INGENIERIA
1.3. Cargo e institución donde labora: DOCENTE DE LA ESCUELA UNIVERSITARIA DE POSGRADO-UNFV
1.4. Nombre del instrumento motivo de evaluación: CUESTIONARIO
1.5. Autor(A) de Instrumento: ESTRADA TORRES, CARLOS GILMER
1.6. Criterios de aplicabilidad:

a. De 01 a 09: (No válido, reformular)
b. De 10 a 12: (No válido, modificar)
c. De 13 a 15: (Válido, mejorar)
d. De 16 a 17: (Válido, precisar)
e. De 19 a 20: (Válido aplicar)

II. ASPECTOS DE VALIDACIÓN

INDICADORES DE EVALUCION DEL INSTRUMENTO	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (13-15)	Muy Bueno (16-18)	Excelente (19-20)
		1	2	3	4	5
1. CLARIDAD	Esta formulado con lenguaje comprensible.					X
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.					X
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.					X
4. ORGANIZACIÓN	Existe una organización lógica.					X
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales					X
6. INTENCIONALIDAD	Esta adecuado para valorar las variables de la Hipótesis.					X
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.					X
8. COHERENCIA	Existe coherencia entre los problemas objetivos, hipótesis, variables e indicadores.					X
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis.					X
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.					X

VALORACIÓN CUANTITATIVA (TOTAL X 0.4): **20.**

VALORACIÓN CUALITATIVA: **VÁLIDO**

OPINIÓN DE APLICABILIDAD: **APLICAR**

Lima, 04 de Diciembre del 2023

DNI No 08512150 Telf.: 934546586

FIRMA DEL EXPERTO INFORMANTE

ANEXO D: Análisis e implementación de estrategias de ciberseguridad en ITIPERU

ANÁLISIS SITUACIONAL E IMPLEMENTACIÓN DE ESTRATEGIAS DE CIBERSEGURIDAD PARA LA CONTINUIDAD DE NEGOCIO DE ITIPERU SAC.

a. ITIPERU SAC

ITI PERU SAC se ha establecido como una empresa líder en tecnologías de la información que brinda soluciones empresariales orientada a modernizar y automatizar procesos estratégicos de nuestros clientes para lograr aumentar su rendimiento y efectividad en sus unidades de negocio. En este entorno dinámico y tecnológicamente avanzado, la seguridad de la información se ha convertido en un pilar fundamental para garantizar la integridad, confidencialidad y disponibilidad de nuestros servicios.

b. Importancia de la ciberseguridad para ITIPERU SAC

La ciberseguridad no es solo una necesidad operativa, sino un compromiso esencial con nuestros clientes y partes interesadas. En un mundo donde las amenazas cibernéticas evolucionan constantemente, mantener seguros nuestros sistemas y datos es crucial para la continuidad de nuestras operaciones y la confianza de nuestros clientes. La protección contra ataques cibernéticos, brechas de datos y otras vulnerabilidades cibernéticas es vital para preservar nuestra reputación y capacidad operativa.

c. Objetivo del reporte

Analizar e implementar estrategias de ciberseguridad robustas en ITI PERU SAC, alineadas con la normativa internacional ISO 27001 y el modelo Zero Trust. La adopción de la norma ISO 27001 proporcionará un marco sólido para la gestión sistemática de la seguridad de la información, mientras que el enfoque Zero Trust permitirá una seguridad más dinámica y adaptativa, basada en la premisa de no confiar y siempre verificar. Al integrar estas estrategias, buscamos mejorar significativamente la robustez de la continuidad del negocio, asegurando que

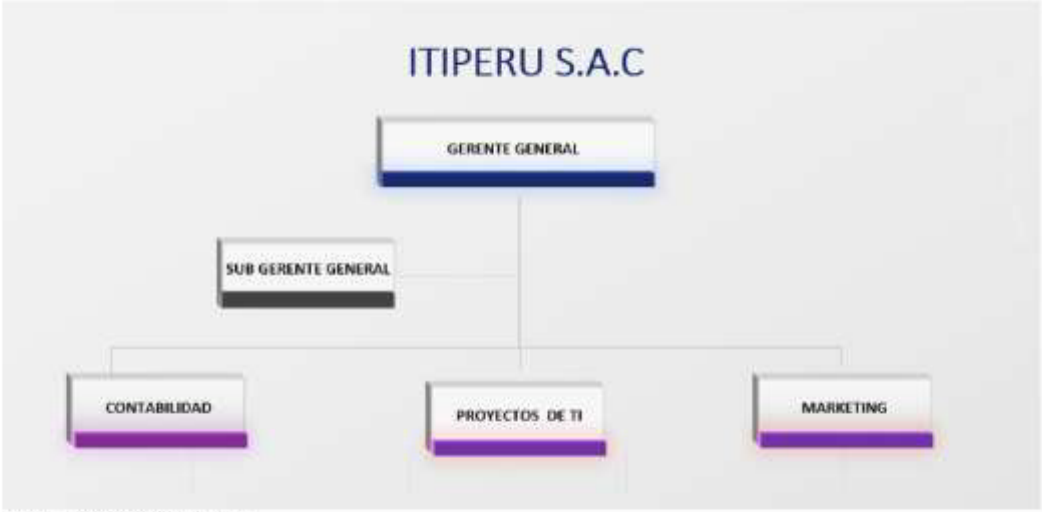
ITI PERU SAC pueda enfrentar y mitigar eficazmente los desafíos de seguridad en el cambiante panorama digital actual.

1. Estructura Organizacional

La estructura organizacional de la empresa ITIPERUSAC se encuentra organizada de la siguiente manera (Figura 1):

Figura 1

Organigrama



Nota. Elaboración propia.

2. Activos

En ITI PERU SAC, los activos son fundamentales para el soporte y la ejecución de nuestras operaciones diarias, abarcando tanto elementos físicos como virtuales.

Tabla 1

Descripción de los activos físico TI

Activos informaticos ITIPERU SAC						
Tipo de Activo	**Marca**	**MODELO**	**Modelo**	**Cantidad**	**Area**	**Estado**
Laptop	Lenovo	ThinkPad E560	Core i7	1	Gerencia	Operativo
Laptop	HP	HP 250 G8	Core i3	1	Contabilidad	Operativo
Laptop	Lenovo	Lenovo V15	core i7	1	Proyectos TI	Operativo
Laptop	Lenovo	Lenovo V15	Core i7	1	Proyectos TI	Operativo
Laptop	Lenovo	Lenovo V15	Core i7	1	Proyectos TI	Operativo
Laptop	HP	HP 250 G8	Core i3	1	Marketing	Operativo

Nota. Elaboración propia.

Tabla 2

Descripción de activos virtuales - Infraestructura Cloud IaaS

CARACTERISTICAS	SERVICIO DE MICROSOFT AZURE
Categoria	Computacion
Tipo de servicio	AKS
Región	Este de EE. UU. 2
Instancia	B8ms (8 vCPU, 32 GB de RAM) - Tiempo: 744 Horas (Pago por uso)
Sistema Operativo	Windows (Licencia incluida)
Almacenamiento	1 disco SSD Estandar de 64GB

Nota. Elaboración propia.

Tabla 3

Descripción de activos virtuales – Máquinas virtuales

CARACTERISTICAS MAQUINAS VIRTUALES		N° DE MAQUINAS VIRTUALES
Caracteristicas	**Especificaciones**	
Sistema Operativo	Windows Server 2022	4
vCPU	4	
RAM	8 GB	
Generación de VM	V2	
Arquitectura de VM	x64	

Nota. Elaboración propia.

Tabla 4

Descripción de activos virtuales - Infraestructura Cloud VPS

CARACTERISTICAS HOSTING		PAGINAS WEB ALOJADAS
Caracteristicas	**Especificaciones**	
CPU	2 Nucleos CPU	**6**
RAM	4 GB	
Almacenamiento	90 GB	

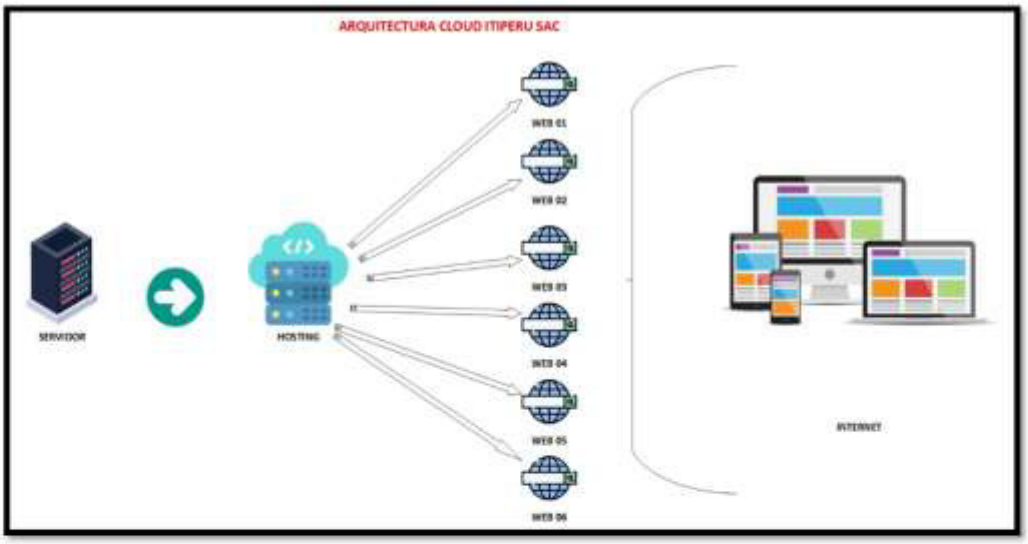
Nota. Elaboración propia.

3. Infraestructura Tecnológica actual

Se describe gráficamente el conjunto de componentes de hardware virtual y software que constituyen la base para el soporte y operación de los sistemas de información y tecnologia de ITIPERU SAC.

Figura 2

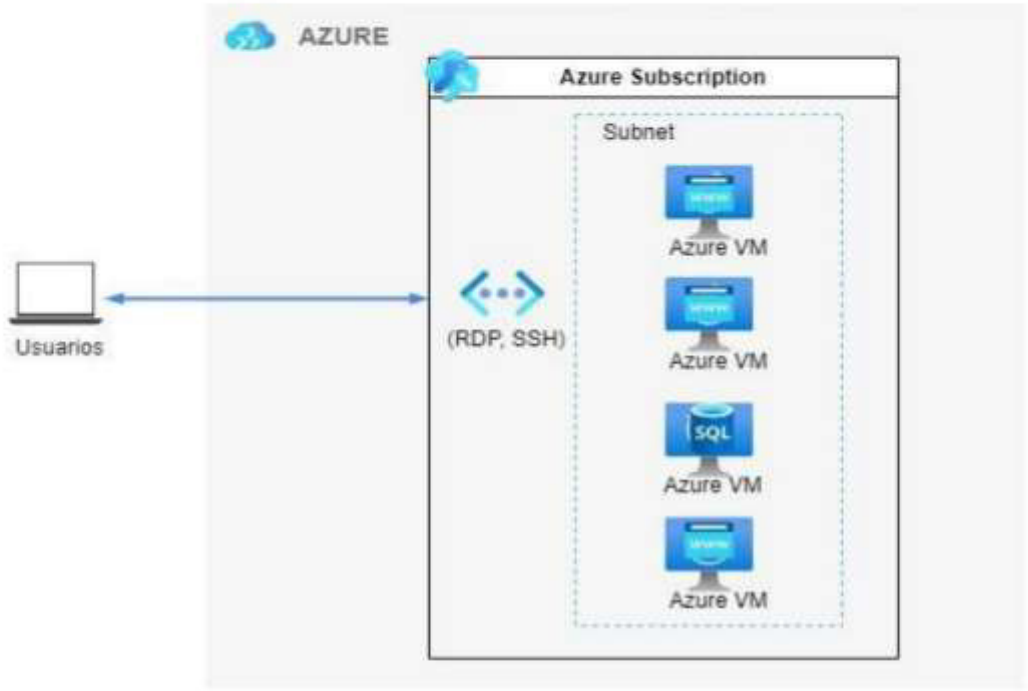
Diseño actual de Arquitectura Cloud VPS



Nota. Elaboración propia.

Figura 3

Diseño de Arquitectura actual de Azure



Nota. Elaboración propia.

4. Desarrollo del proyecto

Para el desarrollo del proyecto se seguirá un enfoque multidisciplinario que integrará recursos humanos especializados, estándares de ciberseguridad y herramientas tecnológicas que a continuación se detallan:

a) **Recursos humanos.** En el contexto del proyecto propuesto en ITIPERU se optará por coordinar con los propios colaboradores que trabajan en la empresa.

Tabla 5

Recursos humanos

Recurso Humano Para el proyecto	
Personal	**Funciones**
Líder del Proyecto (3 meses)	Uno de los trabajadores asumira el rol de líder del proyecto de implementación. Tendra conocimientos en ciberseguridad y comprensión de la norma ISO 27001 y del modelo Zero Trust
Responsable de Políticas de Seguridad (3 meses)	Esta función estara compartida con el líder del proyecto
Técnico o Especialista en TI (3 meses)	Especialista en TI con experiencia práctica en la implementación de controles técnicos, como configuraciones de ciberseguridad en la nube sistemas de detección de intrusiones, y otros elementos relacionados con la ciberseguridad
Personal de Soporte y capacitacion (3 meses)	Todos los trabajadores y clientes deben estar informados y formados en las nuevas políticas y herramientas de seguridad en los entornos cloud

Nota. Elaboración propia.

b) **Herramientas tecnológicas.** Las herramientas que se utilizaran son la norma ISO 27001 y la metodología Zero Trust que permitirán realizar el marco de trabajo de estrategias de ciberseguridad para mejorar la robustez de los entornos cloud.

Tabla 6

Norma ISO 27001

ESTRUCTURA DEL ANEXO A
5. Políticas de seguridad de la información
5.1 Directrices de gestión de la seguridad de la información
5.1.1 Políticas para la seguridad de la información
5.1.2 Revisión de las políticas para la seguridad de la información
6. Organización de la seguridad de la información
6.1 Organización interna
6.1.1 Roles y responsabilidades en seguridad de la información
6.1.2 Segregación de tareas
6.1.3 Contacto con las autoridades
6.1.4 Contacto con grupos de interés especial
6.1.5 Seguridad de la información en la gestión de proyectos
6.2 Los dispositivos móviles y el teletrabajo
6.2.1 Política de dispositivos móviles
6.2.2 Teletrabajo
7. Seguridad relativa a los recursos humanos
7.1 Antes del empleo
7.1.1 Investigación de antecedentes
7.1.2 Términos y condiciones del empleo
7.2 Durante el empleo
7.2.1 Responsabilidades de gestión
7.2.2 Concienciación, educación y capacitación en seguridad de la información
7.2.3 Proceso disciplinario
7.3 Finalización del empleo o cambio en el puesto de trabajo
7.3.1 Responsabilidades ante la finalización o cambio
8. Gestión de activos
8.1 Responsabilidad sobre los activos
8.1.1 Inventario de activos
8.1.2 Propiedad de los activos
8.1.3 Uso aceptable de los activos
8.1.4 Devolución de activos
8.2 Clasificación de la información
8.2.1 Clasificación de la información
8.2.2 Etiquetado de la información
8.2.3 Manipulado de la información
8.3 Manipulación de los soportes
8.3.1 Gestión de soportes extraíbles
8.3.2 Eliminación de soportes
8.3.3 Soportes físicos en tránsito
9. Control de acceso
9.1 Requisitos de negocio para el control de acceso
9.1.1 Política de control de acceso
9.1.2 Acceso a las redes y a los servicios de red
9.2 Gestión de acceso de usuario
9.2.1 Registro y baja de usuario
9.2.2 Provisión de acceso de usuario
9.2.3 Gestión de privilegios de acceso
9.2.4 Gestión de la información secreta de autenticación de los usuarios

9.2.5 Revisión de los derechos de acceso de usuario
9.2.6 Retirada o reasignación de los derechos de acceso
9.3 Responsabilidades del usuario
9.3.1 Uso de la información secreta de autenticación
9.4 Control de acceso a sistemas y aplicaciones
9.4.1 Restricción del acceso a la información
9.4.2 Procedimientos seguros de inicio de sesión
9.4.3 Sistema de gestión de contraseñas
9.4.4 Uso de utilidades con privilegios del sistema
9.4.5 Control de acceso al código fuente de los programas

10. Criptografía

10.1 Controles criptográficos
10.1.1 Política de uso de los controles criptográficos
10.1.2 Gestión de claves

11. Seguridad física y del entorno

11.1 Áreas seguras
11.1.1 Perímetro de seguridad física
11.1.2 Controles físicos de entrada
11.1.3 Seguridad de oficinas, despachos y recursos
11.1.4 Protección contra las amenazas externas y ambientales
11.1.5 El trabajo en áreas seguras
11.1.6 Áreas de carga y descarga
11.2 Seguridad de los equipos
11.2.1 Emplazamiento y protección de equipos
11.2.2 Instalaciones de suministro
11.2.3 Seguridad del cableado
11.2.4 Mantenimiento de los equipos
11.2.5 Retirada de materiales propiedad de la empresa
11.2.6 Seguridad de los equipos fuera de las instalaciones
11.2.7 Reutilización o eliminación segura de equipos
11.2.8 Equipo de usuario desatendido
11.2.9 Política de puesto de trabajo despejado y pantalla limpia

12. Seguridad de las operaciones

12.1 Procedimientos y responsabilidades operacionales
12.1.1 Documentación de procedimientos operacionales
12.1.2 Gestión de cambios
12.1.3 Gestión de capacidades
12.1.4 Separación de los recursos de desarrollo, prueba y operación
12.2 Protección contra el software malicioso (malware)
12.2.1 Controles contra el código malicioso
12.3 Copias de seguridad
12.3.1 Copias de seguridad de la información
12.4 Registros y supervisión
12.4.1 Registro de eventos
12.4.2 Protección de la información del registro
12.4.3 Registros de administración y operación
12.4.4 Sincronización del reloj
12.5 Control del software en explotación
12.5.1 Instalación del software en explotación
12.6 Gestión de la vulnerabilidad técnica

12.6.1 Gestión de las vulnerabilidades técnicas
12.6.2 Restricción en la instalación de software
12.7 Consideraciones sobre la auditoria de sistemas de información
12.7.1 Controles de auditoria de sistemas de información

13. Seguridad de las comunicaciones

13.1 Gestión de la seguridad de las redes
13.1.1 Controles de red
13.1.2 Seguridad de los servicios de red
13.1.3 Segregación en redes
13.2 Intercambio de información
13.2.1 Políticas y procedimientos de intercambio de información
13.2.2 Acuerdos de intercambio de información
13.2.3 Mensajería electrónica
13.2.4 Acuerdos de confidencialidad o no revelación

14. Adquisición, desarrollo y mantenimiento de los sistemas de información

14.1 Requisitos de seguridad en los sistemas de información
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información
14.1.2 Asegurar los servicios de aplicaciones en redes públicas
14.1.3 Protección de las transacciones de servicios de aplicaciones
14.2 Seguridad en el desarrollo y en los procesos de soporte
14.2.1 Política de desarrollo seguro
14.2.2 Procedimiento de control de cambios en sistemas
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
14.2.4 Restricciones a los cambios en los paquetes de software
14.2.5 Principios de ingeniería de sistemas seguros
14.2.6 Entorno de desarrollo seguro
14.2.7 Externalización del desarrollo de software
14.2.8 Pruebas funcionales de seguridad de sistemas
14.2.9 Pruebas de aceptación de sistemas
14.3 Datos de prueba
14.3.1 Protección de los datos de prueba

15. Relación con proveedores

15.1 Seguridad en las relaciones con proveedores
15.1.1 Política de seguridad de la información en las relaciones con los proveedores
15.1.2 Requisitos de seguridad en contratos con terceros
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones
15.2 Gestión de la provisión de servicios del proveedor
15.2.1 Control y revisión de la provisión de servicios del proveedor
15.2.2 Gestión de cambios en la provisión del servicio del proveedor

16. Gestión de incidentes de seguridad de la información

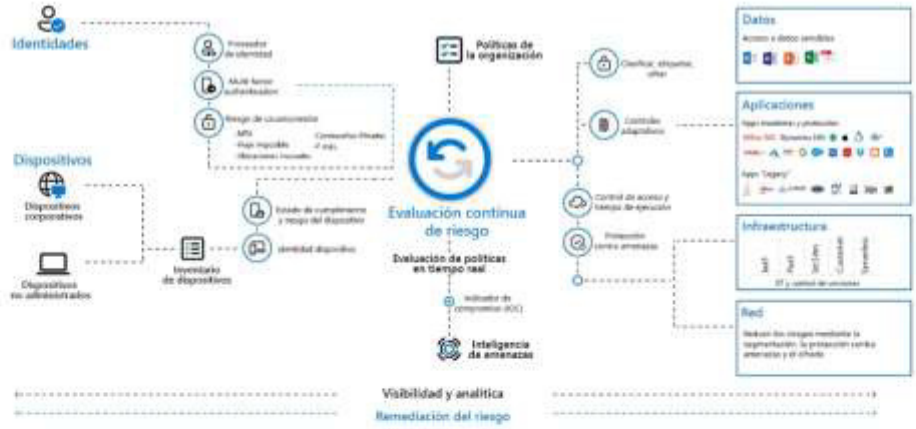
16.1 Gestión de incidentes de seguridad de la información y mejoras
16.1.1 Responsabilidades y procedimientos
16.1.2 Notificación de los eventos de seguridad de la información
16.1.3 Notificación de puntos débiles de la seguridad
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
16.1.5 Respuesta a incidentes de seguridad de la información
16.1.6 Aprendizaje de los incidentes de seguridad de la información
16.1.7 Recopilación de evidencias

17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio
17.1 Continuidad de la seguridad de la información
17.1.1 Planificación de la continuidad de la seguridad de la información
17.1.2 Implementar la continuidad de la seguridad de la información
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
17.2 Redundancias.
17.2.1 Disponibilidad de los recursos de tratamiento de la información
18. Cumplimiento
18.1 Cumplimiento de los requisitos legales y contractuales
18.1.1 identificación de la legislación aplicable y de los requisitos contractuales
18.1.2 Derechos de Propiedad Intelectual (DPI)
18.1.3 Protección de los registros de la organización
18.1.4 Protección y privacidad de la información de carácter personal
18.1.5 Regulación de los controles criptográficos
18.2 Revisiones de la seguridad de la información
18.2.1 Revisión independiente de la seguridad de la información
18.2.2 Cumplimiento de las políticas y normas de seguridad
18.2.3 Comprobación del cumplimiento técnico

Nota. Elaborado en base a la norma ISO 27001

Figura 4

Metodología de Zero Trust



Nota. Zero Trust es un enfoque de seguridad informática que asume que no se debe confiar en ningún actor dentro o fuera de la red sin verificación. Este enfoque es compatible con varias normas y controles de la ISO 27001, que es un estándar internacional para la gestión de la seguridad de la información. Algunos de los controles de la ISO 27001 que el enfoque Zero Trust

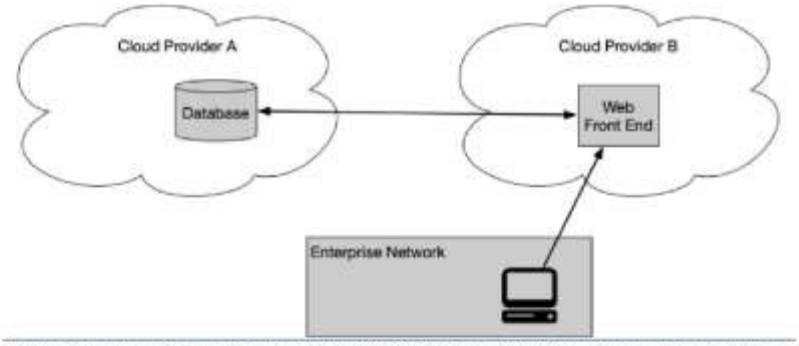
utilizaremos en el estudio de investigación. Fuente: CISET, rescatado de: ¿Por qué tu empresa debería adoptar una estrategia de seguridad Zero Trust? con las soluciones de Microsoft – Softeng.

5. Empresa multinube/nube a nube

En este caso de uso, la empresa tiene una red local, pero utiliza dos o más proveedores de servicios en la nube para alojar aplicaciones/servicios y datos. A veces, la aplicación/servicio está alojado en un servicio en la nube que está separado de la fuente de datos. Para lograr rendimiento y facilidad de administración, la aplicación alojada en el Proveedor de la nube A debería poder conectarse directamente a la fuente de datos alojada en el Proveedor de la nube B en lugar de forzar a la aplicación a volver a través de un túnel a través de la red empresarial.

Figura 5

Múltiples nubes



Nota. Fuente: publicación especial del NIST 800-207 Caso de uso de múltiples nubes

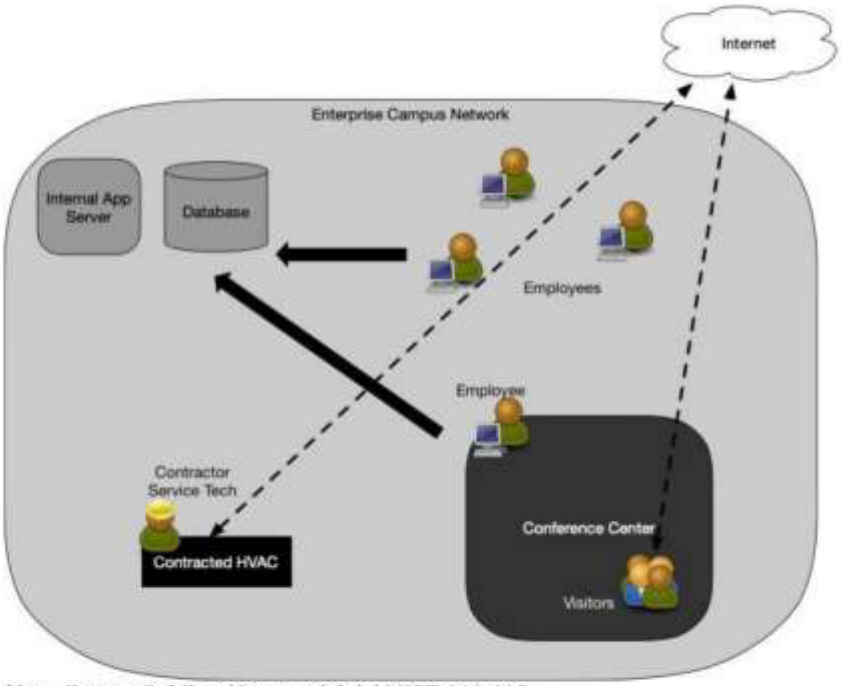
6. Servicios Contratados y/o Acceso para No Empleados

Es una empresa que incluye visitantes en el sitio y/o proveedores de servicios contratados que requieren acceso limitado a los recursos de la empresa para realizar su trabajo empresa tiene sus propias aplicaciones/servicios, bases de datos y activos internos. Estos incluyen servicios contratados a proveedores que ocasionalmente pueden estar en el sitio para brindar mantenimiento

(por ejemplo, sistemas inteligentes de calefacción e iluminación que son propiedad de proveedores externos y están administrados por ellos). Estos visitantes y proveedores de servicios necesitarán conectividad de red para realizar sus tareas. Una empresa de confianza cero podria facilitar esto al permitir que estos dispositivos y cualquier técnico de servicio visitante acceda a Internet mientras oculta los recursos de la empresa.

Figura 6

Acceso para no empleados



Nota. Fuente: Publicación especial del NIST 800-207

7. Análisis situacional en base al Anexo A ISO 27001 y la metodología Zero Trust

Se procede analizar en base análisis situacional con la ISO 27001 según los controles definidos que han sido empleados para el estudio de investigación en la empresa seleccionada y el

Anexo A ISO 27001	Zero Trust
Cuenta: SI /NO	Cuenta: SI /NO

instrumento de estudio, posteriormente analizaremos la metodología Zero Trust conjuntamente con la ISO 27001 que permitirá verificar la vulnerabilidad que se tiene y el impacto que se tiene:

✓ Punto N°01: Identificación inicial de los controles ISO 27001 y la metodología de Zero Trust.

En este paso se identifica los controles de la ISO 27001 que permitirán verificar si la empresa tiene actualmente empleando algunos de los puntos en base al instrumento de investigación realizado aplicado a los recursos del estudio de investigación que son los entornos cloud (las páginas web y las máquinas virtuales), donde estará detallado de la siguiente manera:

Tabla 7

Anexo A9 Controles de acceso de la ISO 27001 y Zero Trust

A.9 Control de acceso	Instrumento	Recursos PG	Recursos MV	Norma Anexo A ISO 27001	Zero Trust
9.1.1	¿Existen procedimientos de autenticación multifactor para el acceso a los recursos críticos?	Páginas web	Máquinas virtuales	NO	NO
9.1.1	Se revisan y actualizan periódicamente los derechos de acceso	Páginas web	Máquinas virtuales	NO	NO
9.2	¿Se registra y monitorea el acceso de usuarios a entornos cloud?	Páginas web	Máquinas virtuales	NO	NO
9.2.1	¿Se utiliza control de acceso basado en roles para limitar el acceso a recursos según la necesidad del usuario?	Páginas web	Máquinas virtuales	NO	NO
9.2.4	¿ Se tiene monitoreo y alertas de seguridad de accesos ?	Páginas web	Máquinas virtuales	NO	NO

Nota. El análisis situacional basado en control de acceso en el Anexo A9 Control de acceso de la ISO 27001 y la metodología Zero Trust indica que, en el caso de ITIPERU, no se han implementado controles de seguridad necesarios para la gestión adecuada del acceso a recursos críticos, tanto en páginas web como en máquinas virtuales. Esta falta de implementación se detalla en varios controles.

Tabla 8

Anexo A10 Criptografía de la ISO 27001 y Zero Trust

A.10 Criptografía	Instrumento	Recursos	Recursos	Norma Anexo A ISO 27001	Zero Trust
10.1.1	Se utiliza cifrado para proteger los datos sensibles de los entornos cloud	Páginas web	Máquinas virtuales	NO	NO
10.1.2	¿Se cuenta con política de controles criptográficos?	Páginas web	Máquinas virtuales	NO	NO
10.1.2	¿Se emplean protocolos seguros (como TLS)?	Páginas web	Máquinas virtuales	NO	NO
10.1.2	¿se cuenta con un plan de acción en caso de fallo o compromiso en los sistemas de cifrado	Páginas web	Máquinas virtuales	NO	NO
10.1.2	¿Se han implementado políticas para el manejo seguro de los certificados digitales?	Páginas web	Máquinas virtuales	NO	NO

Nota. Respecto a los controles de criptografía del Anexo A 10 de la ISO 27001 y bajo la metodología de Zero Trust revela una ausencia total de medidas de cifrado esenciales para la protección de datos. La no implementación de cifrado en entornos cloud, la falta de políticas de controles criptográficos, la ausencia del uso de protocolos seguros como TLS, la inexistencia de un plan de acción ante fallas de cifrado y la omisión en el manejo seguro de certificados digitales,

ponen en evidencia una considerable vulnerabilidad en la seguridad de la información de la empresa, tanto en sus páginas web como en sus máquinas virtuales.

Tabla 9

Anexo A12 Seguridad de las operaciones

A.12 Seguridad de las Operaciones	Instrumento	Recursos	Recursos	Norma Anexo A ISO 27001	Zero Trust
12.1.1	En caso de un incidente de seguridad, ¿cuál sería el impacto en la continuidad del negocio?	Páginas web	Máquinas virtuales	NO	NO
12.1.2	¿Cuál sería el impacto de una brecha de seguridad en la reputación de la empresa?	Páginas web	Máquinas virtuales	NO	NO
12.6	¿Qué impacto tendría un ataque de seguridad en la integridad de los datos críticos?	Páginas web	Máquinas virtuales	NO	NO
12.6	¿Cuál sería el impacto financiero de un incidente de seguridad?	Páginas web	Máquinas virtuales	NO	NO
12.6	¿Cuál sería el impacto por fallas en el alojamiento web ?	Páginas web	Máquinas virtuales	NO	NO
12.6	¿Con qué frecuencia se han detectado vulnerabilidades de seguridad en las páginas web y máquinas virtuales?	Páginas web	Máquinas virtuales	NO	NO
12.4	¿Cuál es la frecuencia de ataques de seguridad experimentados en el pasado?	Páginas web	Máquinas virtuales	NO	NO
12.4	¿Qué tan probable es el aprovechamiento de las vulnerabilidades conocidas por los atacantes?	Páginas web	Máquinas virtuales	NO	NO
12.4	¿Cuál es la probabilidad de que fallas humanas provoquen incidentes de seguridad?	Páginas web	Máquinas virtuales	NO	NO
12.4	¿Cuál es la probabilidad de ataques a los servidores de alojamiento web ?	Páginas web	Máquinas virtuales	NO	NO

Nota. El análisis detalla que ITIPERU no ha establecido medidas de protección operativa en línea con la sección A.12 de la ISO 27001, que es crucial para la prevención y respuesta efectiva ante incidentes de seguridad. La falta de preparación para incidentes de seguridad sugiere que cualquier evento adverso podría tener consecuencias significativas en la continuidad del negocio, la integridad de los datos críticos, la reputación empresarial y la estabilidad financiera Además, la

ausencia de un análisis frecuente de vulnerabilidades y la gestión de amenazas pasadas indica un enfoque reactivo en lugar de proactivo, en contraposición a la filosofía de Zero Trust que demanda una vigilancia y mitigación constantes de riesgos.

Tabla 10

Anexo A13 Seguridad de las comunicaciones

A.13 Seguridad de las comunicaciones	Instrumento	Recursos	Recursos	Norma Anexo A ISO 27001	Zero Trust
13.1	¿Se realizan identifican mecanismos de seguridad en los servicios alojados (páginas web, máquinas virtuales)	Páginas web	Máquinas virtuales	NO	NO
13.2	¿Se cuenta con políticas de seguridad para el uso del correo electrónico y otros medios de comunicación electrónica?	Páginas web	Máquinas virtuales	NO	NO
13.2.1	¿Existen procedimientos para responder a incidentes de seguridad que afecten a las comunicaciones de la empresa?	Páginas web	Máquinas virtuales	NO	NO
13.1.2	¿ Se realiza configuraciones de red adecuadas en las máquinas virtuales ?	Páginas web	Máquinas virtuales	NO	NO
13.2.4	¿ Existe acuerdos de confidencialidad de divulgación de información entre los clientes y la empresa ?	Páginas web	Máquinas virtuales	NO	NO

Nota. Indica que la empresa no ha implementado medidas fundamentales para asegurar las comunicaciones. La ausencia de mecanismos de seguridad en los servicios alojados (páginas web y máquinas virtuales), la falta de políticas de seguridad para el uso del correo electrónico y otros medios de comunicación electrónica, y la inexistencia de procedimientos para responder a incidentes de seguridad en las comunicaciones, señalan un alto riesgo de exposición de información y posibles brechas de seguridad.

Tabla 11

Anexo A15 Relación con proveedores

A.15 Relación con proveedores	Instrumento	Recursos	Recursos	Norma ISO 27001	Zero Trust
15.1	Mantenimiento programado	Páginas web	Máquinas virtuales	NO	NO
15.2	Error la maquinas virtual de base datos		Máquinas virtuales	NO	NO
15.2	Actualización de seguridad	Hosting	Máquinas virtuales	NO	NO
15.2	Interrupción del ISP	Hosting	Máquinas virtuales	NO	NO
15.2	Actualización del sistema de hosting	Hosting	Máquinas virtuales	NO	NO
15.2	Error de configuración máquinas virtuales	Hosting	Máquinas virtuales	NO	NO
15.2	Fallo de aplicación web en WordPress	Hosting		NO	NO
15.2	Error en la actualización de WordPress	Hosting		NO	NO
15.2	Problemas de seguridad en WordPress	Hosting		NO	NO
15.2	Fallo de hardware en Azure		Máquinas virtuales	NO	NO

Nota. Resalta una serie de deficiencias críticas en la gestión de la infraestructura cloud y en la preparación frente a posibles incidentes que podrían afectar la continuidad del servicio. La falta de mantenimiento programado y la ausencia de respuesta a errores tanto en máquinas virtuales como en aplicaciones web, como WordPress, ponen de manifiesto la vulnerabilidad de la organización ante interrupciones del servicio y fallos de seguridad.

Tabla 12

Anexo A16 Tiempo de recuperación de integridad

A.16 Tiempo de recuperación de integridad	Instrumento	Recursos	Recursos	Norma Anexo A ISO 27001	Zero Trust
16.1	Caída de la base de datos de WordPress	Páginas web		NO	NO
16.1	Pérdida de conectividad con Azure		Máquinas virtuales Azure	NO	NO
16.1	Problemas de autenticación en Azure		Máquinas virtuales Azure	NO	NO
16.1	Incompatibilidad de plugin en WordPress	Páginas web		NO	NO
16.1	Problemas de DNS en hosting	Páginas web		NO	NO
16.1	Error de certificado SSL en web	Páginas web		NO	NO
16.1	Fallo de sistema operativo en Azure		Máquinas virtuales Azure	NO	NO
16.1	Ataque de inyección SQL en WordPress	Páginas web		NO	NO
16.1	Saturación de recursos en máquina virtual	Páginas web		NO	NO
16.1	Carga excesiva en servidor web	Páginas web		NO	NO
16.1	Actualización problemática en WordPress	Páginas web		NO	NO

Nota. Muestra una inadecuada gestión de incidentes de seguridad de la información. La organización carece de un plan efectivo de respuesta ante una serie de incidentes potenciales que van desde caídas de bases de datos de WordPress hasta ataques de inyección SQL, pasando por problemas de autenticación en Azure, fallos de DNS y sobrecargas de recursos en máquinas virtuales.

Tabla 13

Anexo A16 Gestión de incidencias de seguridad de la información

A.16 Gestión de incidencias de seguridad de la información	Instrumento	Recursos	Recursos	Norma Anexo A ISO 27001	Zero Trust
16.1.6	Resolución de vulnerabilidades reportadas en WordPress.	Páginas web		NO	NO
16.1.6	Problemas de inyección SQL en sitios WordPress resueltos.	Páginas web		NO	NO
16.1.6	Acceso no autorizado a una VM resuelto con cambio de credenciales.		Máquinas virtuales Azure	NO	NO
16.1.6	Retrasos en la respuesta a incidentes de phishing.	Páginas web	Máquinas virtuales Azure	NO	NO
16.1.6	Rápida mitigación de un ataque de fuerza bruta.	Páginas web	Máquinas virtuales Azure	NO	NO
16.1.6	Revisión de políticas de seguridad tras varios incidentes menores.	Páginas web	Máquinas virtuales Azure	NO	NO
16.1.6	Configuraciones de seguridad mejoradas tras revisión interna.	Páginas web	Máquinas virtuales Azure	NO	NO
16.1.6	Falsas alarmas de malware debido a una actualización de sistema	Páginas web	Máquinas virtuales Azure	NO	NO
16.1.6	Alertas de seguridad en el portal de Azure atendidas prontamente.		Máquinas virtuales Azure	NO	NO
16.1.6	Respuesta rápida a varios intentos de acceso no autorizado a las máquinas virtuales		Máquinas virtuales Azure	NO	NO

Nota. La evaluación de ITIPERU respecto al manejo de incidentes de seguridad de la información según el control A.16 del Anexo A de la ISO 27001, y siguiendo los principios de Zero Trust, indica una ausencia de medidas proactivas y reactivas ante posibles incidentes de seguridad. La falta de resolución de vulnerabilidades conocidas en WordPress, la no atención a problemas de

inyección SQL, la gestión inadecuada de accesos no autorizados a máquinas virtuales y los retrasos en responder a incidentes de phishing son claros indicativos de que no existen protocolos establecidos o efectivos de respuesta ante incidentes.

- ✓ Punto N°02: Realizado el análisis situacional se ha podido identificar en base al resumen general que hay la necesidad de emplear la norma ISO 27001 con los controles ya identificados y la metodología de Zero Trust. A continuación, se detallará el análisis y la solución que se propone:

Tabla 14

Control de Acceso

	Instrumento	Controles ISO 27001	Aplicación de Zero Trust	Recursos PG (Páginas web)	Recursos MV (Máquinas Virtuales Azure)
Control de accesos	¿Existen procedimientos de autenticación multifactor para el acceso a los recursos críticos?	9.1.1 Autenticación multifactor	Implementar MFA para todos los usuarios sin excepción. Considerar el uso de aplicaciones de autenticación, llaves de seguridad físicas, y/o notificaciones push para dispositivos móviles.	Se realizó la Configuracion del MFA mediante plugins que permite la identificacion de dos factores de autentificacion permitiendo tener un mejor control a nivel de administracion de la paginas que tiene tanto de la empresa como sus clientes	Se realizó la Configurarcion del MFA para todos los accesos de administración y usuarios con acceso a datos sensibles en la administracion microsoft azure, office 365 de sus clientes actuales
	Se revisan y actualizan periódicamente los derechos de acceso	9.1.1 Revisión y actualización de derechos de acceso	Establecer politicas que requieran la revisión automática y continua de los derechos de acceso, ajustándolos según el contexto y la evaluación de riesgos en tiempo real.	Se utilizó herramientas de gestión de CMS (contenet Management system) para revisar los roles de usuarios y su adecuación a sus tareas	Se aplicó herramientas de gestión de identidades control de accesos en Azure para revisar y restringir permisos según necesidades
	¿Se registra y monitorea el acceso de usuarios a entornos cloud?	9.2 Registro y monitoreo de accesos	Configurar soluciones de SIEM que proporcionen monitoreo en tiempo real y alertas para detectar y responder a actividades sospechosas.	Se implementó plugis de seguridad que permitan monitoriar el tráfico y la actividad de usuario.	Se utilizó Azure Security Center para monitorizar y registrar la actividad de acceso en las VM.

	¿Se utiliza control de acceso basado en roles para limitar el acceso a recursos según la necesidad del usuario?	9.2 Control de acceso basado en roles	Definir y aplicar políticas de acceso que limiten los permisos al mínimo necesario basado en el rol y las funciones del usuario.	Se aplicó y configuro controles de acceso detallados para usuarios del sitio web basados en su rol y responsabilidades.	Se estableció grupos de seguridad y roles de Azure que definan claramente los niveles de acceso.
	¿Se tiene monitoreo y alertas de seguridad de accesos ?	9.2 Monitoreo y alertas de seguridad de accesos	Desarrollar un sistema integral de alertas que notifique a los administradores sobre posibles brechas o intentos de acceso no autorizados.	Se Configuro soluciones de monitoreo de seguridad para alertar sobre intentos de inicio de sesión fallidos o comportamientos anómalos.	Se configuró alertas de seguridad en Azure que notifiquen a los administradores en tiempo real sobre eventos de seguridad

Tabla 15

Criptografía

	Instrumento	Control ISO 27001	Aplicación de Zero Trust	Recursos PG (Páginas web)	Recursos MV (Máquinas Virtuales Azure)
Criptografía	Se utiliza cifrado para proteger los datos sensibles de los entornos cloud	10.1 Cifrado de datos	Implementar cifrado de datos en reposo y en tránsito para asegurar la confidencialidad e integridad.	Se activó el protocolo HTTPS en todas las páginas web y asegurar el cifrado en las bases de datos y almacenamiento.	Se Configuro cifrado de disco en Azure y habilitar el cifrado de red para todas las comunicaciones.
	¿Se cuenta con politica de controles criptograficos?	10.1.1 Politicas de control criptográfico	Establecer políticas que dicten cómo y cuándo se debe utilizar la criptografía y la gestión de claves.	Se desarrolló una política criptográfica para los sitios web y la gestión de claves.	Se habilito el Azure Key Vault para la gestión centralizada de claves y políticas de cifrado.
	¿Se emplean protocolos seguros (como TLS)?	10.1.2 Uso de protocolos seguros	Emplear siempre protocolos de comunicación seguros y actualizados como TLS para todas las conexiones.	Se habilito las conexiones con el protocolo HTTPS con TLS 1.3 en la configuración del servidor web para mejorar la seguridad y rendimiento	Se configuró que todas las VMs se comuniquen utilizando TLS 1.3 o protocolos seguros.
	¿se cuenta con un plan de acción en caso de fallo o compromiso en los sistemas de cifrado	10.1.2 Plan de acción para fallos de cifrado	Tener un plan de respuesta ante compromisos de sistemas de cifrado.	Se estableció procedimientos de respuesta rápida ante fallos de cifrado y compromisos de claves.	Se implementó alertas de Azure Security Center para identificar fallos de cifrado y responder rápidamente.
	¿Se han implementado politicas para el manejo seguro de los certificados digitales?	10.1 Manejo de certificados digitales	Gestionar los certificados digitales de manera segura y efectiva.	Se implementó y configuro un sistema de gestión de certificados para renovación automática y revocación eficiente.	Se configuró Azure Key Vault para la automatización del ciclo de vida de los certificados SSL/TLS.

Tabla 16

Seguridad de las operaciones

	Instrumento	ISO 27001	Aplicación de Zero Trust	Recursos PG (Páginas web)	Recursos MV (Máquinas Virtuales Azure)
Seguridad de las Operaciones	En caso de un incidente de seguridad, ¿cuál sería el impacto en la continuidad del negocio?	12.1 Impacto en la continuidad del negocio	Implementar una arquitectura redundante y sistemas de failover.	Se ha realizo la configuración e implementación de una solución de autoescalado para garantizar la alta disponibilidad del sitio web.	Se realizó la Configuarcion de Azure Site Recovery y Backup.
	¿Cuál sería el impacto de una brecha de seguridad en la reputación de la empresa?	12.1.2 Impacto de brechas en la reputación	Desarrollar un plan de comunicación de incidentes para mitigar daños a la reputación.	Se llevaron a cabo acciones para fortalecer la gestión de comunicaciones durante situaciones de emergencia mediante la implementación de plantillas de comunicación de crisis en la plataforma WordPress	Se procedió con la organización de un equipo especializado en la respuesta a incidentes de seguridad en el entorno de Microsoft Azure en la empresa
	¿Qué impacto tendría un ataque de seguridad en la integridad de los datos críticos?	12.6 Impacto en la integridad de datos	Utilizar herramientas de monitoreo de integridad de datos y backups automatizados.	Se implementó Implemento el servicio de de backup	Se habilito la herramienta de Azure Backup y Azure Security Center.
	¿Cuál sería el impacto financiero de un incidente de seguridad?	12.6 Impacto financiero de incidentes	Asegurar la infraestructura contra ciberataques y considerar	se realizó la instalacion de plugin para verificar las vulnerabiliades ante un ciberriesgo	Se habilitó el informe de azure site recovery deployment Planner

			seguros de ciberriesgo.		
	¿ cuál sería el impacto por fallas en el alojamiento web ?	12.6 Impacto por fallas de alojamiento web	Emplear CDNs y balanceadores de carga para garantizar la disponibilidad.	Se realizó la configuracion de plugis WP rocket para mejorar y optimizar el caché de navegacion	Se realizó la implementación de balanceador de carga en Azure loader balancer
	¿Con qué frecuencia se han detectado vulnerabilidades de seguridad en las páginas web y máquinas virtuales?	12.6 Frecuencia de vulnerabilidades detectadas	Realizar pruebas de penetración y auditorías de seguridad periódicas.	Se realizó escaneo de seguridad y se programó escaneos de seguridad posteriores para realizar auditorias	Se realizó la habilitación del Azure Security Center para monitoreo continuo.
	¿Cuál es la frecuencia de ataques de seguridad experimentados en el pasado?	12.4 Frecuencia de ataques pasados	Reforzar la defensa contra métodos de ataque conocidos.	Se realizó la verificación e implementación de medidas de seguridad de los sitios web con firewall de aplicación web	Se realizó la aplicación de filtrado basado en inteligencia sobre amenazas mediante directivas de firewall
	¿Qué tan probable es el aprovechamiento de las vulnerabilidades conocidas por los atacantes?	12.4 Probabilidad de explotación de vulnerabilidades	Mantener los sistemas actualizados y parcheados.	se verifico que las páginas web estenAutomatizadas con las actualizaciones de CMS y plugins originales para evitar vulnerabilidades	se realizó la configuración de actualizaciones automáticas en Azure como medidas preventivas ante alguna vulnerabilidad presentada

	¿Cuál es la probabilidad de que fallas humanas provoquen incidentes de seguridad?	12.4 Probabilidad de incidentes por fallas humanas	Fortalecer la formación en seguridad y realizar pruebas de concienciación.	Ante incidentes por fallas se procedió a realizar charlas al personal de la empresa y los clientes como medidas de concientización	Se implementó políticas de acceso condicional y auditorías regulares que con el propósito de fortalecer incidentes por fallas humanas .
	¿Cuál es la probabilidad de ataques a los servidores de alojamiento web ?	12.4 Probabilidad de ataques a servidores de alojamiento web	Mejorar las medidas de seguridad perimetral y la segmentación de red.	Se realizó la configuración de firewalls y sistemas de detección de intrusos mediante la detención y prevención de intrusos (IDS/IPS)	Se configuro el Azure Firewall y NSGs (Network Security Groups) para protección y segmentación.

Tabla 17

Seguridad de las comunicaciones

	Instrumento	ISO 27001	Aplicación de Zero Trust	Recursos PG (Páginas web)	Recursos MV (Máquinas Virtuales Azure)
Seguridad de las Comunicaciones	¿Se realizan identifican mecanismos de seguridad en los servicios alojados (páginas web, máquinas virtuales)	13.1 Seguridad en servicios alojados	Asegurar que todos los servicios web y MV implementen medidas de seguridad actualizadas.	Se implementó WAF, SSL/TLS, y escaneo de vulnerabilidades para las páginas web	Se realizó la Configuracion de firewalls de Azure y asegurar que todas las MV usen NSGs apropiados.
	¿Se cuenta con políticas de seguridad para el uso del correo electrónico y otros medios de comunicación electrónica?	13.2 Políticas de seguridad para comunicación electrónica	Establecer políticas de uso seguro para el correo electrónico y otros medios electrónicos.	Se implementó filtros de spam, DMARC, SPF, y DKIM para el correo electrónico.	se realizó la configuración de seguridad en los servicios de correo electrónico de Azure empleando políticas de filtros de correos spam
	¿Existen procedimientos para responder a incidentes de seguridad que afecten a las	13.2.1 Procedimientos para incidentes en comunicaciones	Desarrollar protocolos para responder rápida y eficazmente a incidentes de seguridad.	Se ha diseñado un plan de acción para la gestión de incidentes específicos en la plataforma WordPress	Se habilito Azure Sentinel para la detección de incidentes y orquestar la respuesta.

	comunicaciones de la empresa?				
	¿ Se realiza configuraciones de red adecuadas en las máquinas virtuales ?	13.1.2 Configuración de red en MV y PG	Asegurar que las configuraciones de red en MV Y PG cumplan con las políticas de seguridad.	Se procedió a realizar una revisión y fortalecimiento de las configuraciones de la red en el entorno de WordPress, lo cual incluirá la implementación de medidas de segregación y aislamiento.	Se implementó segmentación de red y microsegmentación en Azure.
	¿ Existe acuerdos de confidencialidad de divulgación de información entre los clientes y la empresa ?	13.2.4 Acuerdos de confidencialidad	Establecer acuerdos de confidencialidad y políticas de manejo de información.	Se llevó a cabo la elaboración y ejecución de acuerdos de confidencialidad (Non-Disclosure Agreements, NDAs) con todas las partes involucradas en el proyecto de WordPress	Se implementara una gestión eficaz de los acuerdos de confidencialidad, junto con la adopción de mecanismos de acceso seguro a los datos, en la infraestructura de Azure.

Tabla 18

Disponibilidad de servicios cloud

	Instrumento	Control ISO 27001	Acción de Implementación Zero Trust	Recursos PG (Páginas web)	Recursos MV (Máquinas Virtuales Azure)
Disponibilidad de servicios Cloud	Mantenimiento programado	15.1 Mantenimiento programado	Establecer procedimientos de mantenimiento que no interrumpan la disponibilidad del servicio.	Se implementó estrategias de despliegue de mantenimiento de cero-downtime.	Se configuro Azure Automation para mantenimientos programados sin afectar la disponibilidad.
	Error de la máquinas virtual de base datos	15.2 Error en la máquina virtual de base de datos	Automatizar la supervisión y failover de bases de datos.	Se configuro el cluster de bases de datos con failover automático.	Se configuro el Azure SQL Database con grupos de failover automático.
	Actualización de seguridad	15.2 Actualización de seguridad	Automatizar las actualizaciones de seguridad para aplicarse en ventanas de mantenimiento planificadas.	Se empleó herramientas de gestión de parches que permitan actualizaciones fuera de horario pico	Se aplicara Azure Update Management para gestionar y automatizar las actualizaciones de seguridad.
	Interrupción del ISP	15.2 Interrupción del ISP	Diversificar conexiones a internet para mitigar el riesgo de interrupción de un solo ISP.	Se empleó otros hosting que tiene la empresa con IPS libre se configuro failover de DNS para tenerlo como un backup en caso de fallas	Se configuro Azure Traffic Manager para una gestión de tráfico inteligente y redundancia.
	Actualización del sistema de hosting	15.2 Actualización del sistema de hosting	Implementar sistemas de gestión que permitan	Se utilizó tecnologías de contenedores como Ansible para	Se implementó Azure Kubernetes Service para

			actualizaciones sin interrupciones.	actualizaciones rápidas y sin estado.	manejar actualizaciones de sistemas
	Error de configuración máquinas virtuales	15.2 Error de configuración en máquinas virtuales	Usar infraestructura como código para una configuración consistente y revertir rápidamente cambios erróneos.	Se implementó plantillas de configuración y versionado del código.	Se habilito Azure Resource Manager templates para gestión de configuración.
	Fallo de aplicación web en WordPress	15.2 Fallo de aplicación web en WordPress	Crear un entorno de staging para pruebas antes de pasar a producción.	Se realizó la implementación de un sistema de staging y testing antes de actualizar la producción en las páginas de wordPress	Se implementó Azure App Service para entornos de pruebas aislados.
	Error en la actualización de WordPress	15.2 Error en actualización de WordPress	Establecer un proceso de rollback inmediato en caso de actualizaciones fallidas.	Se realizó la configuracion de backup y rollback automáticos.	Se cuenta con Azure Backup para restaurar versiones anteriores si es necesario.
	Problemas de seguridad en WordPress	15.2 Problemas de seguridad en WordPress	Aplicar una política de seguridad de aplicaciones estricta y monitoreo constante.	Se usoplugins de seguridad de WordPress y realizar escaneos de seguridad frecuentes en las páginas web	Se configuró Azure Security Center para alertas de seguridad de aplicaciones en las máquinas virtuales.
	Fallo de hardware en Azure	15.2 Fallo de hardware en Azure	Diseñar sistemas para ser tolerantes a fallos y tener redundancia de hardware.	Se empleara SLAs con proveedores de hosting que incluyen hardware redundante.	Se empleara Azure's SLA para máquinas virtuales y aprovechar su infraestructura de redundancia de hardware.

Tabla 19

Tiempo de recuperación de integridad

	Instrumento	ISO 27001	Acción de Implementación Zero Trust	Recursos PG (Páginas web)	Recursos MV (Máquinas Virtuales Azure)
Tiempo de Recuperación de Integridad	Caída de la base de datos de WordPress	16.1 Caída de la base de datos de WordPress	Implementar soluciones de alta disponibilidad y backup para bases de datos.	Se realizó la configuración backups automáticos y sistemas de failover para las bases de datos.	Se configuró el Azure Backup y Geo-Replication para asegurar la disponibilidad de la base de datos.
	Pérdida de conectividad con Azure	16.1 Pérdida de conectividad con Azure	Asegurar redundancia de conexión y monitorización continua.	Se estableció procedimientos de failover y redundancia con otros proveedores de nube.	Se configuró redundancia de red y conexiones seguras para evitar la pérdida de conectividad.
	Problemas de autenticación en Azure	16.1 Problemas de autenticación en Azure	Implementar políticas de autenticación robustas y revisión constante de identidades.	Se estableció la gestión de identidades y acceso seguro para los servicios de la web.	Aplicar Azure Active Directory y políticas de Conditional Access para gestionar la autenticación.
	Incompatibilidad de plugin en WordPress	16.1 Incompatibilidad de plugin en WordPress	Realizar pruebas de compatibilidad y revisiones antes de la implementación de plugins.	Se utilizara un entorno de staging para probar los plugins antes de la actualización en producción.	No aplica en Azure
	Problemas de DNS en hosting	16.1 Problemas de DNS en hosting	Utilizar servicios de DNS gestionados con	Se Configuro DNS con alta disponibilidad y protección contra DDoS	Se implementó Azure DNS para una gestión robusta y segura del DNS. En las máquinas virtuales

			monitorización y alertas.	con acuerdos con el proveedor	que tiene montado sistemas web
	Error de certificado SSL en web	16.1 Error de certificado SSL en web	Automatizar la renovación y gestión de certificados SSL/TLS.	Se Implementó soluciones de gestión de certificados que incluyan auto-renovación.	Se Gestionó certificados SSL/TLS a través de Azure Key Vault y automatizar su renovación.
	Fallo de sistema operativo en Azure	16.1 Fallo de sistema operativo en Azure	Utilizar imágenes de VM actualizadas y aplicar parches de seguridad.	Mantener los sistemas operativos y el stack de servidor actualizados.	Se usara Azure Update Management para gestionar y automatizar las actualizaciones de sistemas operativos.
	Ataque de inyección SQL en WordPress	16.1 Ataque de inyección SQL en WordPress	Aplicar medidas de protección como WAF y monitorizar las consultas a la base de datos.	Se Implementó WAF para realizar escaneos de seguridad en busca de vulnerabilidades de inyección SQL.	Se implementó WAF de Azure Application Gateway y Azure SQL Database para mitigar ataques.
	Saturación de recursos en máquina virtual	16.1 Saturación de recursos en MV	Monitorizar la carga de trabajo y escalar recursos dinámicamente.	Configuro el monitoreo de recursos y auto-escalado para las páginas web	Se implementó Azure Monitor y Azure Autoscale para gestionar la carga y optimizar el rendimiento.
	Carga excesiva en servidor web	16.1 Carga excesiva en servidor web	Implementar balanceo de carga y caching para distribuir la carga.	Se utilizara servicios de CDN y balanceadores de carga para manejar el tráfico web.	Se configuro Azure Load Balancer y Azure CDN para distribuir eficientemente la carga.
	Actualización problemática en WordPress	16.1 Actualización problemática en WordPress	Establecer protocolos para la gestión y despliegue de actualizaciones.	Se empleó pruebas en un entorno de staging y tener un plan de rollback.	Se utilizara Azure DevOps para gestionar despliegues y rollbacks de actualizaciones.

Tabla 20

Gestión de incidentes de seguridad de la información

	Instrumento	Control ISO 27001	Acción de Implementación Zero Trust	Recursos PG (Páginas web)	Recursos MV (Máquinas Virtuales Azure)
Gestión de incidentes de seguridad de la información	Resolución de vulnerabilidades reportadas en WordPress.	16.1.6 Resolución de vulnerabilidades en WordPress	Implementar procesos automáticos de escaneo y parcheo de vulnerabilidades.	Se aplicó e instalo plugins de seguridad que automaticen el escaneo y apliquen parches de seguridad en las páginas web	No aplica en Azure
	Problemas de inyección SQL en sitios WordPress resueltos.	16.1.6 Solución de problemas de inyección SQL en WordPress	Utilizar herramientas de seguridad web como WAF para prevenir y mitigar inyecciones SQL.	Se implementó y configuro WAFs para detectar y bloquear inyecciones SQL.	Permitir que las configuraciones de seguridad de Azure protejan contra inyecciones SQL.
	Acceso no autorizado a una VM resuelto con cambio de credenciales.	16.1.6 Acceso no autorizado a VMs	Utilizar políticas de acceso condicional y revisión de roles y responsabilidades.	Se aplicó procedimientos de autenticación multifactor y revisión periódica de permisos.	Se implementó Azure Active Directory y Azure Policy para manejar el acceso y las credenciales.
	Retrasos en la respuesta a incidentes de phishing.	16.1.6 Retrasos en respuesta a phishing	Establecer un sistema de alerta temprana y entrenamiento en concienciación sobre phishing.	Se instaló plugis sobre reconocimiento y respuesta al phishing.	Utilizará Azure Sentinel para detectar y responder a intentos de phishing.
	Rápida mitigación de un ataque de fuerza bruta.	16.1.6 Mitigación de ataques de fuerza bruta	Implementar limitación de tasa y bloqueo de IPs sospechosas.	Se Configuro medidas de seguridad para prevenir y responder a ataques de fuerza bruta.	Configuro Azure Firewall y otros mecanismos de seguridad para bloquear ataques de fuerza bruta.

	Revisión de políticas de seguridad tras varios incidentes menores.	16.1.6 Revisión de políticas de seguridad	Realizar auditorías de seguridad regulares y actualizar políticas según sea necesario.	Se revisó y actualizo las políticas de seguridad del sitio web post-incidente.	Se usaran herramientas de Azure para realizar auditorías de seguridad y actualizar políticas.
	Configuraciones de seguridad mejoradas tras revisión interna.	16.1.6 Mejora tras revisión interna	Fomentar un proceso de mejora continua basado en análisis de incidentes.	Se reducirá incidentes de seguridad mediante las herramientas de Roketbot y mejorar las configuraciones en consecuencia.	Se realizara revisiones de seguridad periódicas con Azure Security Center y mejorar la postura de seguridad.
	Falsas alarmas de malware debido a una actualización de sistema	16.1.6 Falsas alarmas de malware	Afinar los sistemas de detección de malware para reducir falsos positivos.	Se ajustara la configuración de herramientas de detección de malware y educar a los usuarios.	Se configurará Azure Security Center para mejorar la precisión de la detección de malware.
	Alertas de seguridad en el portal de Azure atendidas prontamente.	16.1.6 Alertas de seguridad en Azure	Asegurar una respuesta rápida a las alertas de seguridad en el portal de Azure.	Se estableció un equipo de respuesta a incidentes con acceso al portal de administración de las páginas web	Se configuro alertas de seguridad en Azure y definir procedimientos de respuesta ágiles.
	Respuesta rápida a varios intentos de acceso no autorizado a las máquinas virtuales	16.1.6 Respuesta a acceso no autorizado a VMs	Implementar monitoreo de acceso y alertas para respuesta inmediata.	Se Monitorea y se revisara registros de acceso para detectar actividad sospechosa.	Se utilizara Azure Security Center para monitorizar las VMs y responder a accesos no autorizados.

- ✓ Realizado el análisis y la implementación de las estrategias de ciberseguridad donde una de las herramientas como la metodología de Zero Trust permitirá la continuidad del negocio que proporciona un enfoque de seguridad de la información que no presupone confianza alguna.

Tabla 20

Continuidad de negocio

Aspecto de Continuidad del Negocio	Aplicación de Zero Trust	Acciones para Páginas web	Acciones para Microsoft Azure
Diseño de Red y Sistemas	Microsegmentación y Acceso por Necesidad	- Implementar firewalls de aplicación web (WAF). - Segmentar la red interna del hosting. - Limitar el acceso administrativo basado en roles.	- Usar Azure Virtual Network para microsegmentar redes. - Aplicar Azure RBAC para controlar el acceso.
Autenticación y Control de Acceso	Autenticación Multifactor y Gestión Dinámica de Identidades	- Configurar MFA para acceso al CMS. - Usar sistemas de gestión de identidades para acceso a la base de datos y el servidor.	- Implementar MFA en Azure Active Directory. - Configurar Azure AD Identity Protection.
Protección y Resiliencia de Datos	Cifrado y Backups Automatizados	- Cifrar bases de datos y backups. - Automatizar el proceso de backup y almacenarlos en ubicaciones seguras.	- Utilizar Azure Backup con cifrado. - Aplicar políticas de Azure Backup para automatizar y replicar backups.
Respuesta Ante Incidentes	Respuesta Automatizada y Estrategia de Contención Proactiva	- Instalar sistemas de detección y respuesta a intrusiones. - Preparar planes de contención y respuesta para aislar rápidamente ataques.	- Configurar Azure Sentinel para detección y respuesta. - Automatizar respuestas a incidentes con Azure Logic Apps.
Recuperación de Servicios	Recuperación Rápida y Estrategias de Failover	- Establecer SLA con proveedores para garantizar tiempos de recuperación rápidos. -	- Utilizar Azure Site Recovery. - Configurar y probar estrategias de failover en Azure.

		Configurar sistemas redundantes para failover.	
Simulacros y Pruebas	Pruebas de Penetración Regular y Ejercicios de Continuidad	- Realizar pruebas de penetración periódicas. - Simular escenarios de recuperación de desastres.	- Programar y ejecutar pruebas de penetración con herramientas de Azure. - Realizar simulacros de continuidad del negocio en Azure.
Evaluación y Mejora Continua	Revisiones Post-Incidente y Ajuste Dinámico de Políticas	- Analizar y aprender de los incidentes de seguridad. - Actualizar protocolos de seguridad y recuperación.	- Utilizar Azure Security Center para evaluaciones continuas. - Refinar políticas de Azure en base a las revisiones.
Documentación y Conciencia	Documentación Accesible y Capacitación Continua	- Mantener documentación actualizada y accesible para el equipo. - Capacitar al personal en procedimientos de seguridad y recuperación.	- Almacenar documentación en Azure y mantener el acceso controlado. - Utilizar recursos de formación de Azure para el personal

8. Cotización del proyecto de implementación de estrategias de ciberseguridad

A continuación, se presentan costos del proyecto:

Tabla 21

Presupuesto

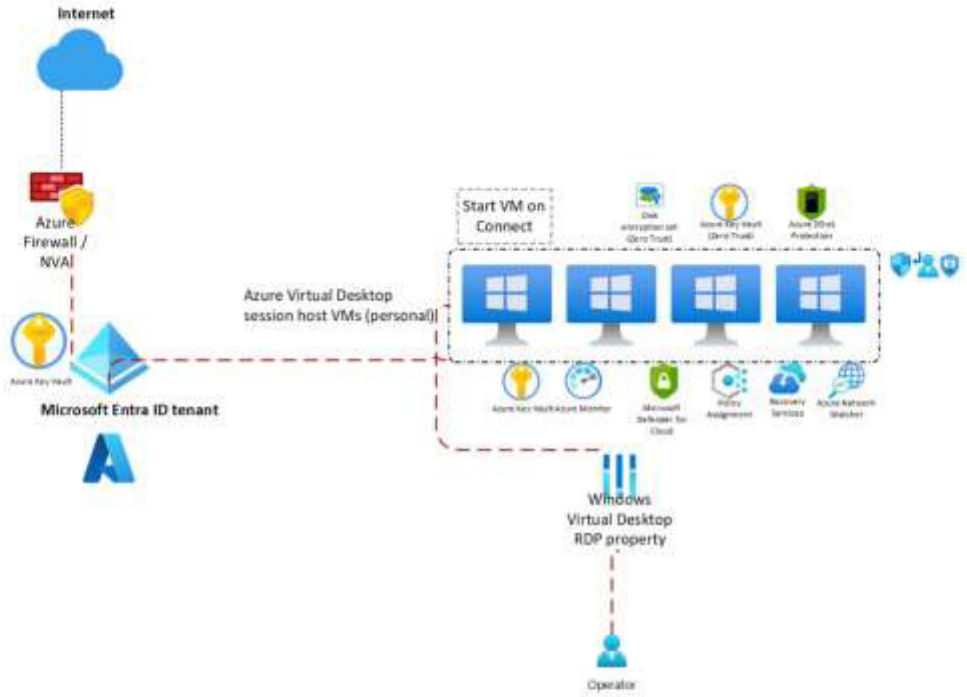
Costos del el proyecto			
Personal	**Funciones**	**Valor Estimado**	
Líder del Proyecto (3 meses)	Uno de los trabajadores asumira el rol de líder del proyecto de implementación. Tendra conocimientos en ciberseguridad y comprensión de la norma ISO 27001 y del modelo Zero Trust	S/	3,600.00
Responsable de Políticas de Seguridad (3 meses)	Esta función estara compartida con el líder del proyecto	S/	-
Técnico o Especialista en TI (3 meses)	Especialista en TI con experiencia práctica en la implementación de controles técnicos, como configuraciones de ciberseguridad en la nube sistemas de detección de intrusiones, y otros elementos relacionados con la ciberseguridad	S/	3,000.00
Personal de Soporte y capacitacion (3 meses)	Todos los trabajadores y clientes deben estar informados y formados en las nuevas políticas y herramientas de seguridad en los entornos cloud	S/	2,800.00
Gastos Administrativos	Estos son costos asociados con la gestión diaria y las operaciones administrativas necesarias para implementar y mantener las políticas y herramientas de seguridad en entornos cloud	S/	4,000.00
Contigencia	Este item se refiere a la asignación presupuestaria destinada a cubrir posibles eventos o circunstancias imprevistas que podrían afectar la implementación de las políticas y herramientas de seguridad.	S/	3,000.00
	Total	S/	16,400.00

9. Modelo de propuesta

Modelo propuesta de estrategias de cibergruidad para la continuidad de negocio operativo en los entornos cloud en la empresa itiperu mediante ISO 27001 y Zero Trust.

Figura 7

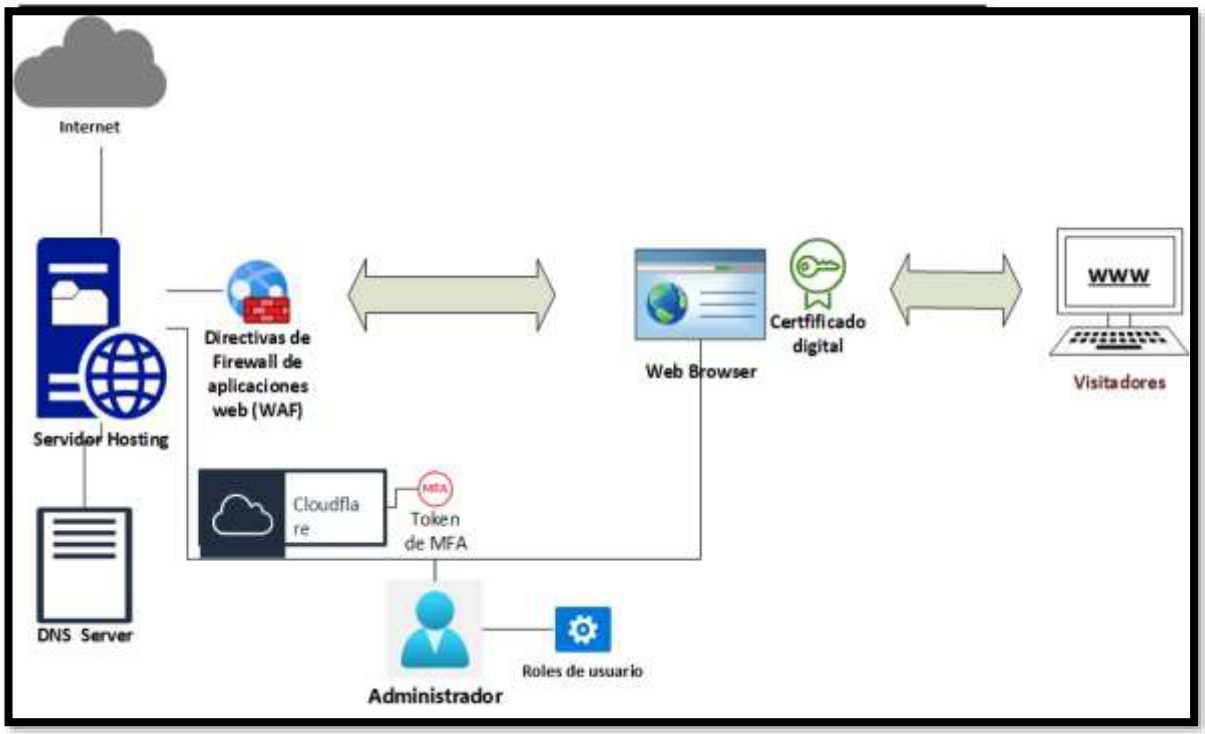
Arquitectura TI propuesta para máquinas virtuales - Azure



Nota. Elaboración propia.

Figura 8

Arquitectura TI propuesta para páginas web



Nota. Elaboración propia.

10. Evidencias

Imagen N°01: Administración de páginas web

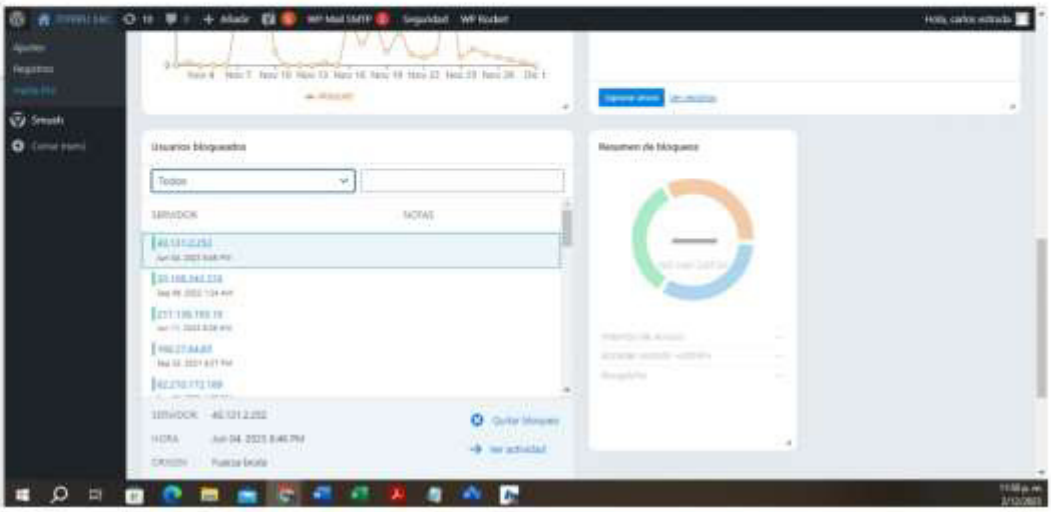


Imagen N°02: Administración de máquinas virtuales (01) en Microsoft Azure

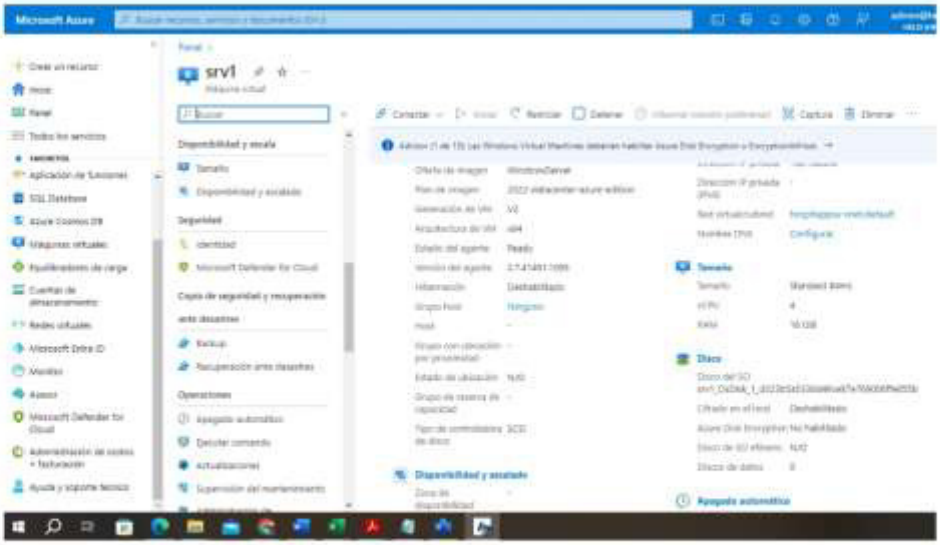


Imagen N°03: Administración de máquinas virtuales (02) en Microsoft Azure

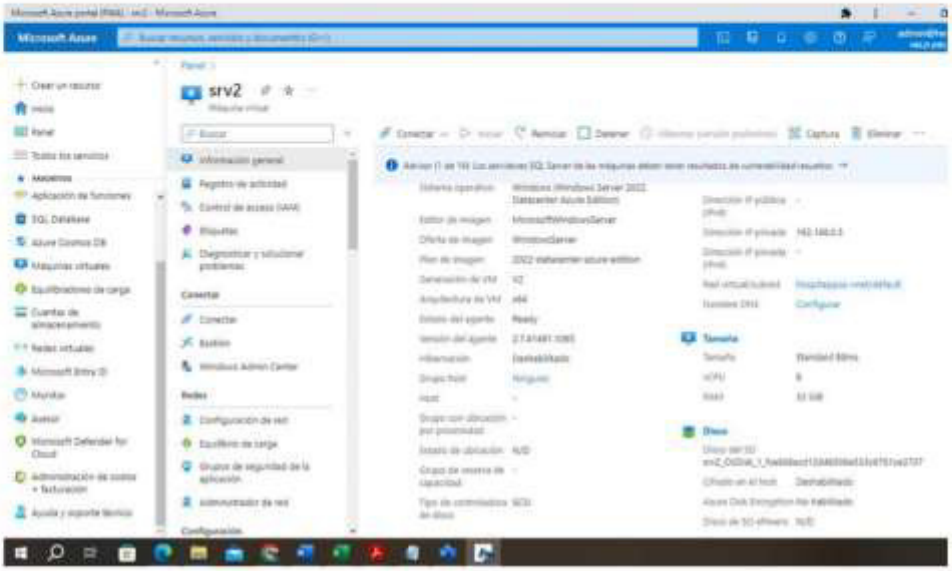


Imagen N°04: Implementación del proyecto de investigación n°1

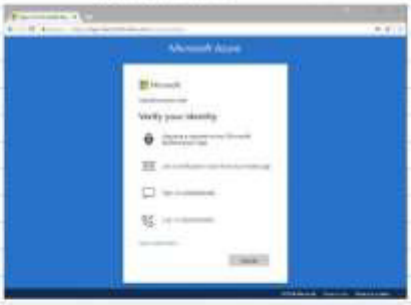
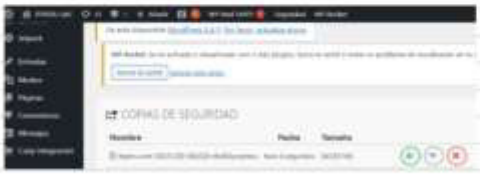
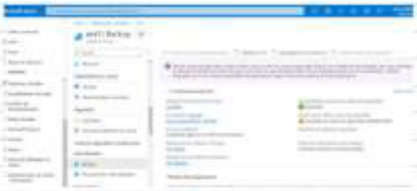
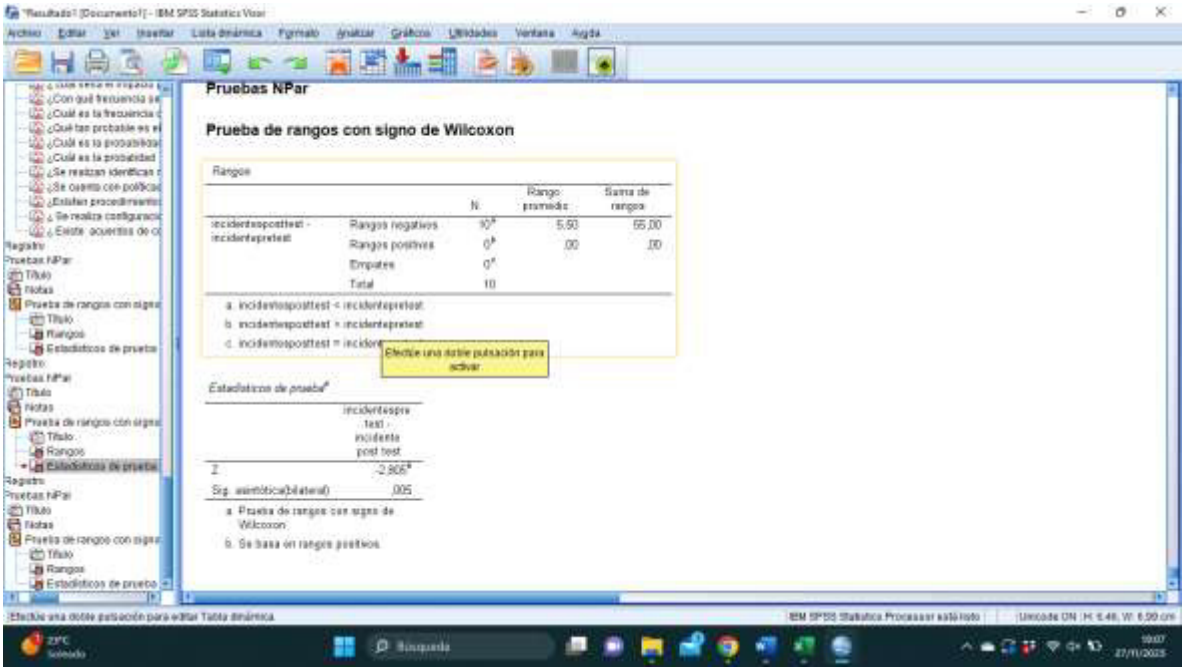
Evidencia N°01	
9.1.1 Autenticación multifactor	
Ingreso a la administracion de paginas web y maquinas virtuales	
Explicacion:	
Al implementar MFA, se protegen las interfaces de administración contra accesos no autorizados y se reduce significativamente el riesgo de ataques de fuerza bruta y otros métodos de intrusión	
Paginas web	
Maquinas virtuales Azure	

Imagen N°05: Implementación del proyecto de investigación n°2

Evidencia N°02	
15.2	
problemas con paginas web y maquinas virtuales	
Explicacion:Establecer un proceso de rollback inmediato en caso de actualizaciones fallidas.	
Paginas web	
Maquinas virtuales Azure	

ANEXO E: Evidencia de programa estadístico

1. Evidencia de SPSS para prueba de Wilcoxon



2. Evidencia de SPSS para prueba de Wilcoxon