UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE NEGOCIOS

PROGRAMA ACADÉMICO DE CONTABILIDAD Y ADMINISTRACIÓN

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

Para optar el título de Contador Público

AUTOR(ES)

Avalos Acosta, Susan (0000-0003-0753-6708)

Vargas Javier, Kelly Isabel (0000-0003-4755-4038)

ASESOR

Esquicha Flores, Luis Enrique (0000-0002-4728-4931)

Lima, 25 de julio de 2022

DEDICATORIA

A Dios por guiarme y por permitirme sentir la fe como el soporte que necesitaba. También a mis padres, hermanos y abuelos por el apoyo contante y su amor.

Susan Avalos Acosta

Este trabajo de investigación está dedicado a mis padres, quienes representan el amor más sincero e incondicional y que con su ejemplo me enseñaron que la unión es el motor más importante de la vida. A mis hermanos, por acompañarme y apoyarme en cada propósito de vida.

Kelly Vargas Javier

AGRADECIMIENTOS

Agradecemos a Dios, por bendecirnos con cada despertar y permitirnos cumplir nuestros objetivos profesionales.

Agradecemos a nuestros padres, por ser nuestro motor e impulso para seguir adelante en cumplir nuestras metas pese a los obstáculos que hemos afrontado a lo largo de nuestras vidas.

Así también, a las personas que nos ayudaron con su tiempo y disposición en brindarnos información para el desarrollo de la presente investigación.

Y finalmente, agradecemos a nuestro asesor de tesis por la motivación y confianza durante estos meses para poder culminar el trabajo de tesis.

RESUMEN

El presente trabajo de investigación tiene como finalidad evaluar y determinar el impacto de la ISO 27001: Seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en el distrito de San Isidro en el año 2021.

La investigación se desarrolló en cinco capítulos y se basa en la teoría, indagación e interpretación de diversos artículos científicos que están dentro del ranking de cuartiles de las mejores investigaciones, así como de Normas Internacionales de Información Financiera (NIIF) para asegurar el cumplimiento del principio contable de negocio en marcha.

En el Capítulo I se aborda el Marco teórico, donde se definen los conceptos y términos más importantes acerca de la ISO 27001: Seguridad de la información, ciberseguridad, ciberataques, principio de negocio en marcha y el sector de servicios tecnológicos. Asimismo, se analiza la aplicación de la ISO 27001: Seguridad de la información en un contexto a nivel local como internacional para obtener una mejor perspectiva acerca del estudio.

En el Capítulo II: Plan de investigación, se define el problema principal y específicos, así como los objetivos e hipótesis general y específicas. Seguidamente, en el Capítulo III: Metodología de investigación, se desarrolla la metodología que es de enfoque mixto. Además, se determina la población, el tamaño de la muestra y los instrumentos que se aplicaron para el análisis cuantitativo y cualitativo.

En el Capítulo IV: Desarrollo de la investigación, se encuentra la aplicación de los instrumentos seleccionados en el capítulo III como la encuesta y entrevista a profundidad. Finalmente, en el Capítulo V: Análisis de los resultados de la investigación, se presentan los

resultados obtenidos de los instrumentos aplicados en la investigación, las conclusiones y recomendaciones.

Palabras clave: ISO 27001; Sistema de gestión de seguridad de la información; Principio de negocio en marcha; Ciberseguridad; Tecnología.

ABSTRACT

The present research work has a purpose to evaluate and determine the impact of ISO 27001: Information Security on the going concern principle for companies that provide technology services in the district of San Isidro in the year 2021.

The research was developed in five chapters and is based on theory, inquiry and interpretation of various scientific articles that are within the quartile ranking of the best research, as well as International Financial Reporting Standards (IFRS) to ensure compliance with the going concern accounting principle.

Chapter I addresses the Theoretical Framework, where the most important concepts and terms about ISO 27001: information security, cybersecurity, cyber-attacks, going concern principle and the technology services sector are defined. Also, the application of ISO 27001: Information Security in a local and international context is analyzed to gain a better perspective on the study.

In Chapter II: Research Plan, the main and specific problem is defined, as well as the general and specific objectives and hypotheses. Then, in Chapter III: Methodology, the research methodology is developed, which is of mixed approach. In addition, the population, the sample size and the instruments applied for the quantitative and qualitative analysis are determined.

In Chapter IV: Development of the research, we find the application of the instruments selected in Chapter III, such as the survey and the in-depth interview. Finally, Chapter V: Analysis of results, presents the results obtained from the instruments applied in the research, conclusions and recommendations.

Keywords: ISO 27001: Information Security; Information security management system; Going concern principle; Cybersecurity; Technology.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Al pasar del tiempo, las empresas han incrementado el uso de la tecnología a causa de la digitalización de sus procesos, lo cual ha conllevado a facilitar el trabajo y la comunicación entre los usuarios internos o externos de las compañías. Asimismo, ha permitido que la expansión nacional e internacional de estas se produzca en un menor tiempo a comparación de años pasados. Sin embargo, este avance y constante actualización también ha expuesto la información de las empresas ante posibles amenazas de vulnerabilidad de los datos, lo cual se ha convertido en una preocupación constante de los altos mandos ejecutivos de una empresa (Ladino, Villa & López, 2011).

Actualmente, uno de los activos más importantes de las compañías es el conjunto de los datos, el tratamiento de este y los sistemas que procesan dicha información. Esto básicamente porque las empresas pueden incurrir en procesos legales, problemas financieros y entre otros si no toman las medidas necesarias para salvaguardar dichos elementos considerados como activos, ya que a la vez esta información puede ser de índole confidencial de usuarios externos a la empresa (Lugo, Carrasquero & Gómez, 2020). Cabe resaltar que esto podría conllevar a una mayor repercusión en empresas que brindan servicios de seguridad de la información, ya que deben cumplir con ciertos estándares internacionales para salvaguardar el procesamiento de datos que los clientes les confían.

El procesamiento de datos, su interacción con la tecnología y las personas conlleva a la transformación de este. Esto es relevante porque a través de dicha transformación se basa la toma de decisiones de los altos mandos de una organización. Esto, de acuerdo con los objetivos y planificación de las empresas, en pocas palabras, es un sistema de información gerencial (SIG). Por ello, en base a la necesidad de ofrecer un soporte a este procesamiento de la información, existen estándares de seguridad que permiten disminuir riesgos de

amenazas de vulnerabilidad de datos. Seguidamente, una de estas normas internacionales es la ISO 27001, la cual se basa en sistemas de gestión de seguridad de la información (SGSI).

Por lo antes mencionado, el propósito de la presente investigación fue determinar el impacto de la ISO 27001: Seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. Asimismo, nos enfocamos en el sector Tecnología debido a que, en la actualidad, las Compañías recopilan información de los usuarios que participan en sus procesos operativos para generar bases de datos, los cuales contribuyen a la toma de decisiones y que son vulnerables a riesgos como ciberataques, hackeo y suplantación de identidad. Esto por la ausencia de la mejora continua en sus procesos, ya que con el paso del tiempo van cambiando de acuerdo con el avance de la tecnología y la automatización de estos. Por ello, nuestro interés fue investigar cómo estos riesgos amenazan a las operaciones propias de un negocio que pertenece a este sector y qué efectos desencadena en la continuidad de este.

CAPÍTULO I: MARCO TEÓRICO

1.1 Estado de la cuestión

Pattanavichai (2018) en su investigación sobre "El modelo de red de diseño para el estándar de gestión de la seguridad de la información depende de la norma ISO 27001" propone instalar una red conocida como cortafuegos, que consiste en conectar una red interna y externa a la organización para prevenir el ingreso de intrusos a la red y detectar posibles ataques a los servidores. Para ello, sugiere que la organización implemente un sistema de gestión de la seguridad basado en los requerimientos de la ISO 27001, con el fin de evidenciar la mejora continua del ciclo PDCA. Las organizaciones con SGSI deberán mejorar la efectividad de este mediante el desarrollo de un plan de acción sobre la seguridad de la información que contenga objetivos, políticas, medidas de control y seguimiento. Contribuye en el estudio porque aporta en la definición de variables.

El artículo científico de Culot, Nassimbeni, Podrecca & Sartor (2021) titulado "La norma de gestión de la seguridad de la información ISO/IEC 27001 de gestión de la seguridad de la información: revisión de la literatura y agenda de investigación basada en la teoría" tuvo como objetivos analizar los conceptos de la ISO 27001 e identificar los problemas y beneficios de la certificación ISO 27001 a nivel empresarial revelando las motivaciones para iniciar el proceso y su resultado en el rendimiento empresarial. Concluye que los problemas potenciales son la falta de apoyo y liderazgo de la alta dirección, flexibilidad de las normas y falta de participación de consultores externos. De esta manera, contribuye en el estudio porque aporta en la justificación del problema, la definición de variables y fundamenta la hipótesis general.

Los posibles elementos que fomentan la certificación ISO 27001 son el tamaño de la empresa, sector empresarial orientado en servicios tecnológicos y la disposición de innovación (Mirtsch, Kinne & Blind, 2021). Asimismo, Tiganoaia (2015) en su estudio señala que las Compañías buscan mejorar la gestión de seguridad de la información para asegurar la eficiencia de las operaciones y el desarrollo económico teniendo como objetivos explicar la importancia de la implementación de un sistema de gestión de seguridad de la información y los procesos de la certificación ISO 27001:2013. De igual manera, aporta en el estudio porque ayuda a definir los principales conceptos de las variables y los problemas e hipótesis específicos.

Santos-Olmo, Sánchez, Caballero, Camacho y Fernández-Medina (2016), en su artículo "La importancia de la cultura de la seguridad en las PYMES frente a la correcta gestión de la seguridad de sus activos" de metodología cualitativa empleó 10 pymes de clientes de la Compañía Sicaman Nuevas Tecnologías S.L. para concluir que el método "Marisma" es el más adecuada para que las pymes implementen un sistema de gestión de seguridad de la información exitoso, ya que es sencilla de trabajar a un bajo costo, mejora los conocimientos de seguridad y brinda datos cuantitativos de las decisiones tomadas por la Compañía. El fin de la investigación fue aportar en la definición de las variables y fundamentar las hipótesis específicas. También Valencia-Duque y Orozco-Alzate (2017) plantea una metodología de implementación de un adecuado SGSI integrado por 4 normas ISO: 27001, 27002, 27003 y 27005 explicando conceptualmente cada norma. Contribuye en el estudio porque aporta en la definición de variables. Asimismo, Mirtsch, Blind, Koch y Dudek (2021) en su investigación de metodología mixta concluyó que la adopción de la ISO 27001 en las Compañías del sector TIC (Tecnologías de la Información y Comunicación) son principalmente impulsadas por requisitos legales, de los clientes e imagen corporativa cuya característica es la falta de beneficios financieros inmediatos, pero que permite evitar

resultados indeseables. De este modo, colabora en definir las variables y a fundamentar el objetivo general.

Deane, Goldberg, Rastrillos y Rees (2019) en su investigación tuvo como objetivo explicar la importancia de establecer una política de seguridad de la información en las empresas y su valor para el mercado de valores teniendo una metodología cuantitativa y llegando a concluir que los anuncios de certificaciones ISO 27001 favorecen ligeramente a las pequeñas empresas pertenecientes a los sectores de manufactura y servicios financieros, puesto que las estadísticas del estudio demuestran la reacción positiva del mercado cuyo fin principal fue fundamentar el objetivo e hipótesis general.

Por su parte, Li, Yen, Chen, Chen, Lu, y Cho (2015) en su investigación tuvo como objetivo analizar los efectos de la virtualización en la seguridad de la información, de igual manera tuvo un alcance de relación explicativa llegando a concluir que la implementación de virtualización en el sector electrónica, tecnología de la información y motriz afecta significativamente en la seguridad de la información en relación a la seguridad física y ambiental. Todo esto de una manera beneficiosa y es así como contribuye en el presente estudio porque aporta con fundamentar la justificación del problema, la definición de variables, preguntas específicas e hipótesis. Por otro lado, las empresas para preservar su , competitividad deben afrontar el reto de la ciberseguridad de hoy en día (Corallo, Lazoi & Lezzi, 2020). Asimismo, Sabillón y Jeimy (2019) en su estudio tuvieron como objetivo determinar los efectos de la ciberseguridad en la continuidad del negocio, del mismo modo tuvo un alcance de relación explicativa, llegando a concluir que el modelo de auditoría en la ciberseguridad no está diseñado para un sector específico o país. Además, la planificación y controles a considerar en la ciberseguridad influyen en afrontar los desafíos de las auditorías. Es así como contribuye con esta investigación porque ayuda a fundamentar la justificación

del problema, la definición de variables, preguntas específicas e hipótesis. Seguidamente, Kianpour, Kowalski y Øverby (2022), el fin de su investigación fue determinar si la ciberseguridad debe ser considerado un bien público. Asimismo, la investigación tuvo un alcance de relación explicativa llegando a concluir que la teoría de los bienes públicos debería cumplir un rol más relevante respecto a cómo tratamos a la ciberseguridad en los diferentes entornos para mantener una infraestructura digital fuerte. De esta manera, aporta con esta investigación, ya que aporta para la definición de variables. El estudio de Li y Liu, (2021) tuvo como objetivo revisar los avances de la ciberseguridad del mismo modo tuvo un alcance de relación explicativa, llegando a concluir que la seguridad cibernética no es netamente gubernamental y que la tecnología de la información son una de las fuentes de poder más relevantes del tercer milenio. Es así como contribuye con esta investigación porque ayuda con la definición de variables. Por su lado, Stiawan, Idris, Abdullah, Aljaber y Budiarto (2017) en su estudio tuvo como objetivo determinar la relevancia de las pruebas de penetración de ciberataques y el análisis de vulnerabilidad de las empresas, de igual manera tuvo un alcance de correlación simple, llegando a la conclusión de que las pruebas de penetración son útiles para detectar y mitigar riesgos de ciberataques. Asimismo, es importante el análisis de la vulnerabilidad de la infraestructura de una red, ya que de esta manera se establecerán acciones a seguir por los colaboradores ante un ciberataque. De esta manera aporta con este estudio porque ayuda a fundamentar la justificación del problema, la definición de variables, preguntas específicas e hipótesis. Finalmente, El-Marsi, Al-Yafi, Addas y Tarhini (2018), su investigación tuvo como objetivo determinar los factores que impulsan a los profesionales de TI a no estancarse en sus carreras, de igual manera tuvo un alcance de relación explicativa llegando a concluir que las habilidades y el talento del profesional de TI desempeña un papel importante en su elección y logros profesionales. De esta manera, aporta con esta investigación, ya que aporta para la definición de variables.

En relación con el principio de negocio en marcha o también llamado empresa en funcionamiento, Yu-Hsin, Yu-Cheng & Yu-Ling (2016) en su investigación identificaron los elementos que un profesional de Contabilidad debe analizar para emitir una opinión sobre la capacidad de una empresa de continuar como negocio en marcha teniendo en cuenta los siguientes aspectos: situación financiera, situación operativa y gestión empresarial. La situación financiera manifiesta los recursos económicos que tiene la compañía para afrontar sus obligaciones de pago y situaciones inciertas del mercado evaluando los siguientes factores: ratio de apalancamiento a corto y largo plazo, capital circulante, ratio de liquidez, entre otros. La situación operativa hace referencia al funcionamiento interno de la compañía medido por la capacidad de crecimiento en el sector, nivel de ingresos, rentabilidad de los activos, pérdidas consecutivas del año actual e inmediato anterior, posible pérdida de personal clave o cliente valioso, aparición de un competidor importante u otros riesgos relacionados con el mercado. La gestión empresarial hace referencia a la independencia que le asiste a un trabajador de la compañía y al contador que emite la opinión de empresa en marcha para realizar sus funciones con imparcialidad a fin de tomar decisiones de manera objetiva, De esta manera contribuye con esta investigación, ya que aporta para la definición de variables. Asimismo, los autores Feng y Li (2014) señalan que uno de los principales factores a considerar para emitir la opinión de negocio en marcha es rentabilidad futura de la compañía, ya que la información financiera debe ser prospectiva con el fin de ayudar en la toma de decisiones. De igual manera, aporta en el estudio porque ayuda a definir los principales conceptos de las variables. Finalmente, Blay, Geiger y North (2011) en su investigación determinaron que mercado considera relevante la opinión de negocio en marcha de los auditores, ya que considera un riesgo potencial en caso no sea favorable. Del mismo modo, consideran que, a mayor riesgo de la empresa, mayor será la probabilidad de

incumplimiento respecto a sus obligaciones financieras en relación con el pago de deudas. Es así como contribuye con esta investigación, ya que ayuda con la definición de variables.

Según Correa y Lopera (2020) en su estudio tuvo como objetivo determinar que las ratios de rentabilidad son las mejores herramientas para detectar insolvencias financieras, del mismo modo tuvo un alcance de relación explicativa, llegando a concluir que las ratios de rentabilidad sí son los mejores indicadores para detectar insolvencias financieras y que los inversores son los que deciden sobre la continuidad del negocio en caso no se cumplan sus expectativas. Es así como contribuye con esta investigación, ya que ayuda con la definición de variables. Asimismo, Berglund, Eshleman y Guo (2018), cuya investigación tuvo como objetivo determinar qué controles financieros son los adecuados para mantener una buena salud en relación con dicho tema, es así como concluyeron que los ratios de rentabilidad, apalancamiento y liquidez son los más relevantes al momento de la evaluación de la situación financiera para emitir una opinión de negocio en marcha. De igual manera aporta en el estudio porque ayuda a definir los principales conceptos de las variables. Seguidamente, Tamulevičienė y Androniceanu (2020) en su investigación tuvo como objetivo la investigación de indicadores para medir los cambios y el valor de una empresa. Asimismo, determinan que estos indicadores se podrían incluir en el sistema de control de gestión de las medianas empresas. Es así, que tuvo un alcance de relación explicativa, ya que llegaron a concluir que cada compañía debe escoger los indicadores más adecuados para medir su valor y los cambios. De esta manera, contribuye con esta investigación, ya que aporta para la definición de variables.

1.2 Descripción situacional sector económico

1.2.1 Descripción del sector

De acuerdo con el estudio de la Oficina Económica y Comercial de la Embajada de España en Lima, el cual fue realizado por Villares (2013), el Sector tecnología está conformado por las Tecnologías de la Información y la Comunicación (TIC). Asimismo, considera que la tecnología es relevante para una economía desarrollada de cualquier país. Seguidamente, menciona que la Information Technology Association of America (ITAA) describe a las tecnologías de la información como el análisis, proyecto, avance, implementación, apoyo y dirección principalmente de aplicaciones de software y hardware. Estos últimos son considerados sistemas informáticos, sin embargo, la diferencia entre ambos es que el software corresponde a aplicaciones informáticas y el Hardware son componentes tangibles de un ordenador.

Por otro lado, menciona que, dentro del sector, los servicios informáticos comprenden la consultoría en relación con el sector en mención, por ejemplo, el desarrollo de las aplicaciones informáticas de acuerdo con la necesidad del usuario. Asimismo, el outsourcing de procesos del sector es considerado como un servicio de este y entre los cuales se encuentran los siguientes:

- Aplicaciones que son maniobradas por los clientes: Customer Realtionship. Management (CRM).
- Recursos humanos.
- Servicios legales.
- Inversiones y finanzas.
- Gestión de la información: bases de datos y flujos de información, telefonía móvil y entre otros.

1.2.2 Evolución del sector tecnología

Un estudio realizado el 2016 por Dominio Consultores, empresa peruana del rubro marketing, inteligencia del mercado y tecnologías de la información, señaló mediante el Canal TI que el crecimiento del mercado TI, aún no lograba despegar a grandes escalas, ya que el crecimiento en ese año fue solo de 1.7%, lo cual se debía a que en ese entonces las herramientas y equipos no eran aún complejos. Por ello, no había tanta demanda de consultorías en relación con este mercado, Sin embargo, el mercado del software iba en crecimiento rápido, ya que las empresas comenzaban a implementar esta herramienta para mantener una adecuada administración y mayor representación en el sector. Asimismo, se esperaba que el sector TI se expanda a pequeñas empresas de ingresos menores que pudieran implementar el servicio cloud computing (computación en la nube) (Canal TI, 2016).

En el estudio “Prospección del mercado de TI en Perú; Banca, retail y trazabilidad”, elaborado por Procomer en el año 2020, indicaron que una de las principales causas en el retraso de ejecución de proyectos en relación con este sector es la baja oferta de programadores, lo cual a la vez genera que el servicio sea tercerizado y, por ende, esto conlleva a que los servicios sean más caros. Seguidamente, mencionan que de un 100% del sector TIC, el mercado TI representa el 37%, frente a un 67% del rubro telecomunicaciones debido a su crecimiento sostenido en los últimos años. Asimismo, el mercado TIC generó $4,381 millones, el cual representa el 2.3% del PBI del 2019. Esto está dividido en $1.608 millones del sector TI y $2.773 millones del mercado de telecomunicaciones, de acuerdo con la Figura 1.

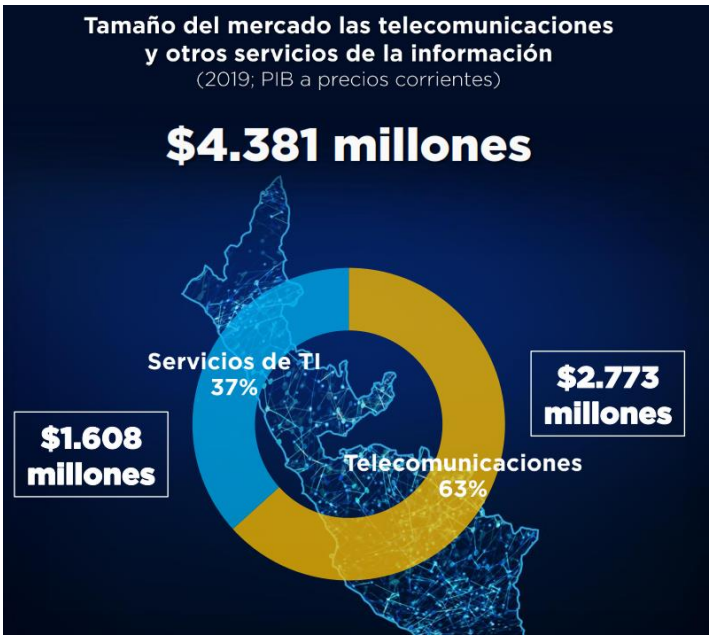

Figura 1. Tamaño del sector TIC en Perú del año 2019. Adaptado de "Prospección del mercado de TI en Perú", por Procomer, 2020

Cabe resaltar que, en el estudio en mención, muestran la evolución del mercado TI en Perú del año 2010 al 2019, el cual se puede observar en la Figura 2. que hubo un ligero crecimiento de 3.4% en el año 2016 respecto al año 2015. No obstante, el crecimiento que se esperaba en el 2017 fue menor y así sucesivamente ha ido en caída hasta cerrar en porcentajes negativos el 2019 con un -0.5% de crecimiento respecto al 2018 (Procomer, 2020).

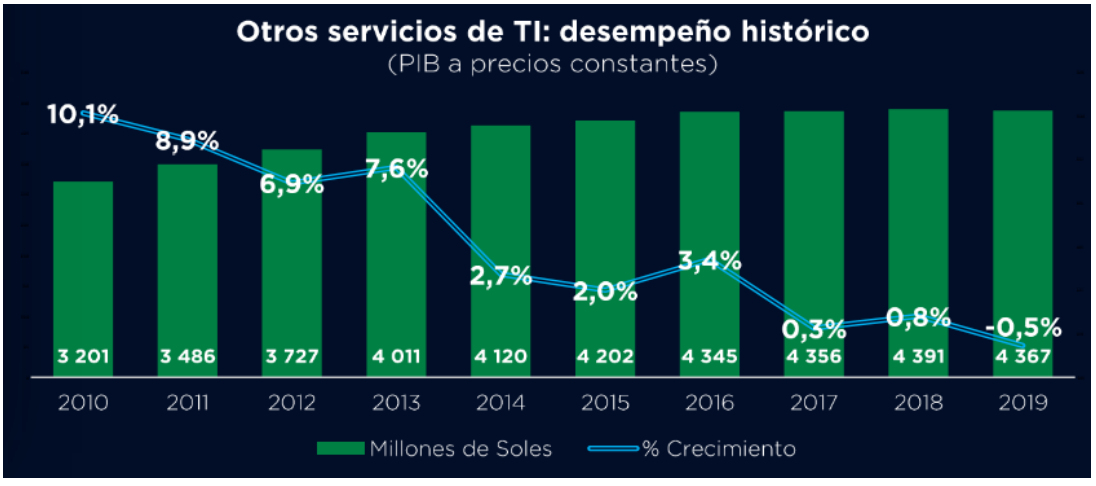

Figura 2. Evolución del mercado TI en Perú. Adaptado de "Prospección del mercado de TI en Perú", por Procomer, 2020

Finalmente, el estudio de Procomer (2020), mencionan que el entorno de ciberseguridad en Perú ha sido impulsado, ya que los servicios de seguridad de la información han crecido en respuesta a la necesidad del sector retail, finanzas, telecomunicaciones y el más reciente fue el Gobierno. Esto, basado en el ente calificador de La Unión Internacional de Telecomunicaciones en el ranking de The Global Cybersecurity Index (índice de ciberseguridad global), en el cual Perú estaba ubicado entre el puesto 90 a 71, ya que el país evidenciaba un gran interés en relación al compromiso con las iniciativas de ciberseguridad y a la vez presentaba oportunidades de mejora en el ámbito de la protección de servicios digitales como también en estándares de seguridad de la información en el sector público. Respecto a lo antes mencionado, cabe precisar que Perú ocupó el puesto 41 global respecto a servicios digitales realizados al Gobierno, lo cual incrementó la demanda de dichos servicios.

De acuerdo con el diario web El Peruano, se espera que Perú alcance una inversión de $5,626 millones de dólares en el largo plazo de acuerdo con lo comentado por el director de Exportaciones de la Promotora de Comercio Exterior Costa Rica (Procomer), Álvaro Piedra. Asimismo, mencionó que Perú se caracteriza por ser uno de los países de Sudamérica con mayor inversión en tecnología, ya que consigna el 2.57% del PBI (Producto Bruto Interno) por arriba del promedio de Latinoamérica que es 2.06% (El Peruano, 2020).

1.2.3 Servicios que ofrece el sector

De acuerdo con la clasificación industrial internacional uniforme (CIIU) de todas las actividades económicas (2010) de revisión 4, indica cuáles son los servicios que presta el sector en mención.

1.2.3.1 Programación informática

Este servicio consiste en el abastecimiento, sondeo, escritura y actualización de programas informáticos.

- Tema y boceto de escritura del código informático de los siguientes componentes:
  - Programas de sistemas operativos que también incluyen reajuste y corrección.
  - Aplicaciones informáticas que también incluyen reajuste y corrección.
  - Bases de datos.
  - Páginas web.
- Adecuación de programas informáticos ya existentes, en otras palabras, adaptación de la aplicación de acuerdo con las necesidades del cliente en base a la funcionalidad de sus sistemas de información.

1.2.3.2 Consultoría de informática y de gestión de instalaciones informáticas

Abarca el boceto y el proyecto de sistemas informáticos en relación con programas, equipos y tecnología de comunicación. Asimismo, hay dos unidades de este servicio, las cuales son las siguientes:

- Programas informáticos: Consiste en la instalación del programa.
- Soporte Físico: Comprende el apoyo a los usuarios con los programas instalados, los cuales pueden ser implementados por terceros o vendedores.

Cabe resaltar que este servicio también comprende el trámite y aplicación de sistemas informáticos como la inclusión o solo la instalación de procesamiento de datos de los usuarios y a la vez el servicio de apoyo vinculado a dichos servicios.

1.2.3.3 Otras actividades de tecnología de la información y de servicios informáticos

Esta sección abarca otras actividades relacionadas a la tecnología de la información y la informática. Cabe resaltar que son actividades que no se encuentran clasificadas en las secciones mencionadas en líneas arriba. Asimismo, los servicios incluidos en esta sección son los siguientes:

- Restauración de datos en caso de problemas informáticos.
- Instalación de programas informáticos.
- Configuración de ordenadores personales.

1.3 ISO 27001: 2013 Seguridad de la información

1.3.1 Seguridad de la información

1.3.1.1 Definición de seguridad de la información

La seguridad de la información es definida como una condición surgida a raíz de la creación y monitoreo de un conjunto de procedimientos de protección de datos que garantizan a una organización continuar con sus operaciones a pesar de los riesgos potenciales asociados a los sistemas de información como delitos cibernéticos (Zapata, Fernández-Alemán & Tovar, 2015). Mientras que Najar y Suárez (2015) definen a la seguridad de la información como un activo importante para las organizaciones, puesto que estas agrupan actividades empleando una plana administrativa, medios de información y comunicación para logar mantenerse en el mercado.

Es fundamental incorporar la seguridad de la información en la gestión empresarial a través de la implementación de un marco de gestión del conocimiento que permite proteger

no solo a la información disponible sobre la seguridad de información sino también a los conocimientos desarrollados y experiencias de los trabajadores.

Para Cárdenas, Martínez y Becerra (2016) el punto de inicio de un marco de gestión del conocimiento es la gobernanza de seguridad de la información que consiste en el compromiso de la alta dirección de la organización de tomar decisiones estratégicas acerca de las acciones a implementar para abordar la seguridad de la información. El paso siguiente es desarrollar una política de seguridad de la información en base a 3 procesos que se describen a continuación:

Formulación: este proceso abarca la evaluación, aprobación y seguimiento de los objetivos trazados. El contenido que debería de desarrollar la política es la siguiente:

- Definición de seguridad de la información
- Responsabilidades de los trabajadores
- Acciones de contingencia
- Gestión de contraseñas
- Control de acceso
- Manejo de virus
- Back up de datos

Implementación: puesta en marcha del contenido de la política aprobado en la etapa de formulación.

Adopción: especifica las funciones y deberes de la alta dirección y trabajadores en relación con la salvaguarda de la información y otras tecnologías permitiendo garantizar la seguridad de estos recursos.

Pattanavichai (2018) proporciona un modelo que sirve como guía para las organizaciones que se encuentran en el proceso de elaboración de políticas de seguridad de la información. Este modelo es conocido como la tríada CIA (Confidencialidad, Integridad y Disponibilidad) tal como se muestra en la Figura 3.

Confidencialidad: también llamado privacidad, se refiere a la restricción del acceso a los sistemas de información de los trabajadores autorizados. Con el fin de proteger los datos susceptibles de eventos nocivos.

Integridad: garantizar el uso fidedigno de los datos.

Disponibilidad: garantizar el funcionamiento adecuado de los recursos tecnológicos.

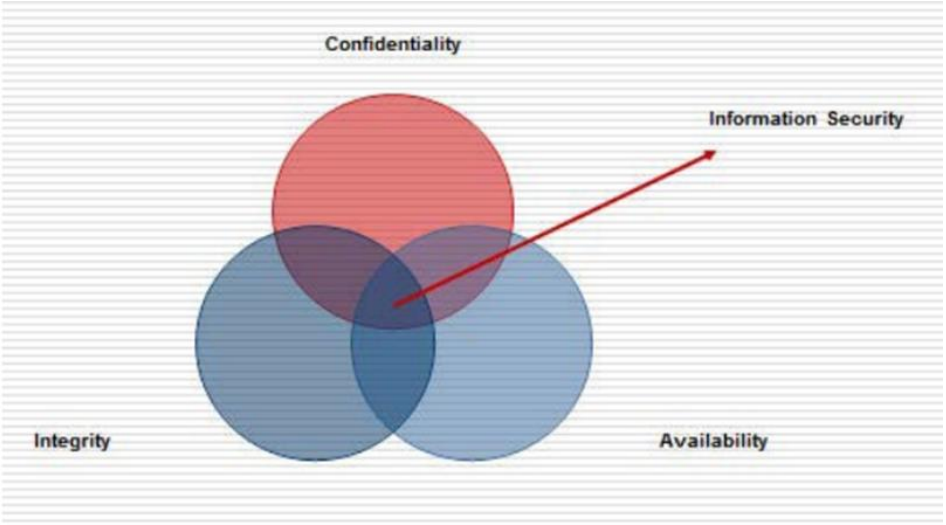

Figura 3. Elementos de la seguridad de la información. Elaborado por Pattanavichai, 2018

Con una política de seguridad de la información establecida, la organización se encuentra en la capacidad de implementar medidas de control que reduzcan los riesgos asociados a la seguridad de la información a través de la gestión de riesgos. Esto consiste en un proceso de evaluación de riesgos potenciales inherentes a las tecnologías de la información que requieren de controles internos para mitigar la probabilidad de ocurrencia

y prevenir amenazas que impacten en el desarrollo normal de las operaciones de la organización, tal como se muestra en la Figura 4.

Figura 4. Relación de los componentes del riesgo. Adaptado por Cárdenas, Martínez y Becerra, 2016

Luego de describir las bases teóricas del marco de gestión del conocimiento, en la Figura 5 se muestra el orden jerárquico de este.

Figura 5. Marco de trabajo de seguridad de la información. Elaborado por Cárdenas, Martínez & Becerra, 2016

1.3.2 Sistema de gestión de seguridad de la información (SGSI)

1.3.2.1 Definición del sistema de gestión de seguridad de la información

El sistema de gestión de seguridad de la información o SGSI consiste en un conjunto de procedimientos, políticas y actividades que garantizan la protección de los recursos de información administrados por una compañía. Es un estándar de gestión que otorga seguridad al ambiente de la información que posee una compañía y mitiga riesgos potenciales asociados a los sistemas de información (Santos-Olmo et al., 2016).

El SGSI basado en la ISO 27001 permite establecer, implementar, ejecutar, monitorear, verificar, mantener y mejorar la seguridad de la información para asegurar el cumplimiento de los objetivos organizacionales (International Organization for Standardization [ISO], 2018). Este sistema es impulsado a través del ciclo de mejora continua de Deming o también llamado Plan-Do-Check-Act cuyas siglas en inglés son PDCA que consiste en 4 pasos: Planificar-Hacer-Verificar-Actuar (PHVA), tal como se muestra en la Figura 6.

Planificar (Plan): consiste en definir los objetivos y las acciones a ejecutar para cumplirlos como un plan de acción. Por ejemplo: implantar políticas, procedimientos y objetivos del SGSI para obtener resultados planificados por la gerencia.

Hacer (Do): puesta en marcha del plan elaborado en etapa de planificación a fin de reunir datos que soporten su funcionalidad. Por ejemplo: poner en prueba la operatividad de las políticas, los controles de gestión de riesgos y procedimientos del SGSI.

Verificar (Check): en esta etapa se examina a detalle los resultados obtenidos de la etapa anterior y los contrasta con los objetivos definidos en el plan de acción. Los resultados son reportados a la alta dirección para la toma de decisiones. Por ejemplo: evaluar y medir la funcionalidad del SGSI.

Actuar (Act): ejecutar acciones preventivas de acuerdo con los resultados obtenidos en la etapa de verificación.

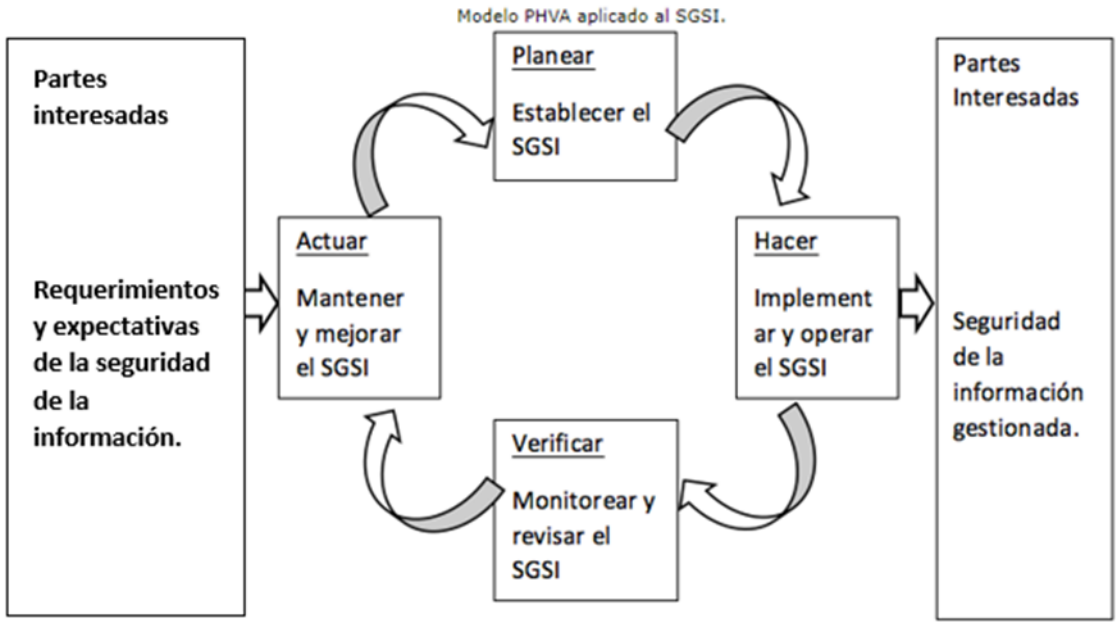

Figura 6. Ciclo PHVA. Adaptado de Revista Espacios

En la siguiente Figura 7 se detallan las actividades de cada fase correspondiente al ciclo PDCA.

PLANIFICAR	Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias Establecer un mapa de procesos Definir autoridades y responsabilidades
HACER	Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles
CONTROLAR	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección
ACTUAR	Adoptar acciones correctivas Adoptar acciones de mejora

Figura 7. Acciones de cada fase del ciclo PHVA. Elaborado por ISOTool

1.3.2.2 Importancia de la implementación del SGSI

Según la ISO (2018), un SGSI es importante para todo tipo de organización ya sea pública o privada, grande o pequeña sin distinguir la industria, puesto que es importante para las actividades de gestión de riesgo. La implementación exitosa otorga las siguientes ventajas competitivas:

- Reducción de riesgos causados por el manejo de recursos tecnológicos.
- Marco estructurado que garantice las diferentes operaciones del negocio.
- Asistencia a la gobernanza de la compañía relacionada a la formación de los directivos y trabajadores sobre la gestión de la seguridad de la información.
- Confianza de los socios comerciales y grupos de interés.

- Mejor gestión económica en la inversión de la mejora continua de la seguridad de la información.

1.3.3 Definición de la familia ISO/IEC 27000

La Organización Internacional de Normalización conocida por sus siglas ISO fue fundada el 23 de febrero de 1947 como un organismo sin fines de lucro cuyo objetivo es la creación de normas internacionales de uso estándar para el mercado global que buscan solucionar problemas actuales con respecto a la salud, medioambiente, comercio, tecnología, entre otros. Trabaja conjuntamente con la Comisión Electrotécnica Internacional conocida por el acrónimo IEC (ISO, 2018). Actualmente, la ISO se encuentra conformado por 165 miembros a nivel global siendo el Instituto Nacional de Calidad reconocido por sus siglas INACAL el único representante de la ISO en el Perú desde el año 2014 (ISO, 2021).

La versión actual de ISO/IEC 27000 corresponde a la quinta edición difundida en el año 2018 en reemplazo de la edición publicada en el 2016 (International Organization for Standardization 27000 [ISO 27000], 2018). La familia de normas comprendidas en ISO/IEC 27000:2018 se centra en definir conceptos vinculados a la norma estándar 27001 y facilitar la comprensión técnica del sistema de gestión de la seguridad de la información clasificándolos en cuatro grupos como se muestra en la Tabla 1.

Tabla 1

Clasificación de las normas que conformar la familia ISO 27000

Norma ISO/IEC	Clasificación
ISO/IEC 27000	Normas que contienen la definición de conceptos relacionados con el sistema de gestión de la seguridad de la información.
ISO/IEC 27001, ISO/IEC 27006, ISO/IEC 27009	Normas que establecen los requisitos de implementación de un SGSI.
ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC 27008, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC 27016, ISO/IEC 27021	Normas que actúan como consulta/guía general.
ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27019, ISO/IEC 27799	Normas que actúan como consulta/guía para sectores específicos.

Nota: Normas que conforman la familia ISO 27000. Adaptado del estándar ISO/IEC 27000, 2018

Valencia-Duque y Orozco-Alzate (2017) proponen la aplicación de las normas ISO/IEC 27002, ISO/IEC 27003 e ISO/IEC 27005 para implementar un adecuado sistema de gestión de seguridad de la información de acuerdo con los requerimientos establecidos en la ISO/IEC 27001:2013, tal como se muestra en la Figura 8.

Figura 8. Normas de la familia ISO/IEC 27000 para establecer un SGSI de acuerdo con ISO/IEC 27001:2013 propuesto por Valencia-Duque y Orozco-Alzate, 2017

A continuación, se definirán las siguientes normas ISO: ISO/IEC 27002, ISO/IEC 27003 e ISO/IEC 27005. Adicionalmente, se considerará el estándar ISO/IEC 27004 porque incluye términos asociados a la norma de estudio ISO 27001.

ISO/IEC 27002: Tecnología de la información - Seguridad técnicas de seguridad - Código de prácticas para controles de seguridad de la información

El estándar brinda a las organizaciones una serie de controles a emplearse en la implementación de un SGSI de acuerdo con las disposiciones de ISO/IEC 27001. Fue creado hace más de 25 años siendo publicada por primera vez en el año 1995 por la Institución Británica de Normalización como BS7799. Luego de cinco años, la Organización Internacional de Normalización (ISO) adaptó el contenido a las necesidades del mercado internacional y lo difundió como ISO 17799. Posteriormente, en el 2005 se actualizó la versión a ISO/IEC 27002:2005 junto con ISO/IEC 27001:2005 (International Organization for Standardization 27002 [ISO 27002], 2013). La versión más reciente se revisó en el 2013 presentando los siguientes cambios: 114 controles de seguridad (contiene 19 controles menos

en comparación de la versión anterior) divididos en 14 categorías. A continuación, detallamos la estructura de la ISO 27002.

- Alcance: indica que el ámbito de la aplicación de la norma se basa en la elección de controles adecuados.
- Referencias normativas: esta norma pertenece a la familia ISO/IEC 27000:2018.
- Términos y definiciones: la explicación de la terminología se encuentra en la ISO/IEC 27000:2018.
- Estructura normativa: señala las cláusulas y grupos de control. Los 114 controles de seguridad se clasifican en tres grupos (a nivel de organización, normativo y técnico) como se muestra en la Tabla 2.
- Políticas de seguridad de la información: brinda alcances sobre la creación de políticas y su contenido.
- Organización de la seguridad de la información: se refiere a la gestión interna de la Administración.
- Seguridad de los recursos humanos: responsabilidad de la gestión del capital humano antes, durante y después de la contratación.
- Gestión de activos: proporciona orientación sobre el manejo adecuado de todo aquello que le pertenece a la compañía y se encuentra bajo el uso de terceros. Por ejemplo: realizar inventarios de activos físicos y electrónicos, codificación de activos, entre otros.

- Control de acceso: configurar los permisos de acceso a los sistemas información, aplicaciones que son propiedad de la compañía, servicios de red, autenticación de usuarios, etc.
- Criptografía: propone controles para proteger la confidencialidad de la información.

- Seguridad física y ambiental: prohibir el ingreso de personas no autorizadas a espacios críticos donde se desarrollan los procesamientos de información generales de la compañía.
- Seguridad de las operaciones: controles que aseguran la continuidad del negocio.
- Seguridad de las comunicaciones: proveer confianza en el uso de la red a través de la creación de dominios: acceso de uso interno y externo.
- Adquisición, desarrollo y mantenimiento de sistemas: el proveedor que brinda el servicio de red debe cumplir los estándares de aseguramiento para el uso interno y el adecuado desarrollo de las operaciones. Por ejemplo: solicitar una prueba de la protección de datos antes de contratar el servicio.
- Relaciones con proveedores: los acuerdos establecidos entre la compañía y el proveedor deben documentarse.
- Gestión de incidentes de seguridad de la información: señala los procedimientos a ejecutar para dar respuesta a los problemas que presente la gestión de la información.
- Aspectos de seguridad de la información de la gestión de la continuidad del negocio: indica que la compañía debe desarrollar lineamientos sobre seguridad de la información para afrontar situaciones adversas que generan riesgo en el funcionamiento operativo del negocio.
- Cumplimiento: señala la realización de las categorías mencionadas en la norma ISO/IEC 27002:2013.

Tabla 2 Grupos de control de la ISO/IEC 27002:2013

Grupos de control de la ISO/IEC 27002:2013

Grupo	Categoría	Número de controles
Seguridad organizacional	Gestión de incidentes de seguridad de la información	7
	Aspectos de seguridad de la información de la gestión de continuidad del negocio	4
	Gestión de activos	10
	Políticas de incidentes de seguridad de la información	2
	Organización de la seguridad de la información	7
	Seguridad de los recursos humanos	6
	Relación con los proveedores	5
Seguridad técnica	Seguridad física y del entorno	15
	Seguridad de las comunicaciones	7
	Adquisición, desarrollo y mantenimiento de sistemas	13
	Control de acceso	14
	Criptografía	2
	Seguridad de las operaciones	14
Seguridad normativa	Cumplimiento	8

Nota: Grupos de control de ISO/IEC 27002:2013. Adaptado de Valencia-Duque y Orozco-Alzate, 2017.

ISO/IEC 27003: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Orientación

La norma brinda una guía para la creación adecuada del sistema de gestión de seguridad de la información según los parámetros de la ISO/IEC 27001. Fue revisada en el año 2017 siendo la versión actual ISO/IEC 27003:2017 reemplazando a la versión publicada

en el 2010. Por un lado, se modificó el término guía por orientación en el título del estándar denominándose actualmente como Sistemas de Gestión de la Seguridad de la información – Orientación, ya que las categorías del 4 al 10 de la estructura de ISO/IEC 27003:2017 favorecen la comprensión de la ISO/IEC 27001:2013. Asimismo, se facilitó la aplicación de la norma ISO/IEC 27003 suprimiendo la obligatoriedad de seguir una secuencia de implementación a través de actividades que se detallaban en la versión del año 2010. Por otro lado, se actualizó el esquema normativo conforme la última versión de la ISO/IEC 27001:2013 (International Organization for Standardization 27003 [ISO 27003], 2017).

ISO/IEC 27004: Tecnología de la información - Seguridad técnicas - Seguridad de la información Gestión de la seguridad de la información - Supervisión medición, análisis y evaluación

El estándar brinda una orientación sobre las técnicas de medición para evaluar la eficiencia del sistema de gestión de seguridad de la información según los requisitos abordados en la ISO/IEC 27001 cuyos resultados influyen en las decisiones de gestión de la administración de la organización. La versión más reciente de la norma corresponde a la edición 2 publicada en el año 2016 en reemplazo de la edición publicada en el 2009 (International Organization for Standardization 27004 [ISO 27004], 2016). Seguidamente, se listan las 8 categorías más los anexos que conforman la estructura.

- Ámbito de aplicación: establece una guía para evaluar el rendimiento del sistema de gestión de seguridad de la información.
- Referencias normativas.
- Términos y definiciones.
- Estructura y descripción: el orden de los ítems busca facilitar el entendimiento y la correspondencia con los requisitos de la norma ISO/IEC 27001:2013.

- Justificación: explicación sobre la importación de la medición y evaluación de resultados.
- Características.
- Tipo de medidas: medidas de rendimiento y medidas de eficacia suelen emplearse para efectos de esta norma estándar.
- Procesos: consiste en identificar las necesidades de información, desarrollar un plan de acción, medir y analizar resultados, y evaluar la efectividad la seguridad de la información.
- Anexo A: Información sobre un modelo de medición de la seguridad de la información.
- Anexo B: Ejemplos de constructo de medición.
- Anexo C: Ejemplo de construcción de medidas.

ISO/IEC 27005: Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información

El estándar tiene como objetivo apoyar a las organizaciones en la comprensión de los requisitos establecidos en la ISO/IEC 27001:2013 desde la perspectiva de la gestión de riesgos (International Organization for Standardization 27005 [ISO 27005], 2018). La versión más reciente de la norma corresponde a la edición 3 publicada en el año 2018 en reemplazo de la segunda edición publicada en el 2011. A continuación, se listan las 12 categorías más los anexos que conforman la estructura.

- Alcance: indica que el ámbito de la aplicación de la norma se basa en la elección de controles adecuados.
- Referencias normativas: esta norma pertenece a la familia ISO/IEC 27000:2018.
- Términos y definiciones: la explicación de la terminología se encuentra en la ISO/IEC 27000:2018.

- Estructura de la norma: en este apartado se mencionan los componentes del estándar.
- Antecedentes: precedentes la gestión de riesgos.
- Descripción general del proceso de gestión de riesgos para seguridad de la información
- Contexto.
- Evaluación de riesgos de seguridad de la información.
- Tratamiento de riesgos de seguridad de la información.
- Aceptación de riesgos de seguridad de la información.
- Comunicación y consulta de riesgos de seguridad de la información.
- Anexo A: Definición del ámbito de aplicación.
- Anexo B: Evaluación de los activos y su impacto.
- Anexo C: Identificación de riesgos comunes.
- Anexo D: Análisis de debilidades.
- Anexo E: Tratamiento de la valoración del riesgo.
- Anexo F: Limitación a los cambios de los riesgos.

1.3.3.1 Definición de la norma ISO 27001:2013 Seguridad de la información

La norma central de la familia ISO/IEC 27000 es la ISO 27001 con la denominación oficial: Tecnología de la información -Técnicas de seguridad –Sistema de gestión de Seguridad de la información – Requisitos, que establece los lineamientos generales normativos de implementación de un sistema de gestión de seguridad eficiente y eficaz para mitigar riesgos potenciales que conlleva la adaptación de tecnologías emergentes asociados a la digitalización de procesos a nivel organizacional.

La ISO 27001 es una de los principales y más aplicados estándares de la familia ISO 27000 a nivel mundial por todo tipo de organización e industria. La norma se divide en dos secciones. La primera sección señala los requisitos para establecer, implementar, ejecutar,

monitorear, verificar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (International Organization for Standardization 27001 [ISO 27001], 2013). Mientras que la segunda sección es el Anexo A que contiene un listado de controles importantes para la seguridad de la información.

El estándar se ha desarrollado a lo largo de dos décadas para brindar a las organizaciones guías actualizadas de seguridad de la información frente al avance de la globalización tecnológica. En la siguiente Figura 9 se observa la línea de tiempo de la evolución de la ISO 27001.

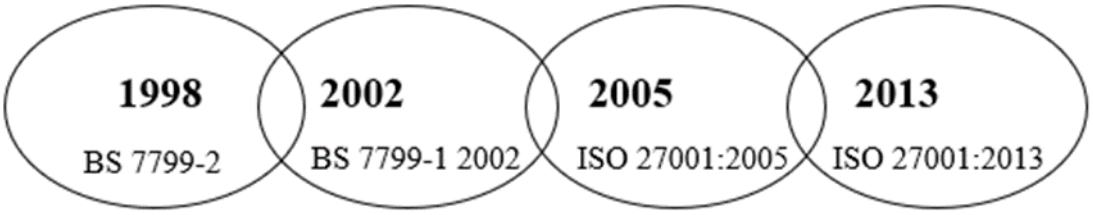

Figura 9. Origen y evolución de la ISO 27001 por la página web www.pmg-ssi.com, 2013

En el 2005 se adoptó la ISO 27001 en reemplazo al estándar BS7799 Parte 2 publicado en el año 1998 y revisado en el 2002, a fin de mejorar el contenido sobre la estructura del modelo PDCA (Plan-Planificar, Do-Hacer, Check-Verificar y Act-Actuar) en la implementación del sistema de gestión de seguridad de la información (Culot et al., 2021). En la etapa de planificación se establece el SGSI en base a los stakeholders de la Compañía, luego se pone en funcionamiento, en la etapa de verificación se supervisa la operatividad del SGSI y en la etapa de actuación, de acuerdo con la revisión y resultados de la eficiencia del SGSI se mantiene y mejora de forma continua. La estructura normativa de esta versión desarrolla 133 controles divido en 11 categorías.

Posteriormente, en el año 2013 se revisó la edición 2005 de la norma ISO 27001 siendo la versión actual que tiene como fin proteger la integridad, confidencialidad y disponibilidad de información (ISO 27001, 2013). La estructura normativa de esta versión revisada desarrolla 114 controles divido en 14 categorías. En la Tabla 3 se muestran los cambios en los controles de las ediciones 2005 y 2013, propuestos por Hamdi, Anir, Abdul y Hassandoust (2019).

Tabla 3

Cambios en el Anexo A de ISO 27001

	ISO 27001:2015	Versión revisada de la norma ISO 27001:2013
A.5	Política de seguridad	Políticas de seguridad de la información
A.6	Organización de la información. Seguridad	Organización de la información. Seguridad
A.7	Gestión de activos	Seguridad de los recursos humanos
A.8	Seguridad de los recursos humanos	Gestión de activos
A.9	Físico-ambiental. Seguridad	Control de acceso
A.10	Comunicaciones y funcionamiento. Gestión	Criptografía
A.11	Control de acceso	Físico-ambiental. Seguridad
A.12	Adquisición y desarrollo de SI y gestión	Seguridad operativa
A.13	Incidente de seguridad de la información. Gestión	Seguridad de las comunicaciones
A.14	Gestión de la continuidad del negocio	Adquisición del sistema, desarrollo y mantenimiento
A.15	Cumplimiento	Relación con los proveedores
A.16	-	Incidente de seguridad de la información. Gestión

A.17	-	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio
A.18	-	Cumplimiento

Nota: Cambios en el Anexo A de ISO 27001. Adaptado de Hamdi, Anir, Abdul y Hassandoust, 2019

La estructura normativa está conformada de la siguiente manera:

- Ámbito de aplicación: se centra en la administración de los riesgos.
- Referencias normativas: normas de la familia ISO 27000 que referencian y son importantes para el entendimiento de la ISO 27001.
- Términos y definiciones: descripción conceptual de los términos empleados en la ISO 27000.
- Contexto de la organización: conocer las expectativas de la compañía y grupos de interés.
- Liderazgo: se refiere a las obligaciones de la alta administración de la compañía respecto a la evaluación permanente y mantenimiento del SGSI.
- Planificación: valoración y tratamiento de los riesgos potenciales de la información.
- Soporte: se refiere a la documentación de la información sobre un SGSI implementado.
- Funcionamiento: planear, implementar y revisar los procesos.
- Evaluación del desempeño: dar seguimiento a la gestión de riesgos.
- Mejora: mejora continua y efectividad del sistema de gestión de seguridad de la información.

1.3.3.2 Importancia de la certificación ISO 27001

La ISO 27001 es la certificación más extensa y conocida después de las normas ISO 9001, ISO 14001 e ISO 45001, respectivamente tal como se muestra en la Tabla 4. La

primera brinda una guía sobre la gestión de procesos asociados a la calidad de los productos o servicios prestados por la compañía, mientras que la ISO 14001 trata sobre las buenas prácticas y la responsabilidad corporativa con el medio ambiente. La ISO 45001 fue diseñada para establecer un ambiente seguro para los trabajadores y mitigar fatores de riesgo que afecten la integridad de estos.

Tabla 4

Número total de certificados válidos y número total de organizaciones

Norma ISO	Total de certificados válidos
ISO 9001	916,842
ISO 14001	348,218
ISO 45001	190,429
ISO 27001	44,486
ISO 22000	33,735
ISO 13485	25,656
ISO 50001	19,721
ISO 20000-1	7,846
ISO 22301	2,205
ISO 37001	2,065
ISO 39001	936
ISO 28000	520

Nota: Número total de certificados válidos y número total de organizaciones. Adaptado de ISO Survey, 2020.

Las tecnologías representan una oportunidad de crecimiento para los negocios, el cual depende principalmente de la capacidad de adaptarse y prepararse para el uso de nuevas tecnologías. De acuerdo con la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD, 2021), los países mejor preparados se encuentran en América del Norte y Europa Occidental mientras que las naciones pertenecientes a África y América

Latina no llegan al índice mínimo de preparación, tal como se muestra en la Figura 10. Sin embargo, los riesgos cibernéticos están latentes a nivel global.

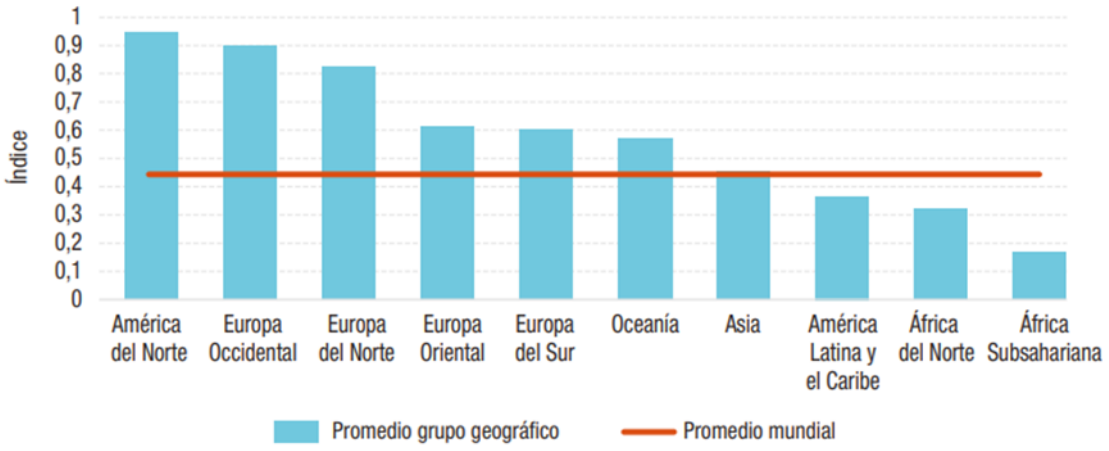

Figura 10. Promedio de la puntuación del índice por grupo geográfico. Elaborado por UNCTAD, 2021

La actual crisis sanitaria del Covid-19 ha marcado un hito en la nueva era de la transformación digital que ha provocado que las compañías destinen mayor inversión para iniciar o mejorar la automatización de sus procesos y afrontar los nuevos retos de la conectividad a distancia. Según El Peruano (2021), como consecuencia de la pandemia provocado por el Covid-19 y el trabajo a distancia más de la mitad del PBI mundial será destinado a la digitalización para el 2022 y dentro de 3 años, el 55% del presupuesto global de las tecnologías de la información se destinará a la transformación digital de los negocios.

Por ello, es fundamental que los altos directivos tomen medidas adecuadas para proteger sus activos de información. Conseguir concientización sobre la gestión de la seguridad entre empleados y directivos es decisivo para garantizar la continuidad del negocio.

De acuerdo con la última encuesta anual que publicó la ISO en el año 2020 sobre el número de certificados válidos a nivel global, la certificación del estándar 27001 ha tenido

un incremento importante del 22.34% que representa a 8,124 nuevas compañías en comparación del año anterior.

Mirtsch, Pohlisch y Blind (2020) en su investigación señalan que la implementación de la ISO 27001 sirve para estructurar procesos dentro de una organización para asegurar la confidencialidad, integridad y disponibilidad de la información. Respecto a la confidencialidad, reduce las brechas de seguridad de la información evitando daños a la reputación y costos. En cuanto a la integridad y disponibilidad, puede ayudar en asegurar la continuidad del negocio previniendo especialmente ataques cibernéticos que afectan a las funciones de las compañías.

1.3.3.3 Ventajas de la certificación a nivel empresarial

La certificación ISO 27001 permite obtener ventajas operativas y organizacionales, respectivamente (Culot et al., 2021). En primer lugar, establecer un sistema de gestión de seguridad de la información de acuerdo con la normativa del estándar 27001 permite incrementar la eficiencia en los procesos de seguridad identificando y mitigando riesgos potenciales propios del entorno tecnológico. En segundo lugar, las ventajas organizacionales hacen referencia a los beneficios financieros generados por la reputación corporativa en el mercado, ya que califica para los socios estratégicos (clientes, proveedores, instituciones financieras, empleados, gobierno e inversores) como una compañía de confianza que garantiza la continuidad de sus operaciones.

Según Tiganoaia (2015), las compañías certificadas poseen dos ventajas marcadas con respecto a las demás y estas se mencionan a continuación:

- Garantía de mercado: obtener una certificación ISO 27001 genera un impacto positivo de la marca en la mente de los consumidores, potenciales clientes y partes

interesadas porque proyecta protección, confidencialidad y seguridad en el uso de la información que se almacena como parte del proceso operativo del negocio.

- Gobernanza: la participación de la gerencia en la mejora continua de la seguridad de la información a través de la administración del sistema de gestión de seguridad de la información y promoviendo una cultura de protección de activos de información contribuye positivamente en la gestión empresarial y en la atracción de nuevos clientes.

1.3.4 Ciberseguridad

1.3.4.1 Definición de Ciberseguridad

De acuerdo con Sabillón y Jeimy (2019) es la evaluación de los activos críticos más relevantes que se deben cuidar de los ataques cibernéticos. En otras palabras, es el análisis de sistemas que pueden ser vulnerados, por ejemplo, en el caso de software, hardware, factores operativos y procesos. Esto con la finalidad de implementar políticas para resguardar la continuidad del negocio. Asimismo, cabe resaltar que la adopción de la ciberseguridad es un cambio importante en la metodología de los procesos de la compañía, ya que es una ventaja competitiva en el mercado de acuerdo con su sector. Puesto a que la implementación de la seguridad informática es diferente en cada sector, ya que se adecua a los procesos de cada empresa. De acuerdo con lo antes mencionado, es importante que las organizaciones bosquejen un escenario vulnerable, ensayos de penetración, valoración de la vulnerabilidad y acciones a realizar respecto a las vulnerabilidades. Asimismo, se deben actualizar los escenarios y más pasos a seguir de acuerdo con los ataques y riesgos cibernéticos en un contexto actual. Finalmente, mencionan que las compañías deben implementar un sistema de ciberseguridad organizacional acorde con su misión, visión, objetivos y entre otros. Para

ello, se requiere una política de gestión de peligros cibernéticos muy bien descrito y una matriz para mitigar o trasladar alguna contingencia cibernética.

Según Li y Liu (2021), la ciberseguridad es un tema importante en relación con la infraestructura de las compañías, ya que esto reflejará un estatus alto en su sector como logros, lo cual evidenciará la capacidad con la que cuenta para proteger la información privada de los clientes ante un competidor. Es decir, una empresa debe brindar seguridad para establecerse y desarrollarse en el mercado.

1.3.4.2 Ciberespacio

El ciberespacio son redes interconectadas entre las redes de comunicación, la infraestructura de TI, procesadores integrados, virtualización de la información y la interacción de la humanidad con este entorno de la tecnología con la finalidad de producir, procesar, almacenar, recuperar, explotar e intercambiar información (Li & Liu, 2021).

Arreola (2019) menciona que el ciberespacio es una herramienta excelente para mitigar amenazas y riesgos. Sin embargo, para aprovechar al máximo esta herramienta se debe plantear e implementar un método seguro, el cual involucre al Estado, empresas del sector privado y público. Por lo antes mencionado, el ciberespacio es un escenario, en el cual se han producido oportunidades y a la vez conflictos producto del desarrollo constante de las comunicaciones y tecnologías de la información.

El ciberespacio es una herramienta excelente que con el paso de los años se ha vuelto un escenario relevante en el aspecto social y económico. No obstante, también se ha vuelto un entorno inseguro producto del cambio constante y avance de la tecnología respecto a los riesgos y amenazas. Por ello, es importante tomar medidas como la ciberseguridad (Diaz, 2021).

1.3.4.3 Usuarios de la ciberseguridad

El sector privado y el público son los usuarios en general para implementar la ciberseguridad, ya que poseen información valiosa como base de datos, sistemas financieros y entre otros. El primero puede brindar servicios al sector público y es así como ambos deben salvaguardar la información de sus sistemas, ya que poseen datos nacionales, lo cual puede conllevar a un conflicto político Nacional o en el peor de los casos internacional en caso la información sea manipulada (Arreola, 2019).

De acuerdo con Kianpour et al. (2022), la ciberseguridad se determina por la interdependencia de usuarios a nivel macro, los cuales son gobiernos, organizaciones y personas. Asimismo, consideran que la interdependencia de dichos usuarios evita regulaciones más estrictas respecto a la ciberseguridad, ya que sugieren que este último debe ser tratado como un bien público para conservar ecosistemas fuertes. Es decir, la ciberseguridad no de ser separado por usuarios, ya que al ser tratado como un bien público, permitirá implementar políticas y planes más sostenibles. Sin embargo, las partes interesadas de diferentes sectores al colaborar podrían evidenciar los intereses contradictorios, ya que la incertidumbre que genera la seguridad cibernética puede producir oportunidades para algunas partes interesadas y amenazas para otras.

1.3.5 Ciberataques

1.3.5.1 Definición de ciberataques

Es cualquier hecho cibernético no autorizado cuyo fin es violar la política de seguridad de un activo cibernético, dañar e interrumpir el acceso de la información o servicios de dicho activo (Li & Liu, 2021). Asimismo, según Stiawan et al, (2017), el ataque cibernético es el acto de la vulneración digital de sistemas de información, cuya finalidad

radica en la filtración de datos personales o de empresas como también la interrupción de funcionamiento de sistemas, el cual genera pérdidas económicas.

De acuerdo con Stiawan et al. (2017), los ataques cibernéticos han evolucionado, ya que se han vuelto más sofisticados, fuertes y fáciles de utilizar, lo que genera sucesos como la destrucción del sistema y la filtración de información personal. Asimismo, la capacidad técnica de cómo hacerles frente a estos ciberataques han declinado ante estas nuevas amenazas. Por ello, es indispensable probar nuevos métodos de defensa frente a una prueba de penetración en un escenario real.

Las pruebas de penetración de acuerdo con Stiawan et al. (2017) son herramientas de evaluación para localizar y afrontar vulnerabilidades en la infraestructura de las redes. Esto con la finalidad se saber qué tan vulnerables son las dichas redes ante los ciberataques. Asimismo, es importante entender cómo protegerse y prevenir este tipo de ataques, sobre todo desde la perspectiva del agresor en relación con qué métodos utilizará, cuál es el móvil que los impulsa a realizar el ataque y cómo los realiza. Es así como la prueba en mención permitirá evaluar los sistemas en general. Seguidamente, mencionan que se realizó un estudio, el cual dividió los ataques en tres grupos de acuerdo con los objetivos de estos, los cuales se detallan a continuación: intentos dañinos, fines financieros (espionaje industrial, fraude y correos maliciosos) y navegación inofensiva. Finalmente, afirman que estos ataques cibernéticos cada día son más fáciles de realizar, ya que algunos implantan virus como los troyanos mediante páginas web o correos. Asimismo, recalan que el éxito de estos ataques depende de tres puntos relevantes:

- Grado de dificultad para hallar el punto vulnerable del sistema.
- Grado de dificultad para escoger el tipo de ataque.

- Grado de dificultad para descifrar de ataque.

Cabe mencionar que un reporte de seguridad del año 2021 de ESET informó que los países que más spyware (programa malicioso espía) detectaron fue Perú, Rusia e Israel. Asimismo, el estudio reveló que el 61% de las empresas de la región de Latinoamérica reportó haber sufrido un caso de seguridad informática, lo cual mencionan que esto no concluye que el resto de las empresas que no reportaron haber sufrido un incidente, no haya sufrido un ciberataque, lo cual es preocupante porque es probable que estas empresas no cuenten con los instrumentos necesarios para detectar este tipo de ataques (Andina, 2021).

1.3.5.2 Tipos de ciberataques

Garcia (2021) indica cuáles son los tipos de ciberataques más comunes:

- Malware spam: Correos masivos que son enviados con la finalidad de dañar el sistema de quien lo abre.

- Malware: Es un tipo de software malicioso que ataca de forma directa el sistema al tratar de modificar el código base con la finalidad de debilitar dicho sistema. Asimismo, este tipo de ataque incluye gusanos, troyanos o ransomware.

- Ransomware: la finalidad de este ciberataque es la encriptación de datos mediante la penetración de un código malicioso en el sistema de la víctima para pedir una recompensa para permitir el acceso a la información de archivos o dispositivos.

- Criptojacking: Este ataque se basa en la creación y adquisición de la criptomoneda con el objetivo de apoderarse de esta para obtener el dominio de la máquina. Cabe resaltar que, con el paso de los años, este tipo de ataque ha ido en aumento.

- Ciber-espionaje: La finalidad principal de este ataque es conseguir información, primordialmente de las instituciones del Estado.

- Phishing: Consiste en la redirección a sistemas o páginas mediante la falsedad de sitos web o correos.

1.3.6 Aplicación de la ISO 27001 en el Perú

1.3.6.1 Normas Técnicas Peruanas sobre la ISO 27001

El Instituto Nacional de Calidad (INACAL) es el único representante de la Organización Internacional de Normalización (ISO) en el Perú desde el año 2014, se encarga de estandarizar las condiciones y brindar orientación para que el proceso de prestación de un servicio y/o producto cumpla con el requerimiento de calidad a fin de beneficiar a las empresas de los distintos sectores (alimentos, construcción, gestión ambiental, hidrocarburos, tecnologías de la información, entre otros) y sus consumidores. Estos requerimientos u orientaciones son establecidos en un documento llamado normas técnicas peruanas.

A continuación, se mencionarán las normas técnicas peruanas (NTP) vigentes en el 2021.

1.3.6.1.1 NTP ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición

Mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso obligatorio de la norma NTP-ISO/IEC 17799:2007 para las entidades del Sistema Nacional de Informática con el fin de promover la seguridad y protección de los datos disponibles de los ciudadanos como parte de la estrategia de digitalización de los servicios públicos del Estado.

1.3.6.1.2 NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos

La ISO/IEC 27001:2014 anula y sustituye a la ISO/IEC 27001:2008, primera versión peruana. La norma fue revisada en el año 2016 teniendo como referencia la versión actualizada de la norma ISO/IEC 27000, con el fin de resguardar la información del país mitigando riesgos de exposición indebida de los datos del ciudadano e implementar servicios digitales que beneficien a estos y al sector empresarial. Para ello, establece los requerimientos y procesos para desarrollar un sistema de gestión de seguridad de la información aplicable a todas las compañías del sector público y privado. Sin embargo, de acuerdo con la Resolución Ministerial N° 004-2016-PCM esta norma es de uso obligatorio para las entidades del Estado.

1.3.6.1.3 NTP-ISO 56002:2021 Gestión de la innovación. Sistema de gestión de la innovación. Orientación. 1a. Edición

La norma se aprobó el 22 de junio de 2021 mediante Resolución Directoral N° 012-2021-INACAL/DN para orientar a las partes interesadas sobre la implementación de un sistema de gestión de la innovación. Este sistema permite formular la visión de la compañía, objetivos, estrategias y políticas que fomenten la innovación tanto en la alta dirección como en los trabajadores para lograr los resultados fijados. La norma es aplicable para compañías públicas o privadas, grandes o pequeñas y de cualquier naturaleza.

Las principales ventajas de desarrollar esta norma se detallan a continuación:

- Mejor gestión ante la incertidumbre.
- Mayor rentabilidad y crecimiento en el mercado.
- Eficiencia de recursos y productividad.
- Mejor valoración de la compañía.

1.3.6.2 Empresas certificadas en ISO 27001 al año 2021

Durante el 2021, ciertas entidades del Estado peruano obtuvieron la certificación ISO 27001:2013 por el eficiente funcionamiento de los sistemas de información empleados en los procesos de gestión de datos de la ciudadanía. Con esta certificación se garantiza el fácil acceso a la información digital a través de las plataformas web de estas instituciones durante las 24 horas (gob.pe, 2021). Estas entidades son:

- Ministerio del Ambiente (Minam)
- Ministerio del Interior (Mininter)
- Ministerio de Defensa

1.4 Principio de negocio en marcha

Es un diagnóstico de empresa en funcionamiento, el cual indica si una empresa se encuentra en crisis financiera. Esto con la finalidad de que los usuarios de los estados financieros evalúen si las futuras operaciones de la compañía se encuentran en riesgo. Asimismo, existen tres factores que influyen en la opinión de negocio en marcha, entre los cuales se encuentra: situación financiera, situación operativa y gestión empresarial (Yu-Hsin et al., 2016). Seguidamente, la NIA 570 "Empresa en funcionamiento" señala que los Estados Financieros se elaboran bajo este principio cuando la alta Dirección de una Compañía tiene la seguridad de continuar con las operaciones en un futuro probable (Norma Internacional de Auditoría 570 [NIA 570], 2016). Asimismo, la NIC 1 "Presentación de Estados Financieros" exige que la Gerencia analice la capacidad de la entidad de continuar como negocio en marcha dentro de los 12 meses siguientes del período sobre el que se informa sin limitarse a dicho tiempo, teniendo en cuenta eventos o factores que pudieran

generar duda sobre su continuidad para revelarse en los estados financieros (Norma Internacional de Contabilidad 1 [NIC 1], 2020).

Según Feng y Li (2014), uno de los factores más importantes a considerar para la evaluación de principio de negocio en marcha es la rentabilidad futura, pese a que la quiebra de las empresas es directamente proporcional a la escasez de liquidez y efectivo. Asimismo, mencionan que los inversionistas decidirían ya no invertir si hay evidencias de que se espera que la empresa siga generando pérdidas. Por ello, es importante la evaluación de la rentabilidad futura, ya que guarda relación con el principio de negocio en marcha. Seguidamente, mencionan que de acuerdo con el Statement on Auditing Standards (SAS) número 59 en relación con la capacidad de empresa en marcha, considera que la información financiera se debe realizar de manera prospectiva para la toma de decisiones.

1.4.1 Situación financiera

Las variables en relación con las finanzas de la empresa son importantes porque son indicadores de la situación financiera de la misma, ya que permiten conocer cuál es su estructura financiera y en qué se basa su solvencia (Yu-Hsin et al., 2016). Asimismo, Berglund et al. (2018) mencionan que entre los principales indicadores a considerar para mantener un adecuado estado financiero para las empresas es la liquidez, rentabilidad, apalancamiento, la emisión de nuevos valores de deuda o de capital y la antigüedad del cliente.

1.4.1.1 Ratios de liquidez

Son herramientas financieras que permiten analizar si una empresa cuenta con la capacidad de pago a tiempo en corto plazo (Corallo et al., 2020). Es decir, contempla la capacidad de la compañía para adquirir efectivo y afrontar sus compromisos de obligaciones

financieras en un mediano plazo, ya que estos ratios a la vez demuestran la competencia de los altos mandos de la empresa para transformar los activos corrientes en efectivo. Seguidamente, se contemplan dos ratios de liquidez (Instituto Nacional de Estadística e Informática, 2019).

- Razón corriente: evalúa de manera muy genérica la correlación que existe entre la posible obtención de liquidez a un corto plazo y la obligación de tesorería en cuanto a cumplir con sus pasivos en un mediano plazo, ya que el no cumplir con sus pasivos en el tiempo establecido, puede generar una para en las actividades relacionadas y ya programadas con dicha acción de cumplimiento de pago de los pasivos antes mencionados (Instituto Nacional de Estadística e Informática, 2019).
- Prueba ácida: Es un indicador minucioso a comparación del ratio de razón corriente, ya que se resta al activo corriente los inventarios porque este último es el menos líquido y a su vez el que más tiempo conlleva a convertirlo en efectivo (Instituto Nacional de Estadística e Informática, 2019).

1.4.1.2 Ratios de rentabilidad

Son el cociente que brinda las herramientas necesarias para analizar la capacidad y eficiencia de las compañías para mantener sus resultados financieros en el tiempo a largo plazo respecto a proyecciones. En pocas palabras, estas herramientas permiten evaluar la capacidad de la empresa en generar ganancias con una mínima inversión. Además, estos ratios deben concordar con los ratios liquidez (Corallo et al., 2020). Asimismo, Correa y Lopera (2020), mencionan que los indicadores de rentabilidad brindan a las empresas herramientas para analizar la eficiencia y su capacidad para mantener sus resultados a largo plazo. Finalmente, consideran que los ratios de rentabilidad y liquidez guardan relación, ya

que la rentabilidad debe ser un indicador importante para los acreedores porque les indica la capacidad de liquidez de la compañía para enfrentar sus deudas a largo plazo.

De acuerdo con el artículo 407, numeral 4 de la Ley General de Sociedades en relación con la disolución de la empresa, se considerará como una causal de disolución cuando las pérdidas disminuyan el patrimonio neto a una cantidad por debajo de la tercera parte del capital pagado. Esto, si las pérdidas en mención no son compensadas o el capital pagado no se incrementa o reduce en valor. Esto de acuerdo con lo mencionado en la web de la Superintendencia del Mercado de Valores (SMV, 2000).

- Margen sobre las ventas: Ayuda a identificar cuánto representa la utilidad de la empresa de un periodo respecto a las ventas realizas el mismo año (Instituto Nacional de Estadística e Informática, 2019).
- Margen de beneficio: Permite identificar cuánto de utilidad de la empresa corresponde a la misma sin considerar el financiamiento externo como ingresos no relacionados a la actividad de la compañía en relación con las ventas del mismo periodo. Es así como este indicador permite a las empresas determinar si las utilidades generadas pueden cubrir el financiamiento (Instituto Nacional de Estadística e Informática, 2019).
- ROA: Este indicador es conocido como la rentabilidad de los activos, ya se calcula el beneficio neto respecto a los activos totales. En otras palabras, muestra la efectividad de gestión de los activos, sin considerar si se obtuvieron con fondos de capital propio o de deuda con terceros (Tamulevičienė y Androniceanu, 2020).

1.4.1.3 Ratios de endeudamiento o de solvencia

Permiten conocer el nivel de dependencia del financiamiento externo de la empresa, así como el apoyo de los propietarios respecto a la estructura de capital. Es conocido que la deuda financiera tiene un menor costo respecto al de los accionistas. Por ello, la empresa debe hallar la estructura de capital más apta para optimizar el valor y la rentabilidad de la compañía (Corallo et al., 2020).

Myers (1984, como se citó en Blay, Geiger y North, 2011) han señalado que el incumplimiento de cualquier reclamo de deuda será más alto en relación con el nivel de riesgo de la empresa, puesto que, si este riesgo es alto, el incumplimiento de deuda será mayor. Por ende, la empresa debería controlar el capital prestado, ya que, si se encuentra en un nivel alto de endeudamiento, esta ya no debería solicitar más préstamo de capital. Asimismo, a mayor endeudamiento a largo plazo, genera menos financiamiento disponible como mayor probabilidad de incurrir en posibles costes de incumplimiento. Es así como esto afectaría en el valor de la empresa en el mercado y se reevaluaría el negocio en marcha de esta.

De acuerdo al Banco Pichincha (2021), los ratios de solvencia permiten a la persona natural o jurídica saber si cuentan con la capacidad de enfrentar satisfactoriamente sus obligaciones financieras de dinero. Asimismo, menciona que hay cuatro indicadores de solvencia, los cuales se detallan a continuación:

- Ratio de endeudamiento: Este indicador financiero ayuda a determinar el cuánta deuda emplea la compañía para financiar sus activos. Es así, como la empresa sincerará cómo está conformado su patrimonio. Asimismo, cabe resaltar que este ratio es conocido como índice de endeudamiento sobre patrimonio neto. En

decir, esta razón nos indica la proporción de deuda a corto plazo que debe la compañía por cada dólar del patrimonio. Del mismo modo, el porcentaje de endeudamiento adecuado dependerá del sector de la empresa en evaluación (Banco Pichincha, 2021).

$$Ratio\ de\ endeudamiento = \frac{Pasivo\ total}{Patrimonio\ neto}$$

- Ratio de endeudamiento a largo plazo: Esta herramienta hace referencia a los pasivos que serán pagados en un tiempo mayor a un año, el cual es traducido a pasivos a largo plazo. Esta herramienta nos muestra la proporción de deuda a largo plazo que debe la compañía por cada dólar del patrimonio (Banco Pichincha, 2021).

$$Endeudamiento\ a\ largo\ plazo = \frac{Pasivo\ no\ corriente}{Patrimonio\ neto}$$

- Ratio de deuda: Esta razón nos permite evidenciar el nivel de financiamiento de que posee la empresa en relación con sus activos totales. En pocas palabras, permite saber a la empresa qué cantidad de sus actividades es financiada por pasivos (Banco Pichincha, 2021).

$$Ratio\ de\ deuda = \frac{Pasivo\ total}{Activo\ total}$$

- Ratio de apalancamiento financiero: Este indicador calcula la correlación que existe entre el capital que se empleó en una actividad determinada y el capital propio. Es decir, el apalancamiento permite invertir más efectivo del que posee la compañía mediante créditos (Banco Pichincha, 2021).

$$Apalancamiento\ financiero = \frac{Activo\ total}{Patrimonio\ neto}$$

1.4.2 Situación operativa

La posición operativa se evalúa mediante la variable de los riesgos operativos del entorno del sector, la rentabilidad, las pérdidas durante dos años consecutivos, nivel de ingresos y la situación operativa interna de la empresa (Yu-Hsin et al., 2016).

1.4.2.1 Factores que impulsan el crecimiento en el sector

- Dinamismo del mercado: este es un factor que ha influido en el sector tecnología, ya que en los últimos 10 años se han producido cambios acelerados por la misma digitalización. Asimismo, estos cambios se han visto reflejados en el mercado del comercio y finanzas que coincidieron en la combinación de soluciones para el usuario en relación con créditos, compras a través de plataformas digitales también conocido como Ecommerce (comercio electrónico), el cual se paga de manera digital, es en ese momento cuando intervienen los bancos, también conocido como Fintech (tecnología financiera), pagos por el medio antes mencionado. Es así como en relación con las operaciones antes mencionadas surge la necesidad de seguridad digital (ciberseguridad) con relación a estos procesos de acuerdo con la Figura 11 (Procomer, 2020).

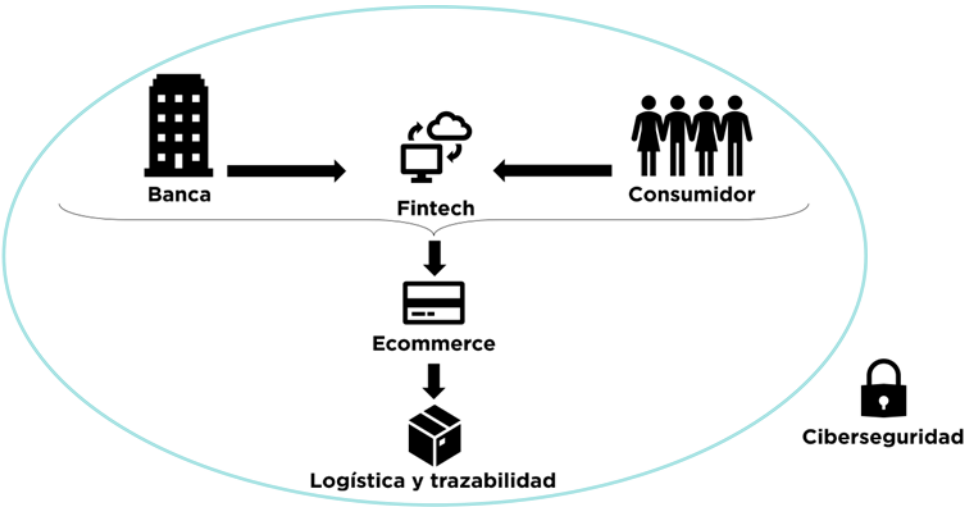

Figura 11. Actores en una compra online. Adaptado de "Prospección del mercado de TI en Perú", por Procomer, 2020

- Fintech: Son empresas intermediarias entre los bancos y las personas mediante canales completamente digitales. Esta plataforma financiera ha sido de gran utilidad para el comercio y a la vez se ha convertido en cliente fuerte para el sector TI. Seguidamente, en el Perú se ha afianzado un sistema financiero conformado por 4 bancos estatales, 16 privados y una decena de otros perfiles crediticios, Asimismo, en el país durante el 2019 contábamos con 120 empresas dedicadas al rubro en mención, el cual creció en un 256% respecto al año anterior con relación al número de empresas dedicas al sector Fintech. Cabe resaltar que somos el segundo país de la región con mayor porcentaje de crecimiento en el sector Fintech (Procomer, 2020).
- Retos para aumentar el uso de TI: Según el estudio realizado por Procomer (2020), el principal desafío recae en la banca y comercio, ya que el 55% de los consumidores duda en brindar información de sus tarjetas de créditos e información personal. Por ello, se debería trabajar en solucionar esta necesidad respecto a la seguridad de las macro y micro transacciones. Así como la

integración de las plataformas involucradas para la validación de datos y el ciclo de facturación. Asimismo, el 75% del comercio es informal, ya que, en repuesta de las medidas sanitarias del 2020, las pequeñas empresas se vieron en la obligación de adaptarse al medio digital para realizar sus transacciones, sin embargo, es sistema operativo no fue formal. Finalmente, el 40% de los clientes prefiere probar o visualizar el producto antes de realizar la compra. Por ello, reduce las compras en línea.

- Escasez de oferta de profesionales en el sector: El país presenta una alta demanda de profesionales en el sector TI, sin embargo, se evidencia un alto déficit de programadores, lo cual conlleva a tercerizar el servicio en un 65%. Es así como este déficit encarece el servicio y a su vez retrasa la puesta en marcha de los proyectos (Procomer, 2020). Asimismo, la preferencia laboral en el mercado ha variado en vista del contexto porque los técnicos dedicados al rubro digital son los más requeridos por las empresas. Esto en vista de la aceleración tecnológica y entre las carreras que se ha visto una mayor demanda es programas de tecnología, tales como: Ciberseguridad, programación y desarrollo web, inteligencia artificial, e-commerce, entre otros. Cabe resaltar, que durante el 2019 la compañía Huawei y Micro Star International (MSI), entre otros, se reunieron para exponer al público joven peruano, lo vital que son las carreras de tecnología en el mundo empresarial, ya que en medio del contexto en el que nos encontramos, los cambios en el sector tecnología ha colisionado en la vida diaria de las empresas y de las personas, lo cual ha generado oportunidades y la vez se evidencia un futuro prometedor para personas que se dediquen a este sector (Andina, 2021).

1.4.2.2 Nivel de ingresos

El sector TI tuvo ligeros crecimientos del 2016 al 2018 respecto a niveles de facturación, sin embargo, el 2019 decreció en -0.5% respecto al 2018, ya que el 2019 facturó S/ 4.367 millones de soles y el 2018 S/4.391 millones. Esto se debió básicamente a la escaza oferta de profesiones dedicados a este rubro. Seguidamente, cabe resaltar que el sector telecomunicaciones y servicios de información (TIC) representó el 2.3% de crecimiento respecto al total del PBI de dicho año. Asimismo, también es importante resaltar que la importación de servicios de información ha crecido el 2018 respecto al 2017 en un 97%, ya que el año 2018 Perú consumió 544 millones de dólares. Finalmente, cabe precisar que durante el 2019 el mercado TI estaba conformado por un 95% de microempresas, 4% de pequeñas empresas y el 1% por mediana y gran empresa (Procomer, 2020).

1.4.2.3 Personal clave

De acuerdo a la investigación de El-Marsi et al. (2018) atraer, desarrollar y retener a los profesionales de tecnologías de la información, se mantiene como una de las principales preocupaciones de los altos mandos de las compañías, ya que el número de graduados de carreras en relación a este sector va en decrecimiento, lo cual agrava el problema, ya que además las instituciones académicas requieren cambios serios para que los egresados estén realmente capacitados ante la evolución constante de este mercado. Asimismo, mencionan que el perfil de un gerente de proyecto de TI difiere del perfil de un profesional técnico de TI, ya que el primero se caracteriza por su nivel de habilidad alto respecto a la comunicación y las demás habilidades en relación con la gestión. Mientras que el segundo guarda relación con la parte operativa, ya que poseen conocimientos técnicos en base a sus experiencias laborales.

Desde el 2019 se produjeron cambios respecto a los perfiles de los profesionales del sector TI, ya que según la DNA Human Capital (empresa de selección de personal), las compañías buscan profesionales de TI con perfiles híbridos, alguien que posea una visión estratégica del sector que piensen "fuera de la caja" ya que deben ser innovadores, creativos, tener autonomía, entre otras habilidades blandas. Seguidamente, las otras habilidades deben ser técnicas de acuerdo con la rama del sector TI a la se dedican. Por ejemplo, el 47% de las empresas solicitan colaboradores de TI con experiencia en ciberseguridad, el 35% en infraestructura de hardware, el 34% en usuario de hardware, un 32% en soluciones networking y el 27% en desarrollo de software. Esta mezcla de habilidades responde a cómo esperan los directivos de la compañía que los profesionales reaccionen ante situaciones complejas (Tecnova, 2019).

El perfil del personal encargado de TI es muy importante, ya que dentro de este sector se encuentra el área de fraude, quien se encarga de monitorear el cumplimiento de las políticas internas y externas de las compañías (Plus TI, 2021). Asimismo, es importante resaltar que las empresas en la actualidad no pueden negar el acceso de los colaboradores a cierta información, aunque sea mínima, pese a que pueden estar expuestos a los tipos de amenazas antes mencionados, lo cual genera una brecha entre el sistema de detección de intrusos y las amenazas. Es así que mientras exista esa brecha, será complejo comprender y mitigar los vacíos de seguridad que exponen la información de la infraestructura de la empresa a informáticos maliciosos. Esto, básicamente porque la amenaza interna no solo es costosa, sino que también es complejo de detectar, ya que es difícil detectar a un colaborador que tiene acceso a información confidencial que quiere venderla a la competencia. Sin embargo, no es imposible, ya que se puede implementar una política de seguridad sólida en dicho caso (Loukaka & Rahman, 2017).

CAPÍTULO II: PLAN DE INVESTIGACIÓN

2.1 Descripción de la problemática

Con el paso de los años, el uso de la tecnología en las empresas ha ido en aumento debido a la digitalización de sus procesos. Ello ha conllevado a facilitar el trabajo y la comunicación entre los usuarios, ya sean internos o externos. Asimismo, ha permitido que la expansión nacional e internacional de las compañías se produzca en un menor tiempo a comparación de años atrás. No obstante, este avance y constante actualización también ha expuesto a las empresas ante riesgos de vulnerabilidad de su información, lo cual se ha convertido en una preocupación constante entre las empresas (Ladino et al., 2011).

Actualmente, uno de los activos más importantes de las compañías es el conjunto de datos, el tratamiento de este y los sistemas que procesan dicha información. Esto básicamente porque las empresas pueden incurrir en procesos legales, problemas financieros, entre otros si no toman las medidas necesarias para salvaguardar dichos elementos considerados como activos, ya que esta información puede ser de índole confidencial de usuarios externos a la empresa (Lugo et al., 2020).

El procesamiento de datos, su interacción con la tecnología y las personas conlleva a la transformación de este. Esto es importante, ya que mediante esta transformación se toman decisiones gerenciales de acuerdo con los objetivos y planificación de las empresas. En pocas palabras, es un sistema de información gerencial (SIG). Por ello, en base a la necesidad de brindar un soporte a este procesamiento de la información, existen estándares de seguridad que permiten mitigar riesgos de amenazas de vulnerabilidad. Una de estas normas internacionales es la ISO 27001, la cual se basa en sistemas de gestión de seguridad de la información (SGSI) (Lugo et al., 2020).

En el Perú, la Presidencia del Consejo de Ministros aprobó el uso obligatorio de la ISO 27001 mediante la Resolución Ministerial Nº 004-2016-PCM dirigido a las Entidades del Estado que integran el Sistema Nacional de Informática, con el fin de resguardar la información del país e implementar servicios digitales que beneficien a los ciudadanos y al sector empresarial. Asimismo, esta Resolución establece los lineamientos para que las Compañías que no se encuentran dentro del ámbito de aplicación, pero busquen obtener la certificación, lo realicen de forma opcional (El Peruano, 2016).

Por otro lado, la Superintendencia Nacional de Aduanas y de Administración Tributaria, emitió la Resolución de Superintendencia Nº 199-2015/SUNAT, con la finalidad de promover la Certificación ISO 27001 en las Compañías que se inscriban en el Registro de proveedores de servicios electrónicos de facturación cuya exigibilidad de implementación sería a partir del 01 de enero de 2019 (SUNAT, 2015). A causa del Covid 19, la SUNAT prorrogó la obligatoriedad hasta el 01 de julio de 2021 mediante la Resolución de Superintendencia Nº 221- 2020/SUNAT emitido en diciembre del 2020. Con la finalidad de resguardar la información tributaria de los usuarios y su confidencialidad (SUNAT, 2020).

La presente investigación se enfocará en empresas que prestan servicios de tecnología de la información de la clase 6209 de la división 62 del CIIU denominado “Otras actividades de tecnología de la información y de servicios informáticos” (CIIU, 2010). Los servicios de la clase en mención comprenden seguridad en la nube (Cloud Security), seguridad de la red (Network Security), protección de datos (Data Protection), seguridad de la tecnología operativa (OT Security) y gestión de acceso a la identidad (Identity Access Management), los cuales se encuentran agrupados dentro del servicio de seguridad de la información (Telefónica Tech, 2020).

- Seguridad en la nube (Cloud Security): Consiste en la implementación de políticas de prevención para asegurar que los sistemas o aplicaciones informáticas, redes físicas, servidores de datos y plataformas virtuales se mantengan seguras en la nube para hacer frente a amenazas internas y externas de los datos que almacenan las empresas, en este caso de los usuarios que confían su información a las empresas que brindan el servicio en mención, ya que los usuarios han decidido optar por la estrategia de digitalización (IBM, 2020).
- Seguridad de la red (Network Security): Agrupa las estrategias y pasos a seguir para salvaguardar la infraestructura de red para evitar la manipulación o daño de la data almacenada a través de accesos no autorizados, los cuales suelen suceder mediante virus, hackers y entre otros. Asimismo, los elementos que componen la red: son hardware, ordenadores, aplicaciones informáticas, sistemas operativos, entre otros (Telefónica Tech, 2020).
- Protección de datos (Data Protection): Consiste en resguardar los datos de una empresa independientemente de su tamaño contra accesos no autorizados en la red, sistemas operativos, aplicaciones informáticas y en la nube. Esto, con el fin de proteger la marca y mantener la confidencialidad de la información del cliente porque las empresas que proveen este tipo de servicio deben mantener un adecuado control de la información, ya que se debe cumplir con el Reglamento General de Protección de Datos cuya finalidad es proteger la información de los usuarios y establecer reglamentos que limiten el acceso a ello, lo cual evitará posibles multas o pérdidas de clientes. Asimismo, cabe resaltar que esto es decisivo para mantener la continuidad del negocio (Telefónica Tech, 2020).

- Seguridad de la tecnología operativa (OT Security): Son practicas tecnológicas para el desarrollo de planes de ciberseguridad de las industrias, pruebas de penetración y entre otros. Esto con la finalidad de proteger los activos de tecnología operativa como sistemas industriales, las redes, infraestructuras críticas (centrales eléctricas, redes de transporte, etc.) de amenazas y ataques cibernéticos (Telefónica Tech, 2020).
- Gestión de acceso a la identidad (Identity Access Management): Consiste en gestionar los accesos o credenciales de los usuarios a la infraestructura de red y a la nube de una empresa. Esto, mediante la generación de cifrado y autenticación que es diferente para cada usuario, lo cual ofrece seguridad en el uso de los sistemas operativos, ya que reduce riesgos de suplantación de identidad y ataques cibernéticos de agentes externos a la empresa (Telefónica Tech, 2020).

La ausencia del estándar ISO 27001 o una implementación inadecuada de este en empresas que brindan servicios de tecnología de información pertenecientes a la CIIU 6209 amplía las brechas en la protección de los datos de los clientes causando daños a su reputación como marca, ya que genera desconfianza en el mercado y representa una desventaja frente a la competencia. Esto impacta negativamente en el desenvolvimiento operativo de la empresa porque es posible que haya pérdida de clientes o de un mercado importante, problemas legales desfavorables a la empresa y pérdida de personal clave que se marche a la competencia, los cuales afectan directamente en la reducción del nivel de ventas e incremento en la estructura de costos y gastos (principalmente por el encarecimiento de la planilla de especialistas calificados). En términos de indicadores, el ratio de liquidez y rentabilidad se verían perjudicados, ya que a consecuencia de menores ventas y aumento de

gastos, el resultado del ejercicio fuera pérdida, esto conllevaría a que los inversionistas obtengan un retorno negativo de su inversión. Asimismo, incumplimiento de los compromisos de corto plazo debido a la incapacidad de obtención de recursos dentro del curso normal de las operaciones. Por lo antes mencionado, nuestro interés es investigar el impacto de la ISO 27001 en la evaluación del principio de negocio en marcha, puesto que de acuerdo con el artículo 407° numeral 4 de la Ley General de Sociedades, una causal de disolución son las pérdidas que disminuyan el patrimonio neto a una cuantía inferior a la tercera parte del capital pagado, salvo que sean regularizadas o que el capital pagado sea aumentado o reducido en cuantía suficiente (El Peruano, 2020).

2.2 Formulación del problema

2.2.1 Problema general

¿Cómo impacta la ISO 27001: Seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021?

2.2.2 Problemas específicos

¿Cómo el sistema de gestión de seguridad de la información impacta en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021?

¿Cómo la ciberseguridad impacta en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021?

¿Cómo los ciberataques impactan en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021?

2.3 Justificación y Relevancia

2.3.1 Justificación teórica

Esta investigación tiene su justificación teórica al presentar información bibliográfica relacionada a las variables ISO 27001: Seguridad de la información y principio de negocio en marcha, pues son fuentes académicas reconocidas que están dentro del ranking de cuartiles de las mejores investigaciones, así como de especialistas sobre el tema. Estas fuentes facilitarán la elaboración de un marco teórico y trabajo firme que ayudará a incentivar nuevos estudios acerca de la ISO 27001: Seguridad de la información en el sector tecnología.

Este estudio buscará aportar información de temas relacionados a la Norma ISO 27001 que favorezcan el entendimiento sobre la importancia de implementar esta ISO a nivel empresarial. Asimismo, exponer el interés de los altos niveles administrativos por gestionar una cultura de información dentro de su organización que garantice la seguridad y la protección de los activos y sus usuarios a través de buenas prácticas como la ciberseguridad (Culot et al., 2021).

Asimismo, se manifestarán los riesgos potenciales que enfrentan las empresas dedicadas a “Otras actividades de tecnología de la información y de servicios informáticos”, entre las cuales se encuentran los servicios de seguridad en la nube (Cloud Security), seguridad de la red (Network Security), protección de datos (Data Protection), seguridad de las cosas (IoT Security) y gestión de acceso a la identidad (Identity Access Management), los cuales se encuentran agrupados dentro del servicio de seguridad de la información (Telefónica Tech, 2020). Asimismo, las empresas de este sector se encuentran expuestas ante las tecnologías emergentes como la vulneración de la información frente a los ciberataques, los cuales generan posibles efectos negativos en la continuidad del negocio. Esto a fin de

evidenciar la importancia de implementar un sistema de gestión de seguridad de la información.

Finalmente, en esta investigación se expondrán los factores requeridos por la NIA 570 “Empresa en funcionamiento” para evaluar el principio de negocio en marcha para empresas que prestan servicios de seguridad de la información en base a factores financieros y operativos. Los factores financieros comprenden los ratios de liquidez y ratios de rentabilidad, debido a su importancia de mantener un adecuado estado financiero. Mientras que los factores operativos guardan relación con la evaluación de pérdida de personal clave, pérdida de clientes o porción de mercado, dependencia significativa de un cliente en especial y contingencias legales desfavorables a la Compañía.

2.3.2 Justificación práctica

La presente investigación sostiene como justificación práctica acerca de la implementación de la ISO 27001: Seguridad de la información. Esto como consecuencia del crecimiento de los ciberataques tanto en empresas grandes como pequeñas, ya que la industria 4.0 (internet industrial) se actualiza constantemente respecto a la virtualización en relación de interconexión, integración de programas, conectividad y entre otros. No obstante, esta digitalización incrementa la vulnerabilidad de las compañías ante los ataques virtuales. Asimismo, esta es una problemática a nivel mundial, por ejemplo, en el 2014, una planta industrial alemana de acero sufrió un ataque cibernético, lograron infiltrarse en sus sistemas para manipular los componentes de control, lo cual generó graves problemas en el horno. Seguidamente, el 48% de los fabricantes del Reino Unido han afrontado ciberataques y el 50% de estas compañías sufrieron grandes pérdidas económicas o tuvieron que parar la marcha de su negocio como consecuencia de lo antes mencionado (Ayerbe, 2018).

Los sectores más vulnerados a nivel mundial son los servicios profesionales, entre los cuales se encuentran las auditoras, consultoras, contadores con un 30%, empresas del sector tecnología con 14%, manufacturas e industrias con 14% y bancos con 8% según el reporte de Chubb (El Comercio, 2021). Asimismo, Perú se encuentra entre los cinco países de Latinoamérica que más ciberataques ha sufrido según Check Point Software Technologies. Seguidamente, Perú se encuentra este 2021 en el tercer lugar de los países más afectados por ciberataques en Latinoamérica respecto a las empresas y en el noveno lugar del mundo por el mismo concepto según revela ESET (Enjoy Safer Technology) (El Comercio, 2021). Asimismo, podemos concluir que Perú al encontrarse entre los países más afectados por ciberataques, el sector de seguridad de la información no hace el frente necesario para salvaguardar la información de sus clientes y así mitigar el impacto de estos ataques. Seguidamente, se hizo público que se filtraron y se vendieron a través de redes sociales los datos personales de los ciudadanos que son administrados por entidades del sector público en Perú, lo cual genera un riesgo para las transacciones seguras. Esto fue denunciado por La Asociación de Bancos (Asbanc) (Gestión, 2022).

La presente investigación ayudará al sector en estudio a comprender la relación existente entre el estándar ISO 27001 y el principio contable de empresa en marcha y el impacto en las empresas que brindan servicios tecnológicos en base a la evaluación de los hechos o condiciones descritos en la NIA 570 “Empresa en Funcionamiento” (pérdida de clientes o de un mercado importante, problemas legales desfavorables a la empresa, pérdida de personal clave y ratios financieros), a fin de prevenir posibles escenarios económicos ante la vulnerabilidad de la información por la situación latente de los ataques cibernéticos.

2.4 Objetivos

2.4.1 Objetivo general

Determinar cómo impacta la ISO 27001: Seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro.

2.4.2 Objetivos específicos

OE1 Determinar cómo impacta el sistema de gestión de seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

OE2 Determinar cómo impacta la ciberseguridad en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

OE3 Determinar cómo impactan los ciberataques en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

2.5 Limitaciones y Parámetros

- La presente investigación se delimita solo a empresas ubicadas en el distrito en San Isidro y para ello se ha recabado información del portal de la SUNAT. No obstante, una limitante es que las empresas no colocan el CIIU de acuerdo con su giro de negocio.
- Las referencias bibliográficas que corresponden a investigaciones científicas se han realizado en países europeos no encontrándose dentro de la delimitación espacial del estudio.

- Gran parte de las empresas debido a la incertidumbre económica han optado por no alquilar oficinas, ya que realizan trabajo remoto. Por ello, solo alquilan el domicilio fiscal para efectos tributarios. No obstante, realizan el cambio de domicilio a diferentes distritos y en varios periodos.
- Las entrevistas y encuestas se llevarán a cabo de manera online debido a la situación de pandemia en que nos encontramos en la actualidad. Asimismo, la cantidad de expertos del tema a entrevistar, ya que dependemos de sus disponibilidades de tiempo.

2.6 Hipótesis

2.6.1 Hipótesis general

La ISO 27001: Seguridad de la información impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

2.6.2 Hipótesis específicas

HE1 El sistema de gestión de seguridad de la información impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

HE2 La ciberseguridad impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

HE3 Los ciberataques impactan negativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

CAPÍTULO III: METODOLOGÍA DE INVESTIGACIÓN

3.1 Operacionalización de las variables

- **Variable independiente**

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores/ITEMS	Nivel de Rangos
Variable Independiente ISO 27001: Seguridad de la información	La ISO 27001 es una de los principales estándares de la familia ISO 27000 a nivel mundial, la cual señala los requisitos para establecer, implementar, ejecutar, monitorear, verificar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, a través de un modelo de mejora continua conocido como PDCA.	Será medido a través de encuestas a los profesionales de tecnología de la información con experiencia igual o mayor a tres años que cuenten con conocimientos básicos acerca de la norma ISO 27001, así como entrevistas a profundidad a especialistas contables con cargo senior a más con experiencia en el sector tecnología.	Sistema de gestión de seguridad de la información	1. Un sistema de gestión de seguridad de la información implementado de acuerdo con el estándar ISO 27001 garantiza la protección de los recursos de información administrados por una entidad.	1. Totalmente en desacuerdo 2. En desacuerdo 3. Ni de acuerdo ni en desacuerdo 4. De acuerdo 5. Totalmente de acuerdo
				2. La certificación ISO 27001 genera un impacto positivo en la mente de los clientes, potenciales clientes y partes interesadas, dado que proyecta protección, confidencialidad y seguridad en el uso de la información que se almacena como parte del proceso operativo del negocio.	
				3. Una de las ventajas competitivas del sistema de gestión de seguridad de la información es la mejor gestión económica en la inversión de la mejora continua de la seguridad de la información.	
				4. Conseguir concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y directivos es decisivo para garantizar la continuidad del negocio.	
				5. Una implementación eficiente y eficaz de la ISO 27001 mitiga riesgos potenciales asociados a la adaptación de tecnologías emergentes relacionados a la digitalización de procesos a nivel organizacional.	
				6. La ISO 27001 sirve para estructurar procesos dentro de una organización para asegurar la continuidad del negocio previniendo especialmente ataques cibernéticos que afectan las funciones de las entidades.	
			Ciberseguridad	7. La adopción de políticas sobre la ciberseguridad representa una ventaja competitiva en el mercado.	
				8. La ciberseguridad es importante en relación con la infraestructura tecnológica, ya que evidencia la capacidad con la que cuenta una entidad para proteger la información privada de los clientes ante un competidor.	
				9. La ciberseguridad aborda políticas de gestión de peligros cibernéticos para mitigar alguna contingencia cibernética y resguardar la continuidad del negocio.	
				10. El ciberespacio es un escenario donde se han producido oportunidades y a la vez conflictos producto del desarrollo constante de las comunicaciones y tecnologías de la información, por lo cual es importante tomar medidas como la ciberseguridad.	
			Ciberataques	11. Los ciberataques violan las políticas de seguridad de un activo cibernético para dañar e interrumpir el acceso de la información o servicios de dicho activo generando pérdidas económicas.	
				12. La ejecución de escenarios realistas sirven para localizar y afrontar vulnerabilidades en la infraestructura de red.	

- **Variable dependiente**

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores/ITEMS	Nivel de Rangos
Variable dependiente: Principio de negocio en marcha	Es un supuesto de que la entidad continuará sus operaciones en un futuro previsible	Será medido a través de encuestas a los profesionales de tecnología de la información con experiencia igual o mayor a tres años que cuenten con conocimientos básicos acerca de la norma ISO 27001, así como entrevistas a profundidad a especialistas contables con cargo senior a más con experiencia en el sector tecnología.	Situación financiera	13. Los indicadores financieros de la empresa son importantes porque miden la situación financiera de la misma.	1. Totalmente en desacuerdo 2. En desacuerdo 3. Ni de acuerdo ni en desacuerdo 4. De acuerdo 5. Totalmente de acuerdo
				14. Los principales indicadores a considerar para mantener un adecuado estado financiero para las empresas son: liquidez, rentabilidad y solvencia.	
				15. Los ratios son indicadores que se calculan de los estados financieros que permiten evaluar posibles riesgos económicos y tomar decisiones para mitigar dichos riesgos.	
				16. Los ratios de rentabilidad permiten evaluar la capacidad de la empresa en generar ganancias con una mínima inversión.	
				17. Los ratios de rentabilidad y liquidez guardan relación entre sí porque son importantes para los acreedores, ya que indican la capacidad que posee la compañía para afrontar sus obligaciones a corto y mediano plazo.	
			Situación Operativa	18. Las entidades con pérdidas netas en periodos consecutivos podrían generar patrimonio negativo, lo cual conllevaría a ser una causal de disolución.	
				19. La situación operativa se evalúa en función de los riesgos operativos del entorno de la empresa.	
				20. La escasez de personal especializado en el sector TI influye en la situación operativa de la empresa.	
				21. El déficit de profesionales en el sector TI encarece el servicio y a su vez retrasa la puesta en marcha de los proyectos.	
				22. Las compañías buscan profesionales de TI con perfiles híbridos como habilidades blandas y habilidades técnicas.	
				23. El perfil del personal encargado de TI es muy importante, ya que dentro de este sector se encuentra el área de fraude, quien se encarga de monitorear el cumplimiento de las políticas internas y externas de las compañías.	

3.2 Diseño metodológico

3.2.1 Alcance de investigación

Según Hernández y Mendoza (2018) los estudios explicativos aportan un sentido de comprensión sobre las variables de estudio, ya que procuran responder por qué ocurren los hechos y de qué manera se manifiestan. El alcance de este estudio es explicativo porque busca analizar los efectos de la ISO 27001: Seguridad de la información en el Principio de negocio en marcha.

3.2.2 Diseño de Investigación

Según Tafur e Izaguirre (2015), en el estudio de diseño no experimental no se ejerce dominio sobre las variables. Asimismo, los autores Hernández y Mendoza (2018), afirman que en una investigación no experimental no se preparan situaciones o contextos que permiten al investigador manipular a la variable independiente para analizar los efectos en las demás variables, sino que solo se observa la realidad existente de las variables sin intervenir en ellas. Este trabajo tiene un diseño no experimental porque no se manipularán las variables de investigación.

El tipo de diseño no experimental es transversal porque el recojo de la información se dará en un único momento, es decir, en el 2021. Además, tiene un enfoque mixto porque integra el análisis del enfoque cuantitativo y cualitativo, a fin de obtener evidencias de diferentes naturalezas que permiten entender el objeto de la investigación (Hernández & Mendoza, 2018).

3.2.3 Enfoque de investigación

Son rutas alternas que conllevan a un objetivo, los cuales podrían ser entender el porqué de un hecho, responder a cuestiones de investigación, entre otros. En otras palabras, la finalidad es la investigación de un problema planteado

El enfoque cuantitativo es idóneo cuando se desea evaluar la dimensión de los fenómenos y confirmar la posibilidad de un hecho. Esto, a través del proceso de planteamiento del problema, la construcción del marco teórico que conlleva a la formulación de hipótesis para luego analizar con procedimientos estadísticos la recolección de datos (Hernández & Mendoza, 2018).

El enfoque cualitativo se traslada de lo particular a lo general. Asimismo, se basa en entrevistas para luego analizar las respuestas de las experiencias de los entrevistados en relación con el planteamiento del problema y de esta manera así generar conclusiones. Este proceso se repetirá con más entrevistas a otras personas. Cabe mencionar que con este enfoque gran parte de las investigaciones no se confirman las hipótesis (Hernández & Mendoza, 2018).

De acuerdo con Hernández y Mendoza (2018), el enfoque mixto es la mezcla del enfoque cuantitativo con el cualitativo, el cual sigue procesos de conjunción, análisis y acopio de los datos de la mezcla de ambos enfoques de la una misma investigación. Esto, con el fin de obtener una figura más completa del problema en estudio.

La metodología para emplear en la presente investigación es enfoque mixto, ya que por el lado cuantitativo aplicaremos encuestas y por la parte cualitativa se realizarán entrevistas a profundidad a expertos en relación con el tema de investigación.

3.3 Investigación cualitativa

La investigación cualitativa permite entender un problema a través de experiencias, percepciones y cualidades de un grupo de personas (Tafur e Izaguirre, 2015). Con esta metodología se puede recolectar información a través de entrevistas, observación y focus group.

3.3.1 Instrumento de recolección de datos

Se realizaron entrevistas a profundidad compuestas por 16 preguntas abiertas dirigidas a profesionales expertos de contabilidad, finanzas y TI sobre el tema de investigación y con conocimientos del sector, que ayudaron a conocer las distintas opiniones de los expertos sobre el tema de investigación. Esto se llevó a cabo mediante una conversación de manera online y siguiendo una guía de entrevista, debido a la situación de pandemia que vivimos actualmente.

3.3.2 Población

La población está conformada por profesionales expertos de contabilidad, finanzas y TI con conocimientos sobre el tema de investigación.

3.3.3 Muestra

Para la muestra se ha seleccionado a los siguientes especialistas que se detallan en la Tabla 5:

Tabla 5

Muestra de especialistas entrevistados

Nombre	Cargo	Área	Empresa
Ronnie Montoro Zevallos	Gerente	Finanzas	Telefónica Ingeniería de Seguridad Perú S.A.C
Marie Ann Chumbimuni	Data Governance	TI	Banco de Crédito del

Presentación	Advanced		Perú
Alex Saldaña Cotrina	Senior	Auditoria financiera	BDO Perú

Nota. Tabla de especialistas entrevistados. Elaboración propia

3.4 Investigación cuantitativa

Según Tafur e Izaguirre (2015), el enfoque cuantitativo permite medir las variables en cantidades siendo la encuesta la herramienta más usada que se basa en un grupo de preguntas elaboradas de acuerdo con las variables y sus dimensiones. Esta herramienta es útil porque facilita recolectar información sobre las percepciones de los expertos acerca de las variables de estudio y analizar los resultados, a fin de validar las hipótesis de la presente investigación. El tipo de investigación es aplicada por sus objetivos extrínsecos, ya que busca resolver las interrogantes a las variables de estudio (Hernández & Mendoza, 2018).

3.4.1 Instrumento de recolección de datos

En la recolección de datos cuantitativos se emplean herramientas de medición con el objetico de recolectar información de las variables del fenómeno a investigar con el número de la muestra. Asimismo, las herramientas a utilizar van de uno a más para recaudar información adecuada. Seguidamente, para la recolección de información se debe realizar un plan minucioso con los pasos a seguir y entre los cuales se encuentra determinar cuáles serán las fuentes para obtener los datos, en dónde encontraremos dicha información, mediante qué herramienta y cómo se va a medir para ser analizados con la finalidad de responder al planteamiento del problema (Hernández & Mendoza, 2018).

Hernández y Mendoza (2018), mencionan que los principales requisitos para recabar información cuantitativa es la imparcialidad, autenticidad y la fiabilidad del o los instrumentos seleccionados. Asimismo, manifiestan que existen tres cuestiones esenciales

para el procedimiento de medición, entre los cuales se encuentra la operacionalización, la codificación y el establecer los niveles de medición. El primero, se basa en la definición de la variable para luego seguir con sus dimensiones, indicadores e ítems. El segundo, consta en establecer un valor aritmético a los ítems de cada categoría. Finalmente, el tercero cuenta con cuatro niveles de medición, los cuales son nivel nominal, ordinal, por intervalos y de razón.

Posterior a lo antes mencionado, se determina que uno de los instrumentos más utilizados para recabar datos de las variables son las encuestas. Por ello, se determina que el procedimiento idóneo para la presente investigación es realizar encuestas (Hernández & Mendoza, 2018).

El objetivo de la encuesta es determinar cómo impacta la ISO 27001: Seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro.

3.4.2 Población

La población comprende a empresas del sector de Tecnología de la Información (TI) en San Isidro, 2021. Se extrajo del portal de la Superintendencia Nacional de Aduanas y Administración Tributaria (SUNAT) la relación de agentes de retención de IGV que comprende un total de 3,771 empresas a nivel nacional. Seguidamente, se recabó la información del total de empresas mediante la página web de consultas múltiples de RUC de la SUNAT, luego se delimitó de acuerdo con las empresas que se encuentran en el distrito de San Isidro y por la CIIU de la división 62, programación informática, consultoría de informática y actividades conexas.

- Clase 6201: programación informática.

- Clase 6202: consultoría de informática y de gestión de instalaciones informáticas.
- Clase 6209: otras actividades de tecnología de la información y de servicios informáticos.

En la presente investigación se seleccionó la clase 6209 (otras actividades de tecnología de la información y de servicios informáticos) así como se obtuvieron 15 empresas del sector en mención, las cuales se detallan en la Tabla 6.

Tabla 6

Población de empresas del sector otras actividades de tecnología de la información y de servicios informáticos en San Isidro

N°	Razón social	Ruc	Distrito
1	Accenture Perú S.R.L.	20520102508	San Isidro
2	Adexus Perú SA	20261898706	San Isidro
3	Corporacion Sapia S.A.	20100083362	San Isidro
4	Dataimagenes S.A.C.	20518240839	San Isidro
5	Desca Perú S.A.C.	20517831582	San Isidro
6	Everis Perú S.A.C.	20521586134	San Isidro
7	Grupo Sypsa S.A.C.	20466261255	San Isidro
8	Indra Perú S.A.	20100123411	San Isidro
9	Inversiones Ancona S.A.C.	20167795120	San Isidro
10	Logicalis Andina S.A.C.	20513610166	San Isidro
11	Miatech International S.A.C.	20470033186	San Isidro
12	N.C.R. del Perú S.A.C.	20100128137	San Isidro
13	Telefonica Ingenieria de Seguridad Perú S.A.C	20459151584	San Isidro
14	Sonda del Perú S.A.	20383773378	San Isidro
15	Telefónica Cybersecurity & Cloud Tech Perú S.A.C.	20606139757	San Isidro

Nota: Se muestra la población de empresas del sector otras actividades de tecnología de la información y de servicios informáticos en San Isidro.

Para llevar a cabo las encuestas y entrevistas, se seleccionará a dos colaboradores de alto mando por empresa obteniendo una población de 30 colaboradores.

3.4.3 Muestra

$$n = \frac{Z^2 * pq * N}{E^2(N-1) + Z^2 * pq}$$

Concepto de cada variable:

n = muestra

Z = nivel de confianza

p = probabilidad de éxito

q = probabilidad de fracaso (p-1)

E = nivel de error

N = población

Valores para la determinación de la muestra en la Tabla 7:

Tabla 7

Determinación del tamaño de la muestra

Parámetro	Insertar valor
N	30
Z	1.96
p	0.5
q	0.5
E	5%
n	28

Nota: Se presenta el tamaño de la muestra cuantitativa a considerar en la investigación.

Luego del cálculo se obtuvo una muestra de 28 encuestas con un nivel de confianza del 95%, las cuales se realizarán a colaboradores que trabajan en empresas del sector Informática y Actividades Conexas en San Isidro.

CAPÍTULO IV: DESARROLLO DE LA INVESTIGACIÓN

Luego de explicar los objetivos de la presente investigación y después de a ver determinado las herramientas de recolección y el tamaño de la muestra cualitativa y cuantitativa. Continuamos con la aplicación de estos con la finalidad de determinar el impacto de la ISO 27001: Seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

4.1 Desarrollo de la entrevista en profundidad

Entrevista 1:

Nombre del entrevistado: Ronnie Montoro Zevallos

Cargo: Gerente de Finanzas y Control

Empresa: Telefónica Ingeniería de Seguridad

ISO 27001

1. **¿Cuál es su opinión con respecto al estándar ISO 27001?**

   Es una herramienta necesaria para proteger la información en estos tiempos actuales donde nos movemos en un entorno tecnológico/informático.

2. **¿Qué opina del principio contable de negocio en marcha de las empresas?**

   Estoy de acuerdo con el principio, ya que una empresa debe ser liquidada solo en el caso de que se pruebe insolvencia en mediano y largo plazo.

3. **Respecto al estándar ISO 27001, ¿Considera que este podría tener algún impacto en el principio contable de la empresa en marcha?**

   Sí, ya que creo que van de la mano. La estandarización que brinda la ISO 27001 debe ser una herramienta que los directivos de la empresa deben usar para asegurar la continuidad de la empresa.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4. **¿Cómo considera que influye la implementación de un sistema de gestión de seguridad de la información conocido también como SGSI en el uso diario de la información que almacena una entidad como parte de su proceso operativo?**

   Definitivamente en un principio va a generar carga operativa, pero esto traerá un impacto positivo en el flujo de la información de la empresa. Asimismo, este impacto debería ser de corto/mediano plazo.

5. **¿Cuáles son las situaciones más comunes por la que las empresas peruanas que prestan servicios tecnológicos requieren de la implementación de un SGSI de acuerdo con el estándar ISO 27001?**

   Disminuir riesgos de perdida de información, lograr eficiencias operativas y económicas como la protección de su información.

6. **En base a su experiencia, ¿Considera que la concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y alta dirección de una entidad es decisiva para garantizar la continuidad del negocio?**

   Definitivamente sí, ya que de esta manera los colaboradores podrán entender el por qué es importante cumplir con las políticas de seguridad de la entidad, ya que su correcta aplicación es uno de los factores importantes para asegurar la continuidad del negocio.

CIBERSEGURIDAD

7. **¿Cuál considera usted que es el objetivo de la ciberseguridad?**

   Protección de la infraestructura computacional de una empresa. Sus redes, las PCs de los trabajadores, etc.

8. **¿Cómo considera que influye la ciberseguridad en la protección de la información privada de los usuarios de una entidad?**

   Tiene mucha influencia positiva porque nos enseña y nos permite cuidar adecuadamente la información de la empresa.

9. **¿Usted cómo considera que la adopción de políticas sobre la ciberseguridad impacta en la perspectiva de los clientes de la empresa de tecnología?**

   Tiene un impacto positivo alto, ya que el cliente se sentirá más seguro al saber que la empresa posee un buen sistema de Ciberseguridad.

CIBERATAQUES

10. **¿Cuál considera usted que es el objetivo de los ciberataques a las empresas?**

    Robo de información sensible para que la puedan usar para temas delictivos que le generen beneficios económicos a costa de ello.

11. **¿Considera usted que no estar preparados ante los ciberataques genera incertidumbre en el negocio en marcha?**

    Por supuesto que sí, ya que la información sensible podría estar expuesta al robo informático, el cual afectaría directamente a la empresa mediante pérdidas económicas.

SITUACIÓN FINANCIERA – RATIOS

12. **¿Cuál considera usted que es el propósito de la aplicación de ratios financieros en las compañías?**

    El Control económico y financiero de la empresa. Asimismo, generar conocimiento y a la vez seguridad a los accionistas de que las cosas se están haciendo bien en la compañía.

SITUACIÓN OPERATIVA

13. **¿Usted cómo considera que el entorno de la empresa influye en la situación operativa de la misma? ¿por qué?**

    El entorno es una variable que influye directamente en la situación de la empresa. EL país, los clientes, la situación política y económica de la región/país hasta internacional influyen en la situación operativa de una empresa. Nos movemos en un entorno sumamente globalizado actualmente.

14. **¿Considera que la escasez de personal calificado genera incertidumbre en la continuidad de las operaciones de una empresa? ¿por qué?**

    Por supuesto que sí, ya que finalmente son las personas las que hacen la diferencia en una empresa. El no contar con personas idóneas para ciertos puestos, traerá para la empresa tarde o temprano alguna problemática operativa.

15. **¿Cree usted que la escasez de personal especializado en el rubro de la empresa impacta en la situación operativa de la misma? ¿por qué?**

    Pienso que sí, tal vez en un corto o mediano plazo, la empresa pueda manejarse sin contar con personal especializado según lo requiera, pero mantengo mi posición que tarde o temprano esto se empezará a notar en la empresa; y si bien no se generen problemas operativos mayores, la empresa no estará maximizando su potencial operativo el cual podría alcanzar.

16. **¿Está de acuerdo que en la actualidad las compañías busquen perfiles de personal que contengan habilidades blandas y habilidades técnicas? ¿por qué?**

    Por supuesto que sí, un profesional actualmente debe contar con estas dos habilidades. En una empresa no solo se gestiona procesos, números y/o maquinas. Se gestionan personas, y para poder relacionarse con sus colaboradores y llevar un adecuado entorno de trabajo entre jefe/colaborador, el primero debe tener habilidades que le permita cumplir con este ideal.

Entrevista 2:

Nombre del entrevistado: Marie Ann Chumbimuni Presentación

Cargo: Data Governance Advanced

Empresa: Banco de Crédito del Perú

ISO 27001

1. **¿Cuál es su opinión con respecto al estándar ISO 27001?**

   Es un estándar de seguridad de información necesario en las empresas que desean proteger su información.

2. **¿Qué opina del principio contable de negocio en marcha de las empresas?**

Considero que es importante para evaluar la situación de la compañía y su continuidad en el tiempo.

3. **Respecto al estándar ISO 27001, ¿Considera que este podría tener algún impacto en el principio contable de la empresa en marcha?**

   Definitivamente sí porque la contabilidad gestiona información financiera y considero que aplicar la ISO 27001 tendría un impacto positivo.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4. **¿Cómo considera que influye la implementación de un sistema de gestión de seguridad de la información conocido también como SGSI en el uso diario de la información que almacena una entidad como parte de su proceso operativo?**

   Considero que implementar un SGSI influiría beneficiosamente en los procesos de una empresa porque ayuda en la mejora continua de los mismos ya que recopila la información tratada por las áreas ya sea desde el almacenamiento en papeles, de forma digital y entre otros.

5. **¿Cuáles son las situaciones más comunes por la que las empresas peruanas que prestan servicios tecnológicos requieren de la implementación de un SGSI de acuerdo con el estándar ISO 27001?**

   Lo requieren principalmente para auditorías internas y externas. Asimismo, minimiza el riesgo ante ataques cibernéticos cuya finalidad es el robo de información.

6. **En base a su experiencia, ¿Considera que la concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y alta dirección de una entidad es decisiva para garantizar la continuidad del negocio?**

   Considero que sí es necesario que desde la alta dirección se concientice que es importante la seguridad de la información, ya que es un trabajo entre todas las áreas

como un solo equipo, ya que varios creen que solo es el trabajo del área de TI de la empresa.

CIBERSEGURIDAD

7. **¿Cuál considera usted que es el objetivo de la ciberseguridad?**

   Proteger la información informática ante ataques cibernéticos. Esto con la finalidad de salvaguardar la continuidad del negocio, ya que afecta la productividad de la compañía.

8. **¿Cómo considera que influye la ciberseguridad en la protección de la información privada de los usuarios de una entidad?**

   Influye favorablemente porque permite prevenir ataques externos por robo de información que es confidencial de los clientes, quienes asimismo confían en que la compañía va a salvaguardar dicha información y no se verá vulnerada ni expuesta.

9. **¿Usted cómo considera que la adopción de políticas sobre la ciberseguridad impacta en la perspectiva de los clientes de la empresa de tecnología?**

   Considero que los clientes sentirían más confianza y seguridad de trabajar con la empresa, ya que es una garantía de que los procesos que sigue la empresa son transparentes y que los controles que manejan mantendrá la integridad de sus datos.

CIBERATAQUES

10. **¿Cuál considera usted que es el objetivo de los ciberataques a las empresas?**

    Obtener la información que almacena la compañía en los diferentes medios tecnológicos con la finalidad de interrumpir los procesos con el fin de beneficiarse económicamente.

11. **¿Considera usted que no estar preparados ante los ciberataques genera incertidumbre en el negocio en marcha?**

Considero que sí porque al no estar preparados ante los ciberataques, esto habilita vulnerabilidades y riesgos económicos. Por ende, afectaría en la continuidad del negocio.

SITUACIÓN FINANCIERA – RATIOS

12. **¿Cuál considera usted que es el propósito de la aplicación de ratios financieros en las compañías?**

    Considero que el propósito es evaluar la situación financiera de la compañía en base a un análisis mediante los ratios que muestran los resultados de la empresa.

SITUACIÓN OPERATIVA

13. **¿Usted cómo considera que el entorno de la empresa influye en la situación operativa de la misma? ¿por qué?**

    Desde mi punto de vista, considero que afecta de forma directa porque si no hay un buen entorno esto afecta en la percepción de los clientes, personal de la empresa, proveedores, inversores y entre otros.

14. **¿Considera que la escasez de personal calificado genera incertidumbre en la continuidad de las operaciones de una empresa? ¿por qué?**

    Sí porque la empresa debería tener al menos algunos especialistas que permitan guiar efectivamente los procesos operativos para que esto no afecte negativamente la continuidad de la empresa.

15. **¿Cree usted que la escasez de personal especializado en el rubro de la empresa impacta en la situación operativa de la misma? ¿por qué?**

    Por supuesto que sí, porque la empresa debe poder tomar decisiones correctas en actividades de su rubro con el apoyo del personal calificado de su empresa.

16. **¿Está de acuerdo que en la actualidad las compañías busquen perfiles de personal que contengan habilidades blandas y habilidades técnicas? ¿por qué?**

    Sí, pienso que las empresas entienden que en la actualidad hay necesidad de contar con personal con equilibrio en habilidades, ya que la idea es que puedan hacer línea de carrera y que la ausencia de algunas habilidades no sean el impedimento para crecer dentro de la empresa para que esta no sea obligada a buscar personal externo y así no perder el tiempo en esta búsqueda si se cuenta con el personal calificado.

Entrevista 3:

Nombre del entrevistado: Alex Saldaña Cotrina

Cargo: Senior de auditoria financiera

Empresa: BDO Perú

ISO 27001

1. **¿Cuál es su opinión con respecto al estándar ISO 27001?**

   Es una norma fundamental para el desarrollo de tecnologías emergentes que son empleadas de acuerdo con el funcionamiento de las empresas y del tamaño de las mismas. Como sabemos, las tecnologías emergentes son innovadoras para el mercado, sin embargo, trae consigo riesgos inherentes que podrían impactar negativamente en la rentabilidad de las empresas.

2. **¿Qué opina del principio contable de negocio en marcha de las empresas?**

   El principio de negocio en marcha es un principio esencial, dado que es la base de elaboración y presentación de estados financieros. La Gerencia debe tener el expertis para evaluar este principio de manera periódica y concluir que la Compañía continuará operando durante los doce meses siguientes.

3. **Respecto al estándar ISO 27001, ¿Considera que este podría tener algún impacto en el principio contable de la empresa en marcha?**

   Considero que una implementación adecuada de la norma ISO 27001 contribuye a mitigar riesgos que podrían afectar la continuidad de las operaciones de una Compañía. Por lo tanto, concluyó que el uso del estándar impacta de manera positiva en el principio mencionado.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4. **¿Cómo considera que influye la implementación de un sistema de gestión de seguridad de la información conocido también como SGSI en el uso diario de la información que almacena una entidad como parte de su proceso operativo?**

   Considero que le otorga mayor protección y seguridad a la información que genera y almacena diariamente una Compañía ante un posible ataque cibernético.

5. **¿Cuáles son las situaciones más comunes por la que las empresas peruanas que prestan servicios tecnológicos requieren de la implementación de un SGSI de acuerdo con el estándar ISO 27001?**

   En el Perú, la cultura tecnológica es baja o casi nula. Hoy en día abundan las aplicaciones informáticas que son muy usadas en las empresas. Sin embargo, desconocen que estas aplicaciones o programas de computadora pueden ser vulnerados por ciertas modalidades de robo cibernético, los cuales afectan directamente a la información privada de la empresa y de los clientes.

6. **En base a su experiencia, ¿Considera que la concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y alta dirección de una entidad es decisiva para garantizar la continuidad del negocio?**

El mercado actual exige que las empresas innoven constantemente, ya que los consumidores requieren respuestas rápidas a sus necesidades. Por ende, la simplificación de los procesos operativos es un problema con el cual lidian los altos mandos de una empresa. Para darle solución al problema mencionado, muchos se inclinan por la transformación digital a través de la automatización total o parcial de ciertas áreas operativas. Sin embargo, dejan de lado un paso previo que vendría a ser la elaboración de un plan de acción y políticas sobre como incentivar la cultura tecnológica en las empresas. Esto es ultimo considero que lo mas importante para tener éxito en la gestión de la seguridad de la información.

CIBERSEGURIDAD

7. **¿Cuál considera usted que es el objetivo de la ciberseguridad?**

   Considero que el principal objetivo de la ciberseguridad es proteger la(s) área(s) de mayor riesgo para una empresa.

8. **¿Cómo considera que influye la ciberseguridad en la protección de la información privada de los usuarios de una entidad?**

   Influye positivamente porque reduce los riesgos a posibles ataques o robos cibernéticos y minimiza las pérdidas económicas para las empresas.

9. **¿Usted cómo considera que la adopción de políticas sobre la ciberseguridad impacta en la perspectiva de los clientes de la empresa de tecnología?**

   Sí, porque la implementación de un plan de ciberseguridad en las empresas le otorga seguridad a los clientes y proyecta interés por la protección de sus datos.

CIBERATAQUES

10. **¿Cuál considera usted que es el objetivo de los ciberataques a las empresas?**

    Obtener datos sensibles que otorguen beneficios económicos.

11. **¿Considera usted que no estar preparados ante los ciberataques genera incertidumbre en el negocio en marcha?**

    Claro que sí, un ciberataque dependiendo de la magnitud de los efectos podría acabar con los recursos disponibles de una empresa y con ello, ser causal de disolución.

SITUACIÓN FINANCIERA – RATIOS

12. **¿Cuál considera usted que es el propósito de la aplicación de ratios financieros en las compañías?**

    Son indicadores que permiten conocer y analizar la situación financiera de una empresa para tomar decisiones.

SITUACIÓN OPERATIVA

13. **¿Usted cómo considera que el entorno de la empresa influye en la situación operativa de la misma? ¿por qué?**

    Sí, los factores internos y externos afectan a la empresa y al desarrollo de sus operaciones. Por ejemplo, la pandemia por el Covid-19 afectó negativamente a la estabilidad económica del mundo, el cual produjo el cierre de muchas empresas que hasta el día de hoy siguen afectadas.

14. **¿Considera que la escasez de personal calificado genera incertidumbre en la continuidad de las operaciones de una empresa? ¿por qué?**

    La ausencia de personal capacitado y experto en cierta especialidad dificultará el flujo de las operaciones de una empresa.

15. **¿Cree usted que la escasez de personal especializado en el rubro de la empresa impacta en la situación operativa de la misma? ¿por qué?**

Por supuesto, como les comenté en la respuesta anterior es fundamental contar con profesionales que posean conocimientos específicos en áreas que son importantes para el crecimiento de una empresa.

16. **¿Está de acuerdo que en la actualidad las compañías busquen perfiles de personal que contengan habilidades blandas y habilidades técnicas? ¿por qué?**
    Sí, nos encontramos en un mundo globalizado y muy cambiante, por lo tanto, los profesionales deben contar con habilidades que le permitan tener una comunicación asertiva y formar relaciones sociales.

4.2 Desarrollo de la encuesta

Para la presente investigación se han empleado encuestas, las cuales comprenden 23 preguntas cada una de ellas. Asimismo, se ha aplicado en ellas la escala de Likert con la finalidad de calificar sobre el nivel de acuerdo o desacuerdo con una calificación que contempla un rango de 1 a 5. Seguidamente, las premisas de la encuesta se han elaborado en base a las dimensiones de las variables de la investigación, las cuales son el sistema de gestión de seguridad de la información, ciberseguridad, ciberataques, situación financiera y situación operativa. Cabe mencionar, que las encuestas se aplicaron a profesionales del área de contabilidad, finanzas y de TI que prestan servicios en el sector tecnología.

El instrumento en mención fue aprobado por un experto con el objetivo de demostrar la fiabilidad y validez de las premisas. Asimismo, se ha utilizado el programa de IBM de nombre SPSS Statistics versión 28.0 para efectuar el análisis y revelar los resultados obtenidos de las encuestas. Los resultados que obtuvimos fueron los siguientes:

Resultados de las dimensiones de la variable independiente

Sistema de gestión de seguridad de la información

Resultados de la pregunta 1

P1 Un sistema de gestión de seguridad de la información implementado de acuerdo con el estándar ISO 27001 garantiza la protección de los recursos de información administrados por una entidad.

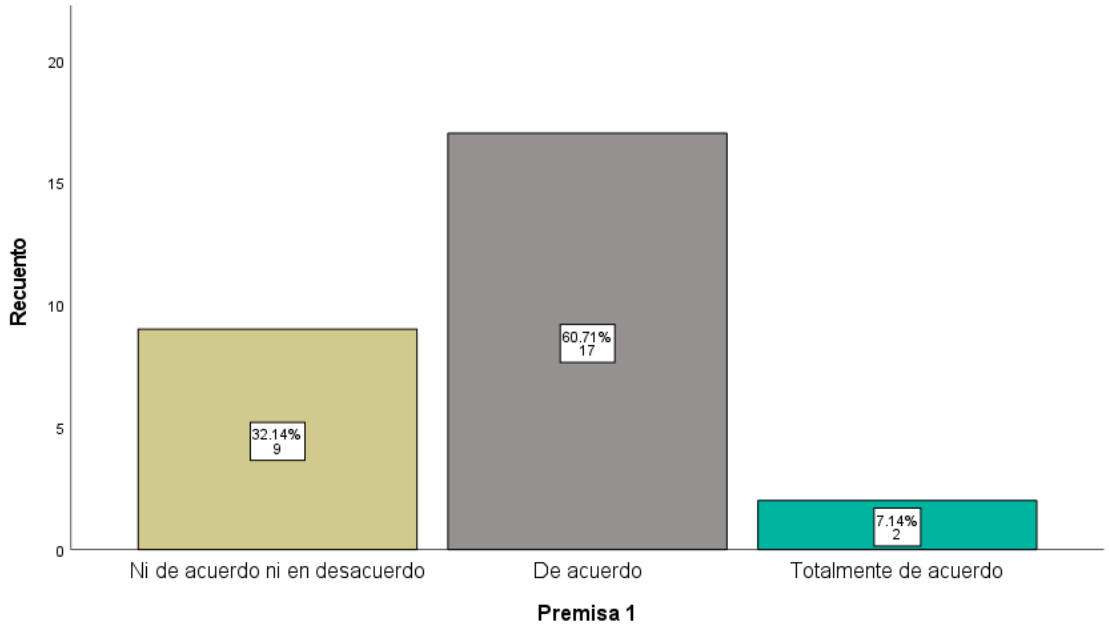

Figura 12. Gráfico sobre los resultados de la premisa 1. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 35.71% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 1, el 57.14% está de acuerdo y un 7.14% está totalmente de acuerdo que el sistema de gestión de seguridad de la información implementado de acuerdo con el estándar ISO 27001 garantiza la protección de los recursos de información administrados por una entidad.

Resultados de la pregunta 2

P2 La certificación ISO 27001 genera un impacto positivo en la mente de los clientes, potenciales clientes y partes interesadas, dado que proyecta protección, confidencialidad y seguridad en el uso de la información que se almacena como parte del proceso operativo del negocio.

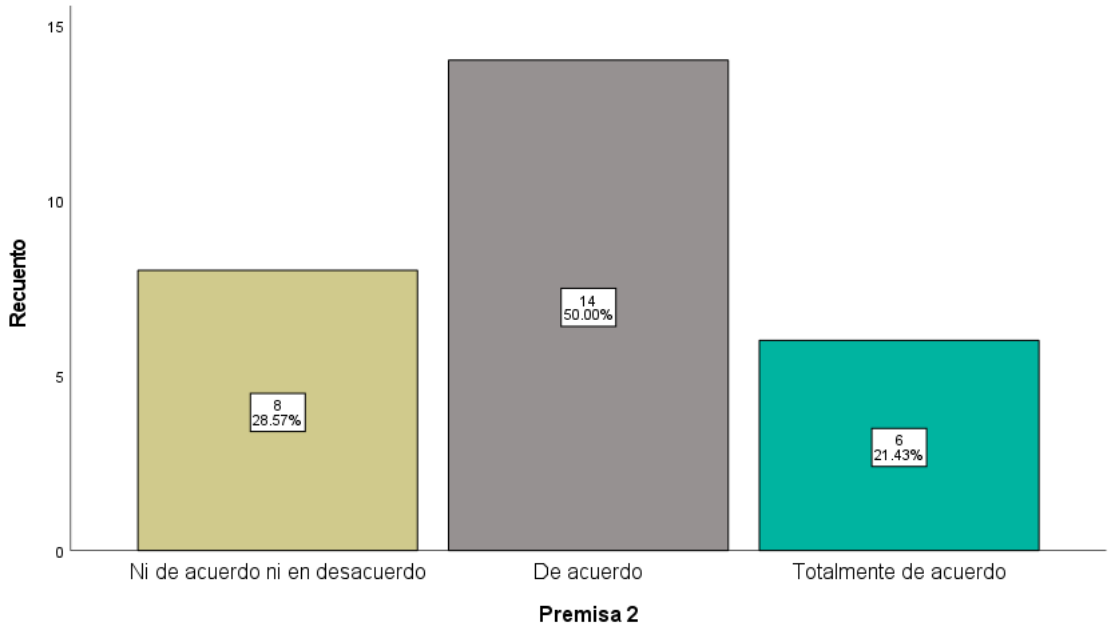

Figura 13. Gráfico sobre los resultados de la premisa 2. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 28.57% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 2, el 50% está de acuerdo y un 21.43% está totalmente de acuerdo que la certificación ISO 27001 genera un impacto positivo en la mente de los clientes, potenciales clientes y partes interesadas, dado que proyecta protección, confidencialidad y seguridad en el uso de la información que se almacena como parte del proceso operativo del negocio.

Resultados de la pregunta 3

P3 Una de las ventajas competitivas del sistema de gestión de seguridad de la información es la mejor gestión económica en la inversión de la mejora continua de la seguridad de la información.

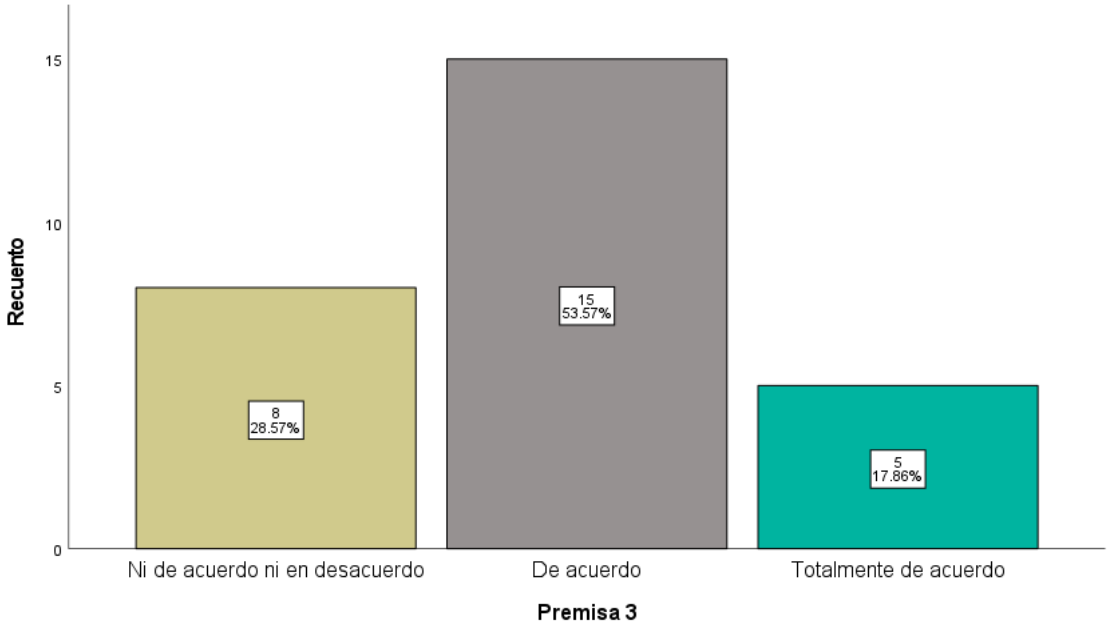

Figura 14. Gráfico sobre los resultados de la premisa 3. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 25% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 3, el 53.57% está de acuerdo y un 21.43% está totalmente de acuerdo que una de las ventajas competitivas del sistema de gestión de seguridad de la información es la mejor gestión económica en la inversión de la mejora continua de la seguridad de la información.

Resultados de la pregunta 4

P4 Conseguir concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y directivos es decisivo para garantizar la continuidad del negocio.

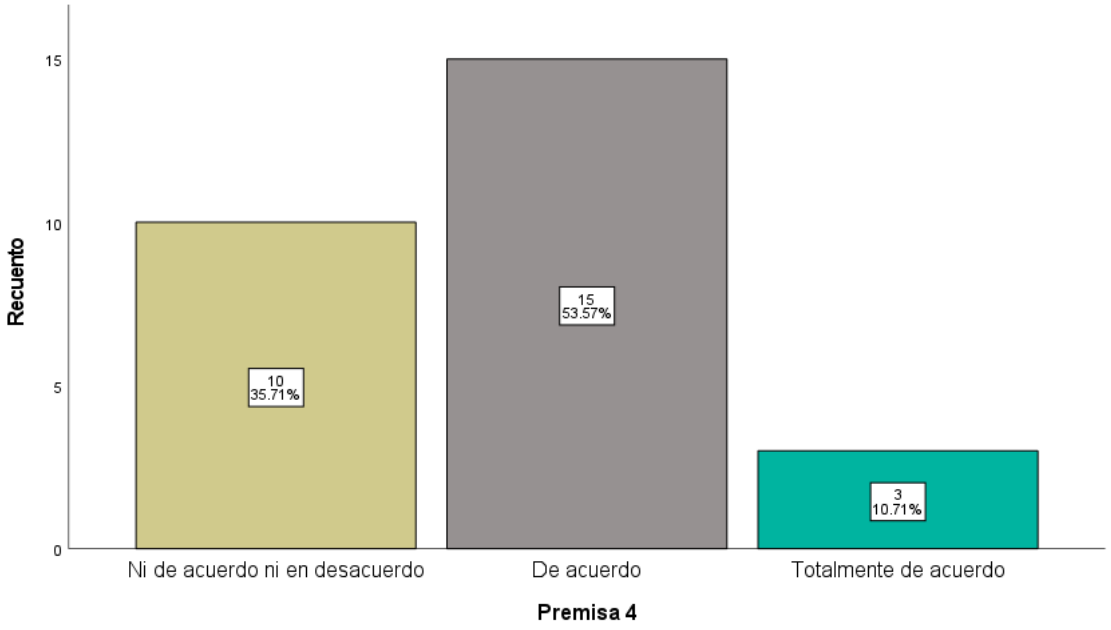

Figura 15. Gráfico sobre los resultados de la premisa 4. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 28.57% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 4, el 60.71% está de acuerdo y un 10.71% está totalmente de acuerdo que conseguir concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y directivos es decisivo para garantizar la continuidad del negocio.

Resultados de la pregunta 5

P5 Una implementación eficiente y eficaz de la ISO 27001 mitiga riesgos potenciales asociados a la adaptación de tecnologías emergentes relacionados a la digitalización de procesos a nivel organizacional.

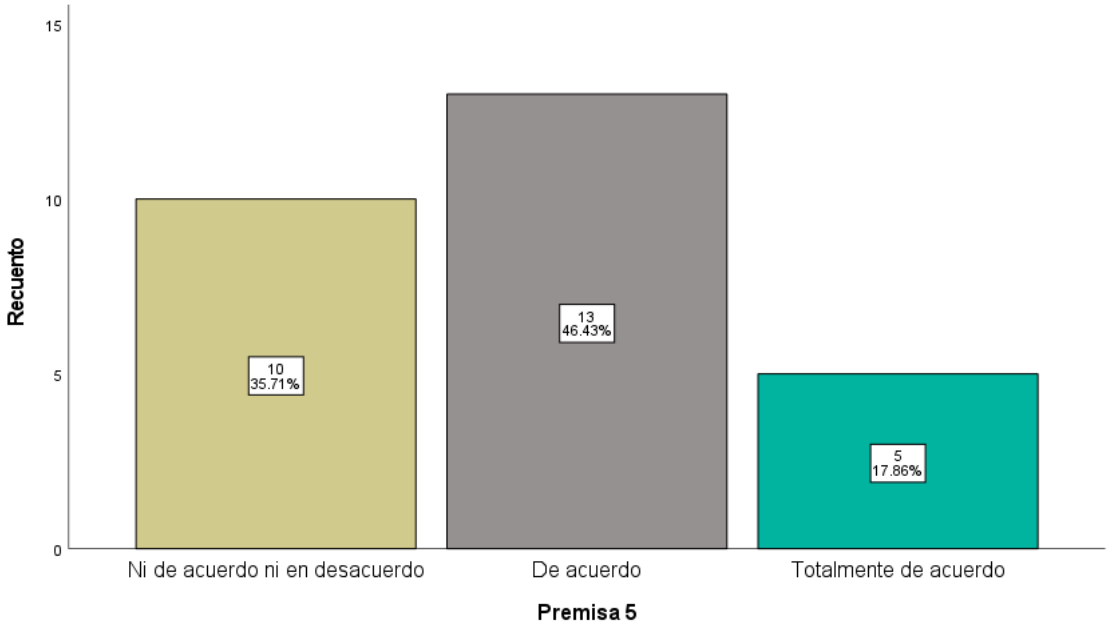

Figura 16. Gráfico sobre los resultados de la premisa 5. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 25% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 5, el 57.14% está de acuerdo y un 17.86% está totalmente de acuerdo que una implementación eficiente y eficaz de la ISO 27001 mitiga riesgos potenciales asociados a la adaptación de tecnologías emergentes relacionados a la digitalización de procesos a nivel organizacional.

Resultados de la pregunta 6

P6 La ISO 27001 sirve para estructurar procesos dentro de una organización para asegurar la continuidad del negocio previniendo especialmente ataques cibernéticos que afectan las funciones de las entidades.

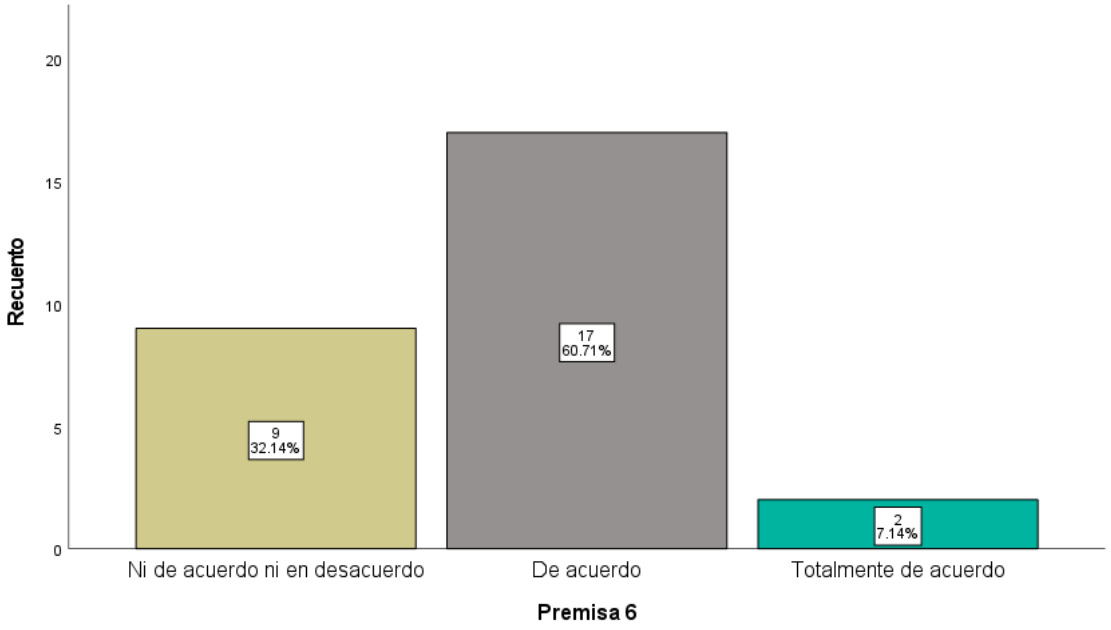

Figura 17. Gráfico sobre los resultados de la premisa 6. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 28.57% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 6, el 64.29% está de acuerdo y un 7.14% está totalmente de acuerdo que la ISO 27001 sirve para estructurar procesos dentro de una organización para asegurar la continuidad del negocio previniendo especialmente ataques cibernéticos que afectan las funciones de las entidades.

Ciberseguridad

Resultados de la pregunta 7

P7 La adopción de políticas sobre la ciberseguridad representa una ventaja competitiva en el mercado.

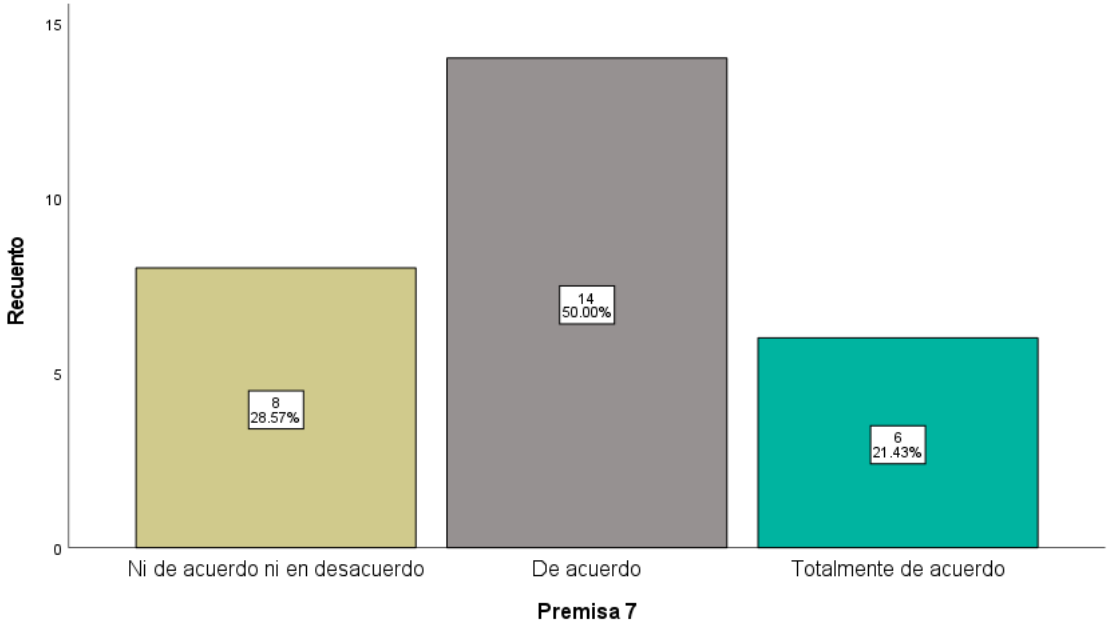

Figura 18. Gráfico sobre los resultados de la premisa 7. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 25% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 7, el 50% está de acuerdo y un 25% está totalmente de acuerdo que la adopción de políticas sobre la ciberseguridad representa una ventaja competitiva en el mercado.

Resultados de la pregunta 8

P8 La ciberseguridad es importante en relación con la infraestructura tecnológica, ya que evidencia la capacidad con la que cuenta una entidad para proteger la información privada de los clientes ante un competidor.

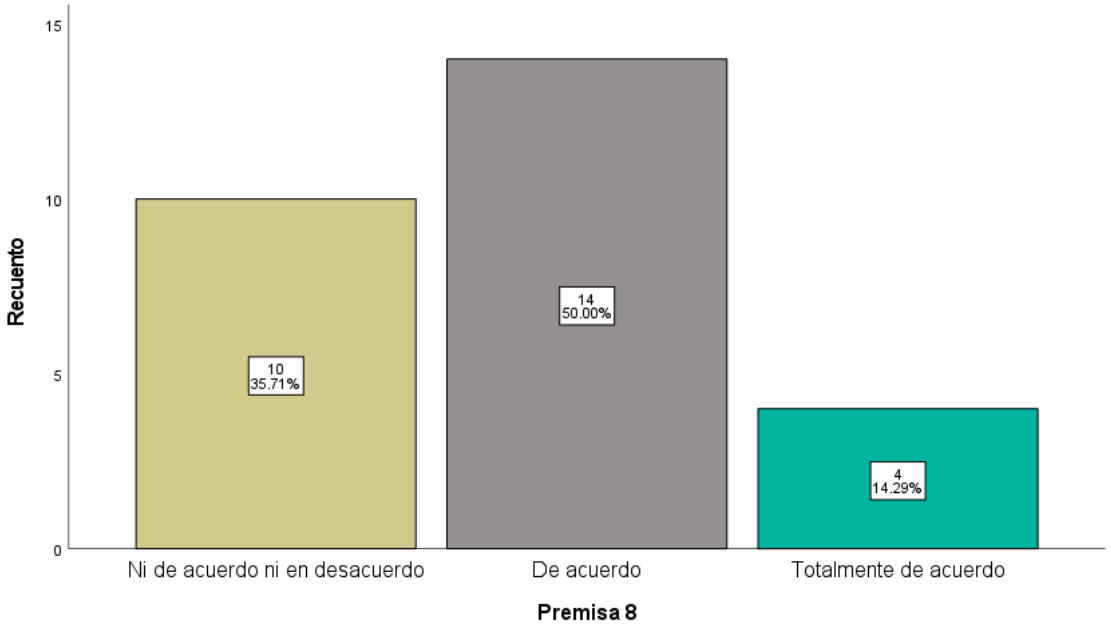

Figura 19. Gráfico sobre los resultados de la premisa 8. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 28.57% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 8, el 53.57% está de acuerdo y un 17.86% está totalmente de acuerdo que la ciberseguridad es importante en relación con la infraestructura tecnológica, ya que evidencia la capacidad con la que cuenta una entidad para proteger la información privada de los clientes ante un competidor.

Resultados de la pregunta 9

P9 La ciberseguridad aborda políticas de gestión de peligros cibernéticos para mitigar alguna contingencia cibernética y resguardar la continuidad del negocio.

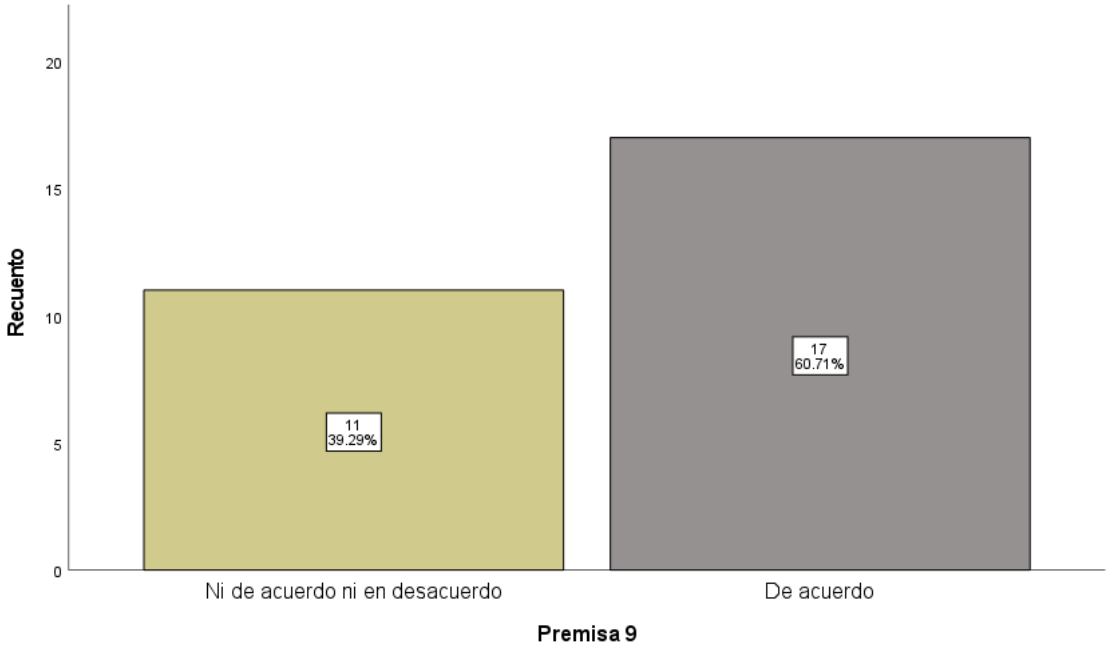

Figura 20. Gráfico sobre los resultados de la premisa 9. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 32.14% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 9, el 60.71% está de acuerdo y un 7.14% está totalmente de acuerdo que la ciberseguridad aborda políticas de gestión de peligros cibernéticos para mitigar alguna contingencia cibernética y resguardar la continuidad del negocio.

Resultados de la pregunta 10

P10 El ciberespacio es un escenario donde se han producido oportunidades y a la vez conflictos producto del desarrollo constante de las comunicaciones y tecnologías de la información, por lo cual es importante tomar medidas como la ciberseguridad.

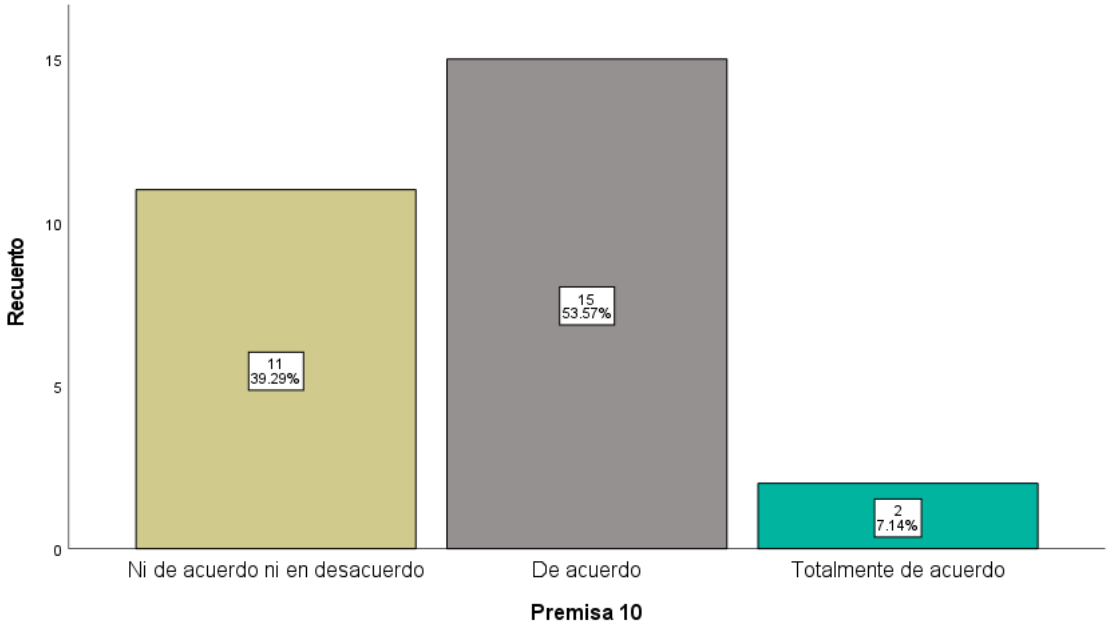

Figura 21. Gráfico sobre los resultados de la premisa 10. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 46.43% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 10, el 50% está de acuerdo y un 3.57% está totalmente de acuerdo que el ciberespacio es un escenario donde se han producido oportunidades y a la vez conflictos producto del desarrollo constante de las comunicaciones y tecnologías de la información, por lo cual es importante tomar medidas como la ciberseguridad.

Ciberataques

Resultados de la pregunta 11

P11 Los ciberataques violan las políticas de seguridad de un activo cibernético para dañar e interrumpir el acceso de la información o servicios de dicho activo generando pérdidas económicas.

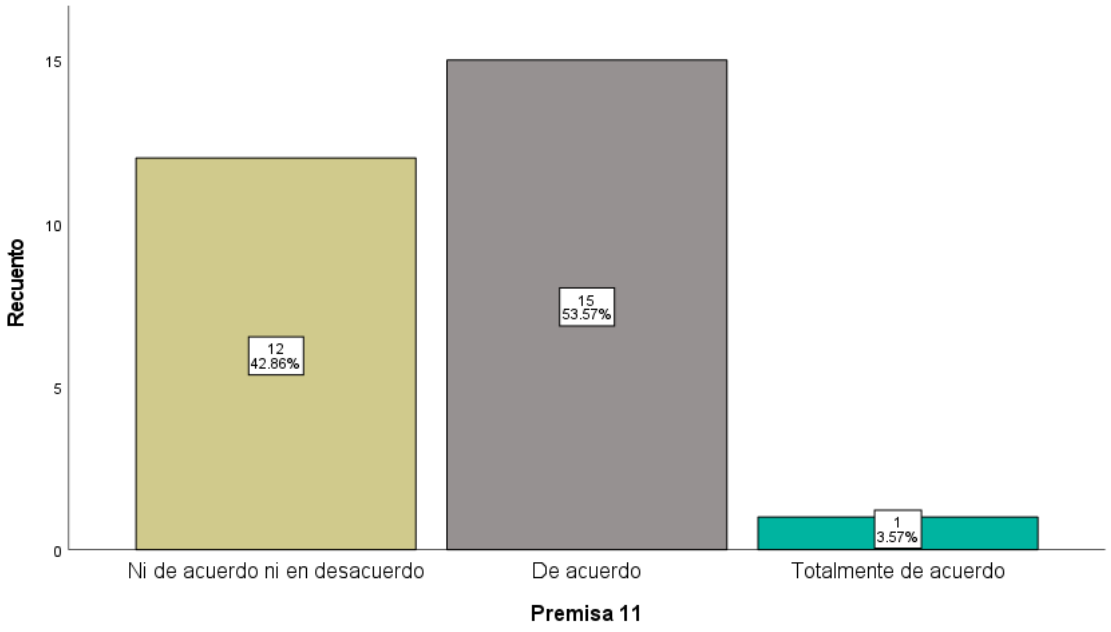

Figura 22. Gráfico sobre los resultados de la premisa 11. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 42.86% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 11, el 53.57% está de acuerdo y un 3.57% está totalmente de acuerdo que los ciberataques violan las políticas de seguridad de un activo cibernético para dañar e interrumpir el acceso de la información o servicios de dicho activo generando pérdidas económicas.

Resultados de la pregunta 12

P12 La ejecución de escenarios realistas sirven para localizar y afrontar vulnerabilidades en la infraestructura de red.

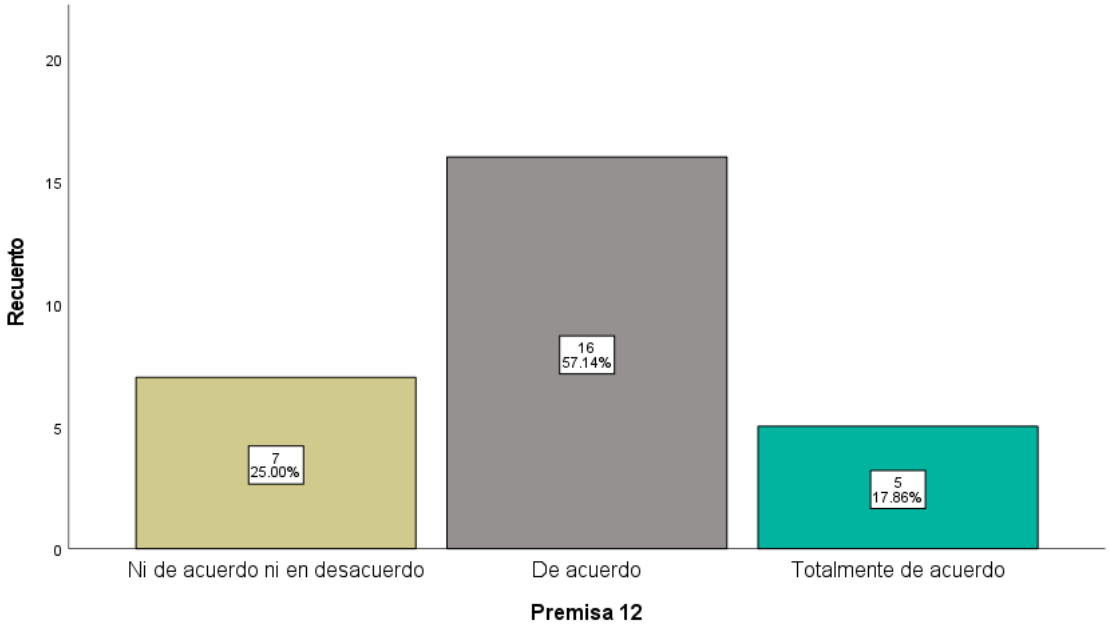

Figura 23. Gráfico sobre los resultados de la premisa 12. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados, el 32.14% de encuestados no se encuentra de acuerdo ni en desacuerdo con la premisa 12, el 53.57% está de acuerdo y un 14.29% está totalmente de acuerdo que la ejecución de escenarios realistas sirve para localizar y afrontar vulnerabilidades en la infraestructura de red.

Situación financiera

Resultados de la pregunta 13

P13 Los indicadores financieros de la empresa son importantes porque miden la situación financiera de la misma.

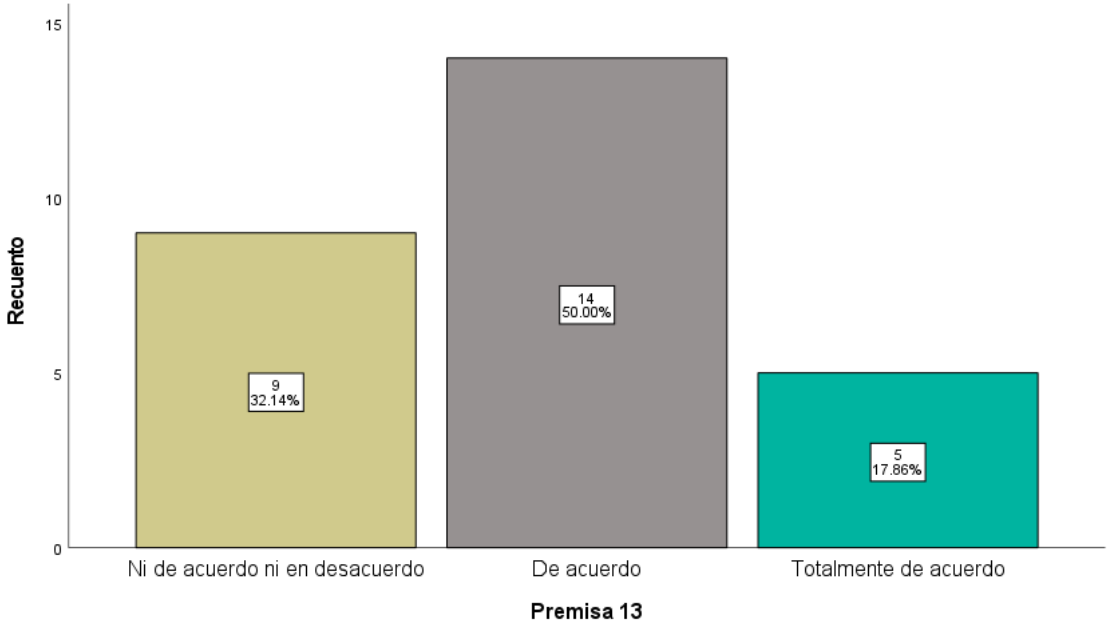

Figura 24. Gráfico sobre los resultados de la premisa 13. Extraído de SPSS 28, 2021

Interpretación:

Los resultados obtenidos de la pregunta 13 manifiesta que el 50% de los encuestados están de acuerdo que la situación financiera de las empresas es medida por los indicadores financieros y por tal motivo son importantes. Asimismo, el 32.14% indicó que no se encuentran de acuerdo ni en desacuerdo y el 17.86% se encuentra totalmente de acuerdo.

Resultados de la pregunta 14

P14 Los principales indicadores a considerar para mantener un adecuado estado financiero para las empresas son: liquidez, rentabilidad y solvencia.

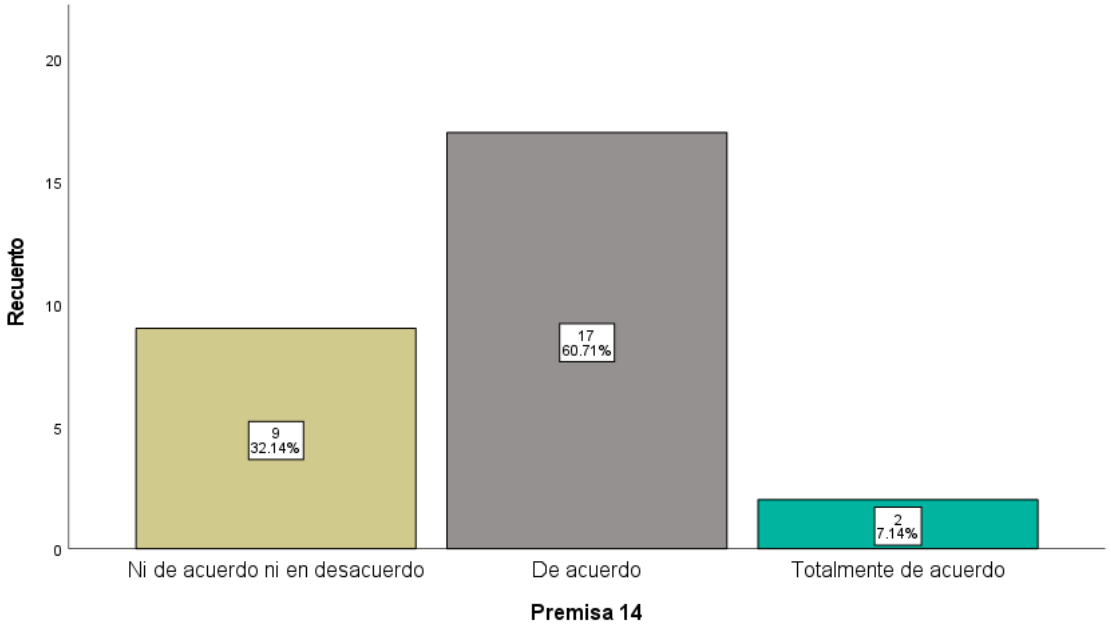

Figura 25. Gráfico sobre los resultados de la premisa 14. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con el gráfico de la premisa 14, el 60.71% de los encuestados está de acuerdo de que la liquidez, rentabilidad y solvencia son los principales indicadores a tener en cuenta para mantener un adecuado estado financiero. Seguidamente, el 32.14% indicó que no se están de acuerdo ni en desacuerdo, mientras que el 7.14% se encuentran totalmente de acuerdo.

Resultados de la pregunta 15

P15 Los ratios son indicadores que se calculan de los estados financieros que permiten evaluar posibles riesgos económicos y tomar decisiones para mitigar dichos riesgos.

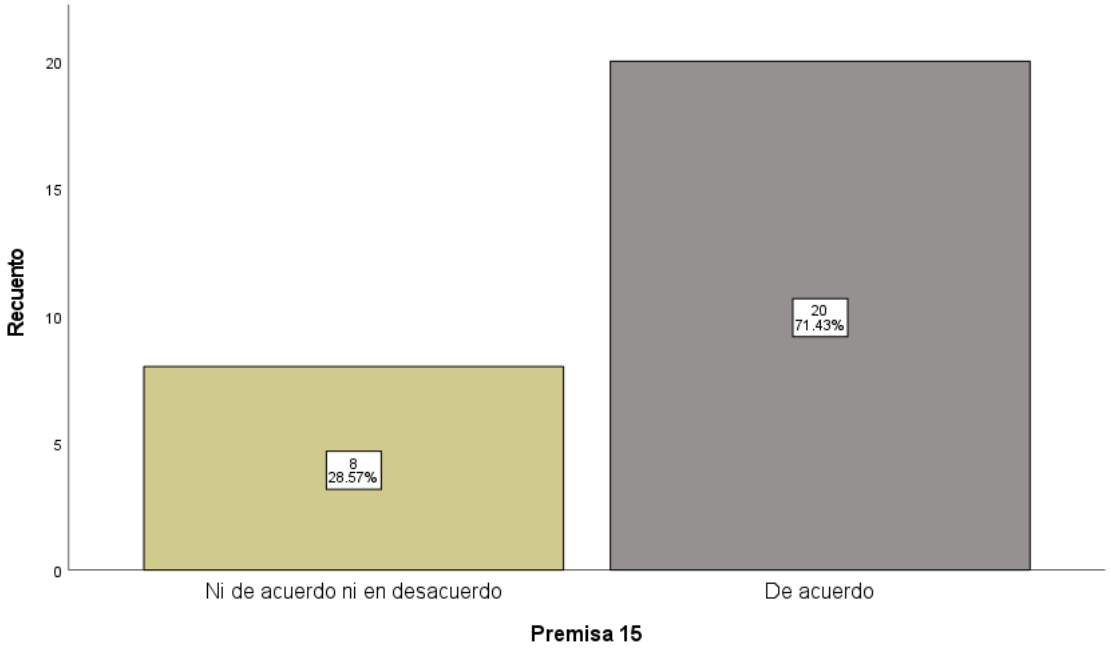

Figura 26. Gráfico sobre los resultados de la premisa 15. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con los resultados del gráfico de la premisa 15, el 71.43% de los encuestados están de acuerdo con que los indicadores financieros permiten evaluar posibles riesgos económicos y la toma de decisiones para mitigar dichos riesgos. Asimismo, el 28.57% indicaron que no se encuentran de acuerdo ni en desacuerdo.

Resultados de la pregunta 16

P16 Los ratios de rentabilidad permiten evaluar la capacidad de la empresa en generar ganancias con una mínima inversión.

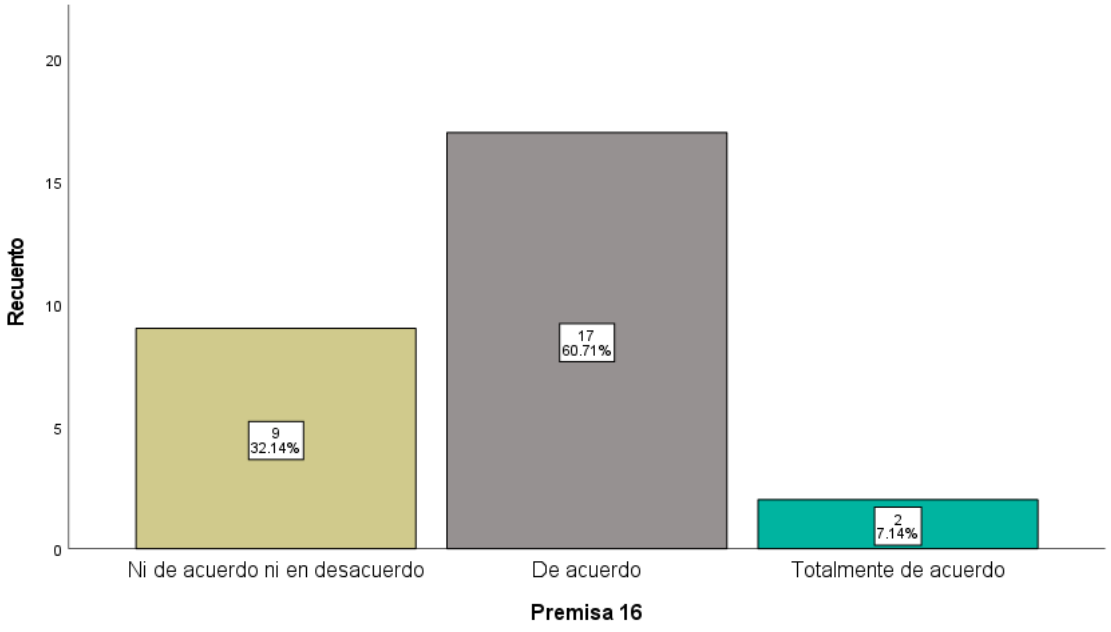

Figura 27. Gráfico sobre los resultados de la premisa 16. Extraído de SPSS 28, 2021

Interpretación:

El gráfico de la premisa 16 evidencia que el 60.71% de los encuestados se encuentran de acuerdo con que la capacidad de las empresas para generar ganancias con una mínima inversión se puede evaluar mediante los ratios financieros. Seguidamente, el 32.14% no se encuentran de acuerdo n en desacuerdo, mientras que el 7.14% está totalmente de acuerdo.

Resultados de la pregunta 17

P17 Los ratios de rentabilidad y liquidez guardan relación entre sí porque son importantes para los acreedores, ya que indican la capacidad que posee la compañía para afrontar sus obligaciones a corto y mediano plazo.

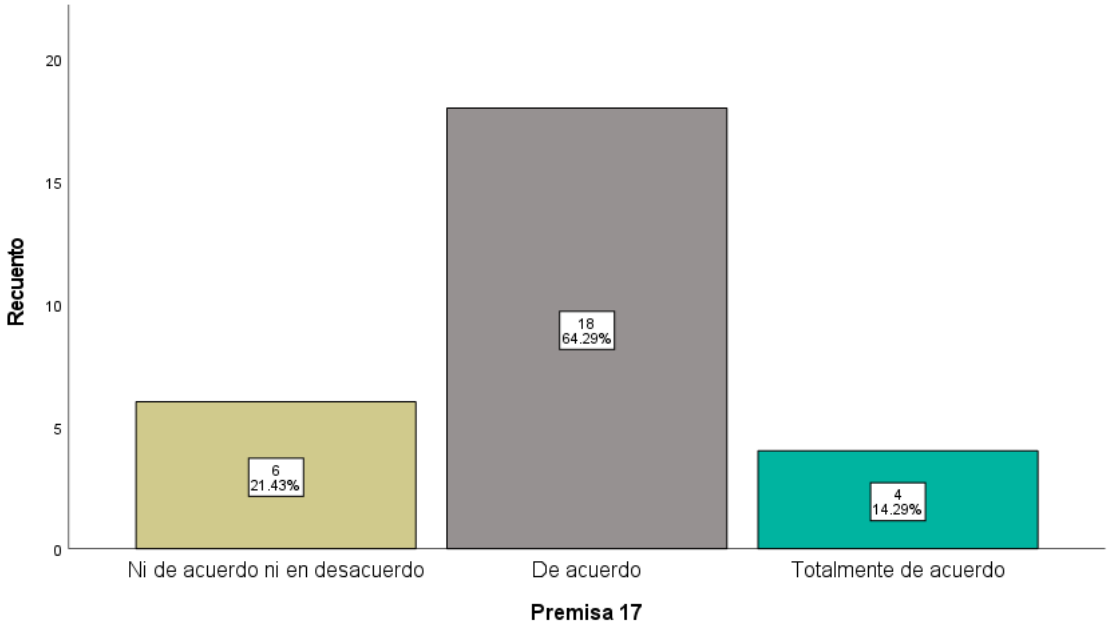

Figura 28. Gráfico sobre los resultados de la premisa 17. Extraído de SPSS 28, 2021

Interpretación:

El gráfico de la premisa 17, evidencia que el 64.29% de los encuestados está de acuerdo con que los ratios que guardan relación y son importantes para los acreedores son el de rentabilidad y liquidez, ya que indican la capacidad que posee la compañía para afrontar sus obligaciones a corto y mediano plazo. Seguidamente, el 21.43% indica que no está de acuerdo ni en desacuerdo, mientras que el 14.29% se encuentra totalmente de acuerdo.

Situación Operativa

Resultados de la pregunta 18

P18 Las entidades con pérdidas netas en periodos consecutivos podrían generar patrimonio negativo, lo cual conllevaría a ser una causal de disolución.

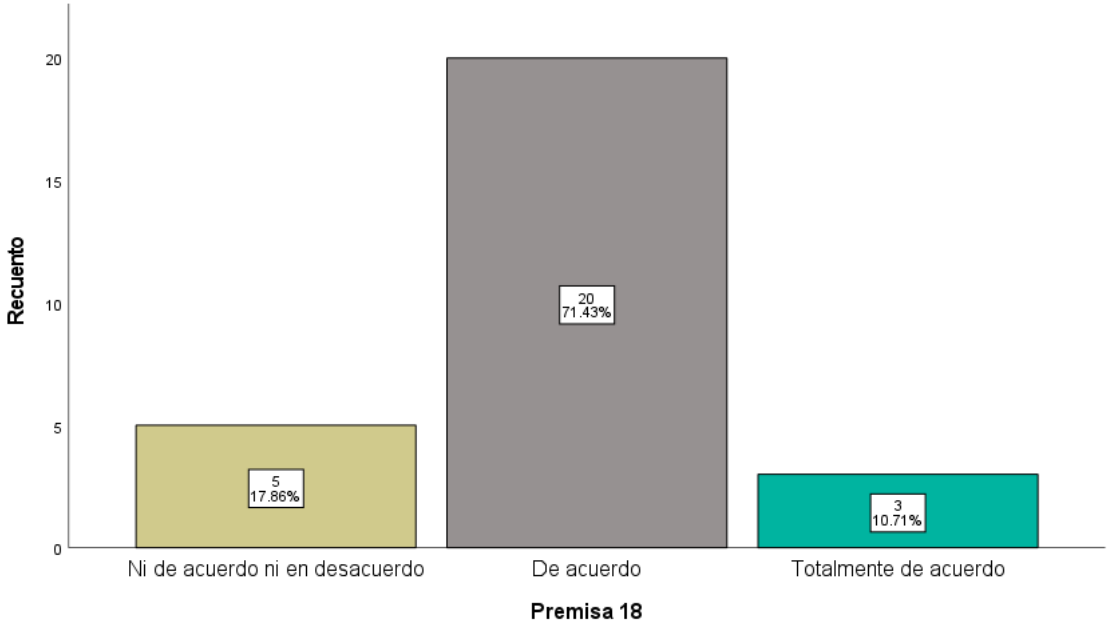

Figura 29. Gráfico sobre los resultados de la premisa 18. Extraído de SPSS 28, 2021

Interpretación:

Los resultados de la premisa 18, revela que el 71.43% de los encuestados se encuentra de acuerdo con que una causal de disolución se podría generar cuando las entidades presentan pérdidas netas en periodos consecutivos. Asimismo, el 17.86% de considera que no están de acuerdo ni en desacuerdo, mientras que el 10.71% está totalmente de acuerdo.

Resultados de la pregunta 19

P19 La situación operativa se evalúa en función de los riesgos operativos del entorno de la empresa.

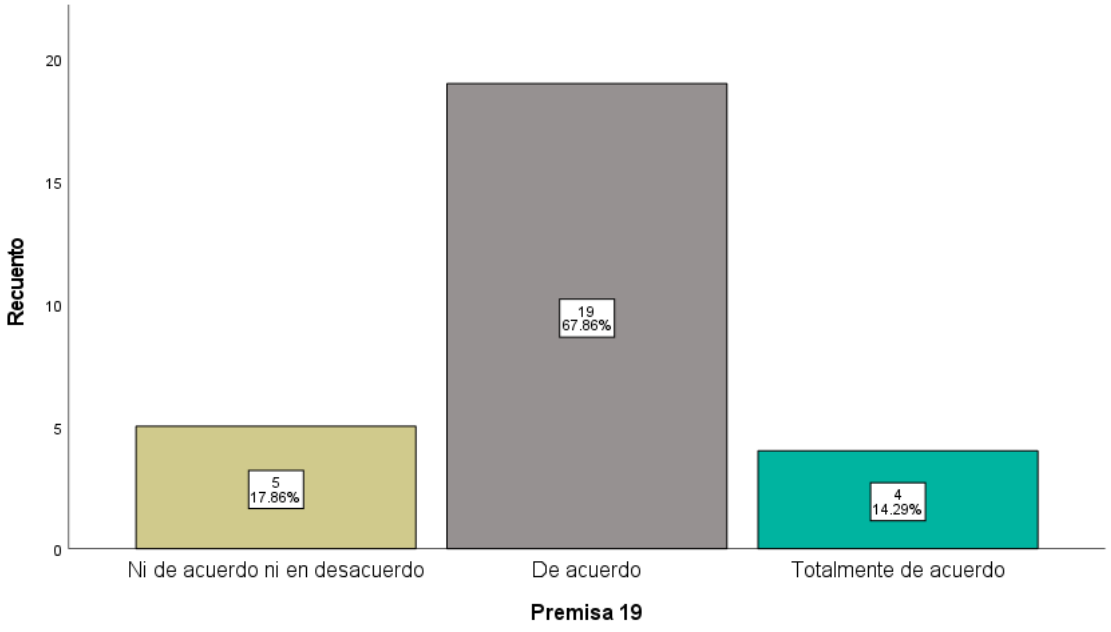

Figura 30. Gráfico sobre los resultados de la premisa 19. Extraído de SPSS 28, 2021

Interpretación:

El gráfico de la premisa 19, muestra que el 67.86% de los encuestados está de acuerdo con que la situación operativa de se evalúa en función de los riesgos operativos del entorno de la entidad. Seguidamente, el 17.86% indicó que n están de acuerdo ni en desacuerdo y el 14.29% está totalmente de acuerdo.

Resultados de la pregunta 20

P20 La escasez de personal especializado en el sector TI influye en la situación operativa de la empresa.

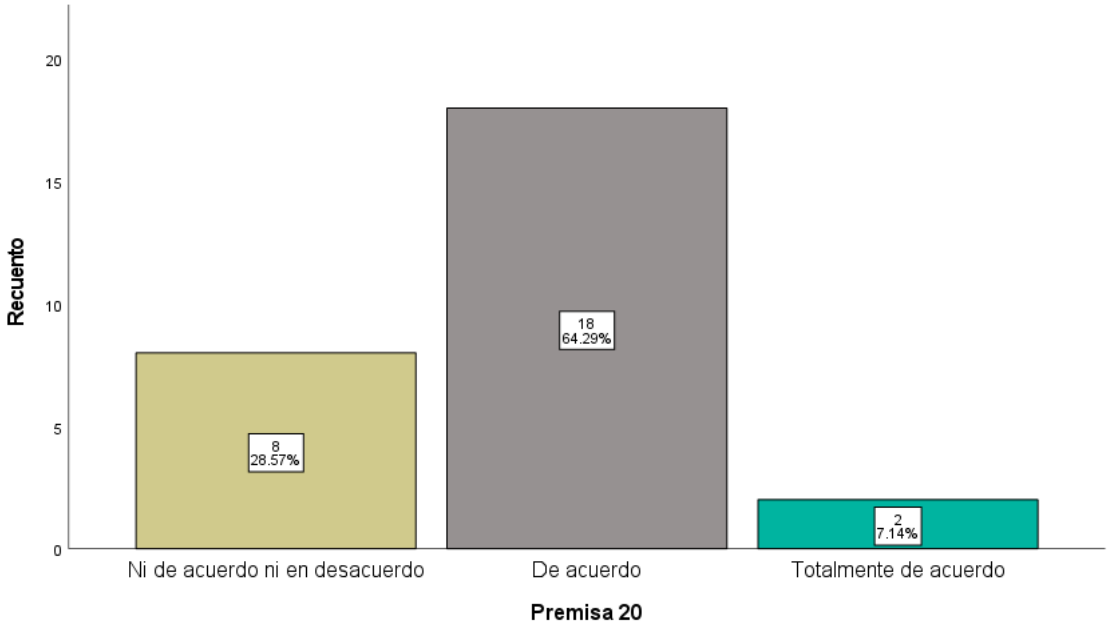

Figura 31. Gráfico sobre los resultados de la premisa 20. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con el gráfico de la premisa 20, el 64.29% de los encuestados indicó que se encuentran de acuerdo con que la situación operativa de la empresa se ve influida por la escasez de personal especializado en el sector TI. Seguidamente, el 28.57% no se encuentra de acuerdo ni en desacuerdo, mientras que el 7.14% está totalmente de acuerdo.

Resultados de la pregunta 21

P21 El déficit de profesionales en el sector TI encarece el servicio y a su vez retrasa la puesta en marcha de los proyectos.

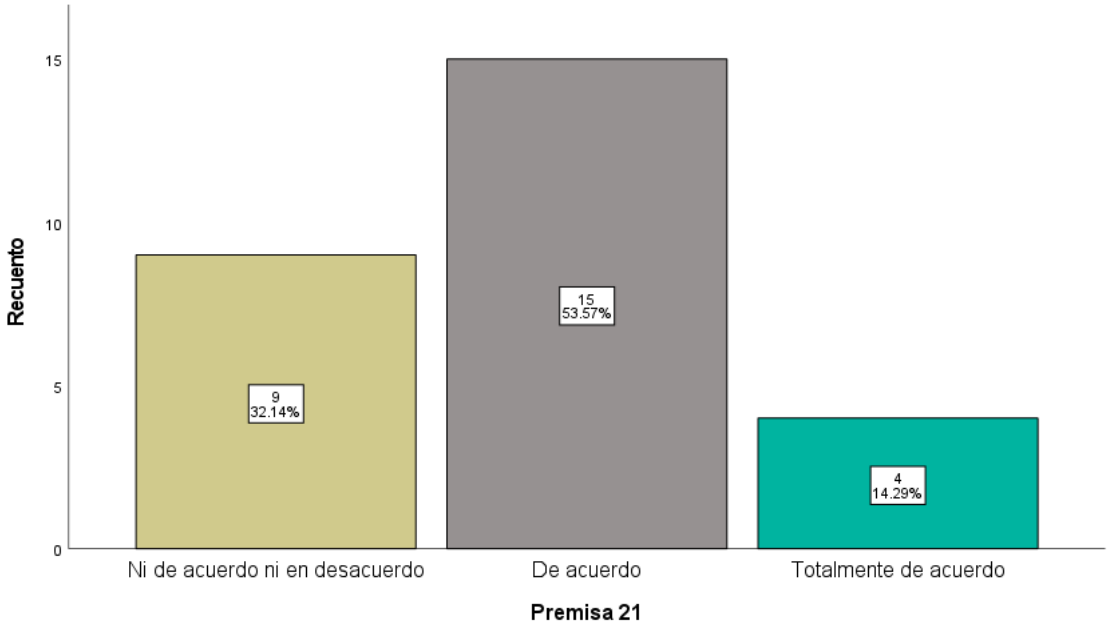

Figura 32. Gráfico sobre los resultados de la premisa 21. Extraído de SPSS 28, 2021

Interpretación:

El gráfico de la premisa 21, muestra que 53.57% de encuestados está de acuerdo con que el déficit de profesionales del sector TI retrasa la puesta en marcha de los proyectos y a la vez encarece el servicio. Asimismo, el 32.14% no están de acuerdo ni en desacuerdo, mientras que el 14.29% se encuentra totalmente de acuerdo.

Resultados de la pregunta 22

P22 Las compañías buscan profesionales de TI con perfiles híbridos como habilidades blandas y habilidades técnicas.

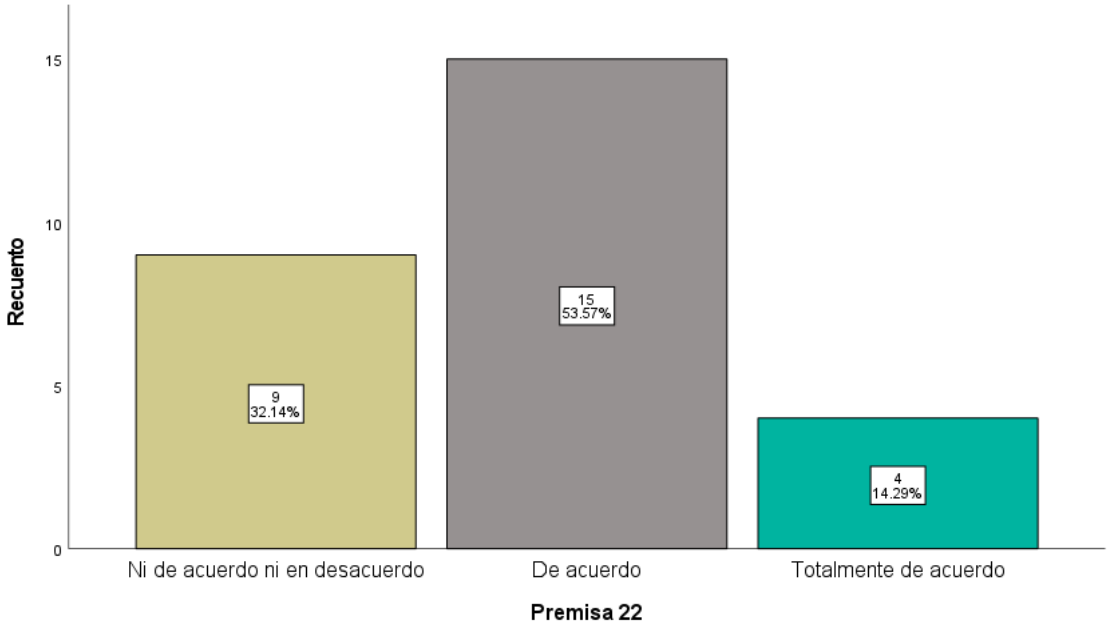

Figura 33. Gráfico sobre los resultados de la premisa 22. Extraído de SPSS 28, 2021

Interpretación:

El gráfico de la premisa 22, muestra que 53.57% de los encuestados está de acuerdo con que los profesionales con perfiles híbridos como habilidades blandas y habilidades técnicas son buscados por las compañías. Seguidamente, el 32.14% no está de acuerdo ni en desacuerdo, mientras que el 14.29% está totalmente de acuerdo.

Resultados de la pregunta 23

P23 El perfil del personal encargado de TI es muy importante, ya que dentro de este sector se encuentra el área de fraude, quien se encarga de monitorear el cumplimiento de las políticas internas y externas de las compañías.

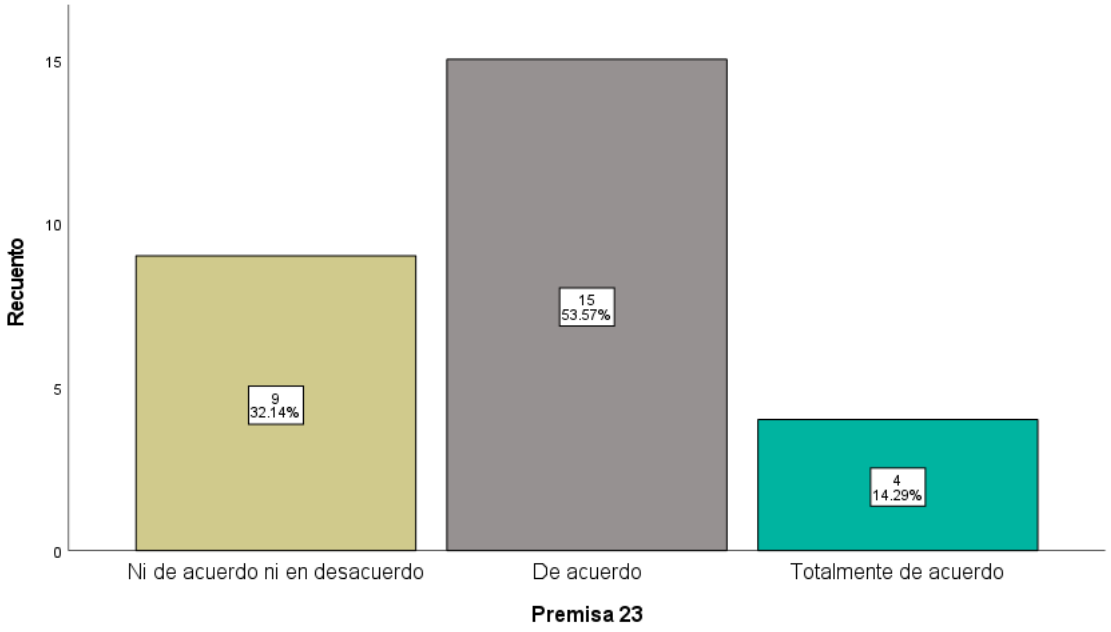

Figura 34. Gráfico sobre los resultados de la premisa 23. Extraído de SPSS 28, 2021

Interpretación:

De acuerdo con el gráfico de la premisa 23, el 53.57% de los encuestados se encuentran de acuerdo con que el perfil de los colaboradores de TI es muy importante, ya que dentro de dicho sector está el área de fraude, quien se encarga de monitorear el cumplimiento de las políticas internas y externas de las compañías. Seguidamente, el 32.14% no está de acuerdo ni en desacuerdo, mientras que el 14.29% está totalmente de acuerdo.

CAPÍTULO V: ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Con el fin de recolectar información útil para el estudio cualitativo y cuantitativo de la presente investigación, se aplicaron entrevistas a profundidad y se realizaron encuestas con el objetivo de comprender y evaluar los resultados de estos.

5.1 Análisis de la entrevista en profundidad

Se realizaron tres entrevistas a profundidad a los expertos de contabilidad, finanzas y TI con conocimientos sobre el tema de investigación. Seguidamente, el estudio cualitativo en referencia a la 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, 2021expidió el siguiente análisis.

a) ISO 27001

Los entrevistados precisan que la ISO 27001 es una norma importante que se debe considerar para el desarrollo de tecnologías emergentes, ya que estas no solo ayudan a las empresas a crecer en el mercado, sino que este avance trae consigo posibles riesgos que exponen a las empresas. Por ello, las empresas deben implementar este estándar para salvaguardar la información.

b) Principio contable de negocio en marcha de las empresas

Los expertos coinciden en que el principio contable de negocio en marcha es fundamental para evaluar la situación de la empresa y la continuidad de esta en el tiempo. Asimismo, precisan que la gerencia debe contar con la experiencia para evaluar dicho principio contable de forma periódica y concluir si la empresa continuará operaciones en los siguientes doce meses.

c) El estándar ISO 27001 podría tener algún impacto en el principio contable de la empresa en marcha

En este punto coinciden que los altos mandos de las empresas deben implementar la ISO 27001, ya que esta va de la mano con el principio contable de negocio en marcha porque impacta de manera positiva en esta última debido a que es uno de los factores que asegura la continuidad de la empresa en el tiempo.

d) Influencia de la implementación de un sistema de gestión de seguridad de la información conocido también como SGSI en el uso diario de la información que almacena una entidad como parte de su proceso operativo

Los entrevistados afirman que la implementación de un SGSI influye de manera favorable en el proceso operativo de las compañías que implementan este sistema porque genera una mejora continua en dichos procesos, ya que agrupa la información independientemente de dónde se encuentre almacenado, ya sea de manera física, digital u otros. Asimismo, consideran que brinda mayor seguridad de la información ente posibles ataques de cibernéticos.

e) Las situaciones más comunes por la que las empresas peruanas que prestan servicios tecnológicos requieren de la implementación de un SGSI de acuerdo con el estándar ISO 27001

Los expertos refieren que las situaciones por las que las empresas deben implementar un SGSI es porque las aplicaciones informáticas que las empresas utilizan pueden ser vulnerados a través del secuestro de datos de clientes que estas manejan. Por ello, las empresas deben lograr eficiencias operativas y económicas en los procesos como disminuir los riesgos a posibles pérdidas de información para que esta esté protegida.

f) La concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y alta dirección de una entidad es decisiva para garantizar la continuidad del negocio

Los entrevistados coinciden que desde los directivos se debe concientizar sobre lo importante que es la seguridad de información, esto a través de un plan de acción y políticas referente a cómo cultivar la cultura tecnológica de la empresa como un equipo entre todas las áreas, ya que varios consideran que de esto solo se debe ocupar el área de TI, lo cual no es así.

g) El objetivo de la ciberseguridad

Los especialistas coinciden en este punto que el objetivo de la ciberseguridad es resguardar la información cibernética de las principales infraestructuras críticas de la compañía, ya que estos ataques cibernéticos podrían afectar la continuidad del negocio porque afecta la productividad de la empresa.

h) La influencia de la ciberseguridad en la protección de la información privada de los usuarios de una entidad

Los entrevistados concuerdan que la ciberseguridad influye positivamente en la protección de datos de los usuarios de la empresa, ya que previene de posibles ataques externos cuya finalidad podría ser el secuestro, robo y exposición de la información confidencial de los clientes.

i) El impacto de la adopción de políticas sobre la ciberseguridad en la perspectiva de los clientes de la empresa de tecnología

Los entrevistados coinciden que la adopción de políticas de ciberseguridad impacta positivamente en la perspectiva de los clientes porque brinda seguridad e integridad de sus datos y de esta manera sentirán mayor confianza de continuar trabajando con la Compañía.

j) El objetivo de los ciberataques a las empresas

Los entrevistados coinciden rotundamente que el objetivo principal de los ciberataques es obtener beneficios económicos mediante el robo de información sensible que almacena la Compañía en las diferentes aplicaciones y software.

k) No estar preparados ante los ciberataques genera incertidumbre en el negocio en marcha

Las respuestas de los entrevistados fueron afirmativas, un ciberataque dependiendo de la magnitud de los efectos podría acabar con los recursos disponibles de una Compañía generando pérdidas económicas y con ello, ser causal de disolución y liquidación de sociedades. Uno de los entrevistados añadió que la falta de preparación hace vulnerable a una Compañía a los riesgos económicos.

l) El propósito de la aplicación de ratios financieros en las compañías

Según las respuestas de los entrevistados, el propósito de los ratios financieros es:

- Generar conocimiento y seguridad a los accionistas sobre el control económico, financiero y el cumplimiento de los objetivos trazados al inicio de cada año.
- Evaluar la situación financiera de la Compañía en base a un análisis mediante los ratios que muestran los resultados operativos de un período.
- Permiten conocer y analizar la situación financiera de una empresa para tomar decisiones.

m) El entorno de la empresa influye en la situación operativa de la misma

Los entrevistados coinciden que el entorno influye directamente en la situación operativa de la empresa. Uno de ellos nos dio como ejemplo la pandemia producida por el Covid-19 que afectó negativamente a la estabilidad económica del mundo, el cual produjo el cierre de muchas empresas que hasta el día de hoy siguen afectadas. Asimismo, afirmaron que la situación política y económica del país hasta internacional influyen en las decisiones diarias que toma la Gerencia para continuar con normalidad las operaciones de una Compañía.

n) La escasez de personal calificado genera incertidumbre en la continuidad de las operaciones de una empresa

Las respuestas de los entrevistados fueron afirmativas, el no contar con personas idóneas para ciertos puestos ocasionará alguna problemática operativa en el mediano plazo. Uno de los entrevistados comentó que es necesario tener algunos especialistas por área que permitan guiar los procesos operativos de la Compañía.

o) La escasez de personal especializado en el rubro de la empresa impacta en la situación operativa de la misma

Los entrevistados asociaron esta pregunta con la anterior y añadieron los siguientes alcances para concluir que la escasez de personal especializado impacta negativamente en la situación operativa de la empresa:

- La escasez de profesionales expertos ocasionará que la empresa no maximice su potencial operativo.

- La falta de personal especializado puede conllevar a tomar decisiones incorrectas en actividades de un rubro que no cuenta con el apoyo profesional adecuado.

p) En la actualidad las compañías busquen perfiles de personal que contengan habilidades blandas y habilidades técnicas

Las respuestas de los entrevistados fueron afirmativas, un profesional debe contar con estas habilidades porque actualmente ya son requeridas por el mercado. Uno de los entrevistados nos comentó dos habilidades importantes basados en su experiencia: comunicación asertiva y habilidades sociales. Otro entrevistado comentó que en la actualidad hay necesidad de contar con personal que tengan proyección de línea de carrera, a fin de no perder tiempo ni recursos en nuevas búsquedas de personal calificado.

5.2 Análisis de la encuesta

Luego de realizar las 28 encuestas a colaboradores del área de contabilidad, finanzas y TI de las compañías del sector tecnología de la información, se procedió con los hallazgos y la validación de la fiabilidad y validez del instrumento de medición.

5.2.1 Descripción de la prueba estadística

De acuerdo con Llinás (2017) el análisis de chi cuadrado es una prueba estadística que tiene como finalidad contrastar que dos variables categóricas estén o no relacionadas entre sí. Para validar si las hipótesis planteadas en el capítulo II de la presente investigación se aceptan o rechazan, efectuaremos la prueba de chi cuadrado mediante el uso del programa estadístico SPSS. Para ello, identificamos las siguientes variables:

- Variable independiente: ISO 27001: Seguridad de la información.
- Variable dependiente: Principio de negocio en marcha.

5.2.2 Confiabilidad del instrumento (alfa de Cronbach)

Con la finalidad de garantizar la fiabilidad y autenticidad de la herramienta de medición se ha empleado el Alfa de Cronbach. Esto, con el objetivo de concluir la coherencia de los datos obtenidos de la presente investigación. Seguidamente, se procesó una base de datos obtenida de las respuestas de las encuestas, la cual se ingresó en el programa estadístico de nombre IBM SPSS Statistics con la finalidad de obtener el cálculo de fiabilidad a través de coeficiente. Asimismo, Rodrigues (2013), menciona que el coeficiente mínimo aceptable es 0.7; el cual indica una buena confiabilidad de los datos.

En la Tabla 8 se muestra que el coeficiente Alfa de Cronbach de la presente investigación es de 0.830. Asimismo, dicho resultado indica que el instrumento de empleado es confiable.

Tabla 8

Estadísticas de fiabilidad

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
0.830	23

Nota: Adaptado de SPSS 28

5.2.3 Contrastación de las hipótesis

Formulación de la hipótesis general:

H0: La ISO 27001: Seguridad de la información no impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

H1: La ISO 27001: Seguridad de la información impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

Para determinar si existe relación, se ha cruzado la variable independiente con la variable dependiente y se obtuvo el siguiente resultado mostrado en la Tabla 9:

Tabla 9

*Tabla cruzada ISO 27001: Seguridad de la información * Principio de negocio en marcha*

Tabla cruzada ISO 27001: Seguridad de la información * Principio de negocio en marcha

			Principio de negocio en marcha		
			Ni de acuerdo ni en desacuerdo	De acuerdo	Total
ISO 27001: Seguridad de la información	Ni de acuerdo ni en desacuerdo	Recuento	3	2	5
		Recuento esperado	.7	4.3	5.0
		% del total	10.7%	7.1%	17.9%
	De acuerdo	Recuento	1	22	23
		Recuento esperado	3.3	19.7	23.0
		% del total	3.6%	78.6%	82.1%
Total		Recuento	4	24	28
		Recuento esperado	4.0	24.0	28.0
		% del total	14.3%	85.7%	100.0%

Nota: Tomado de SPSS 28

Asimismo, se presenta la Tabla 10 con el resultado de la prueba de chi cuadrado de la hipótesis general:

Tabla 10

Chi cuadrado de la hipótesis general

Pruebas de Chi-cuadrado					
	Valor	gl	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación asintótica (unilateral)
Chi-cuadrado de Pearson	10.388[a]	1	.001		
Corrección de continuidad	6.341	1	.012		
Razón de verosimilitud	8.010	1	.005		
Prueba exacta de Fisher				.011	.011
Asociación lineal por lineal	10.017	1	.003		
N de casos válidos	28				

a. 3 casillas (75.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es .14.
b. Sólo se ha calculado para una tabla 2x2

Nota: Tomado de SPSS 28

Interpretación:

De la tabla 10 se obtiene un Sig. 0.001 que es menor a 0.05, por lo tanto, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1). Esto significa que la ISO 27001: Seguridad de la información impacta significativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

Formulación de la hipótesis especifica 1:

H0: El sistema de gestión de seguridad de la información no impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

H1: El sistema de gestión de seguridad de la información impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

Para determinar si existe relación, se ha cruzado la dimensión 1 con la variable dependiente: sistema de gestión de seguridad de la información y principio de negocio en marcha, obteniendo el resultado mostrado en la Tabla 11.

Tabla 11

*Tabla cruzada Sistema de gestión de seguridad de la información * Principio de negocio en marcha*

Tabla cruzada Sistema de gestión de seguridad de la información * Principio de negocio en marcha

			Principio de negocio en marcha		
			Ni de acuerdo ni en desacuerdo	De acuerdo	Total
Sistema de gestión de seguridad de la información	Ni de acuerdo ni en desacuerdo	Recuento	2	1	3
		Recuento esperado	.4	2.6	3.0
		% del total	7.1%	3.6%	10.7%
	De acuerdo	Recuento	2	22	24
		Recuento esperado	3.4	20.6	24.0
		% del total	7.1%	78.6%	85.7%
	Totalmente de acuerdo	Recuento	0	1	1
		Recuento esperado	.1	.9	1.0
		% del total	0.0%	3.6%	3.6%
Total		Recuento	4	24	28
		Recuento esperado	4.0	24.0	28.0
		% del total	14.3%	85.7%	100.0%

Nota: Tomado de SPSS 28

Asimismo, se presenta la Tabla 12 con el resultado de la prueba de chi cuadrado de la hipótesis especifica 1:

Tabla 12

Chi cuadrado de la hipótesis especifica 1

Pruebas de Chi-cuadrado			
	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	7.583[a]	2	.023
Razón de verosimilitud	5.379	2	.068
Asociación lineal por lineal	6.000	1	.014
N de casos válidos	28		

a. 5 casillas (83.3%) han esperado un recuento menor que 5. El recuento mínimo esperado es .14.

Nota: Tomado de SPSS 28

Interpretación:

De la tabla 12 se obtiene un Sig. 0.023 que es menor a 0.05, por lo tanto, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1). Esto significa que el sistema de gestión de seguridad de la información impacta significativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

Formulación de la hipótesis especifica 2:

H0: La ciberseguridad no impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

H1: La ciberseguridad impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

Para determinar si existe relación, se ha cruzado la dimensión 2 con la variable dependiente: Ciberseguridad y principio de negocio en marcha, obteniendo el resultado mostrado en la Tabla 13:

Tabla 13

*Análisis de la tabla cruzada ciberseguridad*Principio de negocio en marcha*

Tabla cruzada ciberseguridad*Principio de negocio en marcha

			Principio de negocio en marcha		
			Ni de acuerdo ni en desacuerdo	De acuerdo	Total
Ciberseguridad	Ni de acuerdo ni en desacuerdo	Recuento	3	2	5
		Recuento esperado	.7	4.3	5.0
		% del total	10.7%	7.1%	17.9%
	De acuerdo Totalmente de acuerdo	Recuento	1	21	22
		Recuento esperado	3.1	18.9	22.0
		% del total	3.6%	75.0%	78.6%
		Recuento	0	1	1
		Recuento esperado	.1	.9	1.0
		% del total	0.0%	3.6%	3.6%
Total		Recuento	4	24	28
		Recuento esperado	4.0	24.0	28.0
		% del total	14.3%	85.7%	100.0%

Nota: Tomado de SPSS 28

Asimismo, se presenta la Tabla 14 con el resultado de la prueba de chi cuadrado de la hipótesis especifica 2:

Tabla 14

Chi cuadrado de la hipótesis especifica 2

Pruebas de Chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	10.405[a]	2	.026
Razón de verosimilitud	8.556	2	.017
Asociación lineal por lineal	5.471	1	.003
N de casos válidos	28		

c. 5 casillas (83.3%) han esperado un recuento menor que 5. El recuento mínimo esperado es .14.

Nota: Tomado de SPSS 28

Interpretación:

De la tabla 14 se obtiene un Sig. 0.026 que es menor a 0.05, por lo tanto, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1). Esto significa que la ciberseguridad impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

Formulación de la hipótesis especifica 3:

H0: Los ciberataques no impactan negativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

H1: Los ciberataques impactan negativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

Para determinar si existe relación, se ha cruzado la dimensión 3 con la variable dependiente: Ciberseguridad y principio de negocio en marcha, obteniendo el resultado mostrado en la Tabla 15:

Tabla 15

Análisis de la tabla cruzada ciberataques Impacto en el principio de negocio en marcha*

Tabla cruzada ciberataques*Principio de negocio en marcha

			Principio de negocio en marcha		
			Ni de acuerdo ni en desacuerdo	De acuerdo	Total
Ciberataques	Ni de acuerdo ni en desacuerdo	Recuento	2	1	3
		Recuento esperado	.74	2.6	3.0
		% del total	7.1%	3.6%	10.7%
	De acuerdo Totalmente de acuerdo	Recuento	2	21	23
		Recuento esperado	3.3	19.7	23.0
		% del total	7.1%	75.0%	82.1%
		Recuento	0	2	2
		Recuento esperado	.3	1.7	2.0
		% del total	0.0%	7.1%	7.1%
Total		Recuento	4	24	28
		Recuento esperado	4.0	24.0	28.0
		% del total	14.3%	85.7%	100.0%

Nota: Tomado de SPSS 28

Asimismo, se presenta la Tabla 16 con el resultado de la prueba de chi cuadrado de la hipótesis especifica 3:

Tabla 16

Chi cuadrado de la hipótesis especifica 3

Pruebas de Chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	7.643[a]	2	.022
Razón de verosimilitud	5.557	2	.062
Asociación lineal por lineal	5.471	1	.019
N de casos válidos	28		

d. 5 casillas (83.3%) han esperado un recuento menor que 5. El recuento mínimo esperado es .29.

Nota: Tomado de SPSS 28

Interpretación:

De la tabla 16 se obtiene un Sig. 0.022 que es menor a 0.05, por lo tanto, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1). Esto significa que los ciberataques impactan negativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.

5.3 Discusión de los resultados

- **Hipótesis general**

  En base a la aplicación del método cuantitativo, se concluye que la ISO 27001: Seguridad de la información impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro en el año 2021. Esta afirmación fue validada a través de la prueba de hipótesis de Chi Cuadrado donde se contrastó la relación de la variable independiente con la variable dependiente. Como resultado se obtuvo un Sig. 0.001 que es menor a 0.05, por lo tanto, la hipótesis general es aceptada.

  Además, los resultados obtenidos en el análisis cualitativo mediante la entrevista a profundidad a profesionales expertos en el tema de investigación sostienen que la ISO en mención genera un impacto positivo en el principio contable de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro en el año 2021, ya que esta ISO contribuye en el desarrollo de tecnologías emergentes, la cual ayuda a mitigar el impacto de los ataques cibernéticos. De esta manera se podrá proteger la información de la empresa y la continuidad de esta en el tiempo.

- **Hipótesis específica 1**

  En base a la aplicación del método cuantitativo, se concluye que el sistema de gestión de seguridad de la información impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro en el año 2021. Esta afirmación fue validada a través de la prueba de hipótesis de Chi Cuadrado donde se cruzaron las respuestas obtenidas de las encuestas y que están directamente relacionadas con la dimensión, sistema de gestión de seguridad de la información, y con la variable dependiente, principio de negocio en marcha. Como resultado se obtuvo un Sig. 0.023 que es menor a 0.05, por lo tanto, la hipótesis específica 1 es aceptada.

  Asimismo, de los resultados obtenidos de las entrevistas a profundidad a profesionales expertos en el tema de investigación, manifiestan que el sistema de gestión de seguridad de la información impacta favorablemente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro en el año 2021, ya que genera una ventaja competitiva y una mejor imagen de esta porque esto deduce que la Compañía se preocupa por la mejora continua de sus procesos para una mayor protección de su data. Finalmente, esto permite a las empresas evitar posibles pérdidas financieras, ya sea por el impacto negativo de los ataques cibernéticos o las contingencias legales que estos acarrean. Además de la mala reputación que podría tener la empresa a raíz de no contar con los adecuados sistemas de gestión de seguridad de la información.

- **Hipótesis específica 2**

  En base a los resultados obtenidos a nivel cuantitativo se concluye que la ciberseguridad impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. Cabe mencionar

que esta afirmación fue validada a través de la prueba de hipótesis de Chi Cuadrado donde se cruzaron las respuestas obtenidas de las encuestas, las cuales están directamente relacionadas con la dimensión ciberseguridad y con la variable dependiente principio de negocio en marcha. Asimismo, se obtuvo como resultado un Sig. 0.026 que es menor a 0.05. Por ello, la hipótesis específica 2 es aceptada.

Además, de los resultados obtenidos en las entrevistas a profundidad a profesionales expertos en el tema de investigación, mencionan que la ciberseguridad impacta favorablemente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021 porque ayuda a mitigar los ataques cibernéticos a las infraestructuras críticas de las compañías, ya que si estas se ven afectadas, influye de manera negativa en su productividad , lo cual conllevaría a una para en la continuidad del negocio. Asimismo, la adopción de políticas de ciberseguridad genera una imagen positiva ante los clientes, ya que esto es traducido en el salvaguardo de su información que no se verá afectada por manipulación o secuestro de la misma.

- **Hipótesis específica 3**

  En base a los resultados obtenidos a nivel cuantitativo se concluye que los ciberataques impactan negativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. Asimismo, cabe precisar que esta afirmación fue validada a través de la prueba de hipótesis de Chi Cuadrado donde se cruzaron las respuestas obtenidas de las encuestas, las cuales están directamente relacionadas con la dimensión ciberataques y con la variable dependiente principio de negocio en marcha. Asimismo, se obtuvo como resultado un Sig. 0.022 que es menor a 0.05. Por tal razón, la hipótesis específica 3 es aceptada.

Asimismo, de los resultados obtenidos en las entrevistas a profundidad a profesionales expertos en el tema de investigación, sostienen que los ciberataques impactan negativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. Esto porque los ciberataques podrían generar grandes pérdidas económicas porque su finalidad es detener los accesos a los sistemas de información o perjudicar la información almacenada de la Compañía, lo cual conllevaría a pérdidas financieras y esto podría generar una disolución o liquidación de la Compañía.

CONCLUSIONES

1. Es sumamente importante que los altos mandos de una Compañía reflexionen sobre la oportunidad que representa invertir en la protección de los activos tecnológicos que se posea o se estime tener en un futuro mediante una adecuada implementación de la ISO 27001 y el fomento de una cultura tecnológica dentro de la organización que aseguren la continuidad de las operaciones ante los efectos de los riesgos inherentes al sector.
2. Un sistema de gestión de seguridad de la información implementado de acuerdo con el estándar ISO 27001 representa una ventaja competitiva, debido a que otorga mayor protección y seguridad a la información interna de una Compañía ante un ataque cibernético previniendo pérdidas financieras. Además, influye positivamente en la imagen corporativa porque demuestra confianza a los clientes.
3. La ciberseguridad genera un impacto positivo en el principio de negocio marcha porque la ciberseguridad aborda políticas de gestión de peligros cibernéticos. Esto con la finalidad de mitigar contingencias cibernéticas y así resguardar la continuidad del negocio.
4. Los ciberataques generan un impacto negativo en el principio de negocio marcha porque vulneran las políticas de seguridad de un activo tecnológico con finalidad de dañar e interrumpir el acceso a la información o servicios de dicho activo, lo cual genera pérdidas económicas para la compañía.

RECOMENDACIONES

1. Sugerimos implementar una cultura tecnológica centrada en el desarrollo de nuevos conocimientos tecnológicos asociados a sistemas y aplicaciones informáticas para formar profesionales cualificados para que puedan desarrollar nuevas investigaciones sobre protección de activos tecnológicos similares al estándar ISO 27001. Esto con el fin de incentivar futuras investigaciones que permitan evaluar si los gastos asociados a la creación de dicha cultura tecnológica se deben activar de acuerdo con la NIC 38 "Intangibles". Asimismo, este trabajo debería ser desarrollado de manera conjunta entre los colaboradores de la parte operativa y los altos mandos de la empresa. Cabe mencionar que de acuerdo con la NIC 38, un intangible es un activo sin característica física, de carácter no monetario y reconocible, pero que si es administrado adecuadamente, este genera competitividad en el mercado. La norma contable hace mención que un activo se reconoce como intangible cuando se cumplen los siguientes criterios. El primero es que este sea identificable, en otras palabras, es cuando se puede disgregar de la Compañía, traspasar, arrendar, vender, entre otros a terceros. Esto, mediante un acuerdo o de forma individual. El segundo, es cuando solo la Compañía tiene el dominio de los beneficios económicos futuros generados del intangible. El tercero, es cuando el activo genera ingresos a causa de la venta, cesión o arrendamiento de este a terceros. Así como una mejora en la estructura de costos y gastos.
2. Se recomienda elaborar una matriz de riesgos para cada activo tecnológico identificando la probabilidad de ocurrencia y las consecuencias que generarían las amenazas al concretarse. Esto, mediante posibles escenarios de riesgos cibernéticos,

ya que con ello se podrán establecer controles internos de prevención, detección y corrección, a fin de minimizar el riesgo a nivel aceptable por la Gerencia.

3. Consideramos que la implementación de un sistema de gestión de seguridad de la información y un plan de ciberseguridad, desde la perspectiva de los altos mandos, no deben ser considerados como un gasto para la empresa, sino como una inversión, ya que la mejora continua no se ve solo en los procesos internos de la empresa, sino en la percepción que poseen los clientes sobre ella porque esta será favorable al saber que dichos procesos no solo son transparentes para salvaguardar la información de los usuarios, sino que están capacitados ante posibles ataques cibernéticos que conllevan a las empresas afectadas a obtener grandes pérdidas económicas. Asimismo, cabe resaltar que en un corto plazo la implementación de la ISO en mención puede ser percibida como un gasto, sin embargo, su implementación influye favorablemente en la percepción de los clientes, lo cual en un mediano plazo se traduce en generación de caja que permite fortalecer el capital corporativo mejorando la rentabilidad.

REFERENCIAS BIBLIOGRÁFICAS

Andina (14 de mayo de 2021). Perú es uno de los países con mayores detecciones de spyware. Recuperado de https://andina.pe/agencia/noticia-peru-es-uno-los-paises-mayores-detecciones-spyware-845135.aspx [Consulta: 15 de enero de 2022].

Andina (19 de febrero de 2021). Falta de profesionales tecnológicos frena transformación digital en sector empresarial. *Andina*. Recuperado de https://andina.pe/agencia/noticia-falta-profesionales-tecnologicos-frena-transformacion-digital-sector-empresarial-834525.aspx [Consulta: 15 de enero de 2022].

Arreola, A. (2019). Ciberseguridad: ¿Por qué es importante para todos? Recuperado de https://books.google.es/books?hl=es&lr=&id=ZqHDDwAAQBAJ&oi=fnd&pg=PT5&dq=qu%C3%A9+es+la+ciberseguridad&ots=yhce082wc4&sig=jG0s4ZJhmstB4vCqrV07eOOdGFs#v=onepage&q&f=false [Consulta: 2 de enero de 2022]

Ayerbe, A. (2018). La ciberseguridad de la industria 4.0: Un medio para la continuidad del negocio. *Visión Empresarial, 410*, 37-46. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6815099 [Consulta: 27 de agosto de 2021].

Banco Pichincha. (05 de febrero de 2021). Ratios de solvencia y endeudamiento que debes calcular para tu empresa [Entrada en blog]. Recuperado de https://www.pichincha.com/portal/blog/post/ratios-solvencia-endeudamiento [Consulta: 15 de febrero de 2022].

Berglund, N., Eshleman, J., & Guo, P. (2018), Información sobre el tamaño del auditor y el negocio en marcha. *A Journal of Practice & Theory, 37* (2), 1-25. doi*:* 10.2308/ajpt-51786

Blay, A., Geiger, M., & North, P. (2011), La opinión de empresa en marcha del auditor como comunicación de riesgo. *A Journal of Practice & Theory, 30* (2), 77-102. doi: 10.2308/ajpt-50002

Canal TI. (s.f). Así se movió el mercado de cómputo este año. Recuperado de https://canalti.pe/?s=As%C3%AD+se+movi%C3%B3+el+mercado+de+c%C3%B3mputo+este+a%C3%B1o [Consulta:16 de enero de 2022].

Cárdenas, L., Martínez, H. & Becerra, L. (2016). Gestión de seguridad de la información: revisión bibliográfica. *El Profesional de la Información, 25*, 931-948. doi: 10.3145/epi.2016.nov.10

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (2021). Informe sobre Tecnología e Información. Recuperado de https://unctad.org/system/files/official-document/tir2020overview_es.pdf [Consulta: 15 de enero de 2022].

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Ciberseguridad en el contexto de la industria 4.0: una clasificación estructurada de activos críticos e impactos comerciales. *Computadoras en la Industria*, *114*, 2-8. doi: 10.1016 / j.compind.2019.103165

Correa, D., & Lopera, M. (2020). Indicadores financieros como instrumento poderoso para predecir la insolvencia; un estudio usando el algoritmo boosting en empresas colombianas. *Estudios Gerenciales: Journal of Management and Economics for Iberoamerica*, *36*, 229-238. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=7514874 [Consulta: 1 de setiembre de 2021].

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). El estándar de gestión de seguridad de la información ISO / IEC 27001: revisión de la literatura y agenda de investigación basada en la teoría. *Revista TQM*, *33* (7), 76-105. doi: 10.1108 / TQM-09-2020-0202

Deane, J., Goldberg, D., Rastrillos, T., & Rees, L. (2019). El efecto de los anuncios de certificación de seguridad de la información sobre el valor de mercado de la empresa. *Information Technology and Management*, *20* (3), 107-121. doi: 10.1007/s10799-018-00297-3

Diaz, Rosa. (2021). Ciberriesgos. Actuarios, (48), 5-8. Recuperado de https://www.actuarios.org/wp-content/uploads/2021/03/Actuarios-48-web-low.pdf [Consulta: 2 de enero de 2022].

El-Marsi, M., Al-Yafi, K., Addas, S. & Tarhini, A. (2018). Determinantes individuales de resultados ocupacionales de TI. *Communications of the Association for Information Systems. 42*, 481-507. doi: 10.17705/1CAIS.04218

El Peruano (22 de noviembre de 2020). Inversión en TIC superará los US$ 3,300 millones. *El Peruano*. Recuperado de https://elperuano.pe/noticia/109483-inversion-en-tic-superara-los-us-3300-millones [Consulta:16 de enero de 2022].

El Peruano (07 de diciembre de 2021). La transformación digital liderará el presupuesto de TI al 2024, según IDC. Recuperado de https://elperuano.pe/noticia/134931-la-transformacion-digital-liderara-el-presupuesto-de-ti-al-2024-segun-idc#:~:text=06%2F12%2F2021%20En%20solo,remoto%2C%20seg%C3%BAn%20la%20consultora%20IDC [Consulta: 15 de enero de 2022].

Feng, M., & Li, C. (2014). ¿Son los auditores profesionalmente escépticos? Evidencia del negocio en marcha de los auditores opiniones y pronósticos de ganancias de la gerencia. *Journal of Accounting Research,52*, 993-1246. doi: 10.1111/1475-679X.12064

Garcia, F. (2021), análisis e implantación de técnicas y herramientas de ethical hacking para la ciberseguridad (Tesis de licenciatura, Universidad Estatal Península de Santa Elena). Recuperado de https://repositorio.upse.edu.ec/bitstream/46000/5917/1/UPSE-TTI-2021-0022.pdf [Consulta: 2 de enero de 2022]

Gestión (22 de mayo de 2022). Filtración de datos personales: lo que dijo Asbanc, Reniec y la reacción desde la PCM. *Gestión*. Recuperado de https://gestion.pe/peru/filtracion-de-datos-personales-lo-que-dijo-asbanc-reniec-y-la-reaccion-desde-la-pcm-rmmn-noticia/ [Consulta: 29 de junio de 2022].

Hamdi, Z., Anir, A., Abdul, N., & Hassandoust, F. (2019). Una revisión comparativa de la implementación del SGSI basado en la serie ISO 27000 en organizaciones de diferentes sectores empresariales. *Conferencia Internacional de Ciencias de la Computación e Ingeniería*, *1339*, 1-8. doi: 10.1088/1742-6596/1339/1/012103

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la Investigación. 6ª ed. México, D.F.:McGraw-Hill

Instituto Nacional de Estadística e Informática (INEI). (2021). Demografía empresarial en el Perú I trimestre de 2021. Lima: INEI. Recuperado de https://www.inei.gob.pe/media/MenuRecursivo/boletines/boletin_demogrwafia_empresarial.pdf: [Consulta:31 de agosto de 2021].

Instituto Nacional de Estadística e Informática (INEI). (2014). Una mirada a Lima Metropolitana. Lima: INEI. Recuperado de https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1168/libro.pdf: [Consulta:31 de agosto de 2021].

Instituto Nacional de Estadística e Informática (INEI). (2019). Perú: Características económicas y financieras de las empresas comerciales, 2017. Lima: INEI. Recuperado de https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1737/libro.pdf [Consulta:16 de enero de 2022].

International Organization for Standarization (ISO). (2013). ISO 27001: 2013. Introducción a ISO 27001 (ISO27001). Recuperado de http://www.27000.org/iso-27001.htm [Consulta: 01 de septiembre de 2021].

International Organization for Standarization (2013). ISO 27002: Tecnología de la información - Seguridad técnicas de seguridad - Código de prácticas para control de la seguridad de la información [Vol. 1]. Geneva: ISO/IEC 2013

International Organization for Standarization (2016). ISO 27004: Tecnología de la información - Seguridad técnicas - Seguridad de la información Gestión de la seguridad de la información - Supervisión medición, análisis y evaluación [Vol. 2]. Geneva: ISO/IEC 2016

International Organization for Standarization (2017). ISO 27003: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Orientación [Vol. 2]. Geneva: ISO/IEC 2017

International Organization for Standarization (2018). ISO 27000: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario [Vol. 2]. Geneva: ISO/IEC 2018

International Organization for Standarization (2018). ISO 27005: Tecnología de la información - Seguridad técnicas - Seguridad de la información Gestión de riesgos [Vol. 3]. Geneva: ISO/IEC 2018

International Organization for Standarization (2020). ISO Survey. Recuperado de https://www.iso.org/the-iso-survey.html [Consulta: 10 de enero de 2022].

International Organization for Standarization (2021). ISO Miembros. Recuperado de https://www.iso.org/members.html [Consulta: 10 de enero de 2022].

Kianpour, M., Kowalski, S.J., & Øverby, H. (2022). Avanzando en el concepto de ciberseguridad como un bien público. *Simulation Modelling Practice and Theory,116*,1-15. doi: 10.1016/j.simpat.2022.102493

Ladino, M., Villa, P., & López, A. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia Et Technica, 1* (47), 334-339. doi: 10.22517/23447214.1177

Lengua, C. (16 de noviembre de 2020). Empresas peruanas en riesgo de ciberataques, ¿qué opciones ofrece el mercado?. *El Comercio*. Recuperado de https://elcomercio.pe/economia/empresas-peruanas-en-riesgo-de-ciberataques-que-opciones-ofrece-el-mercado-ncze-noticia/?ref=ecr [Consulta: 27 de agosto de 2021].

Li, S., Yen, D., Chen, Sh., Chen, P., Lu, W., & Cho, C. (2015). Efectos de la virtualización en la seguridad de la información. *Computer Standards & Interfaces, 42*, 1-8. doi: 10.1016/j.csi.2015.03.001

Li, Y., & Liu, Q. (2021). Un estudio de revisión integral de los ataques cibernéticos y la seguridad cibernética; tendencias emergentes y desarrollos recientes. *Energy Reports,7*, 8176-8186. doi: 10.1016/j.egyr.2021.08.126

Llinás, H. (2017). Estadística inferencial. Colombia, Barranquilla: Universidad del Norte

Lizarzaburu, E., Ampuero, G., Noriega, L., López, L., & Mejía, P. (2017). Gestión de Riesgos Empresariales: Marco de Revisión ISO 31000. *Revista Espacios*, *38* (59), 8.

Lugo, J., Carrasquero, H., &. Gómez, J. (2020). Evaluación de gestión de seguridad de la información en los sistemas de información gerencial como herramienta de competitividad en empresas de servicios de ensayos no destructivos en la ciudad de Lima - Perú. *Qualitas*, *19*, 62-76. Recuperado de https://revistas.unibe.edu.ec/index.php/qualitas/article/view/42/57 [Consulta: 25 de agosto de 2021].

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Gestión de la seguridad de la información en empresas del sector TIC y no TIC: una perspectiva de innovación preventiva. *Computers and Security*, *109* (102383), 1-23. doi: 10.1016 / j.cose.2021.102383

Mirtsch, M., Kinne, J., & Blind, K. (2021). Explorando la adopción de la norma internacional ISO / IEC 27001 del sistema de gestión de seguridad de la información: un análisis basado en la minería web. *IEEE Transactions on Engineering Management*, *68* (1), 87-100. doi: 10.1108/ICS-01-2020-0004

Mirtsch, M., Pohlisch, J., & Blind, K. (2020). Difusión Internacional del estándar de sistemas de gestión de la seguridad de la información ISO/IEC 27001: Explorando el papel de la cultura. *Proceedings of the European Conference on Information Systems (ECIS)*, 1-18. Recuperado de https://pwebebsco.upc.elogim.com/ [Consulta: 15 de enero de 2022].

Najar, J., & Suárez, N. (2015). La seguridad de la información: un activo valioso de la organización. *Revista Vínculos*, *12*, 6-14. doi: 10.14483/udistrital.jour.vinculos.2015.1.axx

Pattanavichai, S. (2018). El modelo de red de diseño para el estándar de gestión de la seguridad de la información depende de la norma ISO 27001. *Revista GSTF sobre Informática*, *5*, 1-11. doi: 10.5176/2251-3043_5.3.379

Plus TI. (2021). Prevención de fraude en sucursales financieras. Lims: Plus T. Recuperado de https://www.plus-ti.com/contacto [Consulta:16 de febrero de 2022].

PMG SSI (2013). La NCh ISO 27001. Origen y evolución. Recuperado de https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/#:~:text=En%20el%20caso%20de%20la,la%20Seguridad%20de%20la%20Informaci%C3%B3n.&text=Esta%20norma%20tuvo%20una%20segunda,7799%2D2%2C%20en%201998 [Consulta: 10 de enero de 2022].

Presidencia del Consejo de Ministros (PCM). (08 de enero de 2016). Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática. [Resolución Ministerial N° 004-2016-PCM]. Recuperado de https://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-

norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/ [Consulta: 19 de agosto de 2021].

Promotora del Comercio Exterior de Costa Rica (PROCOMER). (2020). Prospección del mercado TI en Perú. Recuperado de http://sistemas.procomer.go.cr/DocsSEM/B882B8FA-3A4E-4BB2-BAE8-285FFFDFD807.pdf [Consulta:16 de febrero de 2022].

Rodriguez-Rodriguez, J., y Reguant-Álvarez, M. (2020). Calcular la fiabilidad de un cuestionario o escala mediante el SPSS: el coeficiente alfa de Cronbach. REIRERevista d'Innovació i Recerca en Educació. 13(2), 1.13. https://doi.org/10.1344/reire2020.13.230048

Sabillón, R., & Jeimy, J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas y Tecnologías de Información, 32,* 33-48. Recuperado de https://scielo.pt/scielo.php?script=sci_arttext&pid=S1646-98952019000200004&lng=pt&nrm=iso&tlng=es?script=sci_arttext&pid=S1646-98952019000200004&lng=pt&nrm=iso&tlng=es [Consulta: 23 de agosto agosto de 2021].

Salas, L. (14 de mayo de 2021). Ciberataques: Perú es el tercer país más afectado de Latinoamérica en lo que va del año, según Eset. El Comercio. Recuperado de https://elcomercio.pe/economia/ciberataques-peru-es-el-tercer-pais-mas-afectado-de-latinoamerica-en-lo-que-va-del-ano-segun-eset-bitcoin-amenazas-informaticas-criptomineros-criptomineria-ncze-noticia/ [Consulta: 27 de agosto de 2021].

Santos-Olmo, A., Sánchez, L., Caballero, I., Camacho, S., & Fernández-Medina, E. (2016). La importancia de la cultura de la seguridad en las PYMES frente a la correcta gestión de la seguridad de sus activos. *Internet Futuro, 8* (3), S/N. doi: 10.3390 / fi8030030

Stiawan, D., Idris, M., Abdullah, A., Aljaber, F., & Budiarto, R. (2017). Prueba de penetración de ciberataques y análisis de vulnerabilidades. *International Journal of Online Engineering, 13*, 125-132. doi: 10.3991/ijoe.v13i01.6407

Superintendencia del Mercado de Valores (SMV). (2000). Ley general de sociedades. Recuperado de https://www.smv.gob.pe/sil/LEY0000199726887001.pdf [Consulta:16 de enero de 2022].

Superintendencia Nacional de Administración Tributaria (SUNAT). (23 de julio de 2015). Regulan el Registro de Proveedores de Servicios Electrónicos y modifican la Resolución de Superintendencia N° 097-2012/SUNAT que crea el Sistema de Emisión Electrónica desarrollado desde los sistemas del contribuyente. [Resolución de Superintendencia N° 199-15-SUNAT]. Recuperado de https://www.sunat.gob.pe/legislacion/superin/2015/199-2015.pdf [Consulta: 19 de agosto de 2021].

Superintendencia Nacional de Administración Tributaria (SUNAT). (20 de diciembre de 2020). Flexibilizan disposiciones en la normativa sobre emisión electrónica.

[Resolución de Superintendencia N° 221-20-SUNAT]. Recuperado de https://www.sunat.gob.pe/legislacion/superin/2020/221-2020.pdf [Consulta: 19 de agosto de 2021].

Tafur, R., e Izaguirre, M. (2015). *Cómo hacer un proyecto de investigación: uso de diagramas, matrices y mapas conceptuales.* 2ª ed. Bogotá:Alfaomega

Tamulevičienė, D., & Androniceanu, A. (2020), Selección de los indicadores para medir el valor de una empresa y sus cambios en el sistema de control para las medianas empresas. *Journal of Entrepreneurship and Sustainability Issues, 7* (3), 1440-1458. doi: 10.9770/jesi.2020.7.3(1)

Tecnova. (s.f.). El nuevo perfil de los profesionales TI. Santiago: Tecnova. Recuperado de https://www.tecnova.cl/2019/11/07/el-nuevo-perfil-de-los-profesionales-ti/# [Consulta:16 de febrero de 2022].

Telefónica Tech (2020). Soluciones Cyber Security & Cloud. Recuperado de https://cybersecuritycloud.telefonicatech.com/ [Consulta: 29 de junio de 2022].

Tiganoaia, B. (junio,2015). Algunos aspectos relacionados con el sistema de gestión de seguridad de la información dentro de las organizaciones: adopción de la norma ISO / IEC 27001: 2013. *Studies in Informatics and Control*, *24* (2), 201-210. Recuperado de https://sic.ici.ro/wp-content/uploads/2015/06/SIC_2015-2-Art8.pdf [Consulta: 23 de agosto agosto de 2021].

Valencia-Duque, F., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de ISO / IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informacao*, *22*, 73-88. doi: 10.17013/risti.22.73-88

Yu-Hsin, L., Yu-Cheng, L., & Yu-Ling, L. (2016). Opinión sobre la empresa en funcionamiento: Aplicación de tecnologías de minería de datos. *Journal of Accounting Review*, *63*, 77-108. doi: 10.6552/JOAR.2016.63.3

Zapata, B., Fernández, J. & Toval, A. (2015). Seguridad en la computación en la nube: un estudio de mapeo. *Informática y Sistemas de Información*, *12*, 161-184. doi: 10.2298/CSIS140205086C

ANEXO A: MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES
PROBLEMA GENERAL 1. ¿Cómo impacta la ISO 27001: Seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021? **PROBLEMAS ESPECÍFICOS** 1. ¿Cómo el sistema de gestión de seguridad de la información impacta en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021? 2. ¿Cómo la ciberseguridad impacta en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021? 3. ¿Cómo los ciberataques impactan en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021?	**OBJETIVO GENERAL** 1. Determinar el impacto de la ISO 27001: Seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. **OBJETIVOS ESPECÍFICOS** 1. Determinar cómo impacta el sistema de gestión de seguridad de la información en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. 2. Determinar el impacto de la ciberseguridad en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. 3. Determinar el impacto de los ciberataques en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.	**HIPÓTESIS GENERAL** 1. La ISO 27001: Seguridad de la información impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. **HIPÓTESIS ESPECÍFICAS** 1. El sistema de gestión de seguridad de la información impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. 2. La ciberseguridad impacta positivamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021. 3. Los ciberataques impactan negativamente en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro, 2021.	**1. VARIABLE INDEPENDIENTE:** ISO 27001: Seguridad de la información (Culot, Nassimbeni, Podrecca & Sartor, 2021) ***Dimensiones:*** ● Sistema de gestión de seguridad de la información (Tiganoaia, 2015) ● Ciberseguridad (Delgado & Fernández, 2019) ● Ciberataques (Stiawan, Idris, Abdullah, Aljaber & Budiarto, 2017) **2. VARIABLE DEPENDIENTE:** Principio de negocio en marcha (Yu-Hsin, Yu-Cheng & Yu-Ling, 2016) ***Dimensiones:*** ● Ratios financieros (NIA 570, 2016) ● Situación financiera ● Situación operativa

ANEXO B: ENTREVISTA A PROFUNDIDAD

La Universidad Privada de Ciencias Aplicadas – UPC, agradece su participación en el desarrollo de la presente entrevista de la carrera de contabilidad titulada: 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. La información proporcionada será exclusivamente utilizada para fines del desarrollo de nuestra tesis, por lo que será tratada de manera confidencial.

Nombre del entrevistado:

Cargo:

Empresa:

ISO 27001

1. ¿Cuál es su opinión con respecto al estándar ISO 27001?
2. ¿Qué opina del principio contable de negocio en marcha de las empresas?
3. Respecto al estándar ISO 27001, ¿Considera que este podría tener algún impacto en el principio contable de la empresa en marcha?

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4. ¿Cómo considera que influye la implementación de un sistema de gestión de seguridad de la información conocido también como SGSI en el uso diario de la información que almacena una entidad como parte de su proceso operativo?
5. ¿Cuáles son las situaciones más comunes por la que las empresas peruanas que prestan servicios tecnológicos requieren de la implementación de un SGSI de acuerdo con el estándar ISO 27001?
6. En base a su experiencia, ¿Considera que la concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y alta dirección de una entidad es decisiva para garantizar la continuidad del negocio?

CIBERSEGURIDAD

7. ¿Cuál considera usted que es el objetivo de la ciberseguridad?
8. ¿Cómo considera que influye la ciberseguridad en la protección de la información privada de los usuarios de una entidad?

9. ¿Usted cómo considera que la adopción de políticas sobre la ciberseguridad impacta en la perspectiva de los clientes de la empresa de tecnología?

CIBERATAQUES

10. ¿Cuál considera usted que es el objetivo de los ciberataques a las empresas?
11. ¿Considera usted que no estar preparados ante los ciberataques genera incertidumbre en el negocio en marcha?

SITUACIÓN FINANCIERA – RATIOS

12. ¿Cuál considera usted que es el propósito de la aplicación de ratios financieros en las compañías?

SITUACIÓN OPERATIVA

13. ¿Usted cómo considera que el entorno de la empresa influye en la situación operativa de la misma? ¿por qué?
14. ¿Considera que la escasez de personal calificado genera incertidumbre en la continuidad de las operaciones de una empresa? ¿por qué?
15. ¿Cree usted que la escasez de personal especializado en el rubro de la empresa impacta en la situación operativa de la misma? ¿por qué?
16. ¿Está de acuerdo que en la actualidad las compañías busquen perfiles de personal que contengan habilidades blandas y habilidades técnicas? ¿por qué?

ANEXO C: ENCUESTA

Nombre del entrevistado:

Cargo:

Empresa:

A continuación, marque con un aspa su nivel de acuerdo o desacuerdo con las siguientes afirmaciones

1. Totalmente en desacuerdo 2. En desacuerdo 3. Ni de acuerdo ni en desacuerdo 4. De acuerdo 5. Totalmente de acuerdo

Sistema de gestión de seguridad de la información	1	2	3	4	5
1. Un sistema de gestión de seguridad de la información implementado de acuerdo con el estándar ISO 27001 garantiza la protección de los recursos de información administrados por una entidad.					
2. La certificación ISO 27001 genera un impacto positivo en la mente de los clientes, potenciales clientes y partes interesadas, dado que proyecta protección, confidencialidad y seguridad en el uso de la información que se almacena como parte del proceso operativo del negocio.					
3. Una de las ventajas competitivas del sistema de gestión de seguridad de la información es la mejor gestión económica en la inversión de la mejora continua de la seguridad de la información.					
4. Conseguir concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y directivos es decisivo para garantizar la continuidad del negocio.					
5. Una implementación eficiente y eficaz de la ISO 27001 mitiga riesgos potenciales asociados a la adaptación de tecnologías emergentes relacionados a la digitalización de procesos a nivel organizacional.					
6. La ISO 27001 sirve para estructurar procesos dentro de una organización para asegurar la continuidad del negocio					

previniendo especialmente ataques cibernéticos que afectan las funciones de las entidades.					
Ciberseguridad					
7. La adopción de políticas sobre la ciberseguridad representa una ventaja competitiva en el mercado.					
8. La ciberseguridad es importante en relación con la infraestructura tecnológica, ya que evidencia la capacidad con la que cuenta una entidad para proteger la información privada de los clientes ante un competidor.					
9. La ciberseguridad aborda políticas de gestión de peligros cibernéticos para mitigar alguna contingencia cibernética y resguardar la continuidad del negocio.					
10. El ciberespacio es un escenario donde se han producido oportunidades y a la vez conflictos producto del desarrollo constante de las comunicaciones y tecnologías de la información, por lo cual es importante tomar medidas como la ciberseguridad.					
Ciberataques					
11. Los ciberataques violan las políticas de seguridad de un activo cibernético para dañar e interrumpir el acceso de la información o servicios de dicho activo generando pérdidas económicas.					
12. La ejecución de escenarios realistas sirve para localizar y afrontar vulnerabilidades en la infraestructura de red.					
Situación financiera					
13. Los indicadores financieros de la empresa son importantes porque miden la situación financiera de la misma.					
14. Los principales indicadores a considerar para mantener un adecuado estado financiero para las empresas son: liquidez, rentabilidad y solvencia.					
15. Los ratios son indicadores que se calculan de los estados financieros que permiten evaluar posibles riesgos económicos y tomar decisiones para mitigar dichos riesgos.					

16. Los ratios de rentabilidad permiten evaluar la capacidad de la empresa en generar ganancias con una mínima inversión.					
17. Los ratios de rentabilidad y liquidez guardan relación entre sí porque son importantes para los acreedores, ya que indican la capacidad que posee la compañía para afrontar sus obligaciones a corto y mediano plazo.					
Situación Operativa					
18. Las entidades con pérdidas netas en periodos consecutivos podrían generar patrimonio negativo, lo cual conllevaría a ser una causal de disolución.					
19.. La situación operativa se evalúa en función de los riesgos operativos del entorno de la empresa.					
20. La escasez de personal especializado en el sector TI influye en la situación operativa de la empresa.					
21. El déficit de profesionales en el sector TI encarece el servicio y a su vez retrasa la puesta en marcha de los proyectos.					
22. Las compañías buscan profesionales de TI con perfiles híbridos como habilidades blandas y habilidades técnicas.					
23. El perfil del personal encargado de TI es muy importante, ya que dentro de este sector se encuentra el área de fraude, quien se encarga de monitorear el cumplimiento de las políticas internas y externas de las compañías.					

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE 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

N° Dimensiones/ítems		Pertinencia		Relevancia		Claridad		Sugerencia
PERFIL DEL ENCUESTADO		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
Nombre del encuestado								
Cargo								
Empresa								
Variable 1: ISO 27001: Seguridad de la información								
DIMENSIÓN 1 Sistema de gestión de seguridad de la información		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Un sistema de gestión de seguridad de la información implementado de acuerdo con el estándar ISO 27001 garantiza la protección de los recursos de información administrados por una entidad.	X		X		X		
2	La certificación ISO 27001 genera un impacto positivo en la mente de los clientes, potenciales clientes y partes interesadas, dado que proyecta protección, confidencialidad y seguridad en el uso de la información que se almacena como parte del proceso operativo del negocio.	X		X		X		
3	Una de las ventajas competitivas del sistema de gestión de seguridad de la información es la mejor gestión económica en la inversión de la mejora continua de la seguridad de la información.	X		X		X		

4	Conseguir concientización sobre la gestión de la seguridad y protección de los activos de información entre empleados y directivos es decisivo para garantizar la continuidad del negocio.	X		X		X		
5	Una implementación eficiente y eficaz de la ISO 27001 mitiga riesgos potenciales asociados a la adaptación de tecnologías emergentes relacionados a la digitalización de procesos a nivel organizacional.	X		X		X		
6	La ISO 27001 sirve para estructurar procesos dentro de una organización para asegurar la continuidad del negocio previniendo especialmente ataques cibernéticos que afectan las funciones de las entidades.	X		X		X		
DIMENSIÓN 2 **Ciberseguridad**		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
7	La adopción de políticas sobre la ciberseguridad representa una ventaja competitiva en el mercado.	X		X		X		
8	La ciberseguridad es importante en relación con la infraestructura tecnológica, ya que evidencia la capacidad con la que cuenta una entidad para proteger la información privada de los clientes ante un competidor.	X		X		X		
9	La ciberseguridad aborda políticas de gestión de peligros cibernéticos para mitigar alguna contingencia cibernética y resguardar la continuidad del negocio.	X		X		X		

10	El ciberespacio es un escenario donde se han producido oportunidades y a la vez conflictos producto del desarrollo constante de las comunicaciones y tecnologías de la información, por lo cual es importante tomar medidas como la ciberseguridad.	X		X		X		
DIMENSIÓN 3 **Ciberataques**		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
11	Los ciberataques violan las políticas de seguridad de un activo cibernético para dañar e interrumpir el acceso de la información o servicios de dicho activo generando pérdidas económicas.	X		X		X		
12	La ejecución de escenarios realistas sirve para localizar y afrontar vulnerabilidades en la infraestructura de red.	X		X		X		

Variable 2: Principio de negocio en marcha								
DIMENSIÓN 1 Situación financiera		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
13 13	Los indicadores financieros de la empresa son importantes porque miden la situación financiera de la misma.	X		X		X		
14	Los principales indicadores a considerar para mantener un adecuado estado financiero para las empresas son: liquidez, rentabilidad y solvencia.	X		X		X		
15	Los ratios son indicadores que se calculan de los estados financieros que permiten evaluar posibles riesgos económicos y tomar decisiones para mitigar dichos riesgos.	X		X		X		
16	Los ratios de rentabilidad permiten evaluar la capacidad de la empresa en generar ganancias con una mínima inversión.	X		X		X		
17	Los ratios de rentabilidad y liquidez guardan relación entre sí porque son importantes para los acreedores, ya que indican la capacidad que posee la compañía para afrontar sus obligaciones a corto y mediano plazo.	X		X		X		
DIMENSIÓN 2 Situación Operativa		**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
18	Las entidades con pérdidas netas en periodos consecutivos podrían generar patrimonio negativo, lo cual conllevaría a ser una causal de disolución.	X		X		X		
19	La situación operativa se evalúa en función de los riesgos operativos del entorno de la empresa.	X		X		X		

20	La escasez de personal especializado en el sector TI influye en la situación operativa de la empresa.	X		X		X		
21	El déficit de profesionales en el sector TI encarece el servicio y a su vez retrasa la puesta en marcha de los proyectos.	X		X		X		
22	Las compañías buscan profesionales de TI con perfiles híbridos como habilidades blandas y habilidades técnicas.	X		X		X		
23	El perfil del personal encargado de TI es muy importante, ya que dentro de este sector se encuentra el área de fraude, quien se encarga de monitorear el cumplimiento de las políticas internas y externas de las compañías.	X		X		X		

Observaciones (precisar si hay suficiencia):

Sin observaciones

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ] **Apellidos y nombres del experto validador: Tenorio Bejar, Javier Manuel**

DNI: 45008462

Especialidad del experto validador: Auditor Financiero

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

……

Firma del experto

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.