Universidad Nacional
SAN LUIS GONZAGA

“Año de la recuperación y consolidación de la economía peruana”

CONSTANCIA DE ANTIPLAGIO

El que suscribe director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas de la UNICA, deja constancia que se ha realizado el análisis con el software de verificación de similitud al documento **INFORME FINAL DE TESIS** titulado:

Gestión de tecnologías de información y comunicación para los procesos de seguridad informática en MYPES comerciales, Distrito de Ica, 2024

Presentado por:

GUZMAN CHUQUIHUACCHA HUGO ANTHONY

BACHILLER en **PREGRADO** de la facultad de Ingeniería de Sistemas; cuyo resultado obtenido es **porcentaje de similitud 0%**; por el cual se otorga el calificativo de: **APROBADO,** según el Reglamento de Evaluación de la Originalidad; adjuntando al presente, el reporte de evaluación con el software de verificación de originalidad.

Se expide la presente conformidad para la continuación del trámite respectivo.

Ica, 22 de setiembre de 2025

Dr. LUIS ALBERTO MASSA PALACIOS
Director de la Unidad de Investigación
Facultad de Ingeniería de Sistemas

UNIVERSIDAD NACIONAL “SAN LUIS GONZAGA”
VICERRECTORADO DE INVESTIGACIÓN
FACULTAD DE INGENIERÍA DE SISTEMAS
PROGRAMA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

Gestión de tecnologías de información y comunicación para los procesos de seguridad informática en MYPES comerciales, Distrito de Ica, 2024

Línea de Investigación:

Ciencias naturales, ingeniería y tecnologías sostenibles

INFORME FINAL DE TESIS

Presentado por:

BACH. GUZMAN CHUQUIHUACCHA, Hugo Anthony

Ica, Perú

2025

DEDICATORIA

Dedico esta tesis con todo mi amor a mi familia, especialmente a mis padres, por ser mi base, por su apoyo incondicional y por impulsarme a seguir adelante en cada momento.

Y con el corazón en la mano, dedico este logro a mi querida tía Marina, quien en vida creyó profundamente en mí y fue quien me motivó a dar el primer paso. Sin su impulso, quizás este camino nunca habría comenzado. Aunque ya no esté físicamente, su recuerdo y todo lo que me enseñó seguirán guiándome siempre.

AGRADECIMIENTOS

Agradezco a Dios por darme la fuerza para culminar esta etapa.

A mi asesor, el ingeniero Jhon Romero Lovera, por su orientación, paciencia y valiosos aportes durante el desarrollo de esta tesis.

A mis padres, por su apoyo incondicional, confianza y por acompañarme en cada paso del camino.

Y a todas las personas que, de una u otra forma, me brindaron su ayuda y aliento durante este proceso. Muchas gracias.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente estudio tiene como objetivo analizar cómo la gestión de TIC’s impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024. A través de un enfoque cuantitativo y un diseño correlacional - transversal, se evaluaron los datos obtenidos de una muestra de 338 representantes de las MYPES comerciales del distrito de Ica. Se utilizó el coeficiente de Spearman para determinar la relación entre las variables y se encontró una correlación buena, con un valor de 0.607. Los hallazgos indican que las variables analizadas ejercen una influencia significativa en las prácticas y resultados de las MYPES comerciales en el distrito de Ica. Este hallazgo abre la posibilidad de implementar nuevas estrategias o políticas de gestión que aprovechen esta relación para optimizar la eficiencia y competitividad del sector. En particular, si alguna de las variables refleja un elemento fundamental de la gestión empresarial, como la administración de recursos, el uso de tecnología o la capacitación, las MYPES podrían beneficiarse considerablemente al perfeccionar estos aspectos para impulsar el desarrollo y la sostenibilidad de sus negocios. En este sentido, los hallazgos subrayan la importancia de profundizar en el análisis de cómo estas variables se interrelacionan y afectan el desempeño de las MYPES comerciales en Ica, lo cual representa una oportunidad clave para la mejora continua y el fortalecimiento del sector en la región.

Palabras claves: Gestión de TIC´S, seguridad informática.

ABSTRACT

The present study aims to analyze how ICT management impacts computer security processes for commercial MSMEs, Ica district, 2024. Through a quantitative approach and a correlational-cross-sectional design, the data obtained from a sample of 338 representatives of commercial MSMEs in the Ica district were evaluated. The Spearman coefficient was used to determine the relationship between the variables and a good correlation was found, with a value of 0.607. The findings indicate that the variables analyzed exert a significant influence on the practices and results of commercial MSMEs in the Ica district. This finding opens the possibility of implementing new management strategies or policies that take advantage of this relationship to optimize the efficiency and competitiveness of the sector. In particular, if any of the variables reflect a fundamental element of business management, such as resource management, use of technology or training, MSMEs could benefit considerably from improving these aspects to boost the development and sustainability of their businesses. In this sense, the findings underline the importance of further analyzing how these variables interrelate and affect the performance of commercial SMEs in Ica, which represents a key opportunity for continuous improvement and strengthening of the sector in the region.

Keywords: ICT management, computer security.

I. INTRODUCCIÓN

A. Planteamiento del problema

El entorno tecnológico desarrollo en los ámbitos internacionales según **Pérez [1]** ha demostrado que la seguridad y protección de la información es una necesidad cada vez mayor, ya que, los ataques están abarcando una mayor escala, amenazando a distintas organizaciones indistintamente del tamaño que estas posean. Por su parte, los mecanismos informáticos se han visto reforzados en una medida igual al avance de los ataques, llegando a ser implementadas tanto dentro de empresas públicas como privadas. Asimismo, su utilización responde a la simplificación de diversas actividades llevadas a cabo en las áreas que integran una organización, por lo cual, resulta importante reforzar las defensas vigentes a fin de salvaguardarlas.

En Latinoamérica se precisa una evolución de la infraestructura tecnológica, buscando reforzar el acceso a internet dentro de un entorno seguro. Pese a ello, estos esfuerzos de mejora no han respondido en la misma medida en que los ataques cibernéticos han aumentado y reforzado, esto se debe, a los problemas de inversión por temas políticos. Es decir, existe una integración muy débil de las TIC's tanto a nivel de gestión como productivo, Si bien las medianas y grandes empresas ya habían informatizado su gestión administrativa a diversas escalas antes de la aparición de los ordenadores, fue con su aparición, su coste decreciente, también debido a su uso fácil y flexible, que la informática empezó a penetrar en el mundo de las pequeñas y medianas empresas. medianas empresas industriales latinoamericanas.

La situación en Perú según **Quevedo [2]** pone en evidencia como gran parte de las instituciones no disponen de la información de manera oportuna e incluso siendo víctimas de innumerables intentos de robo de información, perjudicando ambas situaciones a la economía de las empresas y a la toma de decisiones. Asimismo, la seguridad en entornos digitales opera en un entorno asimétrico en el que los piratas informáticos tienen un potencial casi ilimitado para dañar a las empresas, mientras que los defensores no tienen margen de error. Por su parte, las autoridades resaltan la necesidad de invertir en programas de formación para atraer y retener el talento necesario y así mantener la seguridad de las empresas. Además, hacer que el sector sea menos dependiente de los recursos humanos, mediante la innovación en la ciberdefensa automatizada, también se está convirtiendo en un requisito previo esencial.

B. Antecedentes de la investigación

a. Antecedentes internacionales

1. **En 2024, Gordillo & Herrera [3],** se enfocaron en analizar los desafíos y oportunidades que surgen al integrar las Tecnologías de la Información y la

Comunicación (TIC) en las operaciones del Departamento de Talento Humano de un Gobierno Autónomo Descentralizado (GAD) Cantonal. Concretamente, se buscó evaluar el impacto de estas tecnologías en la optimización de los procesos administrativos. Mediante una metodología cualitativa, se recolectaron datos a través de encuestas, observaciones y entrevistas, y se complementó con una revisión exhaustiva de la literatura existente. Los resultados obtenidos evidencian una serie de limitaciones, entre las que destacan la obsolescencia tecnológica, restricciones presupuestarias y la falta de una planificación estratégica para maximizar el uso de los recursos disponibles. Concluyeron que la implementación de las recomendaciones derivadas de este estudio puede significar un avance significativo en la modernización de la gestión del talento humano en el GAD analizado. Al dotar al departamento de equipos adecuados y al optimizar los procesos, se puede agilizar la atención a las necesidades del personal y mejorar la eficiencia general de la organización.

2. **En 2022, López [4],** llevó a cabo una investigación en 2022 cuya finalidad fue evaluar los factores involucrados en las actividades de ataques cibernéticos en contraste con el empleo de TIC's en España. En la metodología se utilizó una investigación cuantitativa, básica (tipo), correlacional (nivel) y no experimental (diseño). De igual manera, en la presente pesquisa, la muestra se integró por empleados y expertos en la materia, siendo recolectado los datos por medio de encuestas y entrevistas respectivamente. Ante ello, el autor finalizó su estudio concluyendo que, existe un incremento en cuanto a la utilización de las TIC's en conjunto con medidas de ciberseguridad, con el fin de proteger datos valiosos para las empresas, siendo una respuesta al aumento de la actividad delictiva por redes.
3. **En 2020, Alfaro [5],** llevó a cabo una investigación en 2020 cuya finalidad fue evaluar la aplicación de protocolos de ciberseguridad para la maximización de la participación del mercado chileno. En la metodología se utilizó una investigación cuantitativa, básica (tipo), explicativo (nivel) y pre experimental (diseño). De igual manera, en la presente pesquisa, la muestra se integró por la información financiera y económica de una empresa chilena, empleándose el análisis econométrico y la revisión bibliográfica para la obtención de información. Ante ello, el autor finalizó su estudio concluyendo que, las aplicaciones de los protocolos de ciberseguridad facilitan la protección de datos para las organizaciones, debido a que, se protege elementos tales como los perfiles de proveedores y clientes.

4. **En 2020, Téllez [6],** llevó a cabo una investigación en 2018 cuya finalidad fue evaluar el rol de las TIC's con respecto al tratamiento de la información en una institución española. En la metodología se utilizó una investigación cualitativa, básica (tipo), descriptiva (nivel) y no experimental (diseño). De igual manera, en la presente pesquisa, la muestra se integró por trabajos investigativos previos, aplicando una análisis documental y revisión bibliográfica para su obtención. Ante ello, el autor finalizó su estudio concluyendo que, las TIC's son un objetivo claro de ataque por parte de los delincuentes informáticos, esto se debe a la cantidad y valor de la información que se maneja, perjudicando en una gran medida a la empresa si dicha información es robada.

b. Antecedentes nacionales

1. **En 2023, Silva [7],** propuso en su estudio diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en una PYME, con el fin de fortalecer su protección frente a amenazas a la seguridad de la información. Se adoptó la norma NTP-ISO/IEC 27001:2014, que ofrece directrices para establecer, mantener y mejorar continuamente un SGSI. A través de su aplicación, se implementó un ciclo de mejora continua enfocado en la identificación y tratamiento de riesgos. Los resultados mostraron que el SGSI mejoró significativamente la confidencialidad, integridad y disponibilidad de los activos de información de la PYME. En conclusión, la norma NTP-ISO/IEC 27001:2014 demostró ser eficaz para gestionar la seguridad de la información en PYMEs, alineándose con las mejores prácticas internacionales.
2. **En 2022, Huaylla & Vargas [8],** El estudio tuvo como objetivo analizar la correlación entre la gestión de las tecnologías de la información y la comunicación (TIC) y la seguridad informática en el Gobierno Regional de Apurímac durante 2021. Utilizando un enfoque cuantitativo y un diseño correlacional-descriptivo, se trabajó con una muestra de 68 empleados seleccionados aleatoriamente de una población de 82, a quienes se les aplicó una encuesta. Los resultados, obtenidos mediante el coeficiente de correlación de Pearson (0.663) y un p-valor de 0.000, demostraron una relación significativa y positiva entre las variables. Se concluyó que una gestión eficiente de las TIC, respaldada por infraestructura tecnológica sólida, arquitectura adecuada, talento humano capacitado y un buen conocimiento de los sistemas, mejora la seguridad informática al garantizar la confidencialidad, integridad y disponibilidad de la información, factores

clave para la toma de decisiones y el cumplimiento de las políticas de seguridad.

3. **En 2021, Crespo [9],** llevó a cabo una investigación cuya finalidad fue evaluar el vínculo entre las TIC's y las actividades de gestión administrativa de una municipalidad. En la metodología se utilizó una investigación cuantitativa, básica (tipo), correlacional (nivel) y no experimental (diseño). De igual manera, en la presente pesquisa, la muestra se integró por 69 colaboradores de la institución antes mencionada, completando una serie de preguntas que integran un cuestionario. Ante ello, el autor finalizó su estudio concluyendo que, se precisa un vínculo bajo pero significativo entre las variables, representado por un valor Rho = 0.317 y un p valor = 0.008 respectivamente.
4. **En 2021, Rossi [10],** llevó a cabo una investigación cuya finalidad fue evaluar los protocolos de ciberseguridad y las amenazas hibridas en Perú respecto a las estrategias de política exterior. En la metodología se utilizó una investigación cualitativa, básica (tipo), descriptiva (nivel) y no experimental (diseño). De igual manera, en la presente pesquisa, la muestra se integró por reportes, informes y trabajos previos relacionados a las variables de investigación, aplicando un análisis de la información. Ante ello, el autor finalizó su estudio concluyendo que, la seguridad en el mundo cibernético se está convirtiendo en una necesidad para responder a las exigencias de las políticas exteriores, con el fin de proteger la información que se comparte entre ellos.
5. **En 2021, Izquierdo [11],** llevó a cabo una investigación en 2021 cuya finalidad fue estudiar los protocolos de ciberseguridad implementados para proteger la información manejada por una farmacia. En la metodología se utilizó una investigación cuantitativa, básica (tipo), correlacional (nivel) y no experimental (diseño). De igual manera, en la presente pesquisa, la muestra se integró por 41 colaboradores de la farmacia, completando una serie de preguntas plasmadas en un cuestionario. Ante ello, el autor finalizó su estudio concluyendo que, se requiere tanto de herramientas tecnológicas como de actividades formativas para llevar a cabo protocolos de seguridad informática dentro de una empresa.

c. Antecedentes locales

La revisión documental de investigaciones previos no generó resultados en cuanto a tesis o artículos científicos que compartan las variables seleccionadas dentro de un enfoque local.

C. Bases teóricas

a. Gestión de TIC´S

Para **Ferrero et al. [12],** son el conjunto de equipamientos y medios a través de los cuales se asegura el análisis, manejo y comprensión de los distintos volúmenes de información. Asimismo, se ven involucradas aquellas actividades orientadas al monitoreo de los sistemas informáticos en búsqueda de garantizar un mayor crecimiento y competitividad dentro de las organizaciones.

Por su parte, las TIC's representan las herramientas que contribuyen a la accesibilidad de los datos y la manipulación de los mismos por medio de distintas tecnologías. Su desarrollo y evolución constante convierte a cada uno de los involucrados en un agente importante y valioso para la cadena de transferencia y manejo de la información, en otras palabras, la cadena de valor respecto al conocimiento genera un impacto significativo en cualquier tipo de información, al brindar de datos oportunos para dar una correcta respuesta a los acontecimientos externos.

Estas tecnologías aportan en gran medida a las distintas organizaciones, representando herramientas que facilitan la transmisión de datos en tiempo real sirviendo de soporte para la toma de decisiones, optimizando actividades que van desde el envío de correos electrónicos hasta el uso de plataformas o softwares especializados.

Para **Crespo [9],** La gestión de las Tecnologías de la Información y Comunicación (TIC) consiste en el conjunto de actividades a través de las cuales las organizaciones supervisan, coordinan y optimizan el empleo de su infraestructura tecnológica, sistemas de información y recursos de comunicación. Su propósito es garantizar que estos elementos contribuyan eficazmente al logro de los objetivos estratégicos y operativos de la entidad.

Las TIC han emergido como un factor estratégico clave para el éxito empresarial. Al permitir la integración de sistemas y la automatización de procesos, las TIC optimizan la eficiencia operativa y facilitan la toma de decisiones basadas en datos. Además, las TIC han democratizado el acceso a la información, lo que ha empoderado a los empleados y ha fomentado una mayor colaboración y agilidad organizacional.

Objetivos principales de la gestión de TIC

- Soporte a la toma de decisiones: Facilitar el acceso a datos relevantes y análisis en tiempo real, proporcionando a los responsables de la organización herramientas y conocimiento que permitan tomar decisiones fundamentadas y estratégicas.
- Optimización de recursos: Garantizar que las inversiones realizadas en tecnología sean eficientemente aprovechadas, maximizando su rentabilidad y asegurando que contribuyan de manera directa al cumplimiento de los objetivos estratégicos de la organización.
- Innovación tecnológica: Fomentar la incorporación de tecnologías emergentes que potencien la capacidad competitiva de la organización, promoviendo mejoras en los procesos, productos y servicios que fortalezcan su posición en el mercado.
- Seguridad de la información: Salvaguardar los activos digitales de la organización frente a posibles amenazas cibernéticas, garantizando la confidencialidad, integridad y disponibilidad de los datos críticos para el funcionamiento empresarial.

Importancia de las tecnologías y comunicación

La relevancia de las Tecnologías de la Información y la Comunicación (TIC) para las empresas, especialmente en lo que respecta a la toma de decisiones, subraya la necesidad de que los gerentes posean un conocimiento profundo sobre estas tecnologías. De acuerdo con **Castañeda [13],** las TIC desempeñan un papel fundamental en el desarrollo y el funcionamiento de las empresas.

- Las Tecnologías de la Información y la Comunicación (TIC) están transformando significativamente la manera en que se llevan a cabo las actividades y se gestionan los recursos dentro de las empresas.
- Estos avances aportan elementos esenciales que facilitan un desarrollo organizacional más eficiente y productivo.
- Las TIC favorecen la agilización de la comunicación interna y externa, promoviendo un trabajo colaborativo y sinérgico.
- Juegan un papel crucial en la promoción de productos en el mercado, contribuyendo al aumento de la productividad empresarial.
- La comunicación asertiva, facilitada por las redes sociales, se ha consolidado como un componente clave en este proceso.

Componentes de las tecnologías de información y comunicación

De acuerdo con **Cortés [14],** las Tecnologías de la Información y la Comunicación (TIC) surgen a partir de tres eventos fundamentales, los cuales constituyen su base conceptual y operativa (párr. 1). Estos elementos son:

- Infraestructura de comunicaciones garantiza la interconexión y transmisión eficiente de datos, asegurando la calidad, seguridad y rapidez de las comunicaciones.
- Hardware, como soporte físico, subyace a todas las operaciones informáticas, desde el procesamiento hasta el almacenamiento de datos.
- Software, como componente lógico, permite la gestión y manipulación de la información.

Clasificación de las tecnologías de información y comunicación.

Marqués [15], destaca que es crucial incluir todas las redes de comunicación social interpersonales, tales como el teléfono o el fax, dentro de la categoría de Tecnologías de la Información y Comunicación (TIC). Esta clasificación puede dividirse en tres grandes grupos:

- Los servicios TIC: comprenden servicios como buscadores, navegadores, banca y comercio electrónico, administraciones públicas, servicios educativos y de salud, blogs, entre otros (párr. 1).
- Las redes: incluyen la telefonía fija y móvil, televisión (digital, satelital, etc.), banda ancha, entre otros.
- Las terminales: abarcan equipos informáticos, dispositivos de vídeo, reproductores de Blu-ray, mp3-4-5, terminales móviles, televisores, consolas, y otros aparatos electrónicos.

Las tecnologías de información y comunicación en las empresas.

Ca' Zorzi [16] destaca la versatilidad de las TIC en el ámbito empresarial, evidenciando su aplicación en una amplia gama de áreas. Desde la inteligencia de mercado y la gestión de la relación con el cliente hasta la automatización industrial y la toma de decisiones, las TIC se han convertido en herramientas indispensables para mejorar la competitividad organizacional. Estas aplicaciones, que van desde las más genéricas, como los sistemas de información, hasta las más especializadas, como los sistemas de inteligencia artificial, permiten a las empresas optimizar sus procesos, acceder a nuevos mercados y fortalecer su posición en el entorno competitivo.

- Uso infraestructural o genérico, que abarca las herramientas básicas para la comunicación, como la telefonía, el correo electrónico y la mensajería

instantánea. Estas tecnologías proporcionan la base para la interacción y el intercambio de información dentro y fuera de la organización.

- Uso especializado se refiere a la aplicación de las TIC en procesos de negocio específicos, como la gestión de la cadena de suministro, la inteligencia de mercado o la toma de decisiones, permitiendo a las organizaciones optimizar sus operaciones y obtener una ventaja competitiva.
    - El impulso de actividades de comercio exterior
    - La gestión de recursos humanos
    - La infraestructura tecnológica que sustenta a toda la organización
    - La administración de la cadena de suministro (SCM)
    - La gestión de relaciones con los clientes
    - La promoción y visibilidad de la empresa en la web
    - La venta a través de canales digitales, tanto en el modelo de negocio directo al consumidor (B2C) como de empresa a empresa (B2B)
    - La optimización de la gestión estratégica
    - El apoyo a la toma de decisiones empresariales mediante la inteligencia de negocios (BI)
    - La gestión financiera a través de sistemas de planificación de recursos empresariales (ERP)
    - La mejora de los procesos De producción mediante el sistema de planificación de recursos de producción (RPM)
    - La distribución de productos y servicios

Dimensiones de tecnología de información y comunicación.

Según las perspectivas de **Rodríguez & Peña [17],** quienes analizan el enfoque integral de las Tecnologías de la Información y Comunicación (TIC), estas se examinan desde cinco dimensiones fundamentales.

Talento humano: Constituye uno de los pilares fundamentales en la gestión de las TIC, dado que las tecnologías avanzadas dependen estrechamente de las habilidades y competencias del personal que las maneja. Esta dimensión engloba la capacidad del personal para gestionar, implementar y utilizar de manera efectiva las herramientas tecnológicas dentro del contexto organizacional. No solo implica la contratación de profesionales cualificados, sino también su desarrollo y capacitación continua en nuevas tecnologías, sistemas y procesos. La formación continua asegura que los empleados estén actualizados con los avances tecnológicos y sean capaces de gestionar de forma eficiente los sistemas de

información. Además, el talento humano desempeña un papel crucial en la implementación de políticas de seguridad y en la resolución de problemas asociados con la infraestructura tecnológica (p. 55).

Conocimiento al negocio: La orientación al negocio se refiere a cómo las TIC se alinean con los objetivos estratégicos y operacionales de la organización. La integración de las tecnologías con las necesidades empresariales es esencial para garantizar que la inversión en TIC tenga un impacto positivo en el rendimiento de la empresa. Esta dimensión implica que las decisiones tecnológicas deben centrarse en la maximización de la competitividad y eficiencia organizacional. Las TIC no deben considerarse un fin en sí mismas, sino como un medio para mejorar los procesos de negocio, aumentar la productividad, optimizar la toma de decisiones y facilitar la innovación dentro de la empresa. Un enfoque orientado al negocio asegura que las tecnologías implementadas respondan a necesidades concretas y contribuyan al logro de los objetivos empresariales.

Arquitectura: La arquitectura en la gestión de las TIC se refiere a la estructura tecnológica que sustenta las operaciones organizacionales, abarcando la infraestructura de hardware, software y redes. Esta dimensión involucra el diseño y la configuración de los sistemas tecnológicos, asegurando que sean escalables, seguros y eficientes. Además, la arquitectura implica la creación de una infraestructura flexible que permita a la empresa adaptarse rápidamente a los cambios en el entorno digital y tecnológico. Un diseño adecuado de la arquitectura tecnológica facilita la integración de diversos sistemas y la gestión fluida de la información, lo cual es crucial para una operación ágil y efectiva. La arquitectura también juega un papel esencial en la seguridad informática, ya que una infraestructura bien diseñada protege los datos y los activos digitales de las amenazas internas y externas.

Relación entre Gestión de TIC y Seguridad Informática

La gestión de las tecnologías de información y comunicación (TIC) y la seguridad informática mantienen una relación intrínseca, dado que ambas se orientan a garantizar la operación eficiente y segura de los sistemas tecnológicos en las organizaciones. Mientras que la gestión de las TIC se enfoca en optimizar el uso estratégico de las tecnologías para alcanzar los objetivos organizacionales, la seguridad informática vela por el funcionamiento de estas tecnologías en un entorno resguardado frente a posibles amenazas y vulnerabilidades.

La incorporación de medidas de seguridad informática dentro de la gestión de las TIC permite a las organizaciones reducir riesgos cibernéticos, asegurar la continuidad operativa y proteger los datos críticos de manera efectiva. Este

enfoque integrado no solo refuerza la confianza en la infraestructura tecnológica, sino que también contribuye al fortalecimiento de la competitividad y sostenibilidad empresarial en un entorno digital en constante evolución.

b. Procesos de seguridad informática

Según Rocha [18], es el conjunto de técnicas especializadas en la protección de los sistemas y datos informáticos contra intrusiones, accesos no autorizados, daños o ataques. Su finalidad radica en asegurar la integridad, confidencialidad y disponibilidad de la información y los recursos informáticos. Implica la implementación de medidas preventivas, como el uso de software antivirus, sistemas de detección de intrusos, firewalls, así como la implementación de protocolos y procedimientos de recuperación en caso de incidente.

En otras palabras, corresponde a la toma en cuenta de un conjunto más amplio de limitaciones, problemas, riesgos y soluciones, para desarrollar la seguridad en la TIC's. Este concepto resulta esencial para mitigar ataques e intentos de phishing, sustracción de información, violaciones de seguridad y eliminación de activos. Todos los dispositivos, como tabletas y teléfonos inteligentes, corren cada vez más riesgos porque ahora almacenan más datos públicos y privados que la mayoría de las computadoras.

Dicho concepto se ha convertido en el eje central de la presente era digital, moldeada por la tecnología ubicua. A medida que las amenazas en línea continúan evolucionando y volviéndose más sofisticadas, la seguridad se ha convertido en una preocupación vital para las empresas, los gobiernos y los individuos. Este ofrece una variedad de perspectivas profesionales desafiantes, que van desde el análisis de seguridad hasta la consultoría en sí mismo, y abarcan una diversidad de habilidades e intereses. La creciente demanda de profesionales garantiza una relativa seguridad laboral en una industria en constante cambio.

Según **Gómez [19],** la seguridad informática puede definirse como el conjunto de medidas destinadas a prevenir la realización de acciones no autorizadas en un sistema o red informática, con el objetivo de evitar posibles perjuicios a la información y proteger sus principios fundamentales: confidencialidad, autenticidad, disponibilidad e integridad (p. 40).

Por otro lado, conforme a la norma ISO 7498, la seguridad informática se entiende como un conjunto de mecanismos diseñados para reducir la vulnerabilidad de los bienes y recursos dentro de una organización. **Gómez [19].**

Según **Romero [20],** la seguridad informática se define como la disciplina encargada de desarrollar y establecer normas, procedimientos, métodos y técnicas

con el propósito de asegurar que un sistema de información sea seguro, confiable y, lo más importante, esté disponible en todo momento.

Importancia de la seguridad informática.

Para **Romero [20],** diversas acciones cotidianas en el uso de la tecnología están orientadas a asegurar la protección de la seguridad informática a lo largo de todo el proceso y los canales por los cuales transitan los datos. De esta manera, resalta la relevancia crucial de la seguridad informática en la gestión de la información, tales como:

- Defenderse de los hackers, quienes pueden paralizar el funcionamiento de los sistemas informáticos, provocando la pérdida de información, fallas en los servidores e impidiendo el acceso a la web.
- Prevenir ataques de virus, como troyanos, gusanos, entre otros.
- Combatir la suplantación de identidad y el espionaje a través de las redes sociales.
- En el ámbito de las comunicaciones, los datos almacenados en un dispositivo pueden ser mal utilizados por usuarios no autorizados.
- Enfrentar la amenaza de intrusos, quienes pueden alterar o modificar los códigos fuente de los programas, o usar imágenes o cuentas de correo electrónico fraudulentas para generar contenido dañino al propietario del usuario.
- La protección y seguridad de los datos debe garantizarse, asegurando su confidencialidad.
- Se debe prevenir el robo de información, incluyendo bases de datos, números de cuentas bancarias, tarjetas de crédito, contraseñas, entre otros.
- Protegerse contra los ciber-delincuentes, que pueden acceder a los sistemas con intenciones maliciosas y dañar otros equipos, sitios web o redes para causar caos.

Clasificación de la seguridad informática.

La seguridad informática, según **Romero et al. [21],** se puede clasificar en tres componentes fundamentales:

- Información: Es el aspecto más crítico de la seguridad informática. Se debe garantizar su protección para evitar que sea accesible a personas no autorizadas, asegurando su integridad y confidencialidad.

- Infraestructura: Es uno de los elementos más vigilados dentro de la seguridad informática, ya que su protección depende de los procesos que se gestionan en la organización, los cuales requieren una supervisión constante para mantener su integridad.
- Usuarios: Son los individuos que, a menudo, resultan difíciles de controlar. Estos pueden cometer errores, olvidar información o enfrentar accidentes que generen la pérdida de trabajo valioso, afectando el desarrollo realizado durante un largo periodo.

Objetivos de seguridad informática.

Según **Gómez [19],** los objetivos fundamentales de la seguridad informática se orientan a:

- Limitar las pérdidas y asegurar la efectiva recuperación del sistema informático en caso de que ocurra una contingencia relacionada con la seguridad.
- Cumplir con el marco legal y los requisitos establecidos por los clientes en los contratos correspondientes.
- Minimizar y gestionar riesgos, así como a detectar posibles contingencias y amenazas que puedan comprometer la información.
- Garantizar el uso adecuado de los recursos y aplicaciones dentro de cualquier sistema informático, promoviendo su correcto funcionamiento. (p. 44).

Factores de seguridad informática.

Según **Gómez [19],** la seguridad informática de un sistema depende de diversos factores, entre los cuales se destacan los siguientes:

- Las restricciones en la asignación de permisos y privilegios a los usuarios, lo cual es fundamental para evitar accesos no autorizados.
- La correcta instalación, configuración y mantenimiento de los equipos tecnológicos e informáticos, garantizando su operatividad y seguridad.
- El soporte técnico proporcionado por los fabricantes de hardware y software, que debe asegurar el funcionamiento continuo y seguro de los sistemas informáticos.
- La sensibilización de las autoridades y responsables de la empresa, quienes deben ser conscientes de la necesidad imperiosa de asignar recursos financieros para garantizar la seguridad informática.

- La formación y la asunción de responsabilidades por parte de los usuarios y operadores de las aplicaciones informáticas, quienes deben estar preparados para manejar adecuadamente los sistemas. (p. 43)

Tipos de seguridad informática.

Según **Molinetti [22],** existen diversas categorías de seguridad informática, las cuales varían en su aplicación e importancia dentro de las organizaciones. Estos tipos de seguridad son los siguientes: (párr. 1):

1. La seguridad de la red se refiere a la protección de información sensible, como documentos, datos personales, bancarios y contraseñas, en Internet, con el fin de prevenir amenazas como la suplantación de identidad, software espía, phishing, virus, entre otros. En el contexto empresarial, esta forma de seguridad es esencial, y se implementan diversos mecanismos para garantizar su efectividad. Entre estos se incluyen:
    - Antispyware: Herramientas que previenen el robo de información confidencial por parte de terceros.
    - Redes Privadas Virtuales (VPN): Infraestructuras de red que extienden una red interna (LAN) hacia la red pública (Internet), proporcionando una capa adicional de seguridad. (párr. 1)
    - Antivirus: Programas diseñados para proteger los sistemas informáticos contra ataques de virus, troyanos y worms.
2. La seguridad del software se enfoca en proteger las aplicaciones contra posibles ataques maliciosos. Aunque un antivirus puede ser una opción útil, la seguridad informática requiere soluciones más especializadas y precisas, tales como:
    - Cortafuegos (firewall): Dispositivos o programas que supervisan y controlan el tráfico de datos dentro de una red. Ejemplos de estos incluyen Application Gateway, Packet Filter y Proxy Server.
    - Software de filtración de contenidos: Herramientas que actúan como un filtro para los usuarios que acceden a Internet, protegiendo contra amenazas como el phishing.
3. La seguridad del hardware se refiere a la protección física de los equipos tecnológicos, e incluye:
    - Sistema de Alimentación Ininterrumpida (SAI) o UPS: Equipos que proporcionan electricidad a los dispositivos tecnológicos en caso de fallos en el suministro eléctrico, garantizando que los datos se almacenen adecuadamente y evitando la pérdida de información.

- Cortafuegos de hardware: Dispositivos físicos que se conectan al router, permitiendo bloquear conexiones potencialmente peligrosas o dañinas.
- Servidores proxy: Equipos dedicados (que también pueden ser software) que funcionan como intermediarios entre una computadora y un servidor determinado, gestionando el tráfico de datos.

Dimensiones de los procesos de seguridad informática.

Según VIU (2023), la seguridad informática abarca cuatro dimensiones fundamentales que deben ser consideradas de manera integral: Estas dimensiones garantizan que la información sea accesible únicamente por las personas autorizadas, que se mantenga intacta y libre de alteraciones no autorizadas, que esté disponible cuando se necesite y que se pueda verificar la identidad de los usuarios y la autenticidad de los datos.

Disponibilidad: Esta dimensión se refiere a la capacidad de garantizar que los sistemas, servicios y datos estén disponibles y operativos para los usuarios autorizados en el momento que lo necesiten. La disponibilidad es un factor clave para el funcionamiento continuo de las organizaciones, ya que permite el acceso ininterrumpido a los servicios esenciales, incluso durante emergencias o fallas técnicas. Para asegurar la disponibilidad, se deben implementar estrategias como respaldos de datos, redundancia en los sistemas y planes de recuperación ante desastres, que garanticen la continuidad de las operaciones ante cualquier eventualidad.

Confidencialidad: Esta dimensión se enfoca en proteger la información contra accesos no autorizados, asegurando que solo las personas o entidades con los permisos necesarios puedan acceder a datos sensibles. La confidencialidad es crucial para resguardar la privacidad de información personal, financiera o comercial, y se alcanza mediante la implementación de medidas como cifrado de datos, autenticación de usuarios y políticas de control de acceso estrictas, que garantizan que la información esté protegida frente a accesos indebidos.

Integridad: La integridad de la información implica mantener la exactitud y confiabilidad de los datos, asegurando que no sean alterados de forma no autorizada, ya sea accidentalmente o de manera maliciosa. La integridad es esencial para asegurar la calidad de la información utilizada en la toma de decisiones y para el correcto funcionamiento de los sistemas. Para proteger la integridad, se utilizan mecanismos como controles de acceso, auditorías y funciones de hash, que permiten verificar que los datos no hayan sido modificados sin autorización, preservando su fiabilidad.

Estas tres dimensiones son interdependientes y deben gestionarse de manera integral para garantizar la seguridad informática en cualquier organización.

Procesos de seguridad informática en las MYPES

VIU [23]: Procesos de seguridad informática en las MYPES

Los procesos de seguridad informática en las micro, pequeñas y medianas empresas (MYPES) consisten en un conjunto de prácticas y políticas diseñadas para proteger los activos digitales de la organización, tales como datos, información financiera y comunicaciones, frente a posibles amenazas internas y externas. Estas acciones incluyen desde la configuración de redes seguras y la capacitación del personal, hasta el desarrollo de protocolos de respuesta ante incidentes cibernéticos.

Los autores analizan las mejores prácticas para garantizar la protección de la información en el contexto de las MYPES, reconociendo su relevancia estratégica.

Importancia de la seguridad informática en las MYPES

La seguridad informática resulta esencial para salvaguardar la confidencialidad, integridad y disponibilidad de la información en un entorno digital cada vez más complejo. Las MYPES, debido a sus recursos limitados, son particularmente vulnerables a los incidentes de seguridad, lo que hace crucial implementar medidas efectivas que reduzcan los riesgos y fortalezcan su resiliencia frente a amenazas cibernéticas.

Procesos clave en la seguridad informática

- **Gestión de riesgos:** Identificación, análisis y mitigación de los riesgos asociados a posibles ataques cibernéticos y vulnerabilidades.
- **Control de accesos:** Implementación de políticas y mecanismos que regulen quiénes pueden acceder a la información y a los sistemas organizacionales, garantizando la restricción de accesos no autorizados.
- **Capacitación continua:** Formación y sensibilización permanente del personal en prácticas de seguridad y uso responsable de las tecnologías, para reducir errores humanos y fortalecer una cultura organizacional de ciberseguridad.

Relación entre la Gestión de TIC y la Seguridad Informática en las MYPES

Zuñiga et al. [24]: Vinculación entre la gestión de TIC y la seguridad informática en las MYPES. La interrelación entre la gestión de las Tecnologías de la Información y Comunicación (TIC) y la seguridad informática en las micro, pequeñas y medianas empresas (MYPES) constituye un aspecto esencial para

garantizar tanto la eficiencia operativa como la protección ante riesgos cibernéticos. Este nexo se fundamenta en el hecho de que una adecuada administración de las TIC puede potenciar significativamente los procesos de seguridad informática, mitigando vulnerabilidades y preservando la integridad de la información digital. En un contexto empresarial cada vez más digitalizado, esta sinergia resulta clave para alcanzar un desempeño sostenible y seguro en las organizaciones.

La gestión de las Tecnologías de la Información y Comunicación (TIC) comprende el conjunto de actividades y procesos orientados a la administración eficaz de los recursos tecnológicos de una organización. Esto incluye la infraestructura, el software, las redes y la formación del personal. Una adecuada gestión de las TIC resulta fundamental para impulsar la productividad en las micro, pequeñas y medianas empresas (MYPES), ya que permite optimizar aspectos clave como la comunicación, la toma de decisiones y la administración de la información. No obstante, el uso de estas tecnologías conlleva riesgos inherentes, tales como accesos no autorizados a los sistemas, pérdida de datos o infiltración de software malicioso, lo que subraya la necesidad de implementar estrategias robustas de seguridad informática.

Heredia [25] subraya la estrecha vinculación entre la gestión de las Tecnologías de la Información y la Comunicación (TIC) y la seguridad informática. Una gestión eficiente de las TIC se erige como la primera línea de defensa contra las amenazas cibernéticas, al integrar medidas de seguridad desde las etapas iniciales del diseño y configuración de los sistemas. De esta manera, las micro, pequeñas y medianas empresas (MIPYMES) pueden construir un entorno tecnológico más seguro y confiable, minimizando los riesgos asociados a los ciberataques.

La gestión estratégica de las TIC, según autores como **Heredia [25]** y **Pacheco & Rodríguez [26],** desempeña un papel crucial en la protección de las PYMES frente a los ciberataques. Al integrar la seguridad informática en la planificación y ejecución de las estrategias tecnológicas, las organizaciones pueden fortalecer su postura de seguridad y minimizar el riesgo de incidentes cibernéticos. Esta relación simbiótica entre la gestión de las TIC y la seguridad informática permite a las PYMES optimizar sus operaciones y alcanzar sus objetivos de negocio de manera segura y confiable.

Importancia para las MYPES

La gestión adecuada de las TIC en las PYMES no solo busca optimizar los procesos internos, sino también fortalecer la resiliencia de la organización frente a los ciberataques. Al integrar medidas de seguridad desde el diseño y la

implementación de los sistemas, las PYMES pueden construir una infraestructura tecnológica más segura y confiable. La seguridad informática, al garantizar la confidencialidad, integridad y disponibilidad de la información, se convierte en un pilar fundamental para el éxito a largo plazo de las PYMES.

Sinergia entre las TIC y la Seguridad Informática

La gestión de las Tecnologías de la Información y la Comunicación (TIC) y la seguridad informática conforman una simbiosis fundamental para el éxito de las micro, pequeñas y medianas empresas (MIPYMES). Esta sinergia se manifiesta en dos dimensiones principales: la implementación de tecnologías proactivas y la adopción de estrategias preventivas. Por un lado, las tecnologías proactivas, como los sistemas de detección de intrusos y los firewalls, actúan como escudos protectores ante las amenazas cibernéticas. Por otro lado, las estrategias preventivas, que incluyen la formación del personal y la creación de protocolos de respuesta a incidentes, garantizan una cultura de seguridad integral en la organización.

- **Enfocando en la importancia de las tecnologías proactivas**

  La gestión de las TIC en las MIPYMES debe ir más allá de la mera implementación de tecnologías. Es fundamental adoptar un enfoque proactivo que permita anticiparse a las amenazas y proteger los activos digitales de la organización. El uso de tecnologías como los sistemas de detección de intrusos, los firewalls y la encriptación de datos permite a las MIPYMES construir una defensa sólida frente a los ciberataques, minimizando el riesgo de incidentes y sus consecuencias.

- **Enfocando en la importancia de las estrategias preventivas**

  La seguridad informática no se limita a la implementación de herramientas tecnológicas. Es fundamental contar con una estrategia integral que abarque aspectos como la formación del personal, la creación de políticas de seguridad y la realización de auditorías periódicas. Al integrar la seguridad en todos los niveles de la organización, las MIPYMES pueden garantizar la protección de sus datos y sistemas, y construir una cultura de seguridad sólida.

D. Marco conceptual

- **Ataque cibernético**

  Un ciberataque puede definirse como cualquier acción hostil llevada a cabo en el ciberespacio con el propósito de vulnerar la seguridad de sistemas informáticos, redes o datos. Estos ataques, que pueden variar desde el robo de información

confidencial hasta la interrupción de servicios críticos, son perpetrados por actores maliciosos con diversos motivos, como el lucro económico, el espionaje industrial o el ciberterrorismo. La amplia gama de técnicas empleadas por los ciberdelincuentes, desde el phishing hasta los ataques de denegación de servicio, subraya la complejidad y la constante evolución de las amenazas cibernéticas.

- **Antivirus**

  Un antivirus es un software de seguridad esencial diseñado para salvaguardar la integridad de los sistemas informáticos al detectar, prevenir y eliminar malware. Al analizar constantemente el sistema en busca de actividades sospechosas, los antivirus actúan como una primera línea de defensa contra una amplia gama de amenazas cibernéticas, desde virus y troyanos hasta ransomware y spyware.

- **Barrera de entrada tecnológica**

  Las barreras de entrada tecnológicas son obstáculos que dificultan el acceso y la adopción de tecnologías avanzadas por parte de nuevos competidores o empresas más pequeñas. Estos obstáculos pueden ser de naturaleza económica, técnica o de conocimiento, y tienen un impacto significativo en la estructura de los mercados y la dinámica competitiva. La inversión inicial requerida, la necesidad de conocimientos especializados y la complejidad de las tecnologías son ejemplos de barreras que pueden limitar la entrada de nuevos actores y consolidar el poder de mercado de las empresas establecidas.

- **Control de accesos**

  Es una medida de seguridad que limita la accesibilidad de los usuarios a determinados módulos o espacios virtuales. Los usuarios deben presentar credenciales que el sistema verifica para poder autorizar el ingreso del usuario. Para los sistemas de control de acceso lógico, el tipo de credencial más común es una contraseña que sólo el usuario conoce.

- **Control de riesgos**

  Es el conjunto de actividades centradas en identificar y analizar a fin de controlar posibles riesgos de carácter de seguridad dentro las actividades diarias o en un proyecto. En otras palabras, tiene como objetivo reducir la probabilidad de fracaso o incertidumbre respecto de uno o varios factores que puedan impactar un negocio.

- **Programación**

  Son todas las acciones de codificación de programas informáticos destinados a multitud de sistemas informáticos (software, sitios web, aplicaciones web y móviles, módulos de extensión, etc.).

E. Problemas de la investigación

a. Problema general

PG: ¿Cómo la gestión de TIC's impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024?

b. Problemas específicos

1. ¿Cómo el talento humano impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024?
2. ¿Cómo la orientación al negocio impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024?
3. ¿Cómo la arquitectura impacta en los procesos de seguridad informática para las MYPES comerciales, distrito Ica, 2024?

F. Justificación

Se justifica en la parte teórica al generar aportes intelectuales y en términos conceptuales sobre las variables objeto de estudio, reforzando las bases para otras investigaciones que se lleven a cabo más adelante. Asimismo, se justifica en la parte práctica al brindar propuestas de mejora según los resultados que se presenten, sirviendo de refuerzo para la toma de decisiones en las MYPES comerciales dentro del distrito de Ica. Se justifica en la parte metodológica al establecer instrumentos y técnicas adecuadas para medir las variables seleccionadas y por ende realizar la comprobación de las hipótesis.

Importancia

La investigación posee una importancia en la medida que comprobará las aportaciones de las TIC's con respecto a las MYPES comerciales en distrito Ica, teniendo como principal foco el tema de la ciberseguridad y resguarda de los datos sobre clientes y proveedores. En otras palabras, se determinarán los criterios más relevantes sobre el acceso y transmisión segura de la información.

G. Objetivos de la investigación

a. Objetivo general

Analizar cómo la gestión de TIC's impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

b. Objetivos específicos

1. Evaluar cómo el talento humano impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.
2. Evaluar cómo la orientación al negocio impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.
3. Evaluar cómo la arquitectura impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

H. Hipótesis de la investigación

a. Hipótesis general

La gestión de TIC’s impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

b. Hipótesis específicas

1. El talento humano impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.
2. La orientación al negocio impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.
3. La arquitectura impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

I. Variables de la investigación

a. Variable independiente

Gestión de TIC’s.

b. Variable dependiente

Procesos de seguridad informática.

J. Operacionalización de variables

Tabla 1. Matriz de operacionalización de variable (X): Gestión de TIC's.

Variable (X)	Definición conceptual	Definición operacional	Dimensión	Indicadores
Gestión de TIC's	Para **Ferrero et al. [12],** son el conjunto de equipamientos y medios a través de los cuales se asegura el análisis, manejo y comprensión de los distintos volúmenes de información. Asimismo, se ven involucradas aquellas actividades orientadas al monitoreo de los sistemas informáticos en búsqueda de garantizar un mayor crecimiento y competitividad dentro de las organizaciones.	La operacionalización de la primera variable, se realizará por medio de la cuantificación de las dimensiones: talento humano, orientación al negocio y arquitectura.	Talento humano	Resultados Capacidad Cumplimiento Liderazgo Recursos
			Orientación al negocio	Efectividad Comunicación Responsabilidad Productividad Conocimiento
			Arquitectura	Conexión Políticas Riesgos Datos Planeación

Tabla 2. Matriz de operacionalización de variable (Y): Procesos de seguridad informática.

Variable (Y)	Definición conceptual	Definición operacional	Dimensión	Indicadores
Procesos de seguridad informática	Según **Rocha [18],** es el conjunto de técnicas y prácticas diseñadas para proteger los sistemas, redes y datos informáticos contra intrusiones, accesos no autorizados, daños o ataques	La operacionalización de la segunda variable, se realizará por medio de la cuantificación de las dimensiones: disponibilidad, confidencialidad y actividades.	Disponibilidad	Usuarios Información Almacenaje Datos Requerimientos
			Confidencialidad	Filtración Duplicidad Incidencias Accesos Codificación
			Integridad	Veracidad Prevención Protección Coherencia Datos Controles

II. ESTRATEGIA METODOLÓGICA

A. Tipo, nivel y diseño de investigación

a. Tipo de investigación

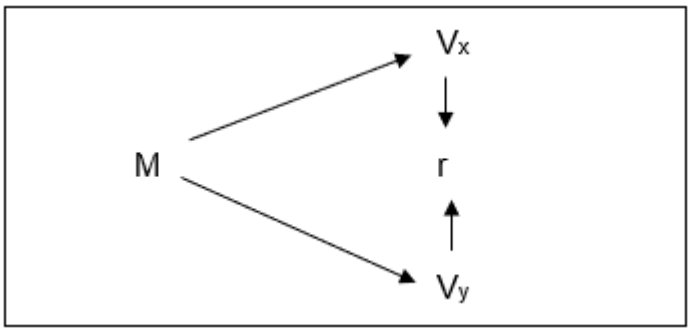
Fue de enfoque cuantitativo, donde **Huaylla y Vargas [8],** exponen que, los datos obtenidos se manejan por medio de elementos estadísticos. Por su parte, el tipo será básico, donde **Rossi [10],** indica que, los aportes se dan de manera teórica para futuros estudios.

b. Nivel de investigación

El nivel correlacional-transversal, según **Chávez y Henríquez [27],** se refiere al análisis de la relación entre al menos dos variables, permitiendo la cuantificación de cada una de ellas (posiblemente interrelacionadas) para luego evaluar y describir su vínculo. Este tipo de análisis se sustenta en hipótesis que deben ser verificadas. Además, como señala **Reyes [28],** el enfoque transversal implica la recopilación de información en un solo punto en el tiempo, con el objetivo de representar los factores involucrados y analizar su frecuencia y correlación en ese momento específico.

c. Diseño de investigación

El estudio fue de tipo no experimental, según lo explica **Valladolid [29].** Este enfoque implica que las observaciones se realizan sin manipular intencionadamente los factores involucrados, limitándose a identificar y registrar las características del fenómeno, las cuales serán analizadas de manera posterior.



Dónde:

M: Muestra de la investigación.

V1: Medición de la Variable 1: Gestión de TIC´S

V2: Medición de la Variable 2: Procesos de seguridad informática

r: Es la conexión que existe en las dos variables.

B. Población, muestra materia de investigación

Población

Según **Reyes [30],** la población se entiende como un conjunto de individuos que cumplen con ciertos criterios específicos y que deben ser considerados como un grupo homogéneo para ser incluidos en el estudio.

La población contó con 2820 MYPES comerciales ubicadas dentro de la provincia de Ica, siendo información estadística obtenida a partir de reportes del Banco Central de Reserva del Perú (BCRP 2023).

Muestra

La muestra se define como un subconjunto representativo de la población de interés, sobre el cual se recolectará información. Esta muestra debe ser claramente definida y delimitada desde el inicio, asegurando que sea representativa y refleje adecuadamente las características de la población en su totalidad.

La fórmula de la muestra contribuirá en calcular el resultado con la formula continuante

$$\mathbf{n} = \frac{\boldsymbol{Z^2 x N x P x R}}{\boldsymbol{E^2 x (N-1) + Z^2 x P x R}}$$

Dónde:

Parámetro	Valor
N = Tamaño de la población	2820
Z = Nivel de confianza	1.96
P = Probabilidad positiva	50%
Q = Probabilidad negativa	50%
E = margen de error	5%

Reemplazando:

$$\mathbf{n} = \frac{\boldsymbol{1.96^2 x 2820 x 0.5 x 0.5}}{\boldsymbol{0.05^2 x (2820-1) + 1.96^2 x 0.5 x 0.5}} = \frac{\boldsymbol{2708328}}{\boldsymbol{8.0079}} = \boldsymbol{338}$$

La muestra se calculó por 338 representantes de las MYPES comerciales del distrito de Ica.

C. Técnica e instrumentos de recolección de datos

Técnicas

La técnica empleada para la recolección de datos fue la encuesta, la cual se define como un proceso sistemático de obtención de información mediante la formulación de un conjunto de preguntas preestablecidas con fines de evaluación. Este enfoque implica la planificación cuidadosa de preguntas orientadas a probar las hipótesis de investigación, así como a analizar los factores e indicadores relevantes. El objetivo

principal de esta técnica es recolectar datos que validen las teorías subyacentes al estudio.

Instrumentos

El instrumento utilizado en este estudio es el cuestionario, una técnica empleada para recopilar información a través del análisis de las respuestas de los participantes. Este método permite obtener de manera estructurada y coordinada parámetros relacionados con las percepciones y opiniones de los individuos ante situaciones complejas. El cuestionario se considera una herramienta altamente versátil, ya que se utiliza para identificar las principales áreas de investigación, las cuales se presentan a partir de hipótesis previas, generando estimaciones detalladas sobre los aspectos clave a explorar.

D. Técnica de procesamiento de datos, análisis e interpretación de resultados

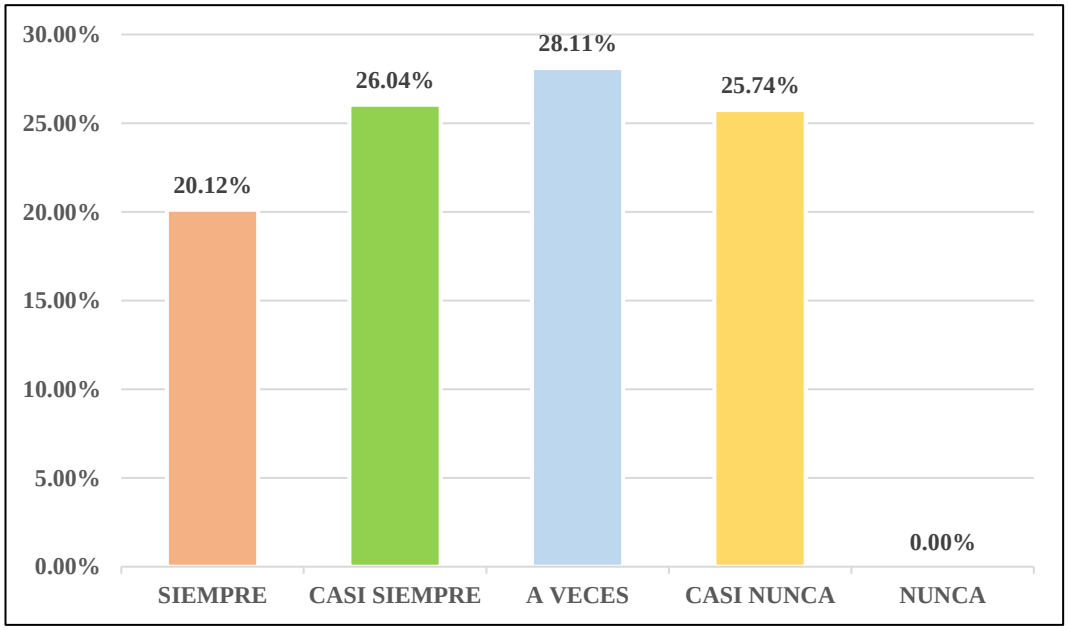
En esta sección del estudio, se detallará el uso de Excel y SPSS para el análisis de la base de datos. SPSS, un software estadístico ampliamente utilizado en el ámbito educativo, es especialmente popular entre las empresas dedicadas a las ciencias sociales y la ingeniería. Este programa es reconocido por su capacidad para gestionar grandes volúmenes de datos y por su interfaz intuitiva, que facilita la realización de diversos análisis estadísticos. Además, se aplicará un análisis inferencial utilizando el coeficiente de correlación Rho de Spearman, con el objetivo de verificar si las hipótesis planteadas se ajustan a la hipótesis alternativa o a la hipótesis nula.

III. RESULTADOS

Tabla 3. ¿El talento humano disponible a cargo de las TIC's reporta continuamente los resultados conseguidos?

Respuesta	Frecuencia	Porcentaje
Siempre	68	20.12%
Casi siempre	88	26.04%
A veces	95	28.11%
Casi nunca	87	25.74%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 1. ¿El talento humano disponible a cargo de las TIC's reporta continuamente los resultados conseguidos?

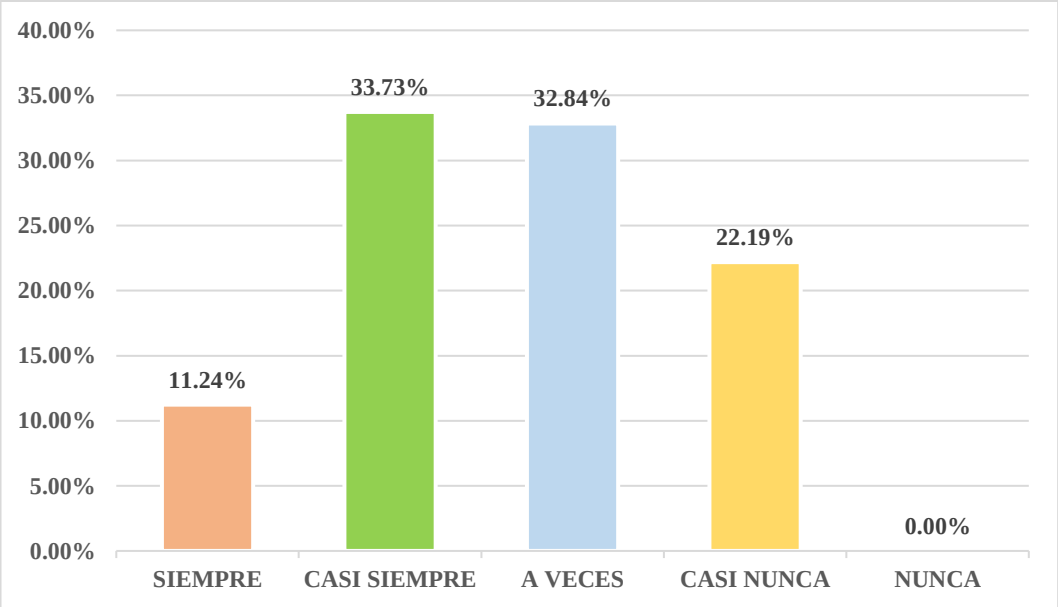


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 28.11% de los representantes de las MYPES comerciales del distrito de Ica, consideraron que "a veces" el talento humano a cargo de las TIC's reporta continuamente los resultados conseguidos. De la misma manera, el 26.04% consideraron que sucede "a veces", el 25.74% manifestaron "casi nunca" y el 20.12% "siempre".

Tabla 4. ¿El talento humano disponible a cargo de las TIC's es capaz de establecer procesos de seguridad en la empresa?

Respuesta	Frecuencia	Porcentaje
Siempre	38	11.24%
Casi siempre	114	33.73%
A veces	111	32.84%
Casi nunca	75	22.19%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 2. ¿El talento humano disponible a cargo de las TIC's es capaz de establecer procesos de seguridad en la empresa?

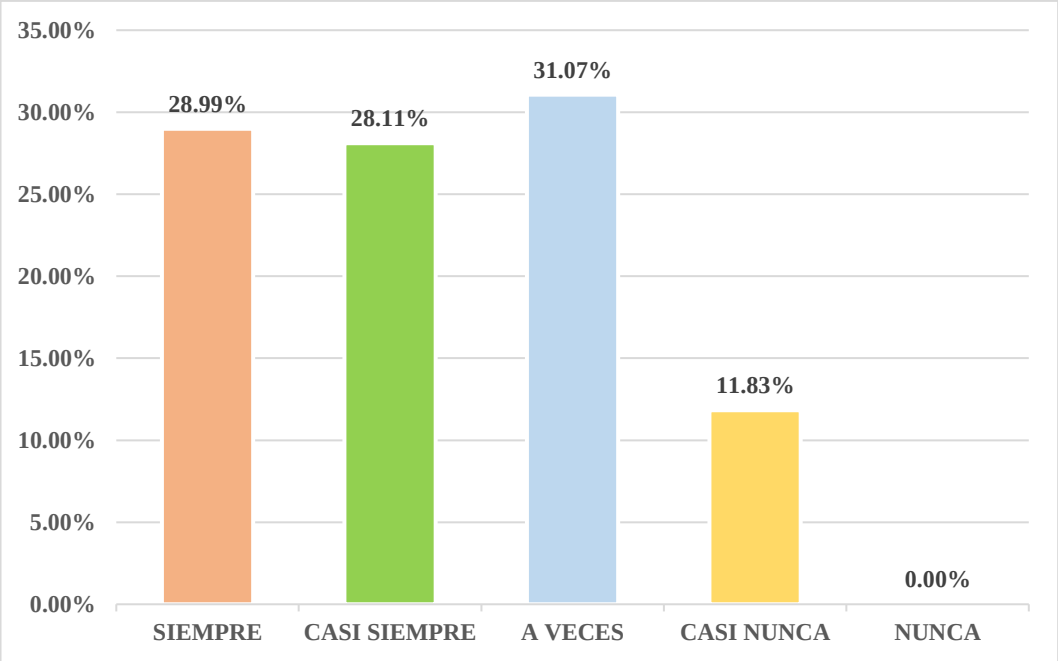


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 33.73% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" el talento humano a cargo de las TIC's es capaz de establecer procesos de seguridad en la empresa. De la misma manera, el 32.84% consideraron que sucede "a veces", el 22.19% manifestaron "casi nunca" y el 11.24% "siempre".

Tabla 5. ¿El talento humano disponible a cargo de las TIC's cumple cabalmente con las actividades asignadas?

Respuesta	Frecuencia	Porcentaje
Siempre	98	28.99%
Casi siempre	95	28.11%
A veces	105	31.07%
Casi nunca	40	11.83%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 3. ¿El talento humano disponible a cargo de las TIC's cumple cabalmente con las actividades asignadas?

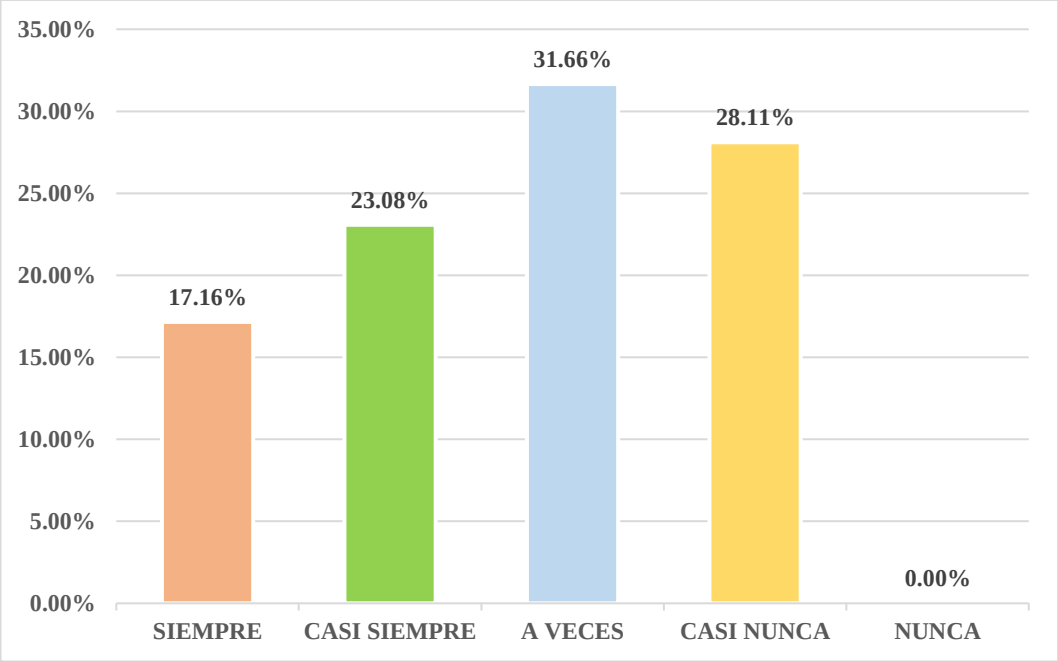


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 31.07% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "a veces" el talento humano a cargo de las TIC's cumple cabalmente con las actividades asignadas. De la misma manera, el 28.99% consideraron que sucede "siempre", el 28.11% manifestaron "casi siempre" y el 11.83% "casi nunca".

Tabla 6. ¿El talento humano disponible a cargo de las TIC's demuestra liderazgo con respecto a sus colegas?

Respuesta	Frecuencia	Porcentaje
Siempre	58	17.16%
Casi siempre	78	23.08%
A veces	107	31.66%
Casi nunca	95	28.11%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 4. ¿El talento humano disponible a cargo de las TIC's demuestra liderazgo con respecto a sus colegas?

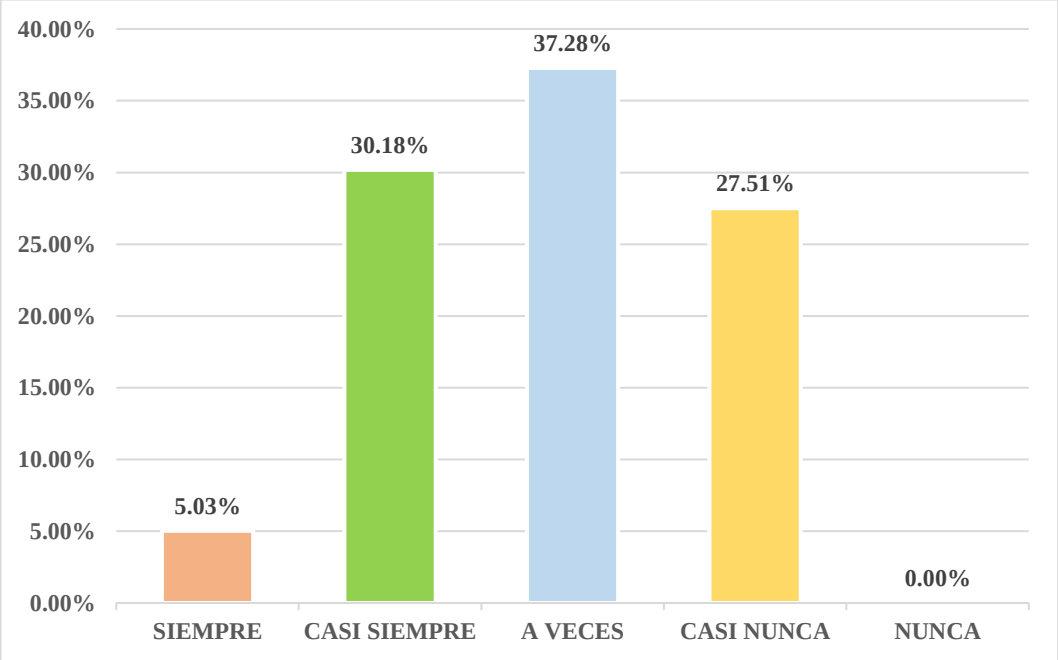


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 31.66% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" el talento humano a cargo de las TIC's demuestra liderazgo con respecto a sus colegas. De la misma manera, el 28.11% consideraron que sucede "casi nunca", el 23.08% manifestaron "casi siempre" y el 17.16% "siempre".

Tabla 7. ¿El talento humano disponible a cargo de las TIC's lleva a cabo sus operaciones teniendo todos los recursos a la mano?

Respuesta	Frecuencia	Porcentaje
Siempre	17	5.03%
Casi siempre	102	30.18%
A veces	126	37.28%
Casi nunca	93	27.51%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 5. ¿El talento humano disponible a cargo de las TIC's lleva a cabo sus operaciones teniendo todos los recursos a la mano?

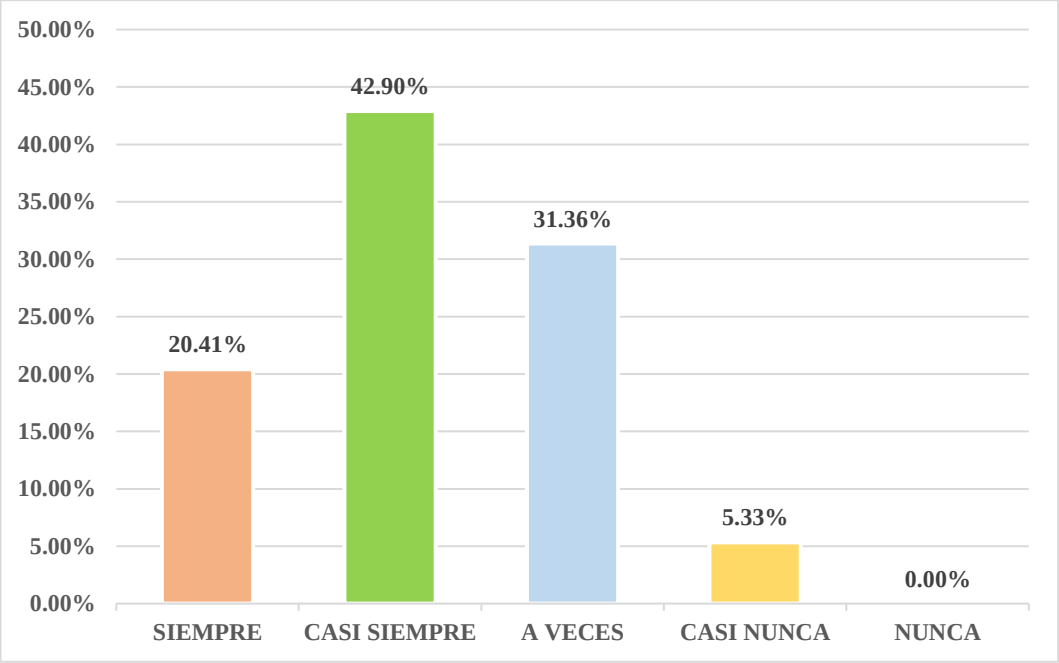


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 37.28% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "a veces" el talento humano a cargo de las TIC's lleva a cabo sus operaciones teniendo todos los recursos a la mano. De la misma manera, el 30.18% consideraron que sucede "casi siempre", el 27.51% manifestaron "casi nunca" y el 5.03% "siempre".

Tabla 8. ¿Se llevan a cabo normas y protocolos que garantizan la efectividad en cuanto a la utilización de las TIC's?

Respuesta	Frecuencia	Porcentaje
Siempre	69	20.41%
Casi siempre	145	42.90%
A veces	106	31.36%
Casi nunca	18	5.33%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 6. ¿Se llevan a cabo normas y protocolos que garantizan la efectividad en cuanto a la utilización de las TIC's?

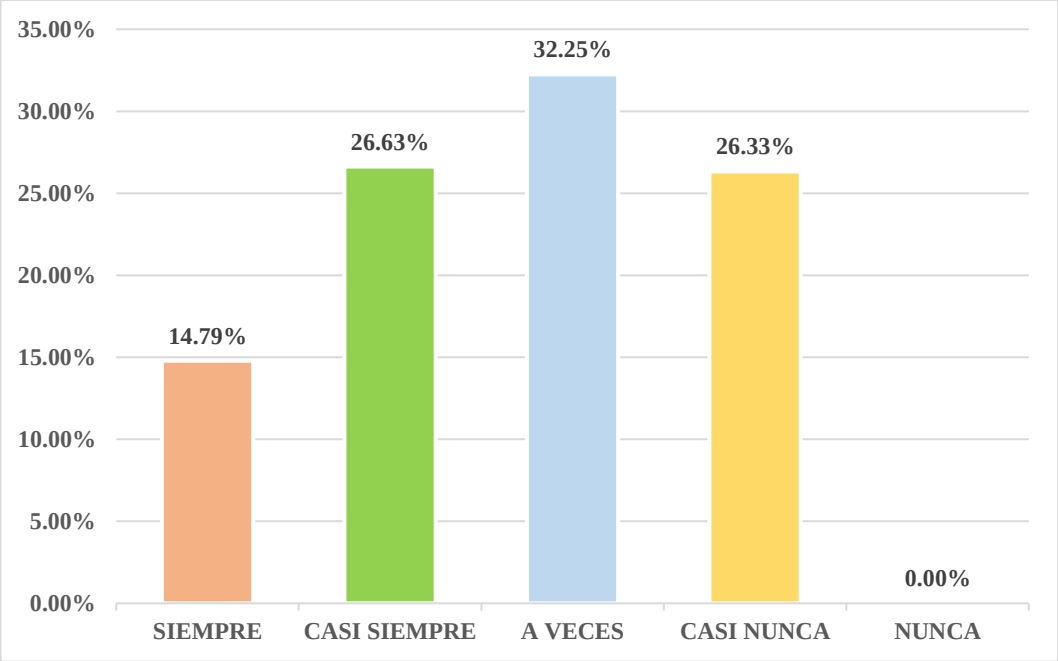


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 42.09% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" se llevan a cabo normas y protocolos que garantizan la efectividad en cuanto a la utilización de las TIC's. De la misma manera, el 31.36% consideraron que sucede "a veces", el 20.41% manifestaron "siempre" y el 5.33% "casi nunca".

Tabla 9. ¿Los trabajadores utilizan las TIC's con la finalidad de optimizar los canales de comunicación en la empresa?

Respuesta	Frecuencia	Porcentaje
Siempre	50	14.79%
Casi siempre	90	26.63%
A veces	109	32.25%
Casi nunca	89	26.33%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 7. ¿Los trabajadores utilizan las TIC's con la finalidad de optimizar los canales de comunicación en la empresa?

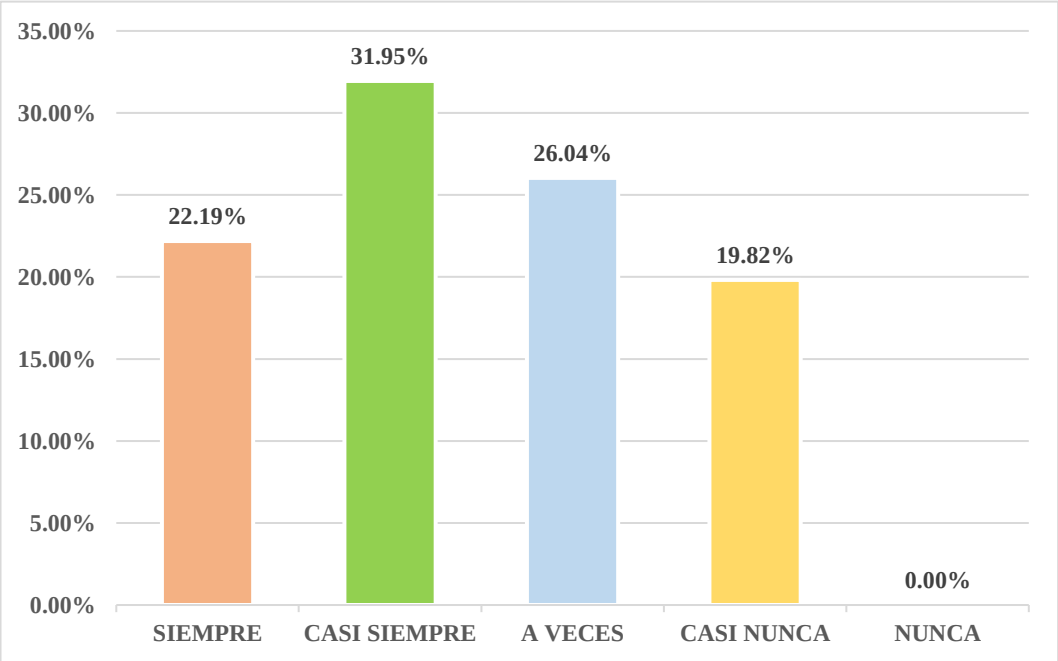


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 32.25% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "a veces" utilizan las TIC's con la finalidad de optimizar los canales de comunicación en la empresa. De la misma manera, el 26.63% consideraron que sucede "casi siempre", el 26.33% manifestaron "casi nunca" y el 14.79% "siempre".

Tabla 10. ¿Los trabajadores del área de TIC's demuestran un gran compromiso y responsabilidad en sus funciones?

Respuesta	Frecuencia	Porcentaje
Siempre	75	22.19%
Casi siempre	108	31.95%
A veces	88	26.04%
Casi nunca	67	19.82%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 8. ¿Los trabajadores del área de TIC's demuestran un gran compromiso y responsabilidad en sus funciones?

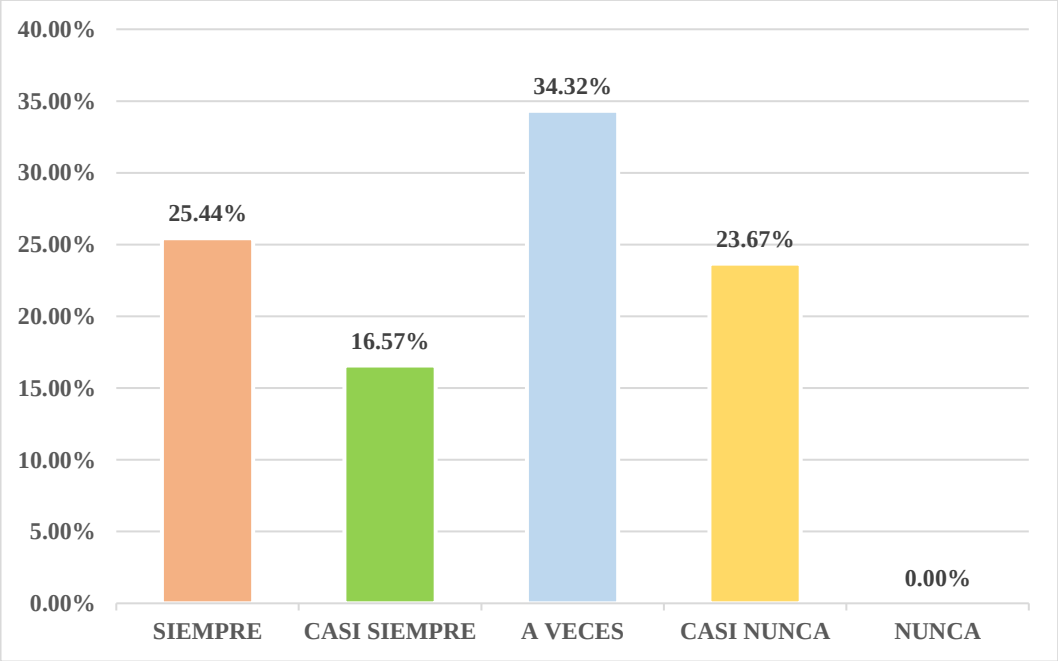


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 31.96% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" los trabajadores del área de TIC's demuestran un gran compromiso y responsabilidad en sus funciones. De la misma manera, el 26.04% consideraron que sucede "a veces", el 22.19% manifestaron "siempre" y el 19.82% "casi nunca".

Tabla 11. ¿Los trabajadores del área de TIC's demuestran un grado de productividad según lo esperado?

Respuesta	Frecuencia	Porcentaje
Siempre	86	25.44%
Casi siempre	56	16.57%
A veces	116	34.32%
Casi nunca	80	23.67%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 9. ¿Los trabajadores del área de TIC's demuestran un grado de productividad según lo esperado?

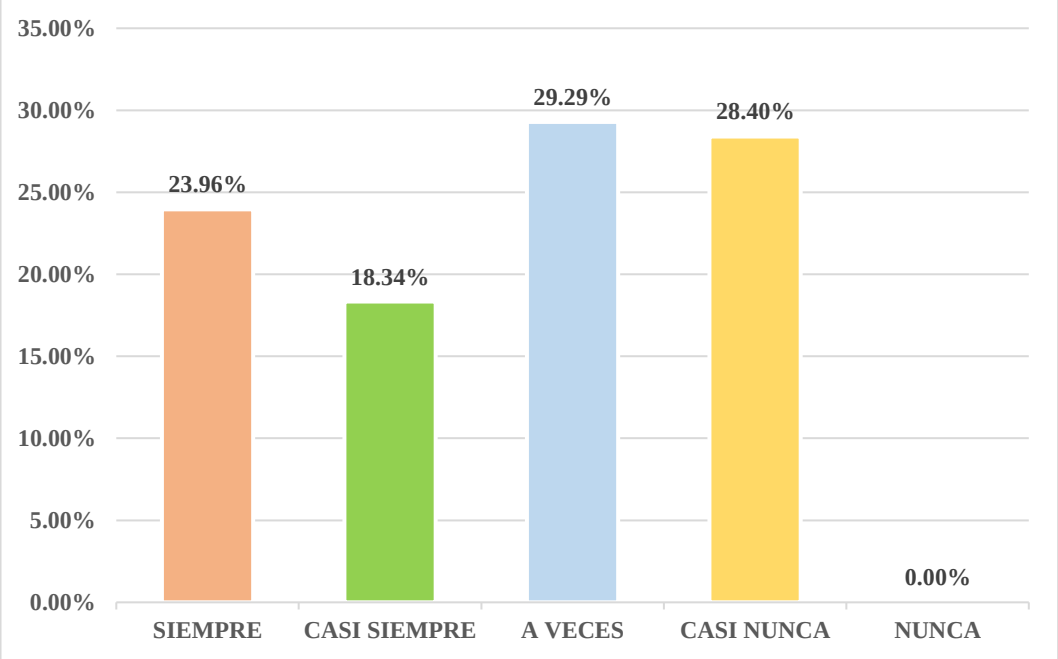


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 34.32% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "a veces" los trabajadores del área de TIC's demuestran un grado de productividad según lo esperado. De la misma manera, el 23.67% consideraron que sucede "casi nunca", el 25.44% manifestaron "siempre" y el 16.57% "casi siempre".

Tabla 12. ¿La empresa dispone del conocimiento necesario para clasificar los activos de carácter informático?

Respuesta	Frecuencia	Porcentaje
Siempre	81	23.96%
Casi siempre	62	18.34%
A veces	99	29.29%
Casi nunca	96	28.40%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 20. ¿La empresa dispone del conocimiento necesario para clasificar los activos de carácter informático?

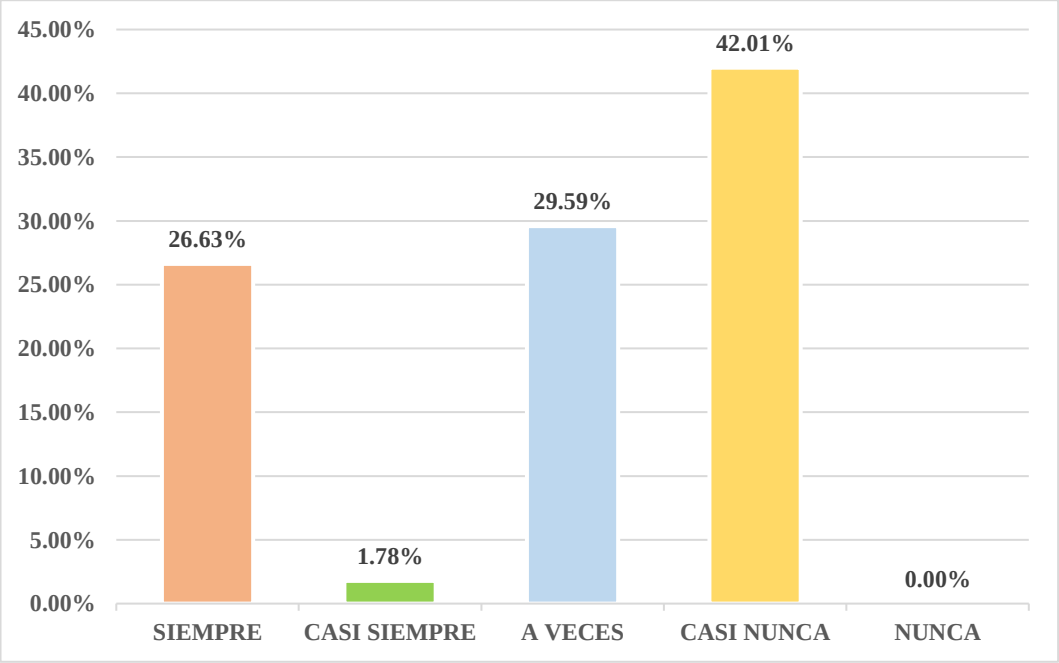


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 29.29% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" dispone del conocimiento necesario para clasificar los activos de carácter informático. De la misma manera, el 28.40% consideraron que sucede "casi nunca", el 23.96% manifestaron "siempre" y el 18.34% "casi siempre".

Tabla 14. ¿La empresa toma en cuenta el aseguramiento de la conectividad al adquirir nuevas tecnologías?

Respuesta	Frecuencia	Porcentaje
Siempre	90	26.63%
Casi siempre	6	1.78%
A veces	100	29.59%
Casi nunca	142	42.01%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 31. ¿La empresa toma en cuenta el aseguramiento de la conectividad al adquirir nuevas tecnologías?

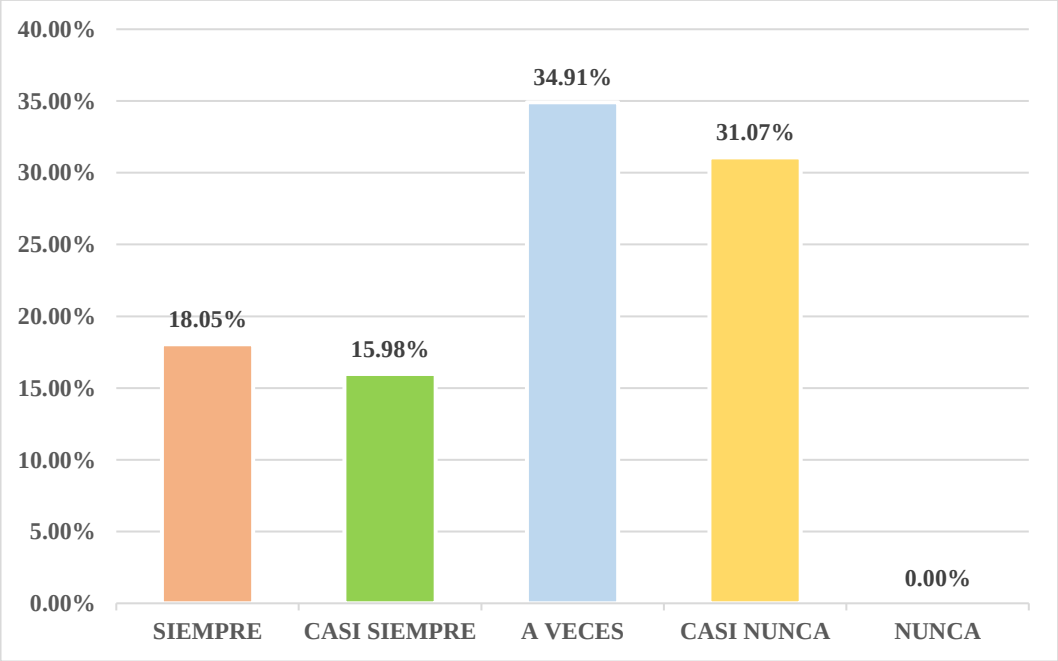


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 42.01% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi nunca" la empresa toma en cuenta el aseguramiento de la conectividad al adquirir nuevas tecnologías. De la misma manera, el 29.59% consideraron que sucede "a veces", el 26.63% manifestaron "siempre" y el 1.78% "casi siempre".

Tabla 14. ¿La empresa toma en cuenta las políticas respecto al manejo de las TIC's?

Respuesta	Frecuencia	Porcentaje
Siempre	61	18.05%
Casi siempre	54	15.98%
A veces	118	34.91%
Casi nunca	105	31.07%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 42. ¿La empresa toma en cuenta las políticas respecto al manejo de las TIC's?

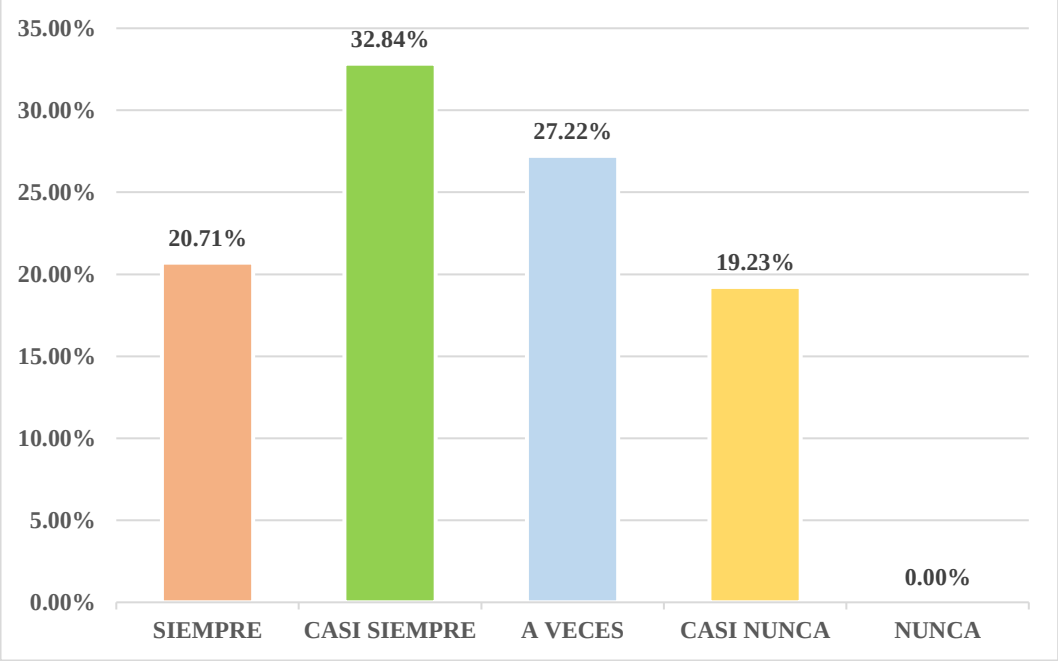


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 34.91% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "a veces" la empresa toma en cuenta las políticas respecto al manejo de las TIC's. De la misma manera, el 31.07% consideraron que sucede "casi nunca", el 18.05% manifestaron "siempre" y el 15.98% "casi siempre".

Tabla 15. ¿La empresa pone en marcha planes y programas para reducir un posible riesgo respecto a la información sensible?

Respuesta	Frecuencia	Porcentaje
Siempre	70	20.71%
Casi siempre	111	32.84%
A veces	92	27.22%
Casi nunca	65	19.23%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 53. ¿La empresa pone en marcha planes y programas para reducir un posible riesgo respecto a la información sensible?

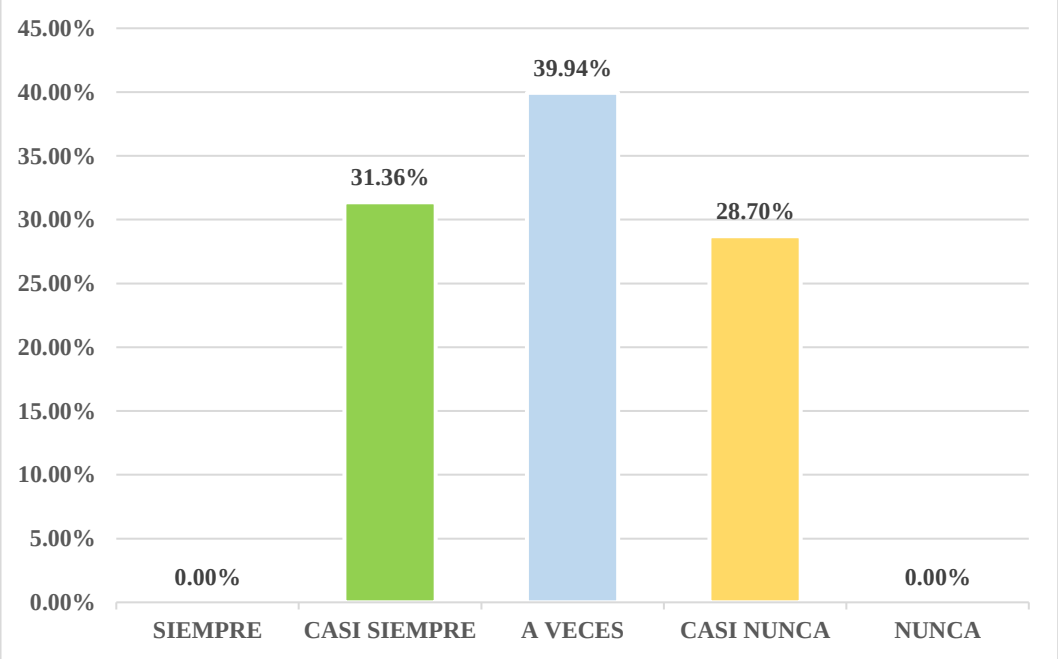


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 32.84% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" la empresa pone en marcha planes y programas para reducir un posible riesgo respecto a la información sensible. De la misma manera, el 27.22% consideraron que sucede "a veces", el 20.71% manifestaron "siempre" y el 19.23% "casi nunca".

Tabla 16. ¿La empresa tiene conocimientos sobre las políticas enfocadas al tratamiento de los datos de clientes y proveedores?

Respuesta	Frecuencia	Porcentaje
Siempre	0	0.00%
Casi siempre	106	31.36%
A veces	135	39.94%
Casi nunca	97	28.70%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 64. ¿La empresa tiene conocimientos sobre las políticas enfocadas al tratamiento de los datos de clientes y proveedores?

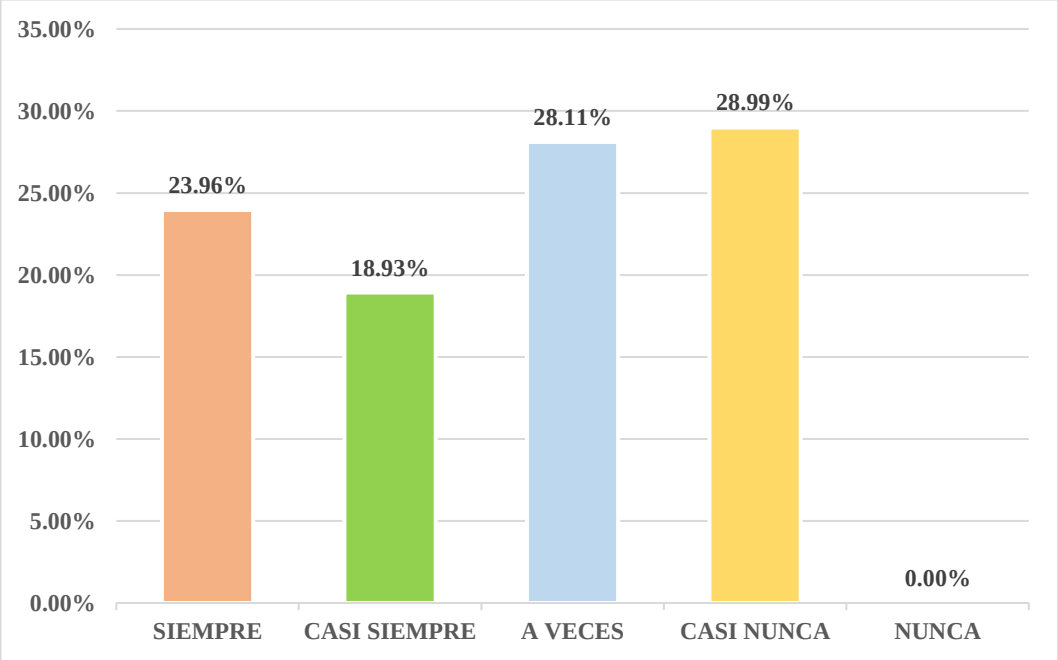


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 39.94% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que “a veces” la empresa tiene conocimientos sobre las políticas enfocadas al tratamiento de los datos de clientes y proveedores. De la misma manera, el 31.36% consideraron que sucede “casi siempre” y el 28.70% “casi nunca”.

Tabla 17. ¿La empresa cumple con todas las actividades planificadas gracias a la utilización de las TIC's?

Respuesta	Frecuencia	Porcentaje
Siempre	81	23.96%
Casi siempre	64	18.93%
A veces	95	28.11%
Casi nunca	98	28.99%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 75. ¿La empresa cumple con todas las actividades planificadas gracias a la utilización de las TIC's?

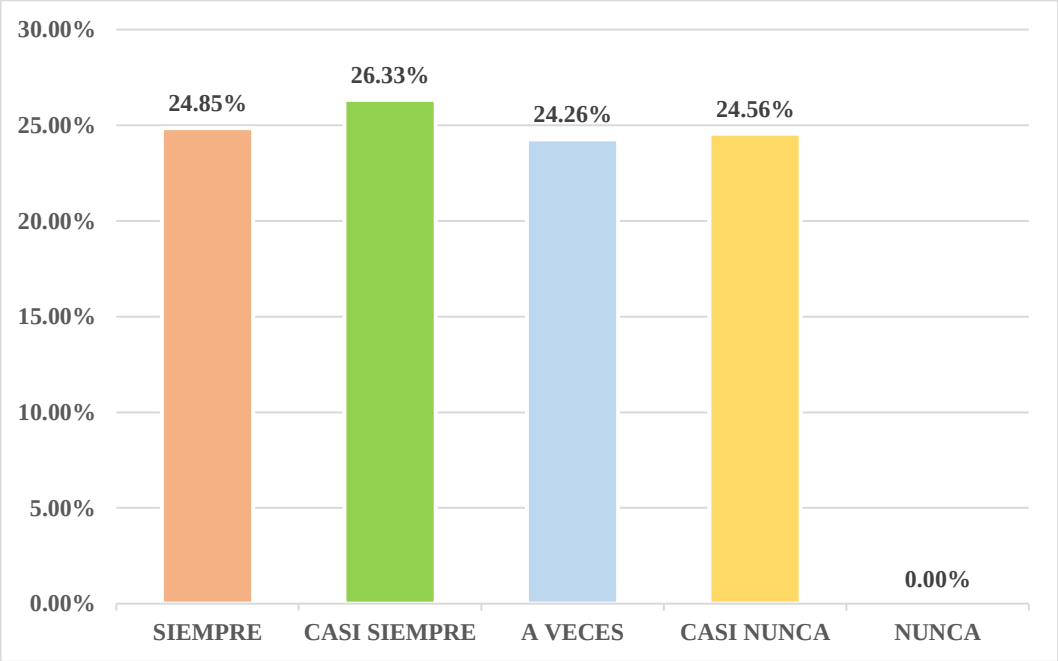


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 28.99% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi nunca" la empresa cumple con todas las actividades planificadas gracias a la utilización de las TIC's. De la misma manera, el 28.11% consideraron que sucede "a veces", el 23.96% manifestaron "siempre" y el 18.96% "casi siempre".

Tabla 18. ¿Las TIC's que utiliza la empresa ayudan a gestionar de forma segura a los usuarios que tienen acceso a los sistemas, garantizando que solo las personas autorizadas puedan entrar?

Respuesta	Frecuencia	Porcentaje
Siempre	84	24.85%
Casi siempre	89	26.33%
A veces	82	24.26%
Casi nunca	83	24.56%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 86. ¿Las TIC's que utiliza la empresa ayudan a gestionar de forma segura a los usuarios que tienen acceso a los sistemas, garantizando que solo las personas autorizadas puedan entrar?

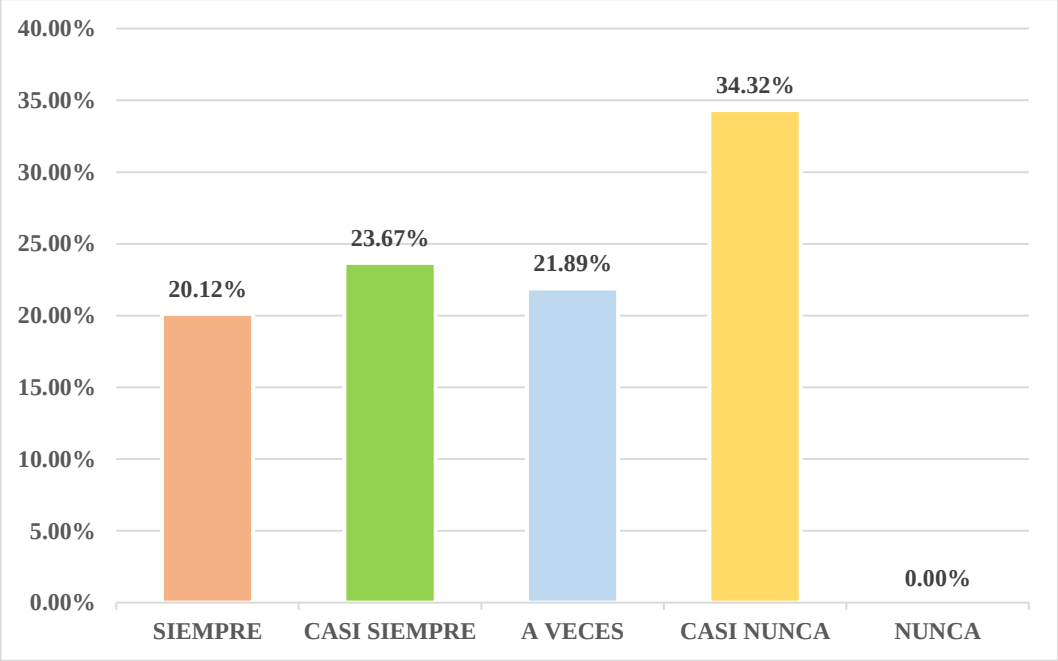


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 26.33% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" las TIC's que utiliza la empresa ayudan a gestionar de forma segura a los usuarios que tienen acceso a los sistemas, garantizando que solo las personas autorizadas puedan entrar. De la misma manera, el 24.26% consideraron que sucede "a veces", el 24.85% manifestaron "siempre" y el 24.56% "casi nunca".

Tabla 19. ¿Las TIC's en la empresa aseguran que la información se comparta de manera rápida y eficiente, cuidando que no se modifique ni pierda durante el intercambio?

Respuesta	Frecuencia	Porcentaje
Siempre	68	20.12%
Casi siempre	80	23.67%
A veces	74	21.89%
Casi nunca	116	34.32%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 97. ¿Las TIC's en la empresa aseguran que la información se comparta de manera rápida y eficiente, cuidando que no se modifique ni pierda durante el intercambio?

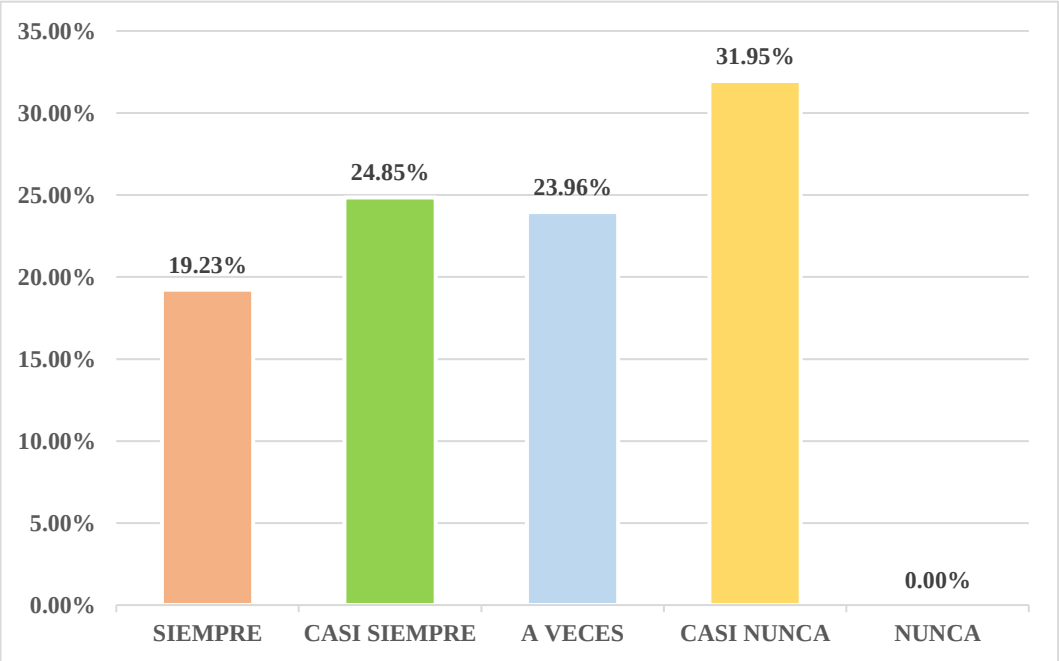


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 34.32% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi nunca" las TIC's en la empresa aseguran que la información se comparta de manera rápida y eficiente, cuidando que no se modifique ni pierda durante el intercambio. De la misma manera, el 23.67% consideraron que sucede "casi siempre", el 20.12% manifestaron "siempre" y el 21.89% "a veces".

Tabla 20. ¿Las TIC's implementadas en la empresa permiten almacenar los datos de manera segura, de modo que estén siempre disponibles para una consulta rápida cuando se necesiten?

Respuesta	Frecuencia	Porcentaje
Siempre	65	19.23%
Casi siempre	84	24.85%
A veces	81	23.96%
Casi nunca	108	31.95%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 108. ¿Las TIC's implementadas en la empresa permiten almacenar los datos de manera segura, de modo que estén siempre disponibles para una consulta rápida cuando se necesiten?

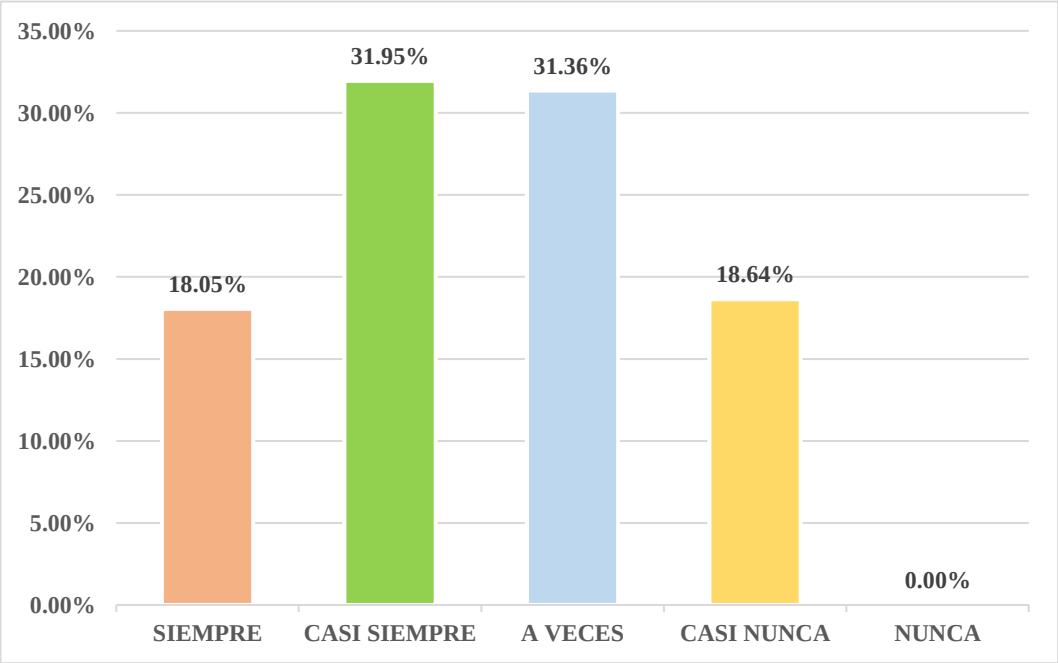


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 31.96% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi nunca" las TIC's implementadas en la empresa permiten almacenar los datos de manera segura, de modo que estén siempre disponibles para una consulta rápida cuando se necesiten. De la misma manera, el 24.85% consideraron que sucede "casi siempre", el 19.23% manifestaron "siempre" y el 23.95% "a veces".

Tabla 21. ¿Los datos que maneja la empresa viajan por canales de comunicación seguros, lo que garantiza que no sean interceptados o alterados?

Respuesta	Frecuencia	Porcentaje
Siempre	61	18.05%
Casi siempre	108	31.95%
A veces	106	31.36%
Casi nunca	63	18.64%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 119. ¿Los datos que maneja la empresa viajan por canales de comunicación seguros, lo que garantiza que no sean interceptados o alterados?

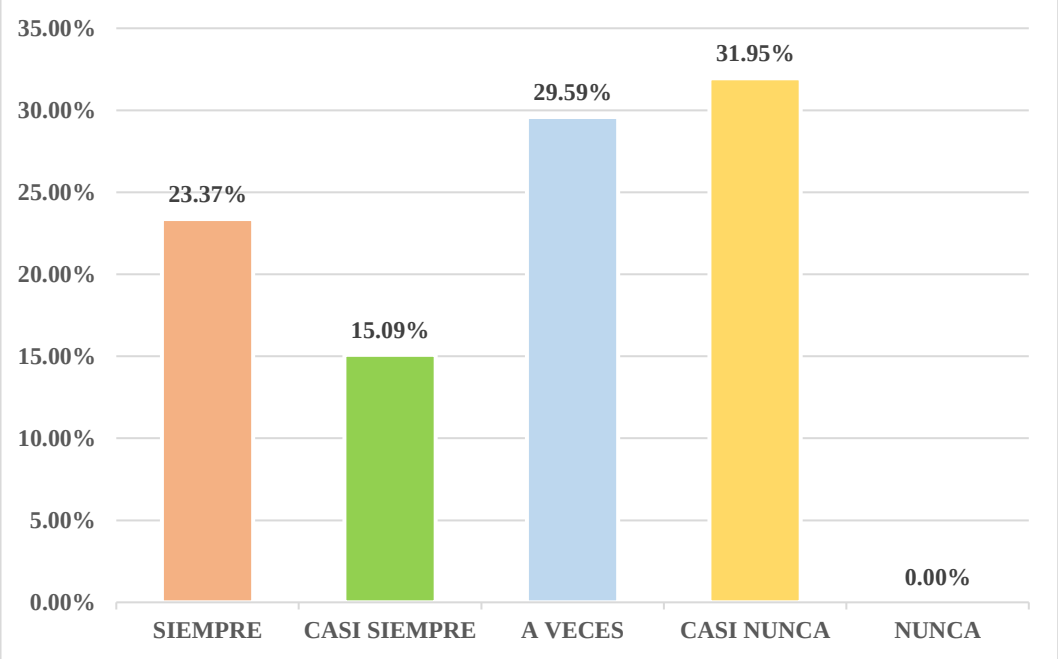


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 31.95% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" los datos que maneja la empresa viajan por canales de comunicación seguros, lo que garantiza que no sean interceptados o alterados. De la misma manera, el 31.36% consideraron que sucede "a veces", el 18.05% manifestaron "siempre" y el 18.64% "casi nunca".

Tabla 22. ¿Los retrasos en la entrega de requerimientos generan problemas que afectan las operaciones diarias de la empresa, como la entrega de productos o servicios?

Respuesta	Frecuencia	Porcentaje
Siempre	79	23.37%
Casi siempre	51	15.09%
A veces	100	29.59%
Casi nunca	108	31.95%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 20. ¿Los retrasos en la entrega de requerimientos generan problemas que afectan las operaciones diarias de la empresa, como la entrega de productos o servicios?

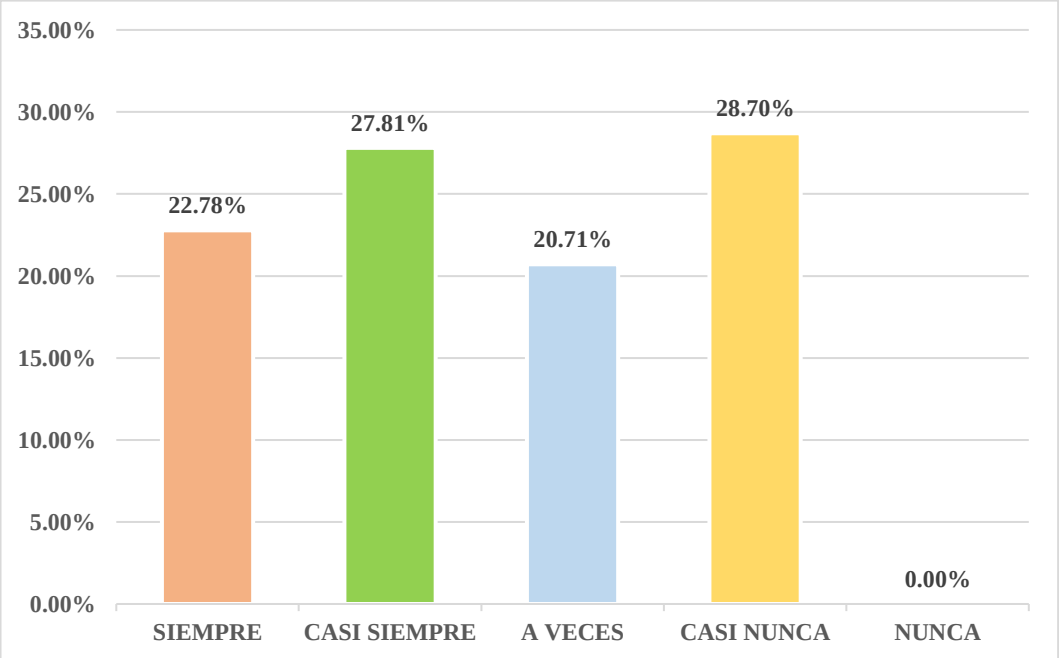


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 31.95% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" los retrasos en la entrega de requerimientos generan problemas que afectan las operaciones diarias de la empresa, como la entrega de productos o servicios. De la misma manera, el 29.59% consideraron que sucede "a veces", el 23.37% manifestaron "siempre" y el 15.09% "casi siempre".

Tabla 25. ¿Los protocolos de seguridad que utiliza la empresa, como contraseñas o sistemas de verificación, ayudan a prevenir que personas no autorizadas puedan acceder a los datos?

Respuesta	Frecuencia	Porcentaje
Siempre	77	22.78%
Casi siempre	94	27.81%
A veces	70	20.71%
Casi nunca	97	28.70%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 212. ¿Los protocolos de seguridad que utiliza la empresa, como contraseñas o sistemas de verificación, ayudan a prevenir que personas no autorizadas puedan acceder a los datos?

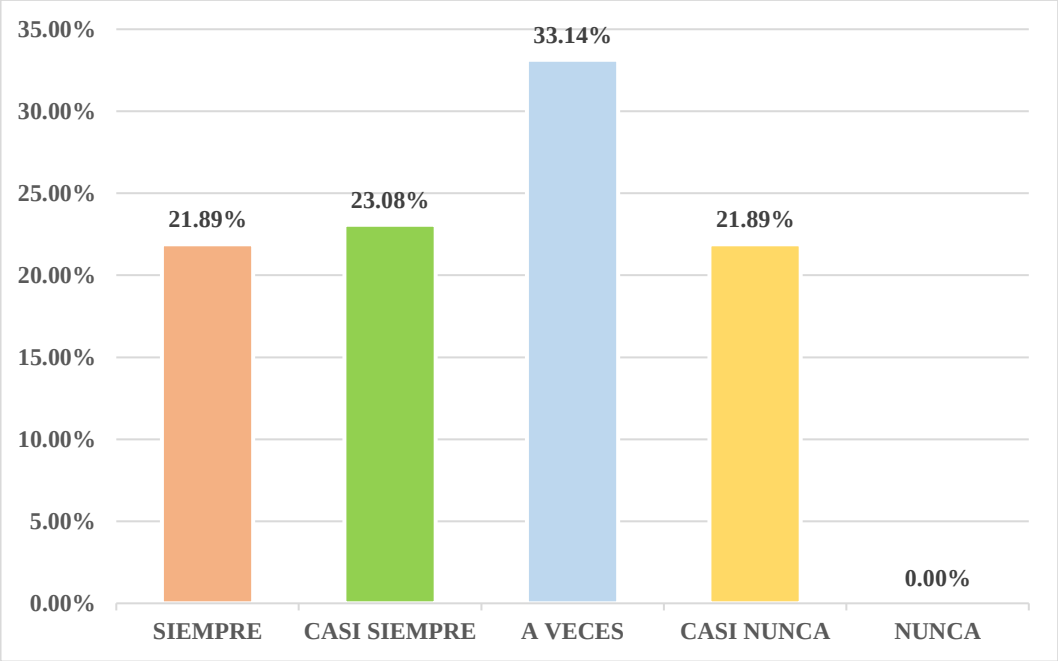


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 27.81% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" los protocolos de seguridad que utiliza la empresa, como contraseñas o sistemas de verificación, ayudan a prevenir que personas no autorizadas puedan acceder a los datos. De la misma manera, el 20.71% consideraron que sucede "a veces", el 22.78% manifestaron "siempre" y el 28.70% "casi nunca".

Tabla 24. ¿Las medidas de seguridad implementadas en la empresa reducen la posibilidad de que existan copias innecesarias o duplicaciones de los datos, evitando confusiones o errores?

Respuesta	Frecuencia	Porcentaje
Siempre	74	21.89%
Casi siempre	78	23.08%
A veces	112	33.14%
Casi nunca	74	21.89%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 22. ¿Las medidas de seguridad implementadas en la empresa reducen la posibilidad de que existan copias innecesarias o duplicaciones de los datos, evitando confusiones o errores?

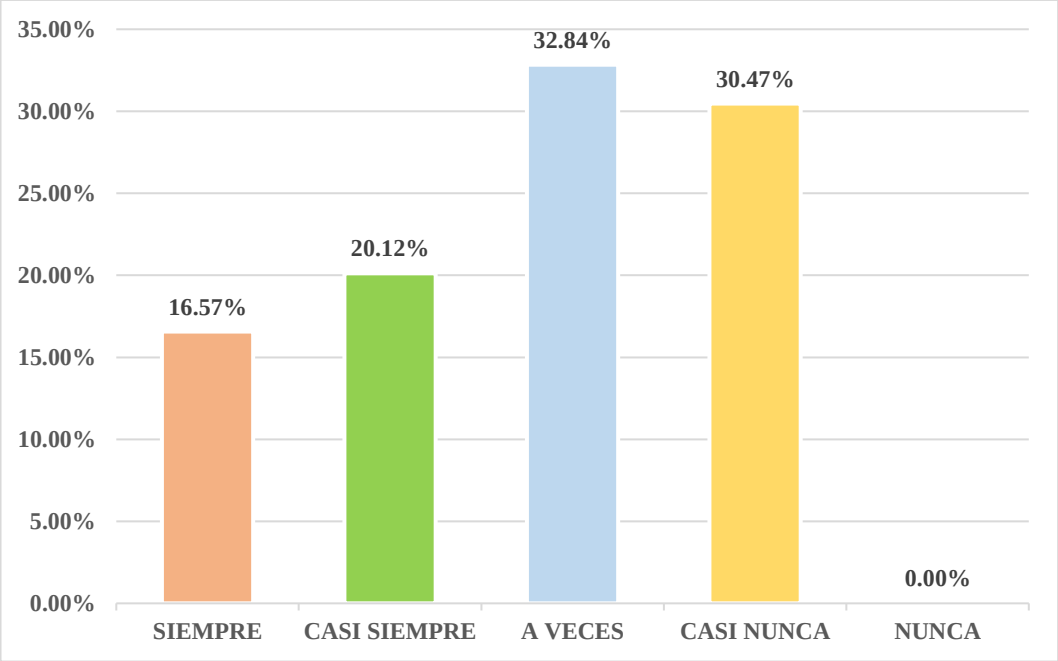


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 33.14% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que “a veces” las medidas de seguridad implementadas en la empresa reducen la posibilidad de que existan copias innecesarias o duplicaciones de los datos, evitando confusiones o errores. De la misma manera, el 23.08% consideraron que sucede “casi siempre”, el 21.89% manifestaron “siempre” y el 21.89% “casi nunca”.

Tabla 25. ¿Las medidas de seguridad permiten que, en caso de un problema o incidente, la empresa pueda responder rápidamente y proteger la información de los usuarios?

Respuesta	Frecuencia	Porcentaje
Siempre	56	16.57%
Casi siempre	68	20.12%
A veces	111	32.84%
Casi nunca	103	30.47%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 23. ¿Las medidas de seguridad permiten que, en caso de un problema o incidente, ¿la empresa pueda responder rápidamente y proteger la información de los usuarios?

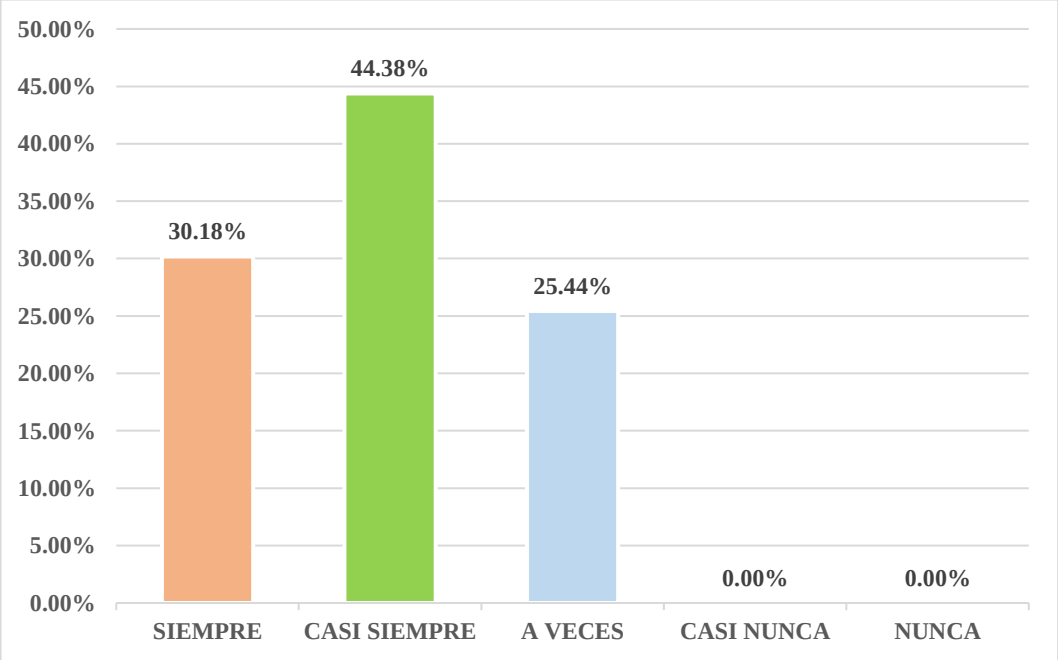


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 32.84% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "a veces" las medidas de seguridad permiten que, en caso de un problema o incidente, la empresa pueda responder rápidamente y proteger la información de los usuarios. De la misma manera, el 20.12% consideraron que sucede "casi siempre", el 16.57% manifestaron "siempre" y el 30.47% "casi nunca".

Tabla 26. ¿Las medidas de seguridad garantizan que solo los empleados autorizados puedan acceder a la información confidencial de la empresa?

Respuesta	Frecuencia	Porcentaje
Siempre	102	30.18%
Casi siempre	150	44.38%
A veces	86	25.44%
Casi nunca	0	0.00%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 24. ¿Las medidas de seguridad garantizan que solo los empleados autorizados puedan acceder a la información confidencial de la empresa?

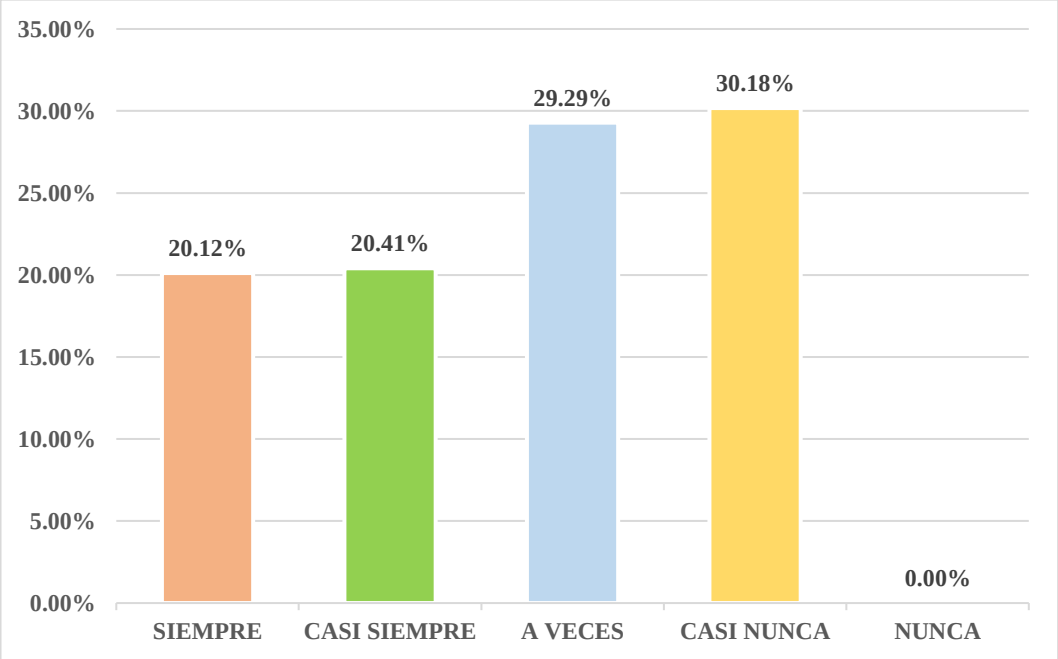


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 44.38% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" las medidas de seguridad garantizan que solo los empleados autorizados puedan acceder a la información confidencial de la empresa. De la misma manera, el 30.18% consideraron que sucede "siempre", el 25.44% manifestaron "a veces".

Tabla 27. ¿Las técnicas de protección de datos utilizadas en la empresa, como la codificación o encriptación, son eficaces para evitar que personas no autorizadas accedan a información sensible?

Respuesta	Frecuencia	Porcentaje
Siempre	68	20.12%
Casi siempre	69	20.41%
A veces	99	29.29%
Casi nunca	102	30.18%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 25. ¿Las técnicas de protección de datos utilizadas en la empresa, como la codificación o encriptación, son eficaces para evitar que personas no autorizadas accedan a información sensible?

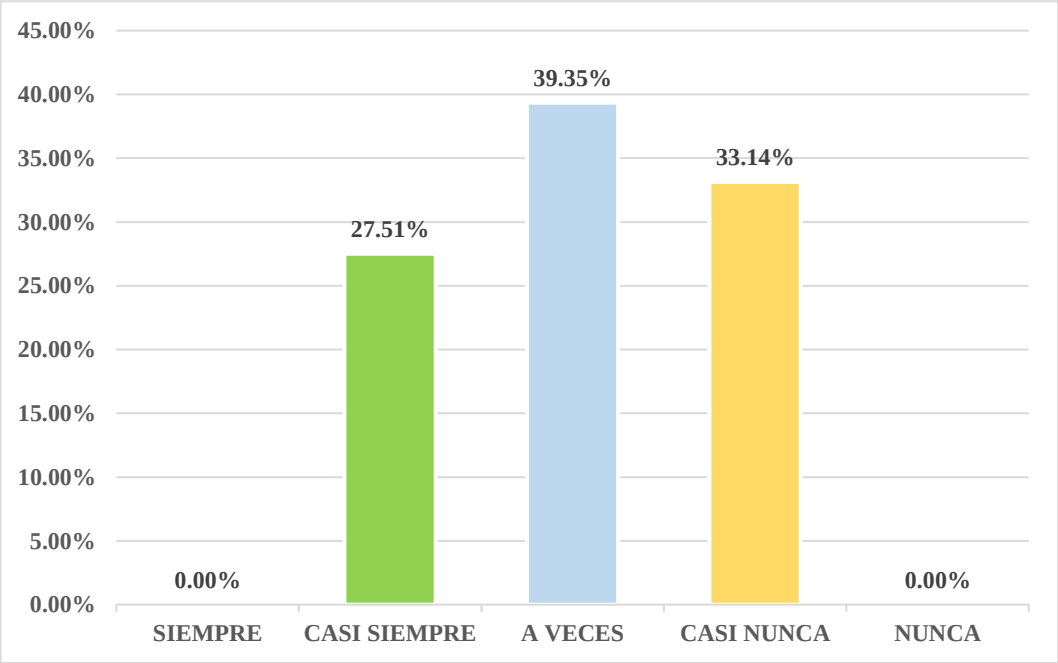


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 30.18% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi nunca" las técnicas de protección de datos utilizadas en la empresa, como la codificación o encriptación, son eficaces para evitar que personas no autorizadas accedan a información sensible. De la misma manera, el 29.29% consideraron que sucede "a veces", el 20.12% manifestaron "siempre" y el 20.41% "casi nunca".

Tabla 28. ¿Las TIC's implementadas en la empresa aseguran que la información siempre se mantenga veraz y exacta, sin que sea alterada de manera no autorizada?

Respuesta	Frecuencia	Porcentaje
Siempre	0	0.00%
Casi siempre	93	27.51%
A veces	133	39.35%
Casi nunca	112	33.14%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 26. ¿Las TIC's implementadas en la empresa aseguran que la información siempre se mantenga veraz y exacta, sin que sea alterada de manera no autorizada?

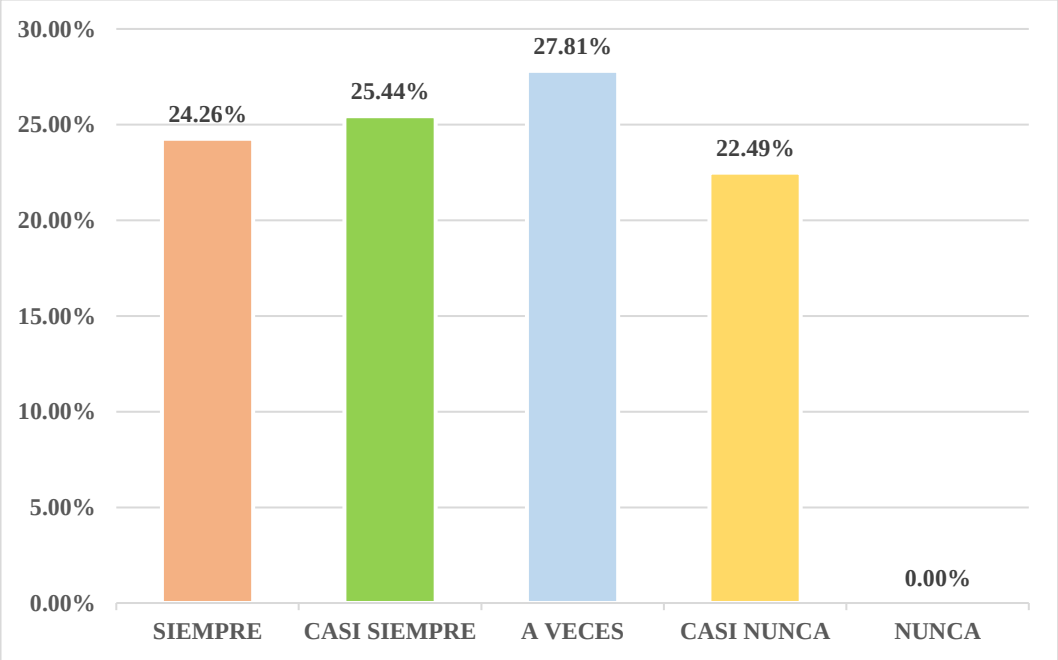


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 39.35% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "a veces" las TIC's implementadas en la empresa aseguran que la información siempre se mantenga veraz y exacta, sin que sea alterada de manera no autorizada. De la misma manera, el 33.14% consideraron que sucede "casi nunca" y el 27.51% "casi siempre".

Tabla 29. ¿Los mecanismos de seguridad de la empresa previenen que la información sea modificada por personas o sistemas que no tienen permiso para hacerlo?

Respuesta	Frecuencia	Porcentaje
Siempre	82	24.26%
Casi siempre	86	25.44%
A veces	94	27.81%
Casi nunca	76	22.49%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 27. ¿Los mecanismos de seguridad de la empresa previenen que la información sea modificada por personas o sistemas que no tienen permiso para hacerlo?

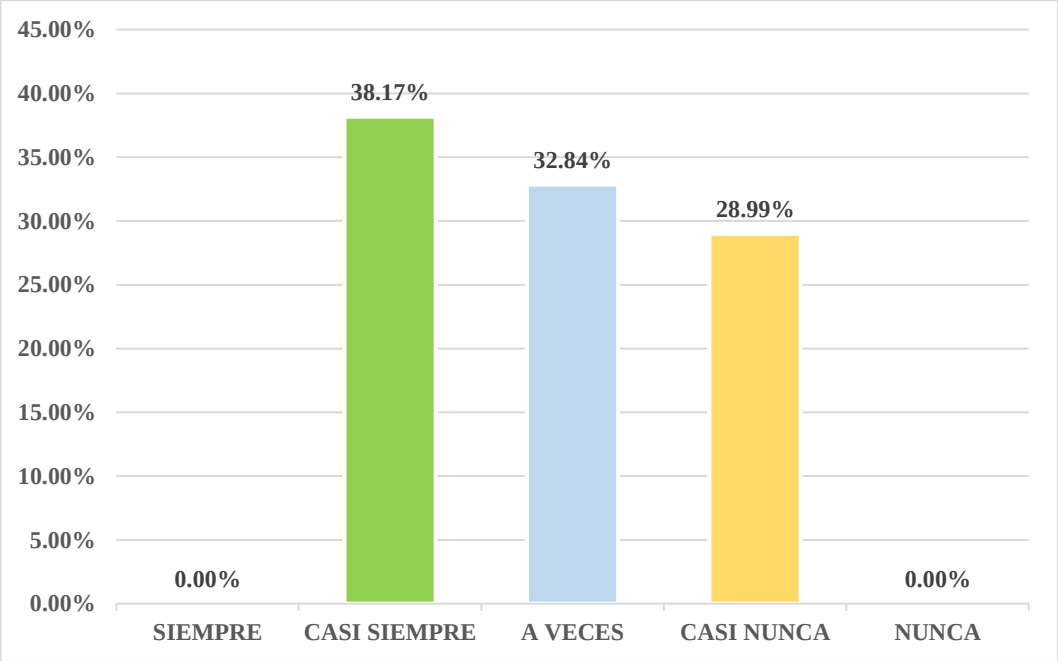


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 25.44% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" los mecanismos de seguridad de la empresa previenen que la información sea modificada por personas o sistemas que no tienen permiso para hacerlo. De la misma manera, el 27.81% consideraron que sucede "a veces", el 24.26% manifestaron "siempre" y el 22.49% "casi nunca".

Tabla 30. ¿La empresa cuenta con medidas para proteger la integridad de los datos, evitando cualquier alteración durante su procesamiento?

Respuesta	Frecuencia	Porcentaje
Siempre	0	0.00%
Casi siempre	129	38.17%
A veces	111	32.84%
Casi nunca	98	28.99%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 28. ¿La empresa cuenta con medidas para proteger la integridad de los datos, evitando cualquier alteración durante su procesamiento?

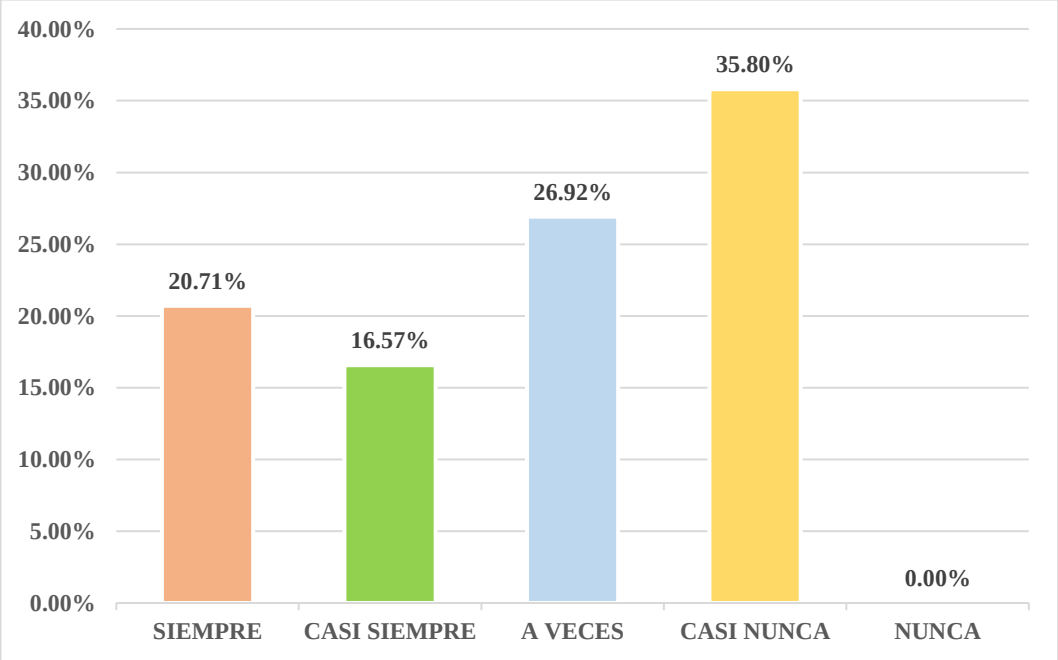


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 38.17% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi siempre" la empresa cuenta con medidas para proteger la integridad de los datos, evitando cualquier alteración durante su procesamiento. De la misma manera, el 32.84% consideraron que sucede "a veces" y el 28.99% "casi nunca".

Tabla 31. ¿Los sistemas que maneja la empresa aseguran que los datos transmitidos lleguen de manera coherente y sin errores, manteniendo su integridad durante el proceso?

Respuesta	Frecuencia	Porcentaje
Siempre	70	20.71%
Casi siempre	56	16.57%
A veces	91	26.92%
Casi nunca	121	35.80%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 29. ¿Los sistemas que maneja la empresa aseguran que los datos transmitidos lleguen de manera coherente y sin errores, manteniendo su integridad durante el proceso?

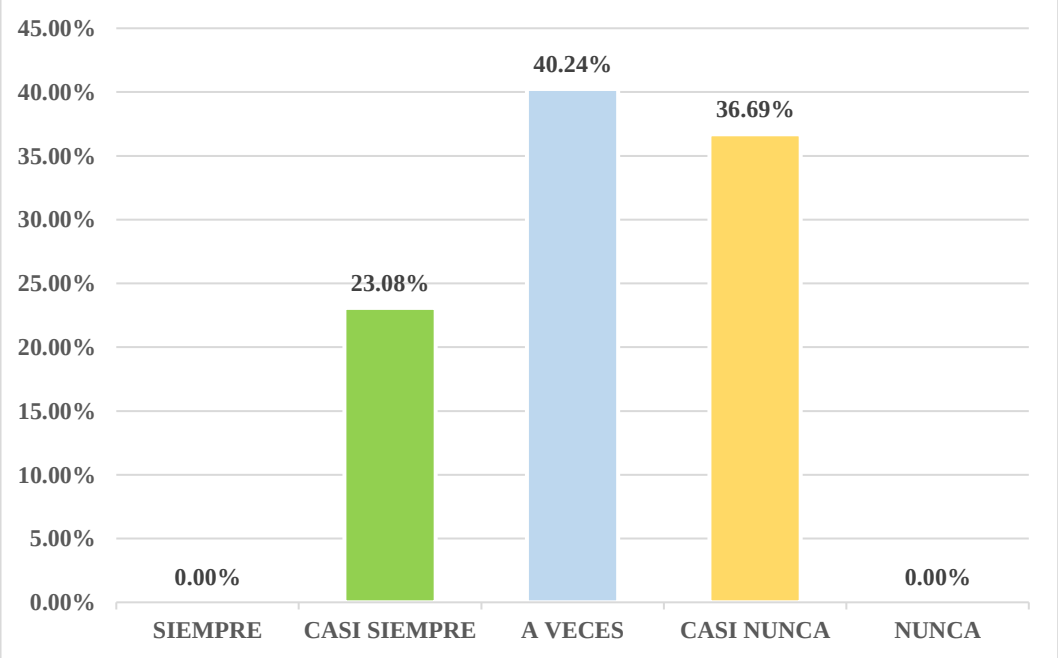


Interpretación: De acuerdo a los resultados obtenidos se detalla que el 35.80% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que "casi nunca" los sistemas que maneja la empresa aseguran que los datos transmitidos lleguen de manera coherente y sin errores, manteniendo su integridad durante el proceso. De la misma manera, el 26.92% consideraron que sucede "a veces", el 20.71% manifestaron "siempre" y el 16.57% "casi siempre".

Tabla 32. ¿Existen controles de seguridad que ayuden a detectar y corregir posibles errores en los datos, garantizando su exactitud y consistencia?

Respuesta	Frecuencia	Porcentaje
Siempre	0	0.00%
Casi siempre	78	23.08%
A veces	136	40.24%
Casi nunca	124	36.69%
Nunca	0	0.00%
Total	**338**	**100%**

Figura 30. ¿Existen controles de seguridad que ayuden a detectar y corregir posibles errores en los datos, garantizando su exactitud y consistencia?



Interpretación: De acuerdo a los resultados obtenidos se detalla que el 40.24% de los representantes de las MYPES comerciales del distrito de Ica. consideraron que “a veces” existen controles de seguridad que ayuden a detectar y corregir posibles errores en los datos, garantizando su exactitud y consistencia. De la misma manera, el 36.69% consideraron que sucede “casi nunca”, el 23.08% manifestaron “casi siempre”.

Comprobación de hipótesis:

Contrastación de hipótesis general:

Hipótesis general:

H0: La gestión de TIC's no impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

H_1: La gestión de TIC's impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

Tabla 6. Comprobación de Hipótesis General:

Correlaciones

			GESTIÓN TIC´S	PROCESO DE SEGURIDAD INFORMÁTICA
Rho de Spearman	GESTIÓN TIC´S	Coeficiente de correlación	1,000	,607**
		Sig. (bilateral)	.	,000
		N	338	338
	PROCESO DE SEGURIDAD INFORMÁTICA	Coeficiente de correlación	,607**	1,000
		Sig. (bilateral)	,000	.
		N	338	338

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación:

La verificación de la hipótesis general arrojó un coeficiente Rho de Spearman de 0.607, lo cual refleja una correlación buena positiva. Además, el valor de significancia obtenido fue de 0.000, lo que confirma que la correlación es estadísticamente significativa. En consecuencia, se acepta la hipótesis alterna y se rechaza la hipótesis nula, demostrando la existencia de una relación entre las variables.

Contrastación de hipótesis específicas:

Comprobando la hipótesis específica 1:

H_0 El talento humano no impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

H_1 El talento humano impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

Tabla 7. Comprobación de Hipótesis Específica 1:

Correlaciones

			TALENTO HUMANO	PROCESO DE SEGURIDAD INFORMÁTICA
Rho de Spearman	TALENTO HUMANO	Coeficiente de correlación	1,000	,243**
		Sig. (bilateral)	.	,000
		N	338	338
	PROCESO DE SEGURIDAD INFORMÁTICA	Coeficiente de correlación	,243**	1,000
		Sig. (bilateral)	,000	.
		N	338	338

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación:

El análisis de la hipótesis específica 1 reveló un coeficiente Rho de Spearman de 0.243, lo que evidencia una correlación baja. Además, el valor de significancia obtenido fue de 0.000, lo que indica que la correlación es estadísticamente significativa. En este contexto, se acepta la hipótesis alterna y se rechaza la hipótesis nula, confirmando la existencia de una relación entre las variables estudiadas.

Comprobando la hipótesis específica 2:

H_0 La orientación al negocio impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

H_1 La orientación al negocio impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

Tabla 8. Comprobación de Hipótesis Específica 2:

Correlaciones

			ORIENTACIÓN AL NEGOCIO	PROCESO DE SEGURIDAD INFORMÁTICA
Rho de Spearman	ORIENTACIÓN AL NEGOCIO	Coeficiente de correlación	1,000	,248**
		Sig. (bilateral)	.	,000
		N	338	338
	PROCESO DE SEGURIDAD INFORMÁTICA	Coeficiente de correlación	,248**	1,000
		Sig. (bilateral)	,000	.
		N	338	338

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación:

El análisis de la hipótesis específica 2 reveló un coeficiente Rho de Spearman de 0.248, lo que evidencia una correlación baja. Además, el valor de significancia obtenido fue de 0.000, lo que indica que la correlación es estadísticamente significativa. En este contexto, se acepta la hipótesis alterna y se rechaza la hipótesis nula, confirmando la existencia de una relación entre las variables estudiadas.

Comprobando la hipótesis específica 3:

H_0 La arquitectura no impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

H_1 La arquitectura impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.

Tabla 36. Comprobación de Hipótesis Específica 3:

Correlaciones

			ARQUITECTURA	PROCESO DE SEGURIDAD INFORMÁTICA
Rho de Spearman	ARQUITECTURA	Coeficiente de correlación	1,000	,250**
		Sig. (bilateral)	.	,000
		N	338	338
	PROCESO DE SEGURIDAD INFORMÁTICA	Coeficiente de correlación	,250**	1,000
		Sig. (bilateral)	,000	.
		N	338	338

**. La correlación es significativa en el nivel 0,01 (bilateral).

Interpretación:

El análisis de la hipótesis específica 3 reveló un coeficiente Rho de Spearman de 0.250, lo que evidencia una correlación baja. Además, el valor de significancia obtenido fue de 0.000, lo que indica que la correlación es estadísticamente significativa. En este contexto, se acepta la hipótesis alterna y se rechaza la hipótesis nula, confirmando la existencia de una relación entre las variables estudiadas.

IV. DISCUSIÓN

En 2024, Gordillo & Herrera [3], tuvieron por fin examinar los retos y oportunidades que emergen al incorporar las Tecnologías de la Información y la Comunicación (TIC) en las actividades operativas del Departamento de Talento Humano de un Gobierno Autónomo Descentralizado (GAD) Cantonal, con un enfoque en evaluar su influencia en la mejora de los procesos administrativos. Los resultados obtenidos indican que, al aplicar las recomendaciones surgidas de este estudio, se podría lograr un avance considerable en la modernización de la gestión del talento humano dentro del GAD estudiado. Este progreso se alcanzaría mediante la provisión de equipos adecuados y la optimización de los procesos, lo que facilitaría una atención más ágil a las necesidades del personal, al tiempo que incrementaría la eficiencia general de la organización.

En 2022, López [4], en su tesis examinaron los factores que intervienen en las actividades de ataques cibernéticos, en contraposición con la implementación de las Tecnologías de la Información y la Comunicación (TIC) en España. A partir de los hallazgos, se concluyó que ha existido un incremento en la adopción de las TIC, junto con la implementación de estrategias de ciberseguridad, como respuesta al crecimiento de la actividad delictiva en el entorno digital, con el fin de salvaguardar la información crítica de las organizaciones.

En 2023, Silva [7], en su estudio diseñó e implementó un Sistema de Gestión de Seguridad de la Información (SGSI) en una PYME, con el fin de fortalecer su protección frente a las amenazas que comprometen la seguridad de la información, siguiendo las directrices de la norma NTP-ISO/IEC 27001:2014. La aplicación de esta norma resultó ser exitosa en la gestión de la seguridad de la información dentro de la PYME, logrando mejoras sustanciales en la confidencialidad, integridad y disponibilidad de los activos de información, y garantizando su alineación con las mejores prácticas internacionales en el ámbito de la seguridad informática.

En 2022, Huaylla & Vargas [8], en su investigación propusieron examinar la relación entre la gestión de las Tecnologías de la Información y la Comunicación (TIC) y la seguridad informática en el Gobierno Regional de Apurímac durante el año 2021. Los resultados obtenidos demostraron una correlación significativa y positiva entre una gestión eficaz de las TIC y la mejora en los aspectos de seguridad informática, respaldada por un coeficiente de correlación de Pearson de 0.663 y un p-valor de 0.000. Se concluyó que la correcta administración de las TIC, junto con una infraestructura tecnológica robusta, personal calificado y un conocimiento profundo de los sistemas, juega un papel crucial en el

fortalecimiento de la seguridad informática, garantizando la confidencialidad, integridad y disponibilidad de la información, elementos fundamentales para la toma de decisiones y el cumplimiento de las normativas de seguridad.

V. CONCLUSIONES

1. En relación con el objetivo general del estudio, este se enfocó en analizar cómo la gestión de TIC's impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica. Los resultados obtenidos mostraron un coeficiente de Rho Spearman de 0.607, lo cual indica la existencia de una correlación buena. lo que sugiere que una adecuada gestión de TIC tiene un impacto favorable en los procesos de seguridad informática en estas organizaciones.
2. En relación con el objetivo específico 1 del estudio, este se enfocó en evaluar cómo el talento humano impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica. Los resultados obtenidos mostraron un coeficiente Rho de Spearman de 0.243, lo cual indica la existencia de una correlación baja. Esto resalta la necesidad de fortalecer las capacidades del talento humano, mediante capacitación y sensibilización, para maximizar su contribución en la seguridad informática de las MYPES.
3. En relación con el objetivo específico 2 del estudio, este se enfocó en evaluar cómo la orientación al negocio impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica. Los resultados obtenidos mostraron un coeficiente Rho de Spearman de 0.248, lo cual indica la existencia de una correlación baja. Esto significa que la orientación al negocio tiene cierta influencia en la seguridad informática, aunque su impacto no es muy significativo.
4. En relación con el objetivo específico 3 del estudio, este se enfocó en Evaluar cómo la arquitectura impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica. Los resultados obtenidos mostraron un coeficiente Rho de Spearman de 0.250, lo cual indica la existencia de una correlación baja. Esto sugiere que la arquitectura tecnológica tiene cierto impacto en la seguridad informática, pero su efecto es limitado.

VI. RECOMENDACIONES

1. Se sugiere diseñar un marco normativo que articule la gestión de tecnologías con estrategias específicas de seguridad, garantizando que las TIC se empleen de manera eficaz como mecanismos para la mitigación de riesgos. Asimismo, es esencial capacitar al personal en el manejo seguro de las TIC, enfatizando la identificación y prevención de amenazas como el phishing, el malware y las vulnerabilidades del sistema. Esta iniciativa fomentará un nivel más alto de compromiso y sensibilización respecto a la importancia de la ciberseguridad en la organización.
2. Integrar herramientas avanzadas de gestión de TIC que incluyan funcionalidades como sistemas de monitoreo, detección de intrusos y encriptación de datos, con el propósito de robustecer la protección de la información. Además, es crucial llevar a cabo evaluaciones periódicas de los procesos de seguridad informática, permitiendo identificar vulnerabilidades y aplicar mejoras oportunas. Por último, garantizar que las decisiones relacionadas con la gestión de TIC estén estrechamente alineadas con los objetivos estratégicos de la organización, diseñadas específicamente para aumentar la resiliencia frente a posibles riesgos cibernéticos.
3. Se recomienda implementar programas de formación continua para todo el personal, con un enfoque en prácticas esenciales de seguridad informática, tales como la correcta gestión de contraseñas, la identificación de amenazas cibernéticas (como phishing o malware) y el uso seguro de las tecnologías disponibles. La sensibilización acerca de los riesgos digitales debe ser un proceso constante y progresivo. Además, es necesario fomentar la importancia de la ciberseguridad como parte integral de la cultura organizacional, asegurando que todos los empleados, sin importar su jerarquía, comprendan y asuman su responsabilidad en la protección de los activos digitales de la empresa.
4. Es esencial identificar y formar a empleados clave en áreas especializadas de seguridad informática, con el objetivo de que sean los primeros en identificar posibles amenazas y actuar de manera preventiva para mitigar riesgos. Además, es necesario desarrollar políticas internas de seguridad informática claras y detalladas, asegurándose de que todos los miembros de la organización las comprendan y las implementen de manera rigurosa. Estas políticas deben abarcar aspectos fundamentales como los protocolos de acceso, la gestión adecuada de datos y los procedimientos a seguir en caso de incidentes de seguridad.
5. Es fundamental llevar a cabo evaluaciones periódicas del desempeño de los colaboradores en cuanto a la adopción y aplicación de buenas prácticas de seguridad informática. Estas evaluaciones podrían incluir, entre otras acciones, simulacros de

ciberataques o auditorías sobre el comportamiento y uso adecuado de las tecnologías de la información y comunicación (TIC).

VII. REFERENCIAS BIBLIOGRÁFICAS

[1] F. Pérez. “Influencia de la gestión y comportamiento de usuarios en el control de la seguridad de la información en Pymes”, tesis de posgrado, Esc. Posgrado, Univ. UISRAEL, Quito, Ecuador, 2023. [En línea]. Disponible en: https://repositorio.uisrael.edu.ec/handle/47000/3559

[2] C. Quevedo. “Ciberdefensa y ciberseguridad en el Perú: realidad y retos en torno a la capacidad de las FF. AA. para neutralizar ciberataques que atenten contra la seguridad nacional”, Revista de Ciencia e Investigación en Defensa, vol. 4, no. 1, pp. 55-76, 2023. [Internet]. Disponible en: https://doi.org/10.58211/recide.v4i1.99

[3] S. Gordillo y M. Herrera. “Influencia de las TIC en la gestión administrativa en el Departamento de Talento Humano del GAD cantonal de Loja, año 2024”. Universidad Nacional de Loja, Ecuador, 2024. [En línea]. Disponible en: https://dspace.unl.edu.ec/jspui/handle/123456789/30544

[4] F. López. “Seguridad colaborativa y tecnologías de información y comunicación”, tesis de posgrado, Esc. Doctorado, Univ. UGR, Granada, España, 2022. [En línea]. Disponible en: https://digibug.ugr.es/bitstream/handle/10481/80676/88372.pdf?sequence=4&isAllowed=y

[5] V. Alfaro. “Estrategia de negocio para el servicio de ciberseguridad Entel S.A.”, tesis de posgrado, Fac. de Ciencias Físicas y Matemáticas, Univ. UCHILE, Santiago de Chile, Chile, 2020. [En línea]. Disponible en: https://repositorio.uchile.cl/handle/2250/176772

[6] E. Téllez. “Tecnologías, seguridad informática y derechos humanos”, Revista Ius Et Scientia, vol. 4, no. 1, pp. 19-39, 2020. http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03. [Internet]. Disponible en: https://revistascientificas.us.es/index.php/ies/article/view/13296/0

[7] A. Silva. “Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021”. Tesis de grado. Univ. Tecnológica del Perú. Lima. [En línea]. Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/5705/A.Silva_Tesis_Titulo_Profesional_2022.pdf?sequence=1&isAllowed=y

[8] A. Huaylla y M. Vargas. “Gestión de tecnologías de información y comunicación y los procesos de seguridad informática en el gobierno regional de Apurímac, 2021”, tesis de pregrado, Fac. de ingeniería, Univ. UTEA, Abancay, Perú, 2022. [En línea]. Disponible en: https://repositorio.utea.edu.pe/server/api/core/bitstreams/3d7cebd5-44ce-4343-8fc8-d8d505393608/content

[9] E. Crespo. “Las TICS y la gestión administrativa en la municipalidad distrital de Luyando Naranjillo, 2020”, tesis de posgrado, Esc. Posgrado, Univ. UNAS, Tingo María, Perú, 2021. [En línea]. Disponible en: https://repositorio.unas.edu.pe/bitstream/handle/20.500.14292/2237/TS_ELC_2021.pdf?sequence=1&isAllowed=

[10] G. Rossi. “La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas”, tesis de posgrado, Maestría en diplomacia y relaciones internacionales, Univ. ADP, Lima, Perú, 2021. [En línea]. Disponible en: http://repositorio.adp.edu.pe/bitstream/handle/ADP/170/2021%20Tesis%20Rossi%20Levano,%20Giancarlo.pdf?sequence=1

[11] J. Izquierdo. “Modelo basado en la gestión de seguridad de la información para contribuir en los procesos de las farmacias de los hospitales II-I en la región Amazonas”, tesis de posgrado, Esc. Posgrado, Univ. USAT, Chiclayo, Perú, 2021. [En línea]. Disponible en: https://tesis.usat.edu.pe/bitstream/20.500.12423/4193/1/TM_IzquiersoCabreraJaime.pdf

[12] E. Ferrero, I. Cantón, M. Menéndez, A. Escapa y A. Bernardo. “TIC y gestión del conocimiento en estudiantes de Magisterio e Ingeniería”. Revista Científica de Comunicación y Educación, vol. 1, no. 66, 2021. [Internet]. Disponible en: https://doi.org/10.3916/C66-2021-05

[13] A. Castañeda. “Análisis del uso de las TICs en MYPES del rubro de Salón & Spa de la ciudad de Chiclayo, 2021”. Tesis de grado. Univ. Católica Santo Toribio de Mogrovejo. [En línea]. Disponible en: https://tesis.usat.edu.pe/bitstream/20.500.12423/6215/8/TL_Casta%C3%B1edaChaconAnthony.pdf

[14] G. Cortés. “TIC definición y componentes, 2021”. [Internet]. Disponible en: https://sites.google.com/site/tecnologiaeducativachepo/tic-antecedentesy-definicion

[15] P. Marqués. “Calidad de la formación virtual y de los materiales multimedia”. XII Congreso Nacional I Iberoamericano de Pedagogía, 2020. Madrid, España.

[16] A. Ca´Zorzi. “Las TIC en el desarrollo de la PyME: Algunas experiencias de América Latina”. Centro internacional de investigaciones para el desarrollo en colaboración con fondo multilateral de inversiones/banco interamericano de desarrollo, p. 91. 2020. [Internet]. Disponible en: https://pymespracticas.typepad.com/ files/tic-y-pymes-en-al-final-2011.pdf

[17] M. Rodríguez y J. Peña. “Medición de capacidad en tecnología de información en las organizaciones”. Artículo científico. Pp. 50-65. [Internet]. Disponible en: http://www.scielo.org.co/pdf/ean/n72/n72a04.pdf

[18] C. Rocha. “La Seguridad Informática”, Revista Ciencia Unemi, vol. 4, no. 5, pp. 26-33, 2011. [Internet]. Disponible en: https://www.redalyc.org/articulo.oa?id=582663867004

[19] A. Gómez. “Enciclopedia de la Seguridad Informática”. 2da. Ed. actualizada. Edit. RA-MA. 2021. [Internet]. Disponible en: https://books.google.com.pe/books?id=Bq8-DwAAQBAJ&pg=PT221&hl=es&source=gbs_selected_pages&cad=2#v=onepage&q&f=false

[20] K. Romero. “Propuesta de seguridad informática para mejorar el proceso de acceso remoto en una entidad financiera”. 2019. Univ. USIL. [En línea]. Disponible en: https://repositorio.usil.edu.pe/entities/publication/adba725c-bbfa-4b18-b768-44b35b4b4f0d

[21] M. Romero, G. Figueroa, D. Vera, J. Álava, G. Parrales, J. Álava, A. Murillo y M. “Introducción a la seguridad informática y el análisis de vulnerabilidades”. 3 ciencias. Editorial Área de Innovación y Desarrollo, S.L. 2018. [Internet]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridadinform%C3%A1tica.pdf

[22] S. Molinetti. “Principales tipos de seguridad informática en las empresas”. 2020. [Internet]. Disponible en: https://empresas.blogthinkbig.com/tipos seguridad-informatica-empresas/

[23] Universidad internacional de Valencia. "¿Qué es la seguridad informática y cómo puede ayudarme?". 2018. [Internet]. Disponible en: https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informaticay-como-puede-ayudarme

[24] A. Zuñiga, I. Serrano, L. Molina. "Seguridad informática en las Pymes de la ciudad de Quevedo". Universidad de Rioja, Ecuador. [En línea]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/7888305.pdf

[25] A. Heredia. "Políticas de fomento para la incorporación de las tecnologías digitales en las micro, pequeñas y medianas empresas de América Latina Revisión de experiencias y oportunidades". Cepal, 2019. [Internet]. Disponible en: https://repositorio.cepal.org/server/api/core/bitstreams/07bb3712-8dbd-40f9-b527-7fb04e67e435/content

[26] D. Pacheco y R. Rodríguez. "Las Tic´s como estrategia competitiva en la gestión empresarial". Revista de Investigación en Ciencias de la Administración ENFOQUES, vol. 3, núm. 12, pp. 286-298, 2019. Centro de Estudios Transdisciplinarios. [Internet]. Disponible en: https://www.redalyc.org/journal/6219/621968062004/html/

[27] M. Chávez y E. Henríquez. "La gestión del conocimiento y su relación con el desempeño laboral de los docentes en las instituciones educativas fiscales de la zona 8 del Ecuador, 2019". Universidad Politécnica Salesiana. Universidad. https://dspace.ups.edu.ec/bitstream/123456789/19092/4/UPS-GT002973.pdf

[28] M. Reyes. "Gestión del conocimiento y cultura organizacional en los colaboradores de la empresa NCH Perú SA Lurín-2019". Universidad Autónoma del Perú. Lima-Perú. [En línea] Disponible en: https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/1855/Reyes%20Caucha,%20Miguel%20Angel.pdf?sequence=1

[29] C. Valladolid. "Gestión del conocimiento y calidad del servicio en la municipalidad provincial de Morropón Piura". Universidad César Vallejo. Piura-Perú. [En línea]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/61560/Valladolid_NCL-SD.pdf?sequence=3

[30] B. Reyes. "Ejecución de obras públicas y generación de valor público en los ciudadanos del distrito de Ayacucho, Huamanga, Ayacucho, 2022". Tesis de Maestría. Universidad César Vallejo. Lima-Perú. [En línea]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/110137/Reyes_PBG-SD.pdf?sequence=1

[31] Y. Lavado. “Influencia del gasto público presupuestal en la ejecución de obras por administración directa de un gobierno local, La Libertad, 2023”. Universidad César Vallejo. Lima-Perú. [En línea]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/138943/Lavado_TYS-SD.pdf?sequence=1

VIII. ANEXOS

Anexo 1

Matriz de consistencia

Título: Gestión de tecnologías de información y comunicación para los procesos de seguridad informática en MYPES comerciales, Distrito de Ica, 2024.

Pregunta general	Objetivo general	Hipótesis general	Variables	Metodología
¿Cómo la gestión de TIC's impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024?	Analizar cómo la gestión de TIC's impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.	La gestión de TIC's impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.	**Variable (X):** Gestión de TIC's **Dimensiones:** • Talento humano. • Orientación al negocio. • Arquitectura. **Variable (Y):** Procesos de seguridad informática. **Dimensiones:** • Disponibilidad. • Confidencialidad.	**Tipo:** Básico. **Nivel:** Correlacional. **Diseño:** No experimental - Transversal. **Población:** 2820 MYPES comerciales del distrito Ica. **Muestra:** 338 MYPES comerciales del distrito Ica. **Técnica de recolección:** Encuesta. **Instrumento de recolección:** Cuestionario.
Preguntas específicas	**Objetivos específicos**	**Hipótesis específicas**		
¿Cómo el talento humano impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024?	Evaluar cómo el talento humano impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.	El talento humano impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.		
¿Cómo la orientación al negocio impacta en los	Evaluar cómo la orientación al negocio impacta en los	La orientación al negocio impacta positivamente en los		

procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024?	procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.	procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.	• Integridad.
¿Cómo la arquitectura impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024?	Evaluar cómo la arquitectura impacta en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024	La arquitectura impacta positivamente en los procesos de seguridad informática para las MYPES comerciales, distrito de Ica, 2024.	

Anexo 2

Instrumento de recojo de datos

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"

Variable Independiente:

GESTIÓN DE TIC'S

Saludos cordiales, el presente cuestionario busca recopilar información con respecto al estudio titulado: "*Gestión de tecnologías de información y comunicación para los procesos de seguridad informática en MYPES comerciales, Distrito de Ica, 2024"*.

Instrucciones: Marcar solo una vez la alternativa conveniente.

Participante: _____

Se debe tener en cuenta la escala para poder marcar con una (X) según su respuesta.

Escala de medición:

1	2	3	4	5
Siempre	Casi siempre	A veces	Casi nunca	Nunca

Variable Independiente: Gestión del conocimiento						
Ítem	**Preguntas**	**Respuestas**				
		1	**2**	**3**	**4**	**5**
	Dimensión 1: Talento humano					
1	¿El talento humano disponible a cargo de las TIC's reporta continuamente los resultados conseguidos?					
2	¿El talento humano disponible a cargo de las TIC's es capaz de establecer procesos de seguridad en la empresa?					
3	¿El talento humano disponible a cargo de las TIC's cumple cabalmente con las actividades asignadas?					
4	¿El talento humano disponible a cargo de las TIC's demuestra liderazgo con respecto a sus colegas?					

5	¿El talento humano disponible a cargo de las TIC's lleva a cabo sus operaciones teniendo todos los recursos a la mano?					
	Dimensión 2: Orientación al negocio					
6	¿Se llevan a cabo normas y protocolos que garantizan la efectividad en cuanto a la utilización de las TIC's?					
7	¿Los trabajadores utilizan las TIC's con la finalidad de optimizar los canales de comunicación en la empresa?					
8	¿Los trabajadores del área de TIC's demuestran un gran compromiso y responsabilidad en sus funciones?					
9	¿Los trabajadores del área de TIC's demuestran un grado de productividad según lo esperado?					
10	¿La empresa dispone del conocimiento necesario para clasificar los activos de carácter informático?					
	Dimensión 3: Arquitectura					
11	¿La empresa toma en cuenta el aseguramiento de la conectividad al adquirir nuevas tecnologías?					
12	¿La empresa toma en cuenta las políticas respecto al manejo de las TIC's?					
13	¿La empresa pone en marcha planes y programas para reducir un posible riesgo respecto a la información sensible?					
14	¿La empresa tiene conocimientos sobre las políticas enfocadas al tratamiento de los datos de clientes y proveedores?					
15	¿La empresa cumple con todas las actividades planificadas gracias a la utilización de las TIC's?					

Variable dependiente: PROCESOS DE SEGURIDAD INFORMÁTICA

Saludos cordiales, el presente cuestionario busca recopilar información con respecto al estudio titulado: *"Gestión de tecnologías de información y comunicación para los procesos de seguridad informática en MYPES comerciales, Distrito de Ica, 2024".*

Participante: _____

Se debe tener en cuenta la escala para poder marcar con una (X) según su respuesta.

Escala de medición:

1	2	3	4	5
Siempre	Casi siempre	A veces	Casi nunca	Nunca

Variable dependiente: Procesos de seguridad informática						
Ítem	**Preguntas**	**Respuestas**				
		1	**2**	**3**	**4**	**5**
	Dimensión 1: Disponibilidad					
1	¿Las TIC's que utiliza la empresa ayudan a gestionar de forma segura a los usuarios que tienen acceso a los sistemas, garantizando que solo las personas autorizadas puedan entrar?					
2	¿Las TIC's en la empresa aseguran que la información se comparta de manera rápida y eficiente, cuidando que no se modifique ni pierda durante el intercambio?					
3	¿Las TIC's implementadas en la empresa permiten almacenar los datos de manera segura, de modo que estén siempre disponibles para una consulta rápida cuando se necesiten?					
4	¿Los datos que maneja la empresa viajan por canales de comunicación seguros, lo que garantiza que no sean interceptados o alterados?					
5	¿Los retrasos en la entrega de requerimientos generan problemas que afectan las operaciones diarias de la empresa, como la entrega de productos o servicios?					

	Dimensión 2: Confiabilidad					
6	¿Los protocolos de seguridad que utiliza la empresa, como contraseñas o sistemas de verificación, ayudan a prevenir que personas no autorizadas puedan acceder a los datos?					
7	¿Las medidas de seguridad implementadas en la empresa reducen la posibilidad de que existan copias innecesarias o duplicaciones de los datos, evitando confusiones o errores?					
8	¿Las medidas de seguridad permiten que, en caso de un problema o incidente, ¿la empresa pueda responder rápidamente y proteger la información de los usuarios?					
9	¿Las medidas de seguridad garantizan que solo los empleados autorizados puedan acceder a la información confidencial de la empresa?					
10	¿Las técnicas de protección de datos utilizadas en la empresa, como la codificación o encriptación, son eficaces para evitar que personas no autorizadas accedan a información sensible?					
	Dimensión 3: Integridad					
11	¿Las TIC's implementadas en la empresa aseguran que la información siempre se mantenga veraz y exacta, sin que sea alterada de manera no autorizada?					
12	¿Los mecanismos de seguridad de la empresa previenen que la información sea modificada por personas o sistemas que no tienen permiso para hacerlo?					
13	¿La empresa cuenta con medidas para proteger la integridad de los datos, evitando cualquier alteración durante su procesamiento?					
14	¿Los sistemas que maneja la empresa aseguran que los datos transmitidos lleguen de manera coherente y sin errores, manteniendo su integridad durante el proceso?					
15	¿Existen controles de seguridad que ayuden a detectar y corregir posibles errores en los datos, garantizando su exactitud y consistencia?					

8.1.1. Consentimiento informado

Anexo 3

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"

Consentimiento Informado para Participantes de Investigación

La razón de la estructura de acuerdo es dar a los individuos datos precisos que den sentido a su interés.

Usted está de acuerdo en aceptar deliberadamente intervenir en esta revisión, para evaluar la asociación entre ***Gestión de tecnologías de información y comunicación para los procesos de seguridad informática en MYPES comerciales, Distrito de Ica, 2024*.**

La vigencia del cuestionario tendrá una duración de 20 minutos más o menos.

Por otra parte, los datos dados por usted pueden ser considerados para esta revisión y su apoyo será totalmente privado, ya que no será utilizado para fines diferentes. Además, si tiene alguna duda sobre la encuesta, no dude en plantearla.

Nombre del Participante (en letras de imprenta) **Firma del Participante** **Fecha:**

	VI: GESTIÓN TIC´S														
	TALENTO HUMANO				ORIENTACIÓN AL NEGOCIO						ARQUITECTURA				
ID	Preg. 1	Preg. 2	Preg. 3	Preg. 4	Preg. 5	Preg. 6	Preg. 7	Preg. 8	Preg. 9	Preg. 10	Preg. 11	Preg. 12	Preg. 13	Preg. 14	Preg. 15
1	2	3	4	4	3	2	3	2	3	4	2	3	3	3	4
2	1	2	4	4	2	3	3	2	3	1	2	4	3	2	4
3	2	1	2	3	3	2	3	2	3	3	4	4	4	2	4
4	2	1	2	1	2	2	3	2	4	3	4	4	4	2	3
1	3	2	2	1	2	2	3	4	4	4	4	3	4	3	2
6	3	2	1	1	2	1	4	4	4	4	4	3	1	3	2
7	3	3	1	3	2	1	4	4	1	4	3	3	1	4	2
8	3	3	1	3	4	1	4	4	1	1	4	3	2	4	3
9	4	3	2	2	4	2	4	3	2	1	4	1	2	4	3
10	4	3	2	2	4	2	1	3	2	2	4	1	2	2	1
11	1	3	3	2	4	3	1	3	3	2	3	1	2	2	1
12	3	4	3	3	3	3	1	3	3	2	3	1	3	2	1
13	1	4	3	3	3	3	1	4	3	2	3	1	3	3	4
14	2	4	3	4	3	3	4	4	3	3	4	4	3	3	4
11	2	4	3	4	4	2	4	3	2	3	2	4	2	3	3
16	3	4	1	1	4	2	4	2	2	1	2	4	2	4	3
17	3	3	1	1	4	2	3	2	3	1	2	3	2	4	2
18	4	3	1	4	4	1	3	1	1	1	2	3	1	4	2
19	4	2	1	3	4	1	3	1	1	3	4	3	1	4	2
20	4	2	4	3	3	1	3	1	1	3	4	2	4	3	3
21	4	1	4	2	3	1	3	1	1	2	1	2	4	3	3
22	3	1	3	2	3	2	2	1	4	2	1	2	3	3	3
23	3	2	3	2	2	2	4	2	4	2	1	3	3	2	4
24	2	2	2	2	2	2	4	2	4	3	1	3	3	2	4
21	2	2	2	3	2	2	1	2	3	3	1	3	3	2	4

26	3	2	3	4	2	3	3	2	3	3	4	4	2	2	1
27	1	3	3	4	3	3	2	3	3	4	4	4	2	2	1
28	1	3	3	4	3	3	2	3	3	4	4	4	2	2	1
29	2	4	3	1	3	3	2	3	3	2	3	1	2	3	1
30	3	4	3	1	3	3	2	4	4	3	3	1	3	3	4
31	3	4	2	4	4	2	2	4	4	3	3	1	2	3	4
32	4	4	2	3	4	2	3	4	4	4	3	1	2	4	4
33	4	3	2	3	4	2	3	3	4	4	3	4	2	3	3
34	4	3	1	3	4	1	3	3	4	1	3	4	1	2	3
31	4	2	1	2	3	1	4	2	1	4	4	3	1	2	3
36	4	2	1	2	3	1	4	2	1	1	4	2	1	3	3
37	3	1	1	2	3	1	4	1	1	3	4	2	1	4	2
38	3	2	1	4	2	1	1	1	1	3	1	2	1	4	2
39	2	2	2	4	2	2	1	1	1	4	1	2	4	4	2
40	2	3	1	4	2	2	4	2	4	4	1	3	4	3	2
41	1	3	1	4	2	2	3	2	4	4	1	3	4	3	3
42	3	4	3	3	3	2	3	2	3	1	1	3	4	3	2
43	2	3	1	3	3	3	2	3	3	1	4	3	4	4	3
44	1	2	3	3	3	3	2	3	3	2	4	4	3	4	3
41	2	2	3	3	4	3	2	3	3	2	4	4	3	4	3
46	2	3	3	1	4	3	2	3	3	2	3	4	3	3	3
47	1	2	3	1	4	3	2	4	4	2	3	1	3	3	4
48	1	1	2	1	4	2	3	4	4	4	3	1	2	3	4
49	2	1	2	1	3	2	3	4	4	2	3	4	2	2	4
10	3	2	2	4	3	2	3	4	4	3	3	4	2	2	1
11	3	2	1	4	3	1	4	3	3	3	4	1	1	4	1
12	4	3	1	3	2	1	4	3	3	4	4	4	1	2	1
13	4	3	1	1	2	4	4	3	1	4	4	3	1	3	1

14	4	3	4	1	3	4	1	2	1	4	4	2	1	3	4
11	2	3	4	1	2	3	1	2	2	4	1	2	2	2	4
16	1	3	3	3	3	3	1	2	2	1	1	2	2	2	2
17	2	4	2	3	2	2	4	1	2	1	1	2	3	2	3
18	2	4	3	2	2	2	4	1	3	1	1	2	3	3	3
19	3	4	3	2	2	2	4	1	3	1	1	3	3	3	4
60	3	4	3	2	2	2	3	2	3	4	4	3	2	3	4
61	3	4	2	3	4	3	3	1	2	4	4	3	2	4	4
62	3	3	2	3	4	3	2	2	2	3	4	4	2	4	1
63	4	3	2	4	4	4	2	2	2	3	4	4	2	4	1
64	4	2	1	4	4	4	2	1	1	2	3	4	3	4	1
61	1	2	1	1	3	4	2	3	4	3	3	4	3	3	1
66	1	1	1	1	3	3	3	2	1	4	3	1	4	2	4
67	1	1	1	4	3	3	3	2	1	4	3	1	1	2	3
68	2	2	1	3	4	1	3	1	1	1	3	1	1	2	2
69	2	2	1	3	4	1	4	1	1	4	4	1	1	3	2
70	3	2	2	2	4	2	4	1	4	1	4	4	2	3	2
71	3	2	2	2	4	2	1	2	4	3	4	4	2	4	3
72	4	3	2	2	4	2	1	3	4	3	4	4	2	4	3
73	4	3	2	2	3	2	3	3	4	4	1	3	2	4	4
74	4	4	3	3	3	3	3	4	3	4	1	3	3	2	1
71	4	4	3	4	3	3	3	4	3	4	1	3	3	2	1
76	3	4	1	4	2	1	2	4	3	1	1	3	4	2	1
77	3	4	1	4	2	2	4	3	1	1	3	3	4	3	1
78	2	3	2	1	2	2	4	2	1	2	4	2	3	3	4
79	2	3	2	1	2	2	1	2	1	2	4	2	3	3	4
80	1	2	2	4	3	2	3	1	1	2	3	3	2	4	3
81	1	2	2	3	3	1	2	1	4	2	4	3	2	4	2

82	1	1	3	3	3	1	2	2	4	4	4	4	2	4	2
83	2	2	3	3	3	1	2	2	1	1	4	4	2	4	2
84	3	2	1	2	4	2	2	2	2	1	1	4	3	3	2
81	3	3	1	2	4	2	2	2	2	1	1	3	3	3	3
86	4	3	1	2	4	3	3	4	3	1	1	3	1	3	3
87	4	4	1	4	4	2	3	4	3	1	4	4	1	2	4
88	4	3	4	4	3	2	3	4	3	4	4	4	3	2	4
89	4	2	4	4	3	2	4	4	3	4	3	1	3	2	1
90	4	2	3	3	3	3	4	3	2	4	3	1	2	2	1
91	3	3	3	1	2	3	4	3	2	3	3	1	2	2	1
92	3	2	2	1	2	3	1	3	2	3	3	3	2	2	4
93	2	1	1	1	2	3	1	3	4	3	3	2	1	3	4
94	2	1	1	3	2	4	4	4	1	3	3	3	1	3	3
91	1	2	1	3	3	4	3	4	1	3	4	3	1	3	3
96	2	2	1	2	3	1	3	3	1	2	4	3	1	4	2
97	3	3	2	2	3	2	2	2	1	2	4	3	2	3	2
98	1	3	2	2	4	2	2	2	1	3	4	2	3	2	2
99	2	3	1	3	4	2	2	1	4	3	4	3	3	2	3
100	2	3	1	3	4	2	2	1	4	4	1	4	4	3	3
101	1	3	1	4	4	3	2	1	3	4	1	4	4	4	3
102	1	4	3	4	3	3	3	1	3	1	1	4	1	4	4
103	2	4	3	1	3	3	3	1	3	2	1	3	2	4	4
104	3	4	3	4	3	3	3	2	3	4	1	3	4	3	4
101	3	4	2	3	3	3	4	2	3	1	4	3	3	3	1
106	4	4	2	3	2	2	4	2	4	3	4	3	2	3	1
107	4	3	2	2	2	2	4	2	4	3	4	1	2	4	1
108	4	3	3	2	2	2	1	3	4	4	3	1	2	4	1
109	4	2	3	3	1	1	1	3	4	4	3	1	1	4	4

110	3	2	4	3	1	1	1	3	3	4	3	1	1	3	4
111	3	1	3	4	1	1	4	4	3	1	3	1	1	3	4
112	2	1	2	4	1	1	4	4	3	1	3	4	1	3	3
113	2	2	3	1	1	1	4	4	3	2	3	4	1	2	3
114	1	2	3	1	2	2	3	3	3	3	4	4	2	2	3
111	1	2	4	1	2	2	3	3	4	3	4	3	2	4	3
116	1	2	4	4	2	2	2	2	4	4	4	3	2	2	2
117	2	3	4	4	2	2	2	2	2	4	1	3	3	3	2
118	3	3	3	3	3	3	2	1	3	2	1	2	3	3	2
119	3	4	3	3	3	3	2	1	3	1	1	2	4	2	2
120	4	4	2	2	3	3	3	1	3	4	1	2	4	2	3
121	4	4	2	2	3	3	3	2	3	3	1	3	4	2	2
122	4	4	1	2	3	3	3	2	3	3	4	3	4	3	3
123	4	3	4	3	2	2	4	2	2	4	4	3	4	3	3
124	4	3	3	3	2	2	4	3	2	2	4	4	3	3	3
121	3	2	1	4	2	2	1	3	2	3	3	4	4	4	3
126	3	2	3	4	3	1	1	3	1	3	3	4	1	4	4
127	2	1	3	4	3	1	3	3	1	4	3	1	1	4	4
128	2	2	1	3	3	1	3	4	1	4	3	1	1	4	4
129	1	2	1	1	2	1	3	4	4	4	3	1	1	3	1
130	1	3	2	1	2	2	2	4	4	4	4	1	2	2	1
131	2	3	2	1	2	2	4	4	4	1	4	4	2	2	1
132	3	4	2	3	2	2	4	3	4	1	4	4	2	2	1
133	2	3	3	3	3	3	1	3	3	3	4	3	3	3	4
134	2	2	3	2	3	3	3	3	3	3	1	2	3	3	4
131	1	2	4	2	3	3	2	2	3	4	1	2	4	4	2
136	1	1	4	2	3	2	2	2	1	4	1	2	4	4	3
137	2	1	4	3	4	2	2	2	1	1	1	2	1	4	3

138	3	2	3	3	4	2	2	1	1	1	1	3	1	2	4
139	3	2	3	4	4	1	2	1	1	4	4	3	4	2	4
140	4	3	3	4	4	4	3	1	4	4	4	3	4	2	4
141	4	3	3	1	3	3	3	2	4	3	4	3	3	3	1
142	4	3	1	1	3	1	3	1	4	3	4	4	3	3	1
143	2	3	1	4	3	1	4	2	3	3	3	4	3	3	1
144	1	3	1	3	2	1	4	2	1	3	3	4	3	4	1
141	2	4	2	3	2	2	4	1	2	2	3	1	2	4	4
146	2	4	2	2	2	2	1	3	2	2	3	1	2	4	3
147	3	4	2	2	2	2	1	2	2	2	3	4	2	4	2
148	3	4	2	2	3	2	4	2	2	2	4	4	2	3	2
149	3	4	3	2	3	3	3	1	3	3	4	1	3	3	1
110	3	3	3	3	3	3	3	1	3	3	4	4	3	3	1
111	4	3	1	4	4	1	2	1	4	4	4	3	1	2	4
112	4	2	2	3	4	2	2	2	4	3	1	2	2	2	4
113	1	2	2	3	4	2	2	3	1	3	1	2	2	2	3
114	3	1	2	4	4	2	2	3	1	4	1	2	2	2	3
111	1	1	2	4	3	2	2	4	1	4	1	2	2	2	2
116	2	2	1	4	3	1	3	4	1	4	3	2	1	2	2
117	2	2	1	4	3	1	3	4	1	4	4	3	1	3	2
118	3	2	1	3	2	1	3	3	4	1	4	3	1	3	3
119	3	2	2	3	2	2	4	2	4	1	3	3	2	3	3
160	4	3	2	3	3	2	4	2	3	1	4	4	2	4	3
161	4	3	3	2	2	3	4	1	3	1	4	4	3	3	4
162	4	4	3	2	3	3	1	1	3	1	4	4	3	2	4
163	4	4	3	2	2	3	1	2	3	1	1	4	3	2	4
164	3	4	3	2	2	3	1	2	3	2	1	1	3	3	1
161	3	4	2	3	2	2	4	2	2	2	1	1	2	4	1

166	2	3	2	3	2	2	4	2	2	2	4	1	2	4	1
167	2	3	2	3	4	2	4	4	2	2	4	1	2	4	1
168	1	2	1	2	4	1	3	4	1	3	3	4	4	3	4
169	3	2	1	2	4	1	3	4	1	3	3	4	2	3	4
170	1	1	1	2	4	1	2	4	1	1	3	4	2	3	4
171	2	2	1	2	3	1	2	3	1	1	3	3	2	4	3
172	3	2	2	3	3	2	2	3	2	1	3	3	2	4	3
173	3	3	2	4	3	2	2	3	2	1	3	3	3	4	3
174	4	3	2	4	4	2	3	3	4	1	4	3	3	3	3
171	4	4	2	4	4	2	3	4	4	4	4	3	4	3	2
176	4	3	3	1	4	2	3	4	1	4	4	2	4	3	2
177	4	2	3	1	4	2	4	3	1	3	4	2	3	2	2
178	4	2	1	4	4	2	4	2	3	3	4	3	3	2	2
179	3	3	1	3	3	3	1	2	3	3	1	3	3	4	3
180	3	2	1	3	3	3	1	1	3	3	1	4	3	2	2
181	2	1	4	3	3	2	3	1	4	2	1	4	2	3	3
182	2	1	4	2	2	2	3	1	4	2	1	4	2	3	3
183	1	2	3	2	2	2	3	1	4	2	1	3	2	2	3
184	2	2	3	2	2	1	2	1	1	2	4	3	2	2	3
181	3	3	2	4	2	1	4	2	1	3	4	4	3	2	4
186	1	3	3	4	3	1	4	2	1	3	4	4	3	3	4
187	2	3	4	4	3	1	1	2	1	3	3	1	4	3	4
188	2	3	4	3	3	1	3	2	1	3	3	1	4	3	1
189	1	3	1	1	3	2	2	3	2	3	3	1	1	4	1
190	3	4	2	1	4	2	2	3	2	3	3	3	2	4	1
191	2	4	2	1	4	2	2	3	2	4	3	2	4	4	1
192	3	4	2	3	4	2	2	4	2	4	3	3	1	4	4
193	3	4	3	3	4	3	2	4	3	2	4	3	3	3	4

194	4	4	3	2	3	3	3	4	3	1	4	3	3	2	2
191	4	3	3	2	3	3	3	3	3	4	4	3	4	2	3
196	4	3	3	2	3	3	3	3	3	3	1	2	3	2	3
197	4	2	4	3	2	3	4	2	1	3	1	4	3	3	4
198	3	2	1	3	2	4	4	2	1	4	1	4	3	3	4
199	3	1	1	4	2	4	4	1	4	2	1	1	3	4	4
200	2	1	2	4	2	3	1	1	4	3	1	1	4	4	1
201	2	2	2	1	3	3	1	1	4	3	4	4	4	4	1
202	3	2	2	1	3	3	4	2	3	4	4	4	4	2	1
203	2	2	2	4	3	2	3	2	1	4	4	1	1	2	1
204	1	2	3	3	4	1	3	2	1	4	3	4	1	2	4
201	2	3	3	3	4	2	2	3	2	4	3	3	2	3	3
206	3	3	1	2	4	2	2	3	2	1	3	2	2	3	2
207	3	4	1	2	4	2	2	3	2	1	3	2	2	3	2
208	4	4	2	2	3	3	2	3	3	1	3	2	3	4	1
209	4	4	2	2	3	3	2	4	3	1	4	2	3	4	1
210	4	4	2	3	3	3	3	4	3	1	4	2	3	4	4
211	4	3	3	4	2	2	3	4	2	4	4	3	2	4	4
212	4	3	3	4	2	2	3	4	2	4	4	3	2	3	3
213	3	2	3	4	3	2	4	3	1	3	1	3	2	3	3
214	3	2	3	1	2	1	4	3	1	3	1	4	1	3	2
211	2	1	3	1	3	4	4	3	1	3	1	4	1	2	2
216	2	2	3	4	2	3	1	2	1	3	1	4	1	2	2
217	1	2	4	3	2	1	1	2	4	2	1	4	1	2	3
218	2	3	4	3	2	1	1	2	4	2	4	1	1	2	3
219	1	3	1	3	2	1	4	1	3	2	4	1	1	2	3
220	1	4	1	2	4	2	4	1	3	2	4	1	2	2	4
221	2	3	1	2	4	2	4	1	3	3	4	1	2	3	4

222	2	2	3	2	4	2	3	2	3	3	3	4	2	3	4
223	1	2	3	4	4	2	3	1	3	4	3	4	2	3	1
224	1	1	2	4	3	3	2	2	4	4	3	4	3	4	1
221	2	1	2	4	3	3	2	2	4	1	3	3	1	3	1
226	3	2	4	3	3	1	2	1	1	2	3	3	2	2	1
227	3	2	4	1	4	2	2	3	2	4	4	3	4	2	4
228	4	3	4	1	4	2	3	2	2	1	4	3	1	3	4
229	4	3	4	1	4	2	3	2	2	3	4	3	3	4	4
230	4	3	4	3	4	2	3	1	2	3	4	2	3	4	3
231	2	3	1	3	4	1	4	1	1	4	1	2	4	4	3
232	3	3	1	2	3	1	4	1	1	4	1	3	4	3	3
233	2	4	1	2	3	1	1	2	1	1	1	3	4	3	3
234	2	4	1	2	3	2	1	3	2	1	1	4	1	3	2
231	3	4	1	3	2	2	3	3	1	1	3	4	1	4	2
236	3	4	2	3	2	3	3	4	1	1	4	4	3	4	2
237	3	4	2	4	2	3	3	4	3	1	4	3	4	4	2
238	3	3	1	2	3	3	2	4	3	4	3	3	4	3	3
239	4	3	4	2	3	3	4	3	3	4	4	4	2	3	2
240	4	2	3	3	2	2	4	2	4	4	4	4	2	3	3
241	2	2	3	3	2	2	1	2	4	3	4	1	1	2	3
242	1	1	2	4	2	2	3	1	4	3	1	1	1	2	3
243	3	1	2	3	1	1	2	1	1	3	1	1	1	4	3
244	2	2	2	4	1	3	2	2	1	3	1	3	4	2	4
241	2	2	1	4	1	3	2	2	1	3	4	2	4	3	4
246	3	2	1	4	1	2	2	2	1	2	4	3	3	3	4
247	3	2	1	3	2	2	2	2	2	2	3	3	3	2	1
248	4	3	1	3	2	2	3	4	2	2	3	3	2	2	1
249	4	3	3	4	3	2	3	4	2	3	3	3	2	2	1

210	4	4	3	4	2	2	3	4	2	3	3	2	2	3	1
211	4	4	3	4	2	3	4	4	3	3	3	4	2	3	4
212	3	4	3	1	2	3	4	3	3	4	3	4	3	3	4
213	3	4	2	1	2	3	4	3	3	4	4	1	3	4	2
214	2	3	2	4	3	3	1	3	1	4	4	1	2	4	3
211	2	3	2	3	3	4	1	3	1	1	4	4	2	4	3
216	1	2	2	3	3	2	4	4	1	1	4	4	2	4	4
217	1	2	2	3	4	2	3	4	1	1	4	1	3	3	4
218	1	1	2	2	4	2	3	3	4	1	1	4	3	2	4
219	2	2	1	2	4	1	2	2	4	4	1	3	4	2	1
260	3	2	1	2	4	1	2	2	4	4	1	2	4	2	1
261	3	3	1	4	3	1	2	1	3	2	1	2	1	3	1
262	4	3	1	2	3	1	2	1	3	3	1	2	2	3	1
263	4	4	1	4	3	1	2	1	3	3	4	2	4	4	4
264	4	3	2	4	2	2	3	1	3	1	4	2	1	4	3
261	4	2	2	4	2	2	3	1	3	3	4	3	2	4	2
266	4	2	2	3	3	2	3	2	4	3	3	3	2	2	2
267	3	3	2	1	2	2	4	2	4	4	3	3	2	2	1
268	3	2	3	1	3	3	4	2	4	4	3	4	3	2	1
269	2	1	3	1	2	3	4	2	3	4	3	4	3	3	4
270	2	1	3	3	2	3	1	3	3	1	3	4	3	3	4
271	1	2	3	3	2	3	1	3	3	1	3	4	3	3	3
272	1	2	3	2	2	3	1	3	3	2	4	1	3	4	3
273	1	3	2	2	4	4	4	4	2	2	4	1	2	4	2
274	1	3	2	2	4	4	4	4	2	2	4	1	2	4	2
271	2	3	3	3	4	3	4	4	2	2	1	1	2	4	2
276	2	3	3	3	4	3	3	3	1	3	1	4	3	3	3
277	1	3	4	4	3	3	3	3	1	3	1	4	3	3	3

278	1	4	4	4	3	2	2	2	1	1	1	4	3	3	3
279	2	4	1	1	3	2	2	2	3	1	1	3	3	2	4
280	3	4	1	1	4	2	2	1	3	1	4	3	4	2	4
281	3	4	1	4	4	2	2	1	3	1	4	3	2	2	4
282	4	4	3	3	4	2	3	1	3	1	4	3	2	2	1
283	4	3	3	3	4	3	3	2	4	4	3	3	2	2	1
284	4	3	2	2	4	3	3	2	4	4	3	2	2	2	1
281	2	2	2	2	3	3	4	2	4	3	3	2	3	3	1
286	1	2	4	2	3	2	4	3	4	3	3	3	3	3	4
287	1	1	4	2	3	2	1	3	3	3	3	3	4	3	4
288	1	1	4	3	2	2	1	3	3	3	4	4	4	4	4
289	2	2	4	4	2	1	3	3	3	2	4	4	4	3	3
290	3	2	4	4	2	1	3	4	3	2	4	4	2	2	3
291	3	2	1	4	2	3	3	4	3	2	4	3	2	2	3
292	4	2	1	1	3	3	2	4	4	2	1	3	2	3	3
293	4	3	1	1	3	2	4	4	1	3	1	4	3	4	2
294	4	3	3	4	3	2	4	3	1	3	1	4	3	4	2
291	4	4	3	3	3	2	1	3	2	4	1	1	4	4	2
296	4	4	3	2	4	4	3	3	2	4	1	1	4	3	2
297	3	4	3	4	4	4	2	2	2	4	4	1	1	3	3
298	3	4	1	4	4	4	2	2	2	4	4	3	2	3	2
299	2	3	1	4	4	3	2	2	3	1	4	2	4	4	3
300	2	3	1	3	3	3	2	1	3	1	4	3	1	4	3
301	1	2	3	1	3	3	2	1	1	1	3	3	3	4	3
302	1	2	3	1	3	2	3	1	1	1	3	3	3	3	3
303	1	1	3	1	2	2	3	2	4	1	3	3	4	3	4
304	1	2	4	4	4	2	3	1	1	1	3	2	4	3	4
301	2	2	4	3	4	2	4	2	1	4	3	4	4	2	4

306	2	3	1	3	1	2	4	2	1	4	4	4	1	2	1
307	1	3	1	3	1	3	4	1	1	2	4	4	1	4	1
308	1	4	2	4	2	3	1	3	1	3	4	3	2	2	1
309	2	3	2	4	2	3	1	2	4	3	4	3	2	3	1
310	3	2	2	4	2	3	4	2	4	3	1	3	2	3	4
311	3	2	2	4	2	3	3	1	3	3	1	3	3	2	4
312	4	2	3	3	3	2	3	1	3	4	1	3	4	2	2
313	4	2	3	3	3	2	2	1	3	4	1	2	4	2	3
314	4	2	1	3	1	2	2	2	3	2	3	2	4	3	3
311	1	3	1	2	1	1	2	3	3	1	4	3	4	3	4
316	1	3	1	2	1	1	2	3	4	4	4	3	1	3	4
317	1	4	1	2	1	1	2	4	4	3	3	4	1	4	4
318	2	4	1	2	4	1	3	4	4	3	3	4	1	4	1
319	3	4	1	3	4	1	3	4	4	4	4	4	1	4	1
320	3	4	2	3	1	2	3	3	3	2	4	3	1	4	1
321	4	3	2	3	1	2	4	2	3	3	4	3	1	3	1
322	4	3	2	3	2	2	4	2	3	3	4	4	2	3	4
323	4	2	2	4	2	2	4	1	3	4	1	4	2	2	3
324	4	2	3	4	2	3	1	1	3	4	1	1	2	2	2
321	4	1	3	4	2	3	1	3	4	4	1	1	2	2	2
326	3	2	3	1	2	3	1	2	3	4	1	1	3	3	1
327	3	2	3	1	2	3	4	2	3	1	1	3	3	3	1
328	2	3	3	4	3	3	4	1	3	1	4	2	1	3	4
329	2	3	3	3	3	2	4	1	2	1	4	2	4	4	4
330	1	4	3	2	3	2	3	1	2	1	4	3	4	3	2
331	1	3	3	3	3	3	3	2	2	1	4	3	1	3	3
332	1	3	3	3	4	3	2	3	4	1	3	4	1	2	3
333	1	2	4	4	4	3	2	3	4	2	3	4	2	2	4

334	2	2	4	4	4	2	2	4	3	2	3	4	3	2	4
331	3	1	1	1	4	3	2	4	3	2	3	3	3	3	4
336	1	2	1	1	3	3	3	4	3	2	3	3	4	3	1
337	2	2	1	4	3	3	3	3	3	3	4	4	2	3	1
338	2	1	3	3	3	4	3	2	3	3	4	4	4	4	1

	VD: PROCESO DE SEGURIDAD INFORMATICA														
	DISPONIBILIDAD							CONFIDENCIALIDAD			INTEGRIDAD				
ID	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
1	3	2	4	2	3	2	3	3	1	3	2	4	3	4	4
2	2	3	2	2	3	3	2	4	2	2	2	1	4	4	3
3	2	3	4	1	4	1	3	4	2	4	4	3	4	4	3
4	2	3	4	1	4	1	3	4	2	4	4	3	2	3	3
1	2	3	4	2	1	4	4	3	2	4	4	4	2	2	4
6	3	4	1	3	1	4	4	3	1	3	4	4	2	2	4
7	3	4	1	3	1	3	4	2	1	2	3	4	3	2	4
8	2	4	4	3	4	3	3	2	1	2	4	1	3	3	4
9	2	4	4	3	4	2	3	2	2	2	4	1	2	3	3
10	2	3	3	2	3	2	2	3	2	1	4	2	2	4	2
11	4	2	3	2	3	2	2	3	3	4	3	2	4	4	3
12	4	2	2	2	3	3	1	4	3	3	3	2	4	4	4
13	4	2	2	1	4	3	4	4	3	4	3	2	2	4	3
14	3	2	2	2	4	4	3	4	3	1	4	3	2	1	3
11	1	4	2	2	1	4	1	1	2	1	2	3	2	1	2
16	1	4	3	3	1	1	4	1	2	1	2	1	4	1	2
17	1	4	3	3	1	1	1	1	2	4	2	1	3	1	2
18	1	4	3	4	2	1	1	4	1	3	2	1	4	4	3
19	1	1	4	4	4	4	4	3	1	3	3	1	4	4	3
20	4	1	4	4	3	3	3	3	1	2	3	4	3	3	4
21	4	1	4	3	3	3	3	2	1	2	3	4	3	3	4
22	4	4	1	2	3	3	2	2	2	2	4	3	2	2	4
23	4	3	1	2	4	2	2	3	2	3	4	3	2	2	4
24	3	2	1	1	4	2	2	3	2	3	4	3	2	3	4
21	2	2	4	1	1	2	1	4	2	4	4	3	3	3	3

26	2	2	4	1	1	4	1	4	3	4	3	2	3	3	3
27	1	2	4	2	2	4	1	1	3	4	3	2	4	4	3
28	1	3	3	2	2	4	1	1	3	4	3	2	4	4	2
29	1	3	3	3	2	1	4	1	3	4	2	2	4	4	2
30	2	4	2	3	3	1	4	4	3	3	2	3	4	4	2
31	2	4	2	4	3	1	3	4	2	3	2	3	3	1	3
32	2	4	2	4	4	1	3	3	2	3	2	4	3	1	3
33	3	1	2	4	4	4	3	3	2	3	3	4	3	1	3
34	3	1	2	4	1	3	2	2	1	2	3	1	2	4	4
31	3	1	3	3	1	2	2	2	1	2	3	4	2	4	4
36	4	4	3	3	4	2	2	2	1	2	3	1	2	3	4
37	4	4	3	2	4	2	1	3	1	2	4	3	2	3	4
38	4	4	4	2	3	4	1	3	1	3	2	3	3	3	3
39	4	3	4	1	3	4	1	4	2	3	2	4	3	3	3
40	3	3	4	1	2	1	3	4	2	3	4	4	3	4	2
41	3	2	4	1	2	2	3	1	2	3	3	4	4	4	2
42	2	2	1	1	2	2	3	1	2	4	3	1	4	4	2
43	2	2	1	2	3	2	4	3	3	4	3	1	4	1	2
44	1	2	1	2	3	3	4	3	3	4	4	2	3	1	3
41	1	2	4	2	4	3	1	2	3	4	4	2	3	1	3
46	1	3	4	3	4	1	2	2	3	1	4	2	2	4	3
47	1	3	3	3	1	4	3	3	3	1	4	2	2	3	4
48	2	3	3	3	3	4	4	3	2	1	3	3	2	2	4
49	2	4	2	4	3	4	3	4	2	4	3	3	2	2	3
10	2	4	2	4	4	2	2	4	2	3	3	1	3	2	3
11	3	4	2	4	4	2	2	4	1	2	2	1	4	2	3
12	3	1	4	4	1	3	2	3	1	2	2	1	4	2	4
13	3	1	4	3	1	1	3	3	1	3	2	1	2	3	4

14	4	1	4	3	1	1	3	2	1	3	2	4	2	3	4
11	4	1	2	4	4	4	4	2	2	4	3	4	2	4	4
16	4	1	2	2	4	4	3	2	2	4	3	3	3	4	3
17	4	1	2	2	3	3	2	3	2	1	3	3	3	4	2
18	3	4	1	1	3	3	3	3	3	1	3	3	2	4	3
19	3	4	1	1	3	2	3	4	3	1	4	3	2	1	4
60	3	4	1	1	4	2	4	4	3	1	4	2	4	1	3
61	2	4	3	1	4	2	4	4	2	1	4	2	4	1	3
62	2	1	3	2	1	3	4	1	2	4	4	2	2	1	2
63	1	2	3	2	1	3	3	1	2	4	3	2	2	4	2
64	1	3	3	2	1	4	3	1	1	4	3	3	2	3	2
61	1	3	1	3	2	4	2	4	1	4	2	3	4	2	3
66	1	3	1	3	4	1	2	3	1	3	2	4	3	3	3
67	3	2	4	3	3	1	1	3	1	1	2	4	4	3	4
68	2	3	2	3	3	1	4	2	1	1	2	1	4	4	4
69	2	3	4	4	3	4	3	2	1	3	4	4	3	4	4
70	2	3	4	3	4	3	1	3	2	2	4	1	3	4	4
71	4	3	4	4	4	3	4	3	2	3	4	3	2	3	4
72	4	4	1	3	1	3	1	4	2	2	4	3	2	2	3
73	4	4	1	4	1	2	1	4	2	1	3	4	2	2	3
74	3	4	4	2	2	2	4	1	3	3	4	4	3	2	3
71	1	4	4	3	2	2	3	1	3	2	4	4	3	3	2
76	1	3	3	2	2	4	3	1	1	4	4	1	4	3	2
77	1	2	3	3	3	4	2	4	2	4	3	1	4	4	2
78	1	2	2	2	3	4	2	4	2	4	3	2	4	4	3
79	1	2	2	3	4	1	2	3	2	3	3	2	4	4	3
80	4	2	2	2	4	1	1	3	2	2	4	2	3	4	3
81	4	4	2	2	1	1	1	2	1	2	2	2	3	1	4

82	4	4	3	2	1	1	1	2	1	2	2	3	3	1	4
83	4	4	3	1	4	4	1	2	1	1	2	3	2	1	4
84	3	4	3	1	4	3	4	3	2	4	2	1	2	1	4
81	2	1	4	2	3	2	4	3	2	3	3	1	2	4	3
86	2	1	4	3	3	2	3	4	3	4	3	1	2	4	3
87	1	1	4	3	2	2	3	3	3	1	3	1	3	3	2
88	1	4	1	3	2	4	3	4	3	1	4	4	3	3	2
89	1	3	1	3	2	4	2	4	3	1	4	4	3	2	2
90	2	2	1	2	3	1	2	4	2	4	4	3	4	2	2
91	2	2	4	2	3	2	2	3	2	3	4	3	4	3	3
92	2	2	4	2	4	2	1	3	2	3	3	3	4	3	3
93	3	2	4	1	4	2	1	2	1	2	3	3	3	3	3
94	3	3	3	2	1	3	1	2	1	2	3	2	3	4	4
91	3	3	3	2	3	3	3	2	1	2	2	2	2	4	4
96	4	4	2	3	3	1	3	3	1	3	2	2	2	4	4
97	4	4	2	3	4	4	3	3	2	3	2	2	2	4	3
98	4	4	2	4	4	4	4	4	2	4	2	3	2	1	2
99	4	1	2	4	1	4	4	4	2	4	3	3	3	1	3
100	3	1	2	4	1	2	1	4	2	4	3	4	4	1	4
101	3	1	3	3	1	2	3	1	3	4	3	4	4	4	3
102	2	4	3	2	4	3	2	1	3	4	3	1	2	4	3
103	2	4	3	2	4	1	4	1	3	3	4	2	2	3	2
104	1	4	4	1	3	1	3	4	3	3	2	4	2	3	2
101	1	3	4	1	3	4	2	3	3	3	2	1	3	3	2
106	1	3	4	1	3	4	2	3	2	3	4	3	3	3	3
107	1	2	4	2	4	3	2	2	2	2	3	3	2	4	3
108	2	2	1	2	4	3	3	2	2	2	3	4	2	4	4
109	2	2	1	3	1	2	3	3	1	2	3	4	4	4	4

110	2	2	1	3	1	2	4	3	1	2	4	4	4	1	4
111	3	2	4	4	1	2	3	4	1	3	4	1	2	1	4
112	3	3	4	4	2	3	2	4	1	3	4	1	2	1	4
113	3	3	3	4	4	3	3	1	1	3	4	2	2	4	3
114	4	3	3	4	3	4	3	1	2	3	3	2	4	3	3
111	4	4	2	3	3	4	4	1	2	4	3	2	3	2	3
116	4	4	2	3	3	1	4	4	2	4	3	2	4	2	2
117	4	4	2	2	4	1	4	4	2	4	2	3	4	2	2
118	3	1	4	2	4	1	3	3	3	4	2	3	3	2	2
119	3	1	4	1	1	4	3	3	3	1	2	1	3	2	3
120	3	1	4	1	1	3	2	2	3	1	2	1	2	3	3
121	2	1	2	1	2	3	2	2	3	1	3	1	2	3	3
122	2	1	2	1	2	3	1	2	3	4	3	1	2	4	4
123	1	1	2	2	2	2	4	3	2	3	3	4	3	4	4
124	1	4	1	2	3	2	3	3	2	2	3	4	3	4	4
121	1	4	1	2	3	2	1	4	2	2	4	3	4	4	4
126	3	4	1	3	4	4	4	3	1	3	4	3	4	1	4
127	2	4	3	3	4	4	1	4	1	3	4	3	4	1	4
128	2	1	3	3	1	4	1	4	1	4	4	3	4	1	3
129	2	2	3	4	1	1	4	4	1	4	3	2	3	1	2
130	4	2	3	4	4	1	3	3	2	1	3	2	3	4	3
131	4	3	1	4	4	1	3	3	2	1	2	2	3	3	4
132	4	3	1	4	3	1	2	2	2	1	2	2	2	2	3
133	3	3	4	3	3	4	2	2	3	1	2	3	2	3	3
134	1	3	2	3	2	3	2	2	3	1	2	3	2	3	2
131	1	4	4	4	2	2	1	3	3	4	4	4	2	4	2
136	1	4	4	2	2	2	1	3	2	4	4	4	3	4	2
137	1	4	4	2	3	2	1	4	2	4	4	1	3	4	3

138	1	4	1	1	3	4	1	4	2	4	4	1	3	3	3
139	4	3	1	1	4	4	4	4	1	3	3	4	4	2	4
140	4	2	4	1	4	1	4	1	1	1	4	4	4	2	4
141	4	2	4	1	1	2	3	1	1	1	4	3	4	2	4
142	4	2	3	2	3	2	3	1	1	3	4	3	3	3	4
143	3	2	3	2	3	2	3	4	1	2	3	3	3	3	4
144	2	4	2	2	4	3	2	3	1	3	3	3	2	4	3
141	2	4	2	3	4	3	2	3	2	2	3	2	2	4	3
146	1	4	2	3	1	1	2	2	2	1	4	2	2	4	3
147	1	4	2	3	1	4	1	2	2	3	2	2	2	4	2
148	1	1	3	3	1	4	1	3	2	2	2	2	3	1	2
149	2	1	3	4	4	4	1	3	3	4	2	3	4	1	2
110	2	1	3	3	4	2	3	4	3	4	2	3	4	1	3
111	2	4	4	4	3	2	3	4	1	4	3	4	2	1	3
112	3	3	4	3	3	3	3	1	2	3	3	4	2	4	3
113	3	2	4	4	3	1	4	1	2	2	3	1	2	4	4
114	3	2	1	2	4	1	4	1	2	2	4	2	3	3	4
111	4	2	1	3	4	4	1	4	2	2	4	4	3	3	4
116	4	2	1	2	1	4	2	4	1	1	4	1	2	2	4
117	4	3	4	3	1	3	3	3	1	4	4	3	2	2	4
118	4	3	4	2	1	3	4	3	1	3	3	3	4	3	4
119	3	4	4	3	2	2	3	2	2	4	3	4	4	3	3
160	3	4	3	2	4	2	2	2	2	1	3	4	2	3	2
161	2	4	3	2	3	2	2	2	3	1	2	4	2	4	3
162	2	1	2	2	3	3	2	3	3	1	2	1	2	4	4
163	1	1	2	1	3	3	3	3	3	4	2	1	4	4	3
164	1	1	2	1	4	4	3	4	3	3	2	2	3	4	3
161	1	4	2	2	4	4	4	3	2	3	3	2	4	1	2

166	1	4	2	3	1	1	3	4	2	2	3	2	4	1	2
167	2	4	3	3	1	1	2	4	2	2	3	2	3	1	2
168	2	3	3	3	2	1	3	4	1	2	3	3	3	4	3
169	2	3	3	3	2	4	3	3	1	3	4	3	2	4	3
170	3	2	4	2	2	3	4	3	1	3	2	1	2	3	4
171	3	2	4	2	3	3	4	2	1	4	2	1	2	3	4
172	3	2	4	2	3	3	4	2	2	4	4	1	3	3	4
173	4	2	4	1	4	2	3	2	2	4	3	1	3	3	4
174	4	2	1	2	4	2	3	3	2	4	3	1	4	4	4
171	4	3	1	2	1	2	2	3	2	4	3	4	4	4	3
176	4	3	1	3	1	4	2	4	3	3	4	4	4	4	3
177	3	3	4	3	4	4	1	4	3	3	4	3	4	1	3
178	3	4	4	4	4	4	4	4	3	3	4	3	3	1	2
179	3	4	3	4	3	1	3	1	3	3	4	3	3	1	2
180	2	4	3	4	3	1	1	1	3	2	3	3	3	4	2
181	2	1	2	3	2	1	4	1	2	2	3	2	2	3	3
182	1	1	2	2	2	1	1	4	2	2	3	2	2	2	3
183	1	1	2	2	2	4	1	3	2	2	2	2	2	2	3
184	1	1	4	1	3	3	4	3	1	3	2	2	2	2	4
181	3	1	4	1	3	2	3	2	1	3	2	3	3	2	4
186	2	1	4	1	4	2	3	2	1	3	2	3	3	2	4
187	2	4	2	2	4	2	2	3	1	3	3	4	3	3	4
188	2	4	2	2	1	4	2	3	1	4	3	4	4	3	4
189	4	4	2	3	3	4	2	4	2	4	3	1	4	4	4
190	4	4	1	3	3	1	1	4	2	4	3	2	4	4	3
191	4	1	1	4	4	2	1	1	2	4	4	4	3	4	2
192	3	2	1	4	4	2	1	1	2	1	4	1	3	4	3
193	1	2	3	4	1	2	1	1	3	1	4	3	2	1	4

194	1	3	3	4	1	3	4	4	3	1	4	3	2	1	3
191	1	3	3	3	1	3	4	4	3	4	3	4	2	1	3
196	1	3	3	3	4	1	3	3	3	3	3	4	2	1	2
197	1	3	1	2	4	4	3	3	3	2	2	4	3	4	2
198	4	4	1	2	3	4	3	2	2	2	2	1	4	3	2
199	4	4	4	1	3	4	2	2	2	3	2	1	4	2	3
200	4	4	2	1	3	2	2	2	2	3	2	2	2	3	3
201	4	4	4	1	4	2	2	3	1	4	4	2	2	3	4
202	3	3	4	1	4	3	1	3	1	4	4	2	2	4	4
203	2	2	4	2	1	1	1	4	1	1	4	2	3	4	4
204	2	2	1	2	1	1	1	3	1	1	4	3	3	4	4
201	1	2	1	2	1	4	3	4	2	1	3	3	2	3	4
206	1	2	4	3	2	4	3	4	2	1	4	1	2	2	3
207	1	4	4	3	4	3	3	4	2	1	4	1	4	2	3
208	2	4	3	3	3	3	4	3	3	4	4	1	4	2	3
209	2	4	3	4	3	2	4	3	3	4	3	1	2	3	2
210	2	4	2	4	3	2	1	2	3	4	3	1	2	3	2
211	3	1	2	4	4	2	1	2	2	4	3	4	2	4	2
212	3	1	2	4	4	3	3	2	2	3	4	4	4	4	3
213	3	1	2	3	1	3	4	3	2	1	2	3	3	4	3
214	4	4	3	3	1	4	3	3	1	1	2	3	4	4	3
211	4	3	3	4	2	4	2	4	1	3	2	3	4	1	4
216	4	2	3	2	2	1	2	4	1	2	2	3	3	1	4
217	4	2	4	2	2	1	2	4	1	3	3	2	3	1	4
218	3	2	4	1	3	1	3	1	1	2	3	2	2	1	4
219	3	2	4	1	3	4	3	1	1	1	3	2	2	4	4
220	2	3	1	1	4	3	4	1	2	3	4	2	2	4	4
221	2	3	1	1	4	3	3	4	2	2	4	3	3	3	3

222	1	4	1	2	1	3	2	3	2	4	4	3	3	3	2
223	1	4	4	2	1	2	3	3	2	4	4	4	4	2	3
224	1	4	4	2	4	2	3	2	3	4	3	4	4	2	4
221	1	1	4	3	4	2	4	2	3	3	3	1	4	3	3
226	2	1	3	3	3	4	4	3	1	2	3	2	4	3	3
227	2	1	3	3	3	4	4	3	2	2	2	4	3	3	2
228	2	4	2	3	2	4	3	4	2	2	2	1	3	4	2
229	3	4	2	4	2	1	3	4	2	1	2	3	3	4	2
230	3	4	2	3	2	1	2	1	2	4	2	3	2	4	3
231	3	3	2	4	3	1	2	1	1	3	3	4	2	4	3
232	4	3	2	3	3	1	1	1	1	4	3	4	2	1	4
233	4	2	3	4	4	4	4	4	1	1	3	4	2	1	4
234	4	2	3	2	4	3	3	4	2	1	3	1	3	1	4
231	4	2	3	3	1	2	1	3	2	1	4	1	3	4	4
236	3	2	4	2	3	2	4	3	3	4	2	2	3	4	4
237	3	2	4	3	3	2	1	2	3	3	2	2	4	3	3
238	3	3	4	2	4	4	1	2	3	3	4	2	4	3	3
239	2	3	4	3	4	4	4	2	3	2	3	2	4	3	3
240	2	3	1	2	1	1	3	3	2	2	3	3	3	3	2
241	1	4	1	2	1	2	3	3	2	2	3	3	3	4	2
242	1	4	1	2	1	2	2	4	2	3	4	1	2	4	2
243	1	4	4	1	4	2	2	3	1	3	4	1	2	4	3
244	3	1	4	1	4	3	2	4	1	4	4	1	2	1	3
241	2	1	3	2	3	3	1	4	1	4	4	1	2	1	3
246	2	1	3	3	3	1	1	4	1	4	3	1	3	1	4
247	2	1	2	3	3	4	1	3	2	4	3	4	4	4	4
248	4	1	2	3	4	4	1	3	2	4	3	4	4	3	4
249	4	1	2	3	4	4	4	2	2	3	2	3	2	2	4

210	4	4	4	2	1	2	4	2	2	3	2	3	2	2	4
211	3	4	4	2	1	2	3	2	3	3	2	3	2	2	4
212	1	4	4	2	1	3	3	3	3	3	2	3	3	2	3
213	1	4	2	1	2	1	3	3	3	2	3	2	3	2	2
214	1	1	2	2	4	1	2	4	3	2	3	2	2	3	3
211	1	2	2	2	3	4	2	4	3	2	3	2	2	3	4
216	1	2	1	3	3	4	2	4	2	2	3	2	4	4	3
217	4	3	1	3	3	3	1	1	2	3	4	3	4	4	3
218	4	3	1	4	4	3	1	1	2	3	4	3	2	4	2
219	4	3	3	4	4	2	1	1	1	3	4	4	2	4	2
260	4	3	3	4	1	2	3	4	1	3	4	4	2	1	2
261	3	4	3	3	1	2	3	3	1	4	3	1	4	1	3
262	2	4	3	2	2	3	3	3	1	4	3	2	3	1	3
263	2	4	1	2	2	3	4	2	1	4	2	4	4	1	4
264	1	4	1	1	2	4	4	2	2	4	2	1	4	4	4
261	1	3	4	1	3	4	1	3	2	1	2	3	3	3	4
266	1	2	2	1	3	1	3	3	2	1	2	3	3	2	4
267	2	2	4	2	4	1	2	4	2	1	4	4	2	3	4
268	2	2	4	2	4	1	3	4	3	4	4	4	2	3	3
269	2	2	4	3	1	4	4	1	3	3	4	4	2	4	3
270	3	4	1	3	1	3	2	1	3	2	4	1	3	4	3
271	3	4	1	4	4	3	2	1	3	2	3	1	3	4	2
272	3	4	4	4	4	3	2	4	3	3	4	2	4	3	2
273	4	4	4	4	3	2	3	4	2	3	4	2	4	2	2
274	4	1	3	4	3	2	3	3	2	4	4	2	4	2	3
271	4	1	3	3	2	2	4	3	2	4	3	2	4	2	3
276	4	1	2	3	2	4	3	2	1	1	3	3	3	3	3
277	3	4	2	2	2	4	2	2	1	1	3	3	3	3	4

278	3	3	2	2	3	4	3	2	1	1	4	1	3	4	4
279	2	2	2	1	3	1	3	3	1	1	2	1	2	4	4
280	2	2	3	1	4	1	4	3	2	1	2	1	2	4	4
281	1	2	3	1	4	1	4	4	2	4	2	1	2	4	4
282	1	2	3	1	1	1	4	3	2	4	2	1	2	1	4
283	1	3	4	2	3	4	3	4	3	4	3	4	3	1	3
284	1	3	4	2	3	3	3	4	3	4	3	4	3	1	2
281	2	4	4	2	4	2	2	4	3	3	3	3	3	1	3
286	2	4	1	3	4	2	2	3	2	1	4	3	4	4	4
287	2	4	1	3	1	2	1	3	2	1	4	3	4	4	3
288	3	1	1	3	1	4	4	2	2	3	4	3	4	3	3
289	3	1	4	4	1	4	3	2	1	2	4	2	3	3	2
290	3	1	4	4	4	1	1	2	1	3	3	2	3	2	2
291	4	4	4	4	4	2	4	3	1	2	3	2	2	2	2
292	4	4	3	4	3	2	1	3	1	1	3	2	2	3	3
293	4	4	3	3	3	2	1	4	1	4	2	3	2	3	3
294	4	3	2	3	3	3	4	4	1	4	2	3	2	3	4
291	3	3	2	4	4	3	3	4	2	4	2	4	3	4	4
296	3	2	2	2	4	1	3	1	2	4	2	4	4	4	4
297	3	2	2	2	1	4	2	1	2	4	3	1	4	4	4
298	2	2	2	1	1	4	2	1	2	3	3	2	2	4	4
299	2	2	3	1	1	4	2	4	3	3	3	4	2	1	3
300	1	2	3	1	2	2	1	3	3	3	3	1	2	1	3
301	1	3	3	1	4	3	1	3	1	3	4	3	3	1	3
302	1	3	4	2	3	3	1	2	1	2	2	3	3	4	2
303	1	3	4	2	3	2	1	2	2	2	2	4	2	4	2
304	1	4	4	2	3	2	4	3	2	2	4	4	2	3	2
301	2	4	4	3	4	2	4	3	2	2	3	4	4	3	3

306	2	4	1	3	4	4	3	4	2	3	3	1	4	3	3
307	2	1	1	3	1	4	3	4	3	3	3	1	2	3	3
308	3	1	1	3	1	4	3	1	3	3	4	2	2	4	4
309	3	1	4	4	2	1	2	1	3	3	4	2	2	4	4
310	3	1	4	3	2	1	2	1	3	4	4	2	4	4	4
311	4	1	3	4	2	1	2	4	3	4	4	2	3	1	4
312	4	1	3	3	3	1	1	4	2	4	3	3	4	1	4
313	4	4	2	4	3	4	1	3	2	4	3	3	4	1	4
314	4	4	2	2	4	3	1	3	2	1	3	1	3	4	3
311	3	4	2	3	4	2	3	2	1	1	2	1	3	3	2
316	3	4	4	2	1	2	3	2	1	1	2	1	2	2	3
317	2	1	4	3	1	2	3	2	1	4	2	1	2	2	4
318	2	2	4	2	4	4	4	3	1	3	2	4	2	2	3
319	1	3	2	3	4	4	4	3	1	2	3	4	3	2	3
320	1	4	2	2	3	1	1	4	2	2	3	1	3	2	2
321	1	4	2	2	3	2	3	4	2	3	3	1	4	3	2
322	1	4	1	1	2	2	3	1	2	3	3	2	4	3	2
323	1	1	1	1	2	4	2	1	2	4	4	2	4	4	3
324	1	1	1	1	2	4	3	1	3	4	4	2	4	4	3
321	2	1	3	1	3	4	2	4	3	1	4	2	3	4	4
326	2	4	3	2	3	1	2	3	3	1	4	3	3	4	4
327	2	4	3	2	4	1	2	3	3	1	3	3	3	1	4
328	3	4	3	2	4	1	3	2	3	4	3	1	2	1	4
329	3	3	1	3	1	1	3	2	2	3	2	4	2	1	4
330	3	3	1	3	2	4	4	3	2	2	2	4	2	1	3
331	4	2	3	3	2	3	3	3	2	2	4	1	2	4	3
332	4	2	2	3	3	2	3	4	1	3	4	1	3	3	3
333	4	2	2	4	3	2	3	4	1	3	3	2	3	2	2

334	4	2	2	3	4	4	4	1	1	1	3	2	3	3	2
331	3	2	4	4	4	4	4	1	2	1	3	2	4	3	2
336	3	3	4	3	1	4	1	1	2	4	2	2	4	2	3
337	2	3	4	4	1	1	2	4	2	3	2	3	4	4	3
338	2	3	2	1	4	1	4	4	2	2	2	3	3	3	3