

ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN



“La Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa Kiaratel Comunicaciones S.A.C – Perú, 2022”

**Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:**

Maestro en
Gestión de Tecnologías de la Información

Autores:

Bach. Bruno Quispe, Eduardo Felix

Docente Guía:

Mg. Díaz Zelada, Yván Francisco

TACNA – PERÚ

2022

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

Agradecimientos

Agradezco a mi mamá que me dio la vida, cuidó mi bienestar, me enseñó el valor de la vida, y me enseñó a seguir luchando.

Dedicatoria

A Dios, por darle un sentido a mi existir y darme la oportunidad de haber concluido con este sueño anhelado.

A mi madre Sonia Quispe, por su labor desplegada y que siempre sus palabras fueron sabias.

Índice General

Agradecimientos	3
Dedicatoria	4
Índices de Tablas	9
Índice Gráfico	12
Resumen	15
Introducción	17
Capítulo I: Antecedentes del Estudio.....	19
1.1 Título del Tema.....	19
1.2 Planteamiento del Problema	19
1.3 Objetivos	20
1.3.1 <i>Objetivos General</i>	20
1.3.2 <i>Objetivos Específicos</i>	20
1.4 Justificación del Estudio	20
1.4.1 <i>Justificación teórica</i>	20
1.4.2 <i>Justificación práctica</i>	21
1.5 Metodología.....	21
1.5.1 <i>Tipo de Investigación</i>	21
1.5.2 <i>Diseño de la Investigación</i>	22
1.5.3 <i>Técnicas e Instrumento</i>	23
1.5.4 <i>Técnica</i>	23
1.5.5 <i>Instrumento</i>	23

1.5.6	<i>Población y Muestra</i>	24
1.5.7	<i>Tratamiento y Procesamiento de Información</i>	25
1.6	Definiciones	27
1.6.1	<i>Variable Independiente: La Ciberseguridad</i>	27
1.6.2	<i>Variable Dependiente: Gestión de Tecnologías de Información</i>	27
1.7	Alcances y Limitaciones	27
1.7.1	<i>Alcances</i>	27
1.7.2	<i>Limitaciones</i>	28
Capítulo II: Marco Teórico		29
2.1	Conceptualización de la(s) Variable(s) o Tópico(s) Clave	29
2.1.1	<i>La Ciberseguridad</i>	29
2.1.2	<i>Gestión de Tecnologías de Información</i>	38
2.2	Importancia de la(s) Variable(s) o Tópico(s) Clave	46
2.3	Modelos de la(s) Variable(s)	49
2.3.1	<i>Operacionalización de Variables</i>	52
2.4	Análisis Comparativo	54
2.5	Análisis Crítico	56
Capítulo III Marco Referencial		57
3.1	Reseña Histórica	57
3.2	Filosofía Organizacional	57
3.2.1	<i>Nuestros valores:</i>	57
3.2.2	<i>Misión:</i>	57

3.2.3	<i>Visión:</i>	57
3.2.4	<i>Objetivos:</i>	58
3.2.5	<i>Compromiso:</i>	58
3.2.6	<i>Posición de la Empresa:</i>	58
3.3	Diseño Organizacional	59
3.4	Productos y/o Servicios	60
3.4.1	<i>Productos</i>	60
3.4.2	<i>Servicios</i>	60
3.5	Diagnóstico Organizacional	64
Capítulo IV	Resultados	68
4.1	Marco Metodológico	68
4.2	Resultados	69
4.2.1	<i>Confiabilidad del Instrumento por Alfa de Cronbach</i>	69
4.2.2	<i>Aplicación de la Estadística Inferencial de las Variables</i>	70
4.2.3	<i>Aplicación de la Estadística Descriptiva de las Variables</i>	75
Capítulo V	Sugerencias	100
5.1	Recomendaciones	100
5.2	Conclusiones	101
5.3	Bibliografía	102
Anexos	108
Anexo 01:	Matriz de Consistencia	109
Anexo 02:	Matriz de Operacionalización de Variables	110

Anexo 03: Instrumento	111
Anexo 04: Validación de Instrumento	115
Anexo 05: Matriz de Datos	118

Índices de Tablas

Tabla 1: Clasificación de la variable independiente	49
Tabla 2: Clasificación de la variable dependiente	50
Tabla 3: Matriz de Dafo.....	67
Tabla 4: Estadísticos de fiabilidad de la variable independiente: la ciberseguridad .	69
Tabla 5: Estadísticos de fiabilidad de la variable dependiente: gestión de tecnologías de información	69
Tabla 6: Pruebas de normalización.....	70
Tabla 7: Correlaciones de hipótesis general	71
Tabla 8: Correlaciones de hipótesis específica 01	72
Tabla 9: Correlaciones de hipótesis específica 02.....	73
Tabla 10: Correlaciones de hipótesis específica 03.....	74
Tabla 11: Correlaciones de hipótesis específica 04.....	75
Tabla 12: Cuadro de frecuencia de la pregunta ¿Cree que el centro de TI de su empresa tiene programas para aumentar la concienciación sobre las amenazas a la ciberseguridad?	75
Tabla 13: Cuadro de frecuencia de la pregunta ¿Está de acuerdo con la aplicación de un sistema de inventarios?.....	76
Tabla 14: Cuadro de frecuencia de la pregunta ¿Cree que el centro de TI de su empresa mantiene suficientes copias de seguridad de los datos de su empresa? ..	77
Tabla 15: Cuadro de frecuencia de la pregunta ¿Cree que el centro de tecnología de la información de su empresa ha instalado suficiente software para proteger la información de su organización de las actividades ilegales de los ciberdelincuentes?	78

Tabla 16: Cuadro de frecuencia de la pregunta ¿Cree que el entorno de TI de la empresa incluye medidas de seguridad física que evitan las actividades ilegales de los ciberdelincuentes?	79
Tabla 17: Cuadro de frecuencia de la pregunta ¿Cree que el entorno de TI de su empresa cuenta con programas de seguridad para protegerse contra los ciberdelincuentes?.....	80
Tabla 18: Cuadro de frecuencia de la pregunta ¿Sabe qué hacer cuando ve actividad delictiva cibernética en uno de los dispositivos de su líder empresarial?	81
Tabla 19: Cuadro de frecuencia de la pregunta ¿Cree usted que el área de TI de la empresa cuenta con personal calificado en ciberseguridad?	82
Tabla 20: Cuadro de frecuencia de la pregunta ¿Cree usted que los sistemas de seguridad existentes por el área de TI de la empresa utilizan aplicación web que neutralizan los ataques de los ciberdelincuentes?	83
Tabla 21: Cuadro de frecuencia de la pregunta ¿Alguna vez ha tenido que detener sus actividades debido a un ataque informático que no fue detectado y bloqueado por los sistemas de seguridad?	84
Tabla 22: Cuadro de frecuencia de la pregunta ¿Crees que se perdieron datos importantes debido a un virus informático el año pasado?.....	85
Tabla 23: Cuadro de frecuencia de la pregunta ¿El centro de TI de su empresa lo ha capacitado en técnicas comunes utilizadas por los ciberdelincuentes?	86
Tabla 24: Cuadro de frecuencia de la pregunta ¿Cree que el departamento de tecnología de la información de la empresa tiene tiempo para capacitar a los empleados de la empresa en las prácticas de TI?	88
Tabla 25: Cuadro de frecuencia de la pregunta ¿Está de acuerdo con la creación de tablas de almacenamiento del sistema?.....	89

Tabla 26: Cuadro de frecuencia de la pregunta ¿Considera usted que el área de TI de la empresa cumple una atención de incidencias de TI?	90
Tabla 27: Cuadro de frecuencia de la pregunta ¿Cree usted que el área de TI de la empresa realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?.....	91
Tabla 28: Cuadro de frecuencia de la pregunta ¿Qué tanto está de acuerdo con el lenguaje de C# para la aplicación en el sistema?.....	92
Tabla 29: Cuadro de frecuencia de la pregunta ¿Qué tan conforme está usted con la seguridad del internet que cuenta la empresa?.....	93
Tabla 30: Cuadro de frecuencia de la pregunta ¿Ha recibido capacitación de parte del área de TI de la empresa respecto al uso adecuado de las tecnologías de la empresa?	94
Tabla 31: Cuadro de frecuencia de la pregunta ¿Considera que el acceso a la información de los sistemas de información es oportuno y seguro?	95
Tabla 32: Cuadro de frecuencia de la pregunta ¿Crees que la dirección de la oficina de TI es correcta?.....	96
Tabla 33: Cuadro de frecuencia de la pregunta ¿Cree usted que el área de TI de la empresa ayuda con las metas trazadas para el área de ventas de la empresa?	97
Tabla 34: Cuadro de frecuencia de la pregunta ¿Cree que el entorno de TI de la empresa cumple con los requisitos tecnológicos de su sección?.....	98
Tabla 35: Cuadro de frecuencia de la pregunta ¿Está satisfecho con el nivel establecido por los profesionales del equipo de TI?.....	99

Índice Gráfico

Gráfico 1: Estructura de la entidad KIARATEL S.A.C	59
Gráfico 2: Gráfico circular de la pregunta ¿Cree que el centro de TI de su empresa tiene programas para aumentar la concienciación sobre las amenazas a la ciberseguridad?	76
Gráfico 3: Gráfico circular de la pregunta ¿Está de acuerdo con la aplicación de un sistema de inventarios?	77
Gráfico 4: Gráfico circular de la pregunta ¿Cree que el centro de TI de su empresa mantiene suficientes copias de seguridad de los datos de su empresa?	78
Gráfico 5: Gráfico circular de la pregunta ¿Cree que el centro de tecnología de la información de su empresa ha instalado suficiente software para proteger la información de su organización de las actividades ilegales de los ciberdelincuentes?	79
Gráfico 6: Gráfico circular de la pregunta ¿Cree que el entorno de TI de la empresa incluye medidas de seguridad física que evitan las actividades ilegales de los ciberdelincuentes?	80
Gráfico 7: Gráfico circular de la pregunta ¿Cree que el entorno de TI de su empresa cuenta con programas de seguridad para protegerse contra los ciberdelincuentes?	81
Gráfico 8: Gráfico circular de la pregunta ¿Sabe qué hacer cuando ve actividad delictiva cibernética en uno de los dispositivos de su líder empresarial?	82
Gráfico 9: Gráfico circular de la pregunta ¿Cree usted que el área de TI de la empresa cuenta con personal calificado en ciberseguridad?	83
Gráfico 10: Gráfico circular de la pregunta ¿Cree usted que los sistemas de seguridad existentes por el área de TI de la empresa utilizan aplicación web que neutralizan los ataques de los ciberdelincuentes?	84

Gráfico 11: Gráfico circular de la pregunta ¿Alguna vez ha tenido que detener sus actividades debido a un ataque informático que no fue detectado y bloqueado por los sistemas de seguridad?.....	85
Gráfico 12: Gráfico circular de la pregunta ¿Crees que se perdieron datos importantes debido a un virus informático el año pasado?	86
Gráfico 13: Gráfico circular de la pregunta ¿El centro de TI de su empresa lo ha capacitado en técnicas comunes utilizadas por los ciberdelincuentes?	87
Gráfico 14: Gráfico circular de la pregunta ¿Cree que el departamento de tecnología de la información de la empresa tiene tiempo para capacitar a los empleados de la empresa en las prácticas de TI?.....	88
Gráfico 15: Gráfico circular de la pregunta ¿Está de acuerdo con la creación de tablas de almacenamiento del sistema?	89
Gráfico 16: Gráfico circular de la pregunta ¿Considera usted que el área de TI de la empresa cumple una atención de incidencias de TI?.....	90
Gráfico 17: Gráfico circular de la pregunta ¿Cree usted que el área de TI de la empresa realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?.....	91
Gráfico 18: Gráfico circular de la pregunta ¿Qué tanto está de acuerdo con el lenguaje de C# para la aplicación en el sistema?	92
Gráfico 19: Gráfico circular de la pregunta ¿Qué tan conforme está usted con la seguridad del internet que cuenta la empresa?.....	93
Gráfico 20: Gráfico circular de la pregunta ¿Ha recibido capacitación de parte del área de TI de la empresa respecto al uso adecuado de las tecnologías de la empresa?	94
Gráfico 21: Gráfico circular de la pregunta ¿Considera que el acceso a la información de los sistemas de información es oportuno y seguro?.....	95

Gráfico 22: Gráfico circular de la pregunta ¿Crees que la dirección de la oficina de TI es correcta?..... 96

Gráfico 23: Gráfico circular de la pregunta ¿Cree que usted que el área de TI de la empresa ayuda con las metas trazadas para el área de ventas de la empresa? 97

Gráfico 24: Gráfico circular de la pregunta ¿Cree que el entorno de TI de la empresa cumple con los requisitos tecnológicos de su sección?..... 98

Gráfico 25: Gráfico circular de la pregunta ¿Está satisfecho con el nivel establecido por los profesionales del equipo de TI? 99

Resumen

Trabajo de investigación actual, su relación con la ciberseguridad y la gestión de tic en la entidad Kiaratel comunicaciones s.a.c – Perú, 2022. Cabe señalar que el desarrollo de esta investigación se origina a causa del mal manejo de la información y pérdida de la data de los clientes en las diversas áreas de la empresa, dado que se producen pérdidas de información, estancamiento económico y robo de información. A través de la relación entre la ciberseguridad y la TIC en la entidad KIARATEL SAC, SJL, 2022.

Este sistema de información ayudará a mejorar las prácticas de seguridad y mantener la lealtad de los clientes. Al definir el cuestionario se consideró la ciberseguridad como variable independiente y la TIC como factor dependiente.

El método utilizado en la investigación es cualitativo y descriptivo con un diseño no experimental y transversal. Se tomó una muestra de 40 personas mediante muestreo probabilístico con una población de 100 personas. Los métodos y herramientas de recopilación de datos son encuestas y encuestas, se hicieron 12 preguntas sobre resiliencia de seguridad cibernética y 12 preguntas sobre diversidad de gestión de información.

En la estadística para el análisis de datos se empleó la herramienta informática SPSS vers.23, quien se encarga de todo el procesamiento de la información mediante la codificación, tabulación, consultas, formulación de hipótesis y estas se muestran dinámicamente en tablas y gráficos para ser comprendidos de manera clara y precisa.

Finalmente, se ve que existe una fuerte relación entre la ciberseguridad y la gestión de tecnologías de la información con un 82,5% de confianza. En KIARATEL SAC, SJL, 2022, se puede concluir que la ciberseguridad y la gestión tecnológica están íntimamente relacionadas.

Palabras clave: seguridad cibernética, gestión de TIC.

Introducción

En la época en que vivimos el desarrollo de las gestiones de tecnologías de la información (TIC) se ha convertido en un factor fundamental para la seguridad en la red de las grandes empresas a nivel mundial, las TIC vienen a ser muy importantes dentro del desarrollo de funciones de la seguridad de los datos de la empresa en la red ya que contribuye en la mejora de los diferentes procesos de gestión en cada área de una organización.

La ciberseguridad en la red busca mejorar la seguridad de los datos que tiene la empresa con la finalidad de encontrar una adecuada eficiencia, en consecuencia, podemos decir que la implementación de las tecnologías de la información busca mejorar la ciberseguridad de la empresa, es una estrategia clave para el crecimiento organizacional y jerárquico institucional en el campo laboral y comercial.

El presente trabajo de investigación denominado “LA CIBERSEGURIDAD Y SU RELACIÓN EN LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA KIARATEL COMUNICACIONES S.A.C – PERÚ, 2022” este trabajo consta de una estructura por capítulos que contienen información relevante que describen y detallan toda investigación.

Capítulo I: “La dificultad y Metodología” es aquí donde explicaremos sobre la presente los problemas de demanda en la empresa y sus causas KIARATEL S.A.C, siendo esto la base de nuestra investigación, así mismo también realizamos un previo análisis sobre la y propuesta de solución tecnológica y justificación con los objetivos planteados para una óptima y adecuada solución según los lineamientos de la empresa. Se indica también un tratamiento de datos siguiendo métodos y técnicas

científicas describiendo el nivel de la investigación del proyecto, también se señala la población y muestra, del mismo modo describimos las técnicas e instrumentos para la recolección de datos para luego realizar el análisis que puedan probar y determinar el resultado de las hipótesis.

Capítulo II: "Fundamentos teóricos" incluye los fundamentos teóricos de la investigación anteriores al proyecto, estos vienen a ser los antecedentes y las bases teóricas que respaldan la investigación, donde encontraremos posturas epistemológicas, información relevante que demuestran mediante modelos de procesos, análisis, hipótesis y experimentos que determinan los resultados óptimos en el ámbito organizacional.

Capítulo III: "marco de referencia" es un documento que describe y define los antecedentes, la teoría, las reglas y/o las directrices de un proyecto, plan de acción o proceso de investigación.

Capítulo IV: "Resultados" demostraremos en tablas los resultados estadísticos de las hipótesis de la investigación con cuadros e imágenes estadísticos que definen el resultado de las preguntas de se analizan diversas tecnologías de ciberseguridad y gestión de la información, cuestionario a los trabajadores de la empresa KIARATEL S.A.C.

Capítulo V: "Conclusiones y Recomendaciones" en estos últimos describiremos de manera clara y precisa sobre la discusión que genera la investigación siguiendo los patrones referentes al tema, Del mismo modo que enfoque de la gestión de la seguridad cibernética y la tecnología de la información en la empresa Kiaratel comunicaciones s.a.c – Perú, 2022, por lo tanto, se señalará que el uso e implementación será óptimo para la organización.

Capítulo I: Antecedentes del Estudio

1.1 Título del Tema

“La Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa Kiaratel Comunicaciones S.A.C – Perú, 2022”

1.2 Planteamiento del Problema

Actualmente Perú y el globo mundial muchas entidades buscan tener un buen diseño de TIC en sus empresas, con el objetivo de poder tener un mejor sistema de ciberseguridad en la red y en las áreas de tecnología de la empresa y así evitar pérdidas de información valiosas para la empresa que puedan generar grandes problemas económicos en un futuro.

En Sudamérica, Ecuador. Según los autores (Vargas, Recalde, & Reyes, 2017) Nos señalan: “La ciberseguridad y la ciberseguridad se han convertido en importantes áreas de investigación científica. De hecho, su investigación se convierte en un trabajo activo-político de defensa del país. En Ecuador, estos problemas se están resolviendo efectivamente. Tras analizar el concepto de seguridad y defensa en el ciberespacio, se recomienda desarrollar un modelo de control local en el ámbito de la ciberdefensa tal y como se recoge en las presentes directrices”.

En el Perú. Según el autor (Zevallos, 2019) Nos describen: “Las organizaciones públicas y privadas experimentan eventos dinámicos con la aparición y el deterioro de las nuevas tecnologías de la información a medida que aumenta el uso de la información”.

En la actualidad la empresa KIARATEL S.A.C, viene atravesando un problema interno, este problema es debido a los escasos de buen diseño de administración tecnológica de la información y debido a esto está ocasionando muchas pérdidas e

información de datos y ataques en la ciberseguridad de la empresa ya que no existen un buen diseño de gestión tecnológica que nos ayude a prevenir y detectar los ataques en la red. Debido a esto la empresa se ve en la urgencia de diseñar un sistema de administración de tecnológica de la información para que de esa manera poder controlar mejor los ataques en la red de la empresa y evitar las pérdidas de datos e información de dicha empresa.

1.3 Objetivos

1.3.1 *Objetivos General*

Determinar la relación entre la ciberseguridad y la gestión de tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.

1.3.2 *Objetivos Específicos*

- Determinar la relación entre la eficiencia de la ciberseguridad y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.
- Determinar la relación entre el mecanismo preventivo, correctivo y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.
- Determinar la relación entre el machine learning y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.
- Determinar la relación entre la prevención de los ciberdelitos y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.

1.4 Justificación del Estudio

1.4.1 *Justificación teórica*

Debido a las diferentes problemáticas que atraviesa la empresa KIARATEL S.A.C, nos vemos en la necesidad de hacer una investigación al área de TI, teniendo como propósito el diseñar un mejor sistema de tic que ayude a evitar pérdidas de datos y ataques en la red de la empresa.

Los efectos de la investigación y la implementación del sistema de tic se podrán utilizar como un aporte a la investigación descriptiva, conocimiento científico y tecnológico, demostrando así, la importancia y utilidad del sistema en el desarrollo organizacional ya que permitirá mejorar los procesos de gestión en la red y evitar pérdidas de datos.

1.4.2 Justificación práctica

Este trabajo se ha realizado para crear un sistema de gestión de tecnología de la información que nos ayudará a gestionar los ataques de seguridad cibernética a través de la implementación del sistema de la empresa KIARATEL S.A.C.

La utilización del sistema, permitirá que el área de TI pueda detectar los ataques a la red de la empresa a tiempo y evitar robos de información por partes de terceras personas, por ende, esto llevará a que la empresa siga mejorando económicamente.

Este sistema en la medida de su utilidad y aplicación en el área de TI de la empresa KIARATEL S.A.C, contribuirá con información importante sobre técnicas y prácticas sobre la función del sistema para la toma de decisiones en la organización. Además, será un aporte como ejemplo para otras empresas que no han podido establecer un sistema de tic dentro su planteamiento estratégico de trabajo.

1.5 Metodología

1.5.1 Tipo de Investigación

El tipo de investigación que propone nuestro estudio es correlacional y descriptiva, debido a que se determinó el nivel entre estos factores midiendo y se determinó la relación entre estos dos factores, se calculó la variable relacionada y se analizó la relación actual.

1.5.1.1 Investigación Descriptiva. Según (Díaz & Calzadilla, 2016) nos dice: “La investigación descriptiva es útil cuando es necesario describir los resultados reales obtenidos como resultado de un estudio observacional. Esta explicación se puede hacer usando métodos cualitativos y más descriptivamente usando métodos cuantitativos. En segundo lugar, tiene una función importante para medir características, propiedades, dimensiones o componentes que se encuentran en el análisis de evaluación; Por lo tanto, mientras que la investigación exploratoria se trata de observar, la investigación descriptiva se trata, en última instancia, de medir tanto como sea posible”.

1.5.1.2 Investigación Correlacional. Según (Hernández, 2014) nos dice: “La investigación correlacional es un tipo de método de investigación no experimental en el que el investigador mide dos variables. Comprende y analiza las relaciones numéricas entre ellos sin la influencia de ningún factor externo”.

Dicho objetivo de estudio es debido a que falta un buen diseño de gestión tecnológica de la información y debido a esto está ocasionando muchas pérdidas e información de datos es por ello se recurre a ejecutar un nuevo diseño de relación entre la ciberseguridad y la gestión del tic en la empresa Kiaratel Comunicaciones S.A.C – Perú, 2022.

El diseño de la investigación para esta investigación será no experimental, corte transversal.

1.5.2 Diseño de la Investigación

El diseño de investigación presentado en nuestro estudio es de tipo no experimental, debido a que no se utilizó la variable ni se le aplicó un estímulo, se observó únicamente en su forma. Y paso a paso, los datos se recopilan simultáneamente para cada observación. (Hernández, Fernández, & Baptista, 2010)

“En la investigación no experimental los fenómenos ocurren de manera independiente y no pueden ser manipulados, no hay un control directo sobre lo que se dice o lo que puede afectarlos” (p.149).

1.5.3 Técnicas e Instrumento

Es importante y necesario tener una comprensión clara de las técnicas y herramientas utilizadas en la investigación. De esta forma demostramos que los métodos que utilizamos para mejorar nuestra formación son las encuestas y sondeos. Se utiliza una encuesta a personas con preguntas cerradas para recolectar información de campo.

1.5.4 Técnica

1.5.4.1 Encuesta. (Niño, 2011) Nos argumenta: “Entendemos y analizamos procesos que permiten la recopilación de datos proporcionados por la mayoría de la población o su selección, para identificar, entre otras cosas, sus puntos de vista, valores, opiniones, actitudes, intereses o actividades. Uso de investigaciones diseñadas para este propósito” (p.63).

La técnica se aplicará a todos los empleados de todas las zonas de la entidad KIARATEL S.A.C, durante el periodo de enero del 2021 hasta enero del 2022, Esto se mide mediante una pregunta de prueba definida en una escala de Likert.

1.5.5 Instrumento

Se utilizó las siguiente Instrumento:

1.5.5.1 Cuestionario. (Hernández, 2014) Nos argumenta: “Las encuestas se utilizan principalmente para recopilar datos; Consiste en una serie de preguntas sobre uno o más ítems medidos. Además, se utilizó una escala tipo Likert para medir la actitud del material educativo. Esta escala está formada por una serie de ítems expresados en forma de enunciados o frases solicitados por los sujetos que les han

sido asignados. Con solo 5 puntos de respuesta, estos son: muy en desacuerdo, en desacuerdo, neutral, de acuerdo, muy de acuerdo; Hacer preguntas es una buena manera. Además, "Totalmente Satisfecho" es el nivel más alto en la escala, es decir, si el empleado logra obtener los puntos especificados, lo está haciendo bien o lo está haciendo bien al responder la pregunta dada".

Este instrumento de obtención de datos o información emplean métodos y técnicas muy diferentes pero favorables para el investigador, la idea es recolectar datos de interés común entre los participantes de ambas variables de estudio para luego entrar a un proceso de análisis estadístico utilizando el programa SPSS V23.

1.5.6 Población y Muestra

1.5.6.1 Población. Esta investigación se realiza teniendo como población a los 100 empleados de todas las zonas de la entidad KIARATEL S.A.C. en el distrito de SJL.

1.5.6.2 Muestra. Si hay una población a estudiar, pero no es adecuada para el estudio debido a su tamaño o tamaño, se debe muestrear a toda la población. Por tal motivo se tomó una muestra de 40 empleados. Todas las sucursales de Kiaratel S.A.C en la provincia de San Juan de Lurigancho. La muestra se calculó estadísticamente, eligiendo una muestra de 40, con un nivel de confianza o significancia del 95% y un margen de error del 5%.

La fórmula para calcular la población.

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Dónde:

n = el tamaño de la muestra 40.

N = tamaño de la población 100.

σ = Desviación estándar de la población 0,5.

Z = Valor obtenido mediante niveles de confianza 95% que confianza equivale a 1,96

e = Límite aceptable de error 5% (0,1).

1.5.6.3 Unidad de Análisis. Un trabajador de todas las áreas de la empresa KIARATEL S.A.C

1.5.7 Tratamiento y Procesamiento de Información

El proceso de recopilación de datos es el proceso que recopila datos e información desde el principio hasta el final de la investigación y, en general, también recopila datos de acuerdo con las pautas de investigación requeridas por la investigación, edición y presentación.

1.5.7.1 Plan de recolección y procesamiento de datos.

- Desarrollar herramientas de recopilación de datos (cuestionario).
- Análisis del documento (cuestionario) antes de presentarlo a los encuestados.
- Los instrumentos serán analizados y aprobados por 2 expertos en el tema.
- Presentación de la encuesta para la recolección de datos mediante cuestionarios en la empresa KIARATEL S.A.C.
- El trabajo de campo se realizó con la normalidad del caso, logrando con éxito lo planificado.

- Finalmente, una vez recolectada la información se procederá a llevar los datos para el procesamiento y analizarlos mediante el programa informático SPSS v23.

1.5.7.2 Proceso de validación del instrumento y su fiabilidad. Todos los datos e información recolectados serán llevados a un proceso de análisis que serán tratados para responder preguntas del problema, para finalmente ser mostrados mediante su presentación con la finalidad que estos ayuden a interpretar y encontrar soluciones al problema, estos pueden ser demostrados mediante técnicas estadísticas o descritas según sea el caso.

1.5.7.3 La validación de Instrumentos. El alfa de Cronbach se usa para medir el nivel de confiabilidad de las escalas de coeficientes o preguntas, y se usa una prueba estandarizada para determinar qué prueba se usa si la prueba Kolmogorov-Smirnov o la prueba de Shapiro- Wilk, estos resultados serán mostrados en la presentación de la tesis donde contará con la validación por expertos metodológicos.

1.5.7.4 Confiabilidad o fiabilidad. Hay diferentes formas de calcular la fiabilidad de una escala. Ambos utilizan métodos y fórmulas que generan índices de confianza. La puntuación va de cero a uno; donde cero representa desconfianza y uno representa alta confianza.

Entonces sabiendo esto procederemos a la aplicación del método de alfa de Cronbach en las variables de estudio de la siguiente manera:

- ✓ Confiabilidad de la herramienta con el estadístico de confiabilidad Alpha de Cronbach para la variable independiente de gestión de tecnologías de la información.
- ✓ Confiabilidad de la herramienta con el estadístico de confiabilidad Alfa de Cronbach para la variable relacionada con la seguridad cibernética.

1.6 Definiciones

En esta sección, los personajes seleccionados para el estudio se describen en acción.

1.6.1 Variable Independiente: La Ciberseguridad

Este es el resultado de la ciberseguridad en la empresa KIARATEL SAC, SJL, 2022. La evaluación de este cambio se evaluó con un cuestionario de 12 puntos con una escala Likert de 1 a 5. Se dividen en cuatro grupos; dimensión el ciclo de vida de la ciberseguridad; la dimensión seguridad informática; la dimensión ciberseguridad y ciencia de datos y la dimensión prevención y sanción de los ciberdelitos.

1.6.2 Variable Dependiente: Gestión de Tecnologías de Información

Este es el resultado del cuestionario de gestión de TI de Kiaratel SAC, SJL de 2022. La evaluación de este cambio se realizó con cuestionarios de doce puntos calificados en una escala Likert de 1 a 5. Se dividen en cuatro grupos en cuanto a los síntomas; dimensión TIC y la comunicación; la dimensión aspectos fundamentales de los SI; la dimensión sistema de inteligencia tecnológica y la dimensión sistemas de información administrativos.

1.7 Alcances y Limitaciones

El estudio se realizó midiendo la relación de la empresa de comunicaciones Kiaratel SAC - Perú con la gestión de ciberseguridad y TIC en el 2022.

1.7.1 Alcances

- Las empresas deberían dar una capacitación a su personal del área de TI de la empresa del ataque de la ciberseguridad y cómo prevenirlos.
- Realizar esta investigación significa tener el conocimiento para reconocer las diferentes condiciones del entorno de TI en diferentes campos de la empresa KIARATEL SAC, ubicada en LIMA.

1.7.2 Limitaciones

- El tiempo del que dispone un tesista es limitado debido a los patrones de trabajo actuales que provocan retrasos en el avance del proyecto de investigación.
- Falta de personal para inspeccionar.
- Folleto sobre riesgos de ciberseguridad y su impacto en la prevención del fraude en empresas móviles.

Capítulo II: Marco Teórico

2.1 Conceptualización de la(s) Variable(s) o Tópico(s) Clave

2.1.1 La Ciberseguridad

Según (Caamaño & Gil, 2020) nos define que “En este mundo global donde las instituciones, los países y las sociedades están bajo la amenaza de ciberataques, las vulnerabilidades económicas, políticas y sociales afectan gravemente no solo las elecciones, sino también la estabilidad administrativa y económica para generar confianza entre los grupos de interés”.

Concluyó que la ciberseguridad es la práctica de proteger sistemas, redes y aplicaciones de ataques digitales. Por lo general, estos ciberataques están diseñados para acceder, modificar o destruir datos confidenciales; defraudar al usuario o usuarios o interrumpir la continuidad del negocio. La implementación actual de las medidas de seguridad digital depende de que haya más dispositivos conectados que humanos y que los atacantes sean más efectivos.

2.1.1.1 El Ciclo de Vida de la Ciberseguridad. Según (Sáinz, 2016) nos dice “Es importante que los sistemas de ciberseguridad estén integrados con datos que proporcionen este aprendizaje e información de diferente naturaleza. Por lo tanto, como en otros campos, el intercambio de datos y la construcción de modelos de código abierto se convierten en un factor importante para resolver el problema” (pág. 21).

Concluyó que la ciberseguridad es la protección de la información digital en los sistemas conectados. La ciberseguridad se considera parte de la seguridad de la información y se define como la gestión de los riesgos que afectan el mantenimiento, almacenamiento y transmisión de los sistemas de información y la protección de los

activos de información. La ciberseguridad también se centra en la información digital y los sistemas asociados que la crean, almacenan o transmiten, por lo que está estrechamente relacionada con la seguridad informática.

a) Prevención. Según (Sáinz, 2016) nos dice “En el marco del enfoque global mencionado anteriormente, el consumidor y la empresa deben abordar la protección desde diferentes ángulos. Por otro lado, es valioso que los humanos sean entendidos de las amenazas cambiantes, el posible fraude y las contramedidas disponibles” (pág. 22).

Se observó que la prevención es aún más importante tomar medidas para evitar que los incidentes sucedan con mayor frecuencia. Lo más importante es el control de acceso, la seguridad, el firewall, la protección y el uso de antivirus potentes.

b) Detección. Según (Sáinz, 2016) nos dice: “Desafortunadamente, si se ha producido un ataque y las computadoras o los sistemas están infectados, es importante tomar precauciones de varias maneras. Por otro lado, ofrezca una solución profesional y si se produce un robo de identidad, póngase en contacto con las fuerzas gubernamentales y militares y emprenda acciones legales para detener los delitos cometidos” (pág. 22).

Concluyó que la visión será una solución útil para evitar que vuelva a suceder. Las principales medidas en esta parte de la investigación son tecnológicas, ya que es importante monitorear los sistemas para detectar cualquier intento sospechoso, pero también podemos encontrar medidas legales e institucionales.

c) Respuesta. Según (Sáinz, 2016) nos dice: “Restaurar sistema es un servicio que permite al usuario restaurar el estado de su computadora y aplicaciones al estado en el que se encontraban antes de que ocurriera el problema, solucionando así el problema” (pág. 32).

Se concluyó que la respuesta radica en cómo responde la organización a las amenazas de TI, como los ataques cibernéticos, las brechas de seguridad y las interrupciones del servidor.

d) Eficiencia a las Medidas de Ciberseguridad. Según (ROMERO, 2018) nos señala “Incluye redes de comunicación de tecnología de la información y otros sistemas tecnológicos, incluidos Internet, redes telefónicas, sistemas de control industrial y procesadores y controladores integrados accesibles de forma remota”.

Se concluye que una buena seguridad tiene como fundamento interactuar al máximo las funciones del sistema y de quienes lo poseen. El trabajo de mantenimiento efectivo tiene como objetivo lograr el objetivo para el cual se diseñó el sistema o la medida.

2.1.1.2 Seguridad Informática. Según (Rocha, 2011) nos dice “El propósito de la seguridad de la investigación es proteger la investigación almacenada donde sea que esté: en papel, en discos de computadora o en la memoria de quienes la conocen”.

Se concluye que mientras que seguridad de la Información describe los métodos y medidas utilizados para proteger los archivos de información en diferentes tipos y países; Seguridad Informática le informará de las formas y medios para proteger la confidencialidad, acceso e integridad de la información. También describe la actividad de prevención de ataques maliciosos contra ordenadores, etc.

a) Los Virus Informáticos. Según (Correa, Carlos, & Velarde, 2006) nos define “El virus no vino de la nada. Como se trata de software, un programador debe ser alguien que tenga un conocimiento amplio y relevante de los problemas relacionados con el hardware y, especialmente, el lenguaje de programación, este último puede ser

un lenguaje de bajo nivel como el lenguaje ensamblador o el lenguaje de programación”.

Se concluyó que un virus informático es una pieza de software que altera el funcionamiento normal de cualquier dispositivo informático sin el consentimiento o el conocimiento del usuario y tiene un efecto particularmente adverso en el dispositivo.

b) Mecanismos Preventivos. Según (romero, 2018) nos dice “Las medidas preventivas incluyen una serie de inspecciones periódicas, reemplazo o actualizaciones de hardware, software o varias partes donde los sistemas y procedimientos pueden probarse de acuerdo con los procedimientos de la empresa”.

Se concluyó que Las aplicaciones de defensa son aplicaciones que tienen como objetivo prevenir ataques informáticos. En particular, realizan un seguimiento de la información y los equipos, registran los eventos que ocurren en la organización y controlan todo, desde quienes tienen acceso a ellos.

c) Mecanismos Correctivos. Según (Romero, y otros, 2018) nos dice “es donde el reloj es reducido, entonces en estos casos el tiempo es importante, pero también es limitado. Una entidad o un cliente puede conseguir el efectivo, pero el horario es imposible”.

Se concluyó que la metodología de reparación debe reparar cualquier daño o daño causado por un ataque cuando el sistema es reparado y devuelto a su estado original. Cabe señalar que esto solo funciona después de recibir daño.

d) Mecanismos Detectivos. Según (ROMERO, 2018) nos define “Las técnicas expuestas se basan en la idea de que un atacante puede comprometer la seguridad y manipular algo o crear una falla”.

Se concluye que los métodos de detección se llevan a cabo antes del evento y su tarea es detectar la presencia de personas no autorizadas en una parte del sistema.

Son conocidos por enviar notificaciones y registrar eventos. Después de que el evento ha sucedido y su trabajo es arreglar los resultados.

e) *Encriptación en Seguridad Informática.* Según (Solís, Pinto, & Solís, 2017) nos dice “El uso de protocolos de seguridad y métodos de cifrado depende del éxito del método matemático por el cual se crean, cifrando y descifrando la información, y como resultado, la seguridad de la información está en constante evolución para garantizar la confidencialidad, alcance y verdad”.

Se concluye que, en seguridad informática, el cifrado es la conversión de datos de un formato legible a un formato cifrado. Los datos cifrados solo se pueden leer o modificar después de haberlos escrito. El cifrado es la base de la seguridad de los datos. Esta es la forma más fácil e importante de garantizar que la información de la computadora no sea robada o leída por alguien que quiera hacer un mal uso de ella.

2.1.1.3 *Ciberseguridad y Ciencia de Datos.* Según (Camilo, García, Osorio, & Navarro, 2018) nos define “La seguridad informática o ciberseguridad no es un problema nuevo como lo fueron los primeros ordenadores en red, el crecimiento de Internet; popularidad de los teléfonos inteligentes; y la aparición y el desarrollo de tecnologías como Internet de las cosas, ciudades inteligentes sostenibles y redes inteligentes han aumentado en importancia y complejidad”.

Se concluye que, en ciencia de datos, existen dos tipos de modelos basados en estadísticas basados en el análisis de la distribución de datos y la probabilidad de estimar probabilidades a partir de ecuaciones matemáticas que se deben seguir y restricciones asociadas a los datos. analizado; y un modelo basado en algoritmos de aprendizaje automático que tiene como objetivo encontrar los mejores datos de comunicación (tonos y comandos) y evaluar los resultados de los algoritmos adecuados para el problema.

a) Ciencia de Datos. Según (Camilo, García, Osorio, & Navarro, 2018) nos define “La ciencia de datos busca encontrar valor a partir de diferentes fuentes de información, incluidos datos que pueden ser inconsistentes y en diferentes formas, utilizando métodos y herramientas, incluidos métodos estadísticos, extracción de datos, aprendizaje automático y visualización”.

Se concluyó que la ciberseguridad es una rama de la informática responsable de desarrollar e implementar formas de proteger la infraestructura y el tic. Considerando la importancia de contar con sistemas seguros que garanticen la confidencialidad, integridad y disponibilidad de los datos: métodos de análisis de ciber riesgos, métodos y herramientas de desarrollo de software y hardware, sistemas de seguridad, etc.

b) Machine Learning. Según (Urbina & de la Calleja, 2017) nos describe “Tal vez aprender, obtener conocimiento, desarrollar habilidades, organizar el conocimiento y descubrir hechos, etc. Es una característica del pensamiento humano”.

Se concluyó que el aprendizaje automático es una disciplina de inteligencia artificial que utiliza algoritmos para dar a las computadoras la capacidad de reconocer patrones y hacer predicciones en grandes conjuntos de datos.

c) Ciberseguridad en Android. Según (Camilo, García, Osorio, & Navarro, 2018) nos define “Todas las aplicaciones de Android están empaquetadas en un archivo APK que contiene el código de la aplicación, los recursos y un archivo AndroidManifest.xml. En segundo lugar, proporciona información sobre el rendimiento y la configuración de seguridad de cada aplicación”.

Se concluye que la seguridad móvil se refiere a los métodos, la infraestructura y el software que se utilizan para proteger cualquier dispositivo móvil. A medida que

estos dispositivos ganen popularidad entre los consumidores, seguirán siendo el objetivo principal de los piratas informáticos, no las computadoras de escritorio.

d) Ciberseguridad en Aplicaciones Web. Según (Camilo, García, Osorio, & Navarro, 2018) nos define “Detectar páginas maliciosas no es lo más importante para proteger a organizaciones e individuos de brechas de seguridad, pero también ayuda a mitigar problemas futuros con agentes externos que causen daños graves a la lógica del sistema”.

Se concluyó que la ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

2.1.1.4 Prevención y Sanción de los Cibercrimitos. Según (Pons, 2017) nos describe “Entre los delitos denunciados en Internet encontramos: estafa, hurto, defraudación, mentira y hurto de caudales públicos. Con las recientes reformas legales, han surgido algunos delitos que utilizan las tecnologías de la información y la comunicación, como los delitos electrónicos contra la libertad humana, el acceso a la intimidad y la revelación de la vida privada, el acceso ilegal a la información y los datos, los delitos intelectuales y los malos tratos contra las personas. Contacto sexual con menores a través de Internet u otros medios”.

Se concluyó que las protecciones de las víctimas permiten que las víctimas tomen medidas inmediatas para prevenir el delito cibernético (especialmente para aquellos con el conocimiento, las habilidades y las capacidades) o para prevenir los intentos delictivos de cometer estos delitos. Una crítica importante a estos métodos es que asignan la responsabilidad de prevenir el ciberacoso a las víctimas, no a las organizaciones que necesitan protegerlas de daños.

a) Cibercrimitos. Según (Pons, 2017) nos define “El delito cibernético, que generalmente se refiere a actividades ilegales en Internet, tiene cuatro características principales: fácil aplicación; requieren menos recursos que el daño que causan; pueden vivir voluntariamente en un área sin tener presencia física en la comunidad debajo de ellos; y aprovechar los mecanismos disciplinarios que pueden existir en algunos estados, conocidos como ciber refugios, por falta de voluntad política para regular y sancionar estas prácticas”.

Se concluyo que el cibercrimen son las acciones ilícitas que se realizan en el entorno digital a través de las redes informáticas y se pueden dividir en los que se aprovechan de la debilidad de las computadoras y los que se aprovechan de la ignorancia y la apatía de la gente son dos grupos. Para no caer en la trampa de los ciberfraudes y navegar por Internet de forma segura, se recomienda estar al tanto de estos nuevos tipos de fraude digital y ser conscientes de que hay personas sin escrúpulos que quieren aprovecharse del desconocimiento de los usuarios detrás de ellos. Internet.

b) La Ingeniería Social. Según (Gómez I. , 2015) nos define “centrarse en lo que une o divide a las personas y, en el caso de la interacción social, cómo y de qué manera el intercambio une o divide a las personas. Necesitamos una comprensión integral del todo, no solo de las partes de la red que conectan las relaciones sociales, para esto necesitamos un enfoque sistemático”.

Se concluye que la ingeniería social es un conjunto de técnicas utilizadas por los ciberdelincuentes para engañar a los usuarios desprevenidos para que transmitan información confidencial, infecten sus computadoras con malware o se conecten a sitios web infectados. Además, los delincuentes pueden aprovechar la falta de información de los usuarios; Debido al rápido desarrollo de la tecnología, muchos

usuarios y empleados desconocen el verdadero valor de los datos personales y la mejor forma de protegerlos.

c) Los Delitos en Línea. Según (Colón & Cuenca, 2014) nos define “En un sentido amplio, el delito electrónico es cualquier delito o delito que utiliza la tecnología como medio, herramienta o propósito, actividad ilegal de las computadoras, procesos y funciones que operan o como herramienta. significa o hace”.

Se concluyó que el desarrollo, la efectividad y el uso generalizado de las nuevas herramientas tecnológicas permitieron destruir las oportunidades de los delincuentes, utilizar las grandes ventajas de las TIC para organizar y realizar actos delictivos, superar los obstáculos en la vida comunitaria. El uso de técnicas de hacking y acceso ilegal a dispositivos se ha convertido en una nueva forma de delincuencia en la era digital.

d) Delitos de Pi en el ciberespacio. Según (Pons, 2017) nos define “Que el delito es lo que el crimen es para el cibercrimen”. Los terroristas pueden usar herramientas informáticas como armas ofensivas para lanzar cualquier número de ataques contra computadoras, redes o la información que contienen. También pueden usar ataques y causar daños físicos en sistemas y redes personales usando cualquiera de las acciones anteriores”.

Se concluyó que los ciberespacios se ven reforzados por hechos relacionados con el crecimiento del conocimiento. Esto puede ser en parte con el propósito de capacitar a miembros y organizaciones militares para participar en actividades futuras en los sectores o regiones antes mencionados para mejorar la cooperación y compartir las mejores prácticas entre diferentes países. Los titulares de derechos participan en todas estas actividades donde se comparte información o buenas prácticas. Este

intercambio de mejores prácticas también se realiza a través de una red de fiscales, jueces y jueces.

2.1.2 Gestión de Tecnologías de Información

Según los autores (Ayala & Gonzales, 2015) Nos argumentan: “Conjunto de tecnologías para descubrir, crear, procesar y transmitir información presentada en diferentes códigos (texto, imagen, audio, video)” (p.27).

Se concluyó que la gestión de servicios de tecnología de la información es una disciplina basada en criterios basados en las necesidades del cliente final, la planificación del servicio de TI y las necesidades de la empresa.

2.1.2.1 Tecnologías de la Información y la Comunicación. Según (Ayala & Gonzales, 2015) nos define “El uso de las TIC en los sectores social y económico ha creado una serie de conceptos nuevos, como comercio electrónico, comercio electrónico, gobierno electrónico, salud electrónica, aprendizaje electrónico, participación electrónica, tecnología electrónica, tecnología electrónica. . . - entre otros: empresa, correo electrónico, banda ancha, domótica”.

Se concluyó que las tecnologías de la TIC se utilizan para transmitir teléfonos móviles y voz a través de redes informáticas a través de un solo cable o sistema de conexión. Existe un fuerte incentivo económico para integrar una red telefónica en un sistema de red informática que utiliza cableado común, distribución de señales y sistemas de control. TIC, radio, televisión, telefonía móvil, ordenadores y dispositivos de red, sistemas de satélite, etc. Es un término general que abarca todas las formas de comunicación, incluidas las siguientes, así como los diversos servicios y herramientas que ofrecen, como videoconferencias y aprendizaje a distancia.

a) Fundamentos de las Tic. según (Nolasco & Ojeda, 2016) nos describe “La importancia de enfocar el uso de las TIC en la educación desde una perspectiva

internacional significa estar de acuerdo en el nivel conceptual de la creación de indicadores efectivos”.

Se concluyó que el tic y el lenguaje son los materiales y métodos utilizados para producir y transmitir información, en particular la tecnología de la información, Internet y teléfono. Las TIC incluyen el conjunto de sistemas utilizados para gestionar la información, especialmente los ordenadores y programas necesarios para transmitir, almacenar, gestionar, transmitir y acceder a la información.

b) Evolución de las Tic. Según (Tricoci, Corral, & Oriolo, 2020) nos indica “está aumentando debido al desarrollo de las TIC, las condiciones especiales de este tipo de empresas. Encontrando una relación directa entre el acceso y uso de internet en el lugar de trabajo y el desempeño económico de la empresa, debido a que las empresas con mayor acceso son más importantes en el sector servicios”.

Se concluyó que la revolución tecnológica por la que ha atravesado la administración desde principios de los años 70 se encuentra en distintas etapas. Algunos cambios deben divulgarse específicamente para que sean realmente nuevos o para incluir cambios significativos en la forma en que trabajamos o tratamos con las autoridades públicas y las empresas.

c) Impacto de las Tic. Según (Ayala & Gonzales, 2015) nos define “El impacto económico de las TIC difiere entre países, incluso entre aquellos que tienen acceso a la misma tecnología. Es necesario desarrollar programas de TIC en las siguientes áreas: educación, investigación y desarrollo”.

Se concluyó que las TIC brindan la organización del conocimiento y toda oportunidad, teniendo en cuenta la calidad, con la difusión de nuevas formas de organización, comunicación, educación y formación en todos los ámbitos de la vida

humana y del desarrollo de esta y de la sociedad. ofertas obtiene resultados. la gente es igual.

d) Las Tic como Agentes del Cambio. Según (Zunino, Berdún, & Amandi, 2001) nos describe “Las clases que definen un tipo particular de agente se asociaron con la clase Brain, lo que permitirá que cada instancia de estas clases pase una instancia de Brain que represente la instancia del intérprete de Prolog”.

Se concluyó que, las ventajas competitivas de la aplicación de las TIC incluyen varios factores de los procesos operativos y de planificación. Desde un punto de vista operativo, ofrece ventajas como una mayor eficiencia (p. ej., automatización de procesos regulatorios) y como característica única ayuda a mejorar (p. ej., facilita la información y la formación de conocimiento en alianzas con otras empresas). Además, se puede decir que las TIC crean procesos, permiten que los productos se transformen en productos, ayudan a los procesos en cuestión y, por lo tanto, pueden contribuir al crecimiento de la PTF.

e) Infraestructura de las Tic. Según (Morillo, 2003) nos describe “Crea una arquitectura común basada en computadoras y dispositivos móviles y equipos móviles encargados de la transmisión de video, también es una variante que puede enviar y recibir voz y datos. El diseño técnico de monitoreo remoto soporta el monitoreo de cualquier edificio o programa que requiera monitoreo continuo”.

Se concluyó que la infraestructura de TIC se refiere a lo que se necesita para operar y administrar el entorno de TI de una empresa. La infraestructura de TI se puede alojar en la nube o en las instalaciones.

2.1.2.2 Aspectos Fundamentales de los Si. Según (Lapiedra, Devece, & Guiral, 2011) nos dice “La información en la empresa debe funcionar para obtener la

información necesaria y realizar cambios en las competencias de los integrantes de la empresa, según sea necesario para la gestión. implementar las decisiones tomadas”.

Se concluye que un sistema es un tipo especial de sistema que puede: Se define de muchas maneras. Es un grupo de cosas que trabajan juntas para apoyar el funcionamiento de una empresa o negocio. Es un conjunto de objetos o componentes relacionados para recopilar, transferir y distribuir datos y proporcionar un método de retroalimentación para lograr el propósito.

a) Componentes de los Si. Según (Pons, 2017) nos define “Los sistemas de información incluyen: hardware y software de computadora, dispositivos móviles, bases de datos, recursos humanos y procesos”.

Se concluyó que los componentes del sistema operativo son una colección de componentes relacionados que trabajan juntos para recopilar, procesar, almacenar y distribuir información para respaldar la toma de decisiones. También apoyan la planificación, gestión, seguimiento y control de la organización.

b) Funciones del Si. Según (Lapiedra, Devece, & Guiral, 2011) nos dice “Los sistemas de información se desarrollan para ayudar a las empresas a lograr sus objetivos”.

Se concluye que la función SI es una de las funciones de Excel más populares y te permite hacer comparaciones lógicas entre valores y resultados esperados. Por lo tanto, una sentencia IF puede tener dos consecuencias. El primer resultado si la comparación es correcta, el segundo si la comparación es falsa.

c) El SI y la Cadena de Valor. Según (Quintero & Sánchez, 2006) nos índice “Por lo tanto, el valor corporativo son las actividades centrales y las actividades de apoyo relacionadas que crean valor para el cliente. Esta cadena también permite

determinar los diversos costos de la organización a través de las diversas actividades que forman parte de la producción”.

Se concluye que una cadena de valor es un modelo de negocio que describe todas las actividades involucradas en la producción de un producto o servicio. Para las empresas manufactureras, esta cadena incluye los pasos que mueven el producto desde la producción hasta la distribución.

d) El Si y la Infraestructura de Empresa. Según (Lapiedra, Devece, & Guiral, 2011) nos describe “No podemos vincular el tic de la empresa a actividades similares. El método de información no es un departamento nuevo ni un componente asociado de ningún departamento funcional existente”.

Se concluyó que una infraestructura de TI flexible, fiable y segura puede ayudar a las empresas a alcanzar sus objetivos y obtener una ventaja competitiva en el mercado. Además, si la infraestructura de TI no se implementa correctamente, las empresas pueden enfrentar problemas de conectividad, diseño y mantenimiento, como corrupción y fallas en el sistema. En general, la propiedad utilizada correctamente puede ser un factor importante para determinar si un negocio es rentable.

2.1.2.3 Sistema de Inteligencia Tecnológica. Según (Urretavizcaya, 2001) nos dice “Intelligent Systems Learning (STI) tiene la misión clara de desarrollar métodos de aprendizaje personalizados para diferentes usuarios/estudiantes. Sin embargo, en la gestión de entendimiento en el salón no se presta la debida atención a la distribución y uso de los materiales educativos, especialmente los métodos intelectuales que apoyan el aprendizaje.”.

Se concluyó que las habilidades técnicas son un conjunto de sistemas y herramientas proporcionados para administrar y crear conocimiento mediante el análisis de datos que ya existen dentro y fuera de la organización o empresa.

a) Generación de Conocimiento. Según (Castillo, 2007) nos describe “Es una parte importante del sistema de tecnología de la información porque valorar el valor de la información ha llevado a las empresas a crear, usar, distribuir o desechar de nuevas formas”.

Se concluyó que la producción de conocimiento es el trabajo de adquirir y crear conocimiento externo mediante el uso del conocimiento que tienen las personas. Durante la transferencia de información, se analizan las áreas de intercambio de información y los procesos técnicos que la proporcionan.

b) Casos de Implementación. Según (Castellanos, 2007) nos describe “La implementación del sistema de información técnica se llevó a cabo en cada uno de los niveles de control tecnológico antes mencionados, contando con la asesoría y apoyo de expertos en cuanto al uso de métodos y creación de conocimiento y planificación estratégica”.

Se concluyó que usar casos para implementar o implementar una idea propuesta, ya sea un programa de computadora, un programa, un modelo científico, un diseño, un estándar, un algoritmo o una regla.

c) Roadmapping Tecnológico. Según (Albiol & Lloveras, 2019) nos describe “Una hoja de ruta tecnológica o de innovación es un plan a largo plazo para lograr uno o más objetivos con una solución técnica/técnica específica, este plan puede estar basado en un nuevo proceso, nuevo producto o nueva tecnología”.

Se concluyó que technology Pathways es eficaz para la identificación y aprendizaje de tecnologías que permite evaluar los cambios en tecnologías

interesantes en el mercado y, en última instancia, orientar la estrategia organizacional y los procesos de toma de decisiones. Estas herramientas pueden ayudarnos en un análisis externo de la organización, como un mapa de patentes, o un análisis interno que nos permita desarrollar una "hoja de ruta" de sus actividades estratégicas. Para ello, la inteligencia tecnológica juega un papel estratégico.

d) El Conocimiento y la Tecnología en el Desarrollo Empresarial. Según (Castellanos, 2007) nos describe “El conocimiento y el aprendizaje son componentes de las relaciones que aseguran la comunicación entre los diferentes niveles. Las organizaciones en proceso de aprendizaje continuo deben desarrollar la capacidad de adaptarse y anticiparse a los cambios que se produzcan en su misión”.

Se concluyó que la gestión de la tecnología es un campo único que combina la ingeniería, la ciencia y los conocimientos de gestión para planificar, desarrollar e implementar soluciones tecnológicas que ayuden a alcanzar los objetivos estratégicos y organizacionales.

2.1.2.4 Sistemas de Información Administrativos. Según (Zuñá, Arce, Romero, & Soledispa, 2019) nos describe “Los sistemas de gestión estándar integran módulos de marketing (o ventas), cobros, pagos y compras. Las funciones de productividad y recursos humanos no se desarrollan aquí ya que son específicas de una determinada actividad empresarial y por tanto no se implementa un programa de procesos común o compartido como en otros módulos”.

Se concluyó que el sistema de información administrativa, SIA, es un programa informático que tiene como función principal el registro de información sobre los trámites administrativos, incluidos los trámites y servicios administrativos para los ciudadanos y la administración pública.

a) Función Comercialización. Según (Camilo, García, Osorio, & Navarro, 2018) nos dice “El papel del marketing se encuentra en el corazón de la solución del sistema de gestión: la generación de ventas permite llevar productos específicos al mercado al mismo tiempo que se inicia la inversión financiera que sirve para sostener y expandir el proceso de fabricación. . y así comienza a introducir elementos del programa de transformación”.

Se concluyó que la actividad de marketing es una serie de actividades que tienen lugar desde el momento. Transporte de productos agrícolas desde las fincas donde se producen hasta el consumidor o productor.

b) Función Compras. Según (Nogales, 2007) nos describe “Un término más común es la gestión de la cadena de suministro, que abarca la filosofía de que los clientes y proveedores ven sus negocios como extensiones uno del otro”.

Se concluye que la función de compras asegura el éxito de las actividades de la empresa en el suministro de bienes y servicios necesarios para la operación y funcionamiento de la empresa y en la gestión de los servicios.

c) Función cobranzas. Según (Izar & Ynzunza, 2017) nos describe “Los instrumentos de crédito son instrumentos soportados, en los que se envía al cliente con los bienes la prueba del contrato de préstamo, que generalmente es una factura, se firma el consentimiento del cliente cuando es necesario y se aprueba la cuenta. aceptado”.

Se concluye que el deber de la empresa de cobrar los deberes administrativos asociados con el pago a los proveedores por los servicios prestados a sus clientes. Ver resúmenes de TC, extractos bancarios, consultar cuentas de clientes, crear órdenes de pago, comparar facturas, registrar el progreso de los sistemas de pago y cobro.

d) Función Pagos. Según (Castellanos, 2007) nos describe “El pago y el cobro se pueden realizar de diferentes formas según el tipo de empresa, los proveedores o la distribución geográfica y la estructura organizativa”.

Se concluye que el servicio de pago es un servicio financiero. Se ejecuta para medir el método del pagaré del préstamo de acuerdo con la tasa de interés fija y el cronograma de pago regular. Registro de costos.

e) Función Contable. Según (Quintero J. , 2013) nos dice “Estos incluyen los métodos económicos de las personas en las ciencias contables y administrativas, la condición económica de las personas, empresas y organizaciones, y el análisis de las cosas en su comportamiento, comportamiento y uso de acuerdo con los problemas de las personas”.

Se concluyó que la función contable comprende el registro de todas las actividades económicas realizadas en la empresa, incluyendo la contabilidad de ingresos y gastos, y el registro de las mismas transacciones de forma legal y de acuerdo con la norma legal.

2.2 Importancia de la(s) Variable(s) o Tópico(s) Clave

Sustituir la ciberseguridad por un proceso es importante porque se analiza y se descompone en métricas y diferencias, elementos que determinan su integración en la gestión de las tecnologías de la información.

La variable seguridad cibernética toma la importancia de la hipótesis, debido a que la variable relevante depende de que estará relacionada con la gestión de tecnologías de la información, por lo que debe explicar una dimensión de descripción amplia, clara y completa. actividad, comportamiento y o. Habilidad en términos de variable dependiente.

Dado que esta tesis se encuentra en el campo de las tecnologías de la información, la revolución de la seguridad cibernética cobra importancia en términos de seguridad informática ya que mejora las capacidades de seguridad del sitio web de la empresa.

Así mismo, (Patiño, 2021) nos define “La ciberseguridad ha sido una prioridad desde principios del siglo XIX. Los sistemas digitales y los ordenadores han aumentado en los últimos años. Por lo tanto, la misma situación de dependencia crea una debilidad en este sistema. Sin embargo, la ciberseguridad se entiende como un intento de preservar la integridad e integridad de los sistemas digitales e informáticos con el fin de garantizar los principios de privacidad de la información, confiabilidad en el intercambio seguro de datos, y el funcionamiento y disponibilidad de la información, arquitectura técnica. en infraestructura de tic”.

La inclusión de la tecnología es importante porque muchos de los estudios desarrollados en ella muestran la relevancia de la estructura de la educación (UNESCO, 2018, p.36) y también porque es posible desarrollar ideas propuestas por los estudiantes. hacer el centro de toda actividad está diseñado para lograr el aprendizaje.

Las variables ciberseguridad y tic es importante porque según (ROMERO, 2018) “es importante hoy y su preservación también es importante porque aquí se crean muchos procesos de producción y hay un vínculo entre las sociedades, lo que es considerado por muchos países como la quinta área militar del mundo, mar, aire. y fuera. El ciberespacio se usa cada vez más como escenario político, económico y militar donde los conflictos están vinculados a campañas en línea para actos de agresión en el mundo real. Además, el sandbox es anónimo y no tiene mucho espacio

físico en comparación con otros campos de batalla; es decir, no tiene una expansión particular”.

En cuanto a la tesis, el cambio es significativo porque sus objetivos incluyen la transición de un modelo de gestión de tecnologías de la información basado en la transferencia de conocimiento a un modelo de ciberseguridad efectivo en el que la empresa juega un papel principal en la seguridad del proceso web. En la empresa privada que forma parte de este trabajo, es importante que se pueda identificar tendencias, problemáticas y posibles soluciones que ayuden a mejorar los sistemas de ciberseguridad en la empresa y por ende la gestión de tecnologías de la información. Por otro lado, los cambios en el gobierno de TI se están volviendo estratégicamente importantes a medida que la interacción directa y significativa con el sector privado cambia la seguridad cibernética y su alcance. Por un lado, la tecnología de la información es diferente, “las TIC deben mejorar el comportamiento de los evaluadores, enfocarse en lo aprendido y aplicar los resultados esperados. Las experiencias internacionales son importantes para aprovechar al máximo los recursos disponibles en la organización” (Cambar, Graterol, & Añez, 2009).

Al mismo tiempo el manejo de las tecnologías de la información es diferente, es importante como un objetivo del sistema que muestra buenos y visibles resultados entre las políticas de seguridad web, y el objetivo es mostrar al país en el centro de lo que constituye la web. mejora de la seguridad y la calidad. Fortalecer contra los ataques. Empresa de Sistemas Web. En este trabajo de investigación cobra importancia el cambio en las tecnologías de la información como resultado de la integración de las tecnologías de la información con la seguridad real, ya que al conocerla mejor podemos encontrar elementos de las tecnologías de la información que muestran una integración incompleta o insuficiente. Asimismo, en nuestra

empresa, mientras se realizan cambios en el manejo de las tecnologías de la información para aumentar la intensidad de la lección, mientras el docente desarrolla los métodos de enseñanza para generar el conocimiento de los alumnos, parece una meta inalcanzable descrita en la evaluación. Cuando estos dos campos se unen, es deseable proporcionar métodos de enseñanza y aprendizaje flexibles, interactivos y efectivos a través de la integración de las tecnologías existentes, por lo que se deben definir cuidadosamente los cambios para implementarlos.

2.3 Modelos de la(s) Variable(s)

La variable independiente “la ciberseguridad “definida como:

Tabla 1

Clasificación de la variable independiente

Por su posición:	Independiente
Por su naturaleza:	Cuantitativa
Por sus valores:	Discreta
Por sus valores de medición:	Ordinal
Dimensiones:	4

Nota: Elaboración propia

Se evalúa mediante un modelo de calificación Likert, que se define como una herramienta que puede calcular diferencias y respuestas en una escala Likert de muy en desacuerdo, en desacuerdo, indeciso, de acuerdo y muy en desacuerdo. Permite a la persona medir su comportamiento y hacer saber a los empleados de la empresa cuánto le queda a cada palabra. El estándar de medición utilizado:

- TD: Total desacuerdo
- D: Desacuerdo
- N: Neutro
- A: De Acuerdo
- TA: Totalmente de acuerdo

Esto es útil en situaciones en las que queremos que alguien adopte su punto de vista. En este caso, los grupos de retroalimentación trabajan para obtener la opinión del empleado sobre la declaración dada.

La variable dependiente “gestión de tecnologías de información” definida como:

Tabla 2

Clasificación de la variable dependiente

Por su posición:	dependiente
Por su naturaleza:	Cuantitativa
Por sus valores:	Discreta
Por sus valores de medición:	Ordinal
Dimensiones:	4

Nota: Elaboración propia

Se evalúa con el modelo de calificación de Likert, que se define como una herramienta que puede medir diferencias con preguntas de escala de Likert, y las respuestas son muy en desacuerdo, en desacuerdo, indeciso, de acuerdo y muy en desacuerdo, permitimos la medición. y evaluación. mide su correlación con la variable independiente. Se ha discutido el cambio en la gestión de las tecnologías de la información como un problema de integración a través del análisis y la mirada crítica del investigador, los criterios utilizados son:

- TD: Total desacuerdo
- D: Desacuerdo
- N: Neutro
- A: De Acuerdo
- TA: Totalmente de acuerdo

Esto es útil en situaciones en las que queremos que alguien adopte su punto de vista. En este caso, los grupos de retroalimentación trabajan para obtener la opinión del empleado sobre la declaración dada.

2.3.1 Operacionalización de Variables

VARIABLES	DIMENSIONES	INDICADORES	PREGUNTA	ESCALA DE MEDICIÓN	INSTRUMENTO
VARIABLE INDEPENDIENTE VI.- LA CIBERSEGURIDAD	D.1 EL CICLO DE VIDA DE LA CIBERSEGURIDAD D.2 SEGURIDAD INFORMÁTICA D.3 CIBERSEGURIDAD Y CIENCIA DE DATOS D.4 PREVENCIÓN Y SANCIÓN DE LOS CIBERDELITOS	PREVENCIÓN DETECCIÓN RESPUESTA EFICIENCIA A LAS MEDIDAS DE CIBERSEGURIDAD LOS VIRUS INFORMÁTICOS MECANISMOS PREVENTIVOS MECANISMOS CORRECTIVOS MECANISMOS DETECTIVOS ENCRIPCIÓN EN SEGURIDAD INFORMÁTICA CIENCIA DE DATOS MACHINE LEARNING CIBERSEGURIDAD EN ANDROID CIBERSEGURIDAD EN APLICACIONES WEB CIBERDELITOS LA INGENIERÍA SOCIAL LOS DELITOS EN LÍNEA DELITOS DE PI EN EL CIBERESPACIO	¿Cree usted que el área de TI de la empresa cuenta con programas para concientizar las amenazas en la ciberseguridad? ¿Cree usted que el área de TI de la empresa resguarda los backups de la información de la empresa adecuadamente? ¿el área de TI de la empresa restringe el uso de los sistemas informáticos de la organización al personal no autorizado? ¿Cree usted que el área de TI de la empresa ha incorporado software de seguridad adecuados para proteger la información de la organización de actividades las ilícitas de los cibercriminales? ¿Cree usted que el área de TI de la empresa ha incorporado medidas de seguridad físicas que neutralicen las actividades ilícitas de los cibercriminales? ¿Cree usted que el área de TI de la empresa tiene incorporado planes de protección de detección contra los cibercriminales? ¿Tiene usted conocimiento de cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones? ¿Cree usted que el área de TI de la empresa cuenta con personal calificado en ciberseguridad? ¿Cree usted que los sistemas de seguridad existentes por el área de TI de la empresa utilizan aplicación web que neutralizan los ataques de los ciberdelincuentes? ¿Alguna vez ha tenido que detener sus actividades por causa de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad? ¿el área de TI de la empresa lo ha capacitado a usted sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	LIKERT: 1. Totalmente en desacuerdo 2. Desacuerdo 3. Neutral 4. De acuerdo 5. Totalmente de acuerdo.	Cuestionario

VARIABLE DEPENDIENTE VD.- GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	I.1 TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN	FUNDAMENTOS DE LAS TIC	¿Considera usted que en el último año se ha perdido información importante por culpa de algún virus informático?	LIKERT: 1. Totalmente en desacuerdo 2. Desacuerdo 3. Neutral 4. De acuerdo 5. Totalmente de acuerdo.
		EVOLUCIÓN DE LAS TIC	¿Considera usted que el área de TI de la empresa cuenta con planes de capacitaciones de TI oportunas al personal de la empresa?	
		IMPACTO DE LAS TIC	¿Considera usted que el área de TI de la empresa cumple una atención de incidencias de TI?	
		LAS TIC COMO AGENTES DEL CAMBIO	¿Cree usted que el área de TI de la empresa cuenta con herramientas para la protección contra amenazas externas y ambientales respecto a la información?	
	I.2 ASPECTOS FUNDAMENTALES DE LOS SI	INFRAESTRUCTURA DE LAS TIC	¿Cree usted que el área de TI de la empresa realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?	
		COMPONENTES DE LOS SI	¿Considera usted que el área de TI de la empresa realiza mantenimientos oportunos a los dispositivos de la organización?	
		EL SI Y LA CADENA DE VALOR	¿Qué tan conforme está usted con la seguridad del internet que cuenta la empresa?	
		EL SI Y LA INFRAESTRUCTURA DE EMPRESA	¿Ha recibido capacitación de parte del área de TI de la empresa respecto al uso adecuado de las tecnologías de la empresa?	
	I.3 SISTEMA DE INTELIGENCIA TECNOLÓGICA	GENERACIÓN DE CONOCIMIENTO.	¿Considera usted que la de la oficina dirección de tecnología de información es adecuada?	
		CASOS DE IMPLEMENTACIÓN	¿Considera usted que la disponibilidad de la información de los sistemas de información es oportuna y segura?	
		ROADMAPPING TECNOLÓGICO		
		EL CONOCIMIENTO Y LA TECNOLOGÍA EN EL DESARROLLO EMPRESARIAL		
	I.4 SISTEMAS DE INFORMACIÓN ADMINISTRATIVOS	FUNCIÓN	¿Cree que usted que el área de TI de la empresa ayuda con las metas trazadas para el área de ventas de la empresa?	
		COMERCIALIZACIÓN		
		FUNCIÓN COMPRAS	¿Cree usted que el área de TI de la empresa responde adecuadamente a las necesidades tecnológicas de su área?	
		FUNCIÓN COBRANZAS	¿Está conforme con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	
	FUNCIÓN PAGOS			
	FUNCIÓN CONTABLE			

2.4 Análisis Comparativo

Tópico	Autor	Definición	Comentario
LA CIBERSEGURIDAD	(Camilo, García, Osorio, & Navarro, 2018)	La ciberseguridad es el área de las ciencias de la computación encargada del desarrollo e implementación de los mecanismos de protección de la información y de la infraestructura tecnológica (p.25).	La ciberseguridad es el campo de TI responsable de desarrollar e implementar mecanismos para proteger la información.
	(Camaño & Gil, 2020)	En este mundo globalizado, las organizaciones, los estados y la sociedad en general, han sido amenazadas y los ataques cibernéticos, que representan un comportamiento económico, político y social indeseable que afecta no solo la toma de decisiones, sino también la gobernanza y la estabilidad económica para ganar confianza e interés.	Las organizaciones, los estados en su conjunto se han visto afectados por ciberataques que, desde los contextos económico, emergen como debilidades que afectan en gran medida no sino también la estabilidad administrativa y económica para crear confianza entre los grupos de interés
	(Sáinz, 2017)	La ciberseguridad involucra temas complejos y su resolución requiere voluntad política para desarrollar e implementar un plan de desarrollo de infraestructura y servicios digitales que incluya múltiples procesos	La ciberseguridad trata temas complejos y resolverlos requiere voluntad política para diseñar e implementar un plan de desarrollo de infraestructura y servicios incluya una estrategia multidisciplinar, ajustada,

**GESTIÓN DE
TECNOLOGÍAS DE
INFORMACIÓN**

(Ayala & Gonzales,
2015)

adecuados, eficientes y eficiente y fácil de controlados. gestionar.

Las Tecnologías de la Información y la Comunicación (TIC) se desarrollan a partir de los avances científicos en la informática y las telecomunicaciones. Es un conjunto de tecnologías que posibilitan el acceso, un conjunto de tecnologías producción, procesamiento y comunicación de descubrimiento, creación, procesamiento y comunicación de información presentada en diferentes códigos. (p.27).

(Cruz, Pozo, Aushay
& Arias, 2019)

Las Tecnologías de la Información y la de Comunicación (TIC) se desarrollan a partir de los avances científicos de las TI de ahí la importancia del acceso a la tecnología en el proceso de producción, interacción, telecomunicaciones, de ahí procesamiento, gestión y la importancia de la transmisión de la tecnología que accede al información. proceso de producción, interacción.

(Marques, 2018)	<p>las TIC, considerado como el nuevo paradigma para la educación en el contexto de la organización del conocimiento con la ayuda de las computadoras, los teléfonos, los medios de comunicación y especialmente Internet, que hace que todo tipo de información sea accesible en cualquier momento y en cualquier lugar y facilita métodos de comunicación que están disponibles en todas partes. una vez.</p>	<p>El tic y el lenguaje son herramientas para fortalecerla enseñanza y el aprendizaje, aumentar las oportunidades para acceder al conocimiento, desarrollar habilidades colaborativas o inculcar valores, entre otros.</p>
-----------------	---	--

2.5 Análisis Crítico

Las variables se evalúan en la misma situación que en el Postest, es decir, en una situación natural donde se estudia y mide la combinación de dos sujetos. Luego, se determinan los cambios en los que los cambios independientes en ciberseguridad inciden en la dependencia de la gestión de TIC en la entidad, y se analizan las similitudes y diferencias analizando las condiciones de los experimentos. Termina analizando la relación entre las 2 medidas midiendo sus marcas.

Capítulo III Marco Referencial

3.1 Reseña Histórica

Kiaratel la cual en un principio se denominó M y C S.R.L fundada en 1992, es una empresa que tiene como principal misión brindar soluciones en el campo de las redes y telecomunicaciones para el desarrollo del mercado peruano. Con un fuerte deseo de brindar servicios y sistemas de telecomunicaciones a los sectores financiero y comercial, y la necesidad de mantener y desarrollar su competitividad y crecimiento, Kiaratel decidió invertir en el establecimiento e integración de una empresa capaz de brindar productos y servicios a sus clientes. compañías. y las instituciones de nuestro país son muy convenientes.

3.2 Filosofía Organizacional

3.2.1 *Nuestros valores:*

La integridad es una de nuestras herramientas más importantes, y para los miembros y clientes de nuestra empresa, la honestidad significa respeto en todo lo que hacemos.

3.2.2 *Misión:*

Brindando servicios de telefonía móvil de alta calidad, amplia cobertura y siempre pudiendo anticipar las necesidades de comunicación de sus clientes.

3.2.3 *Visión:*

Por ello, nuestra misión en Kiaratel Comunicaciones SAC es construir un negocio y brindar las mejores soluciones en base a los objetivos de nuestros clientes a través de habilidades de innovación y diferenciación en la industria de las telecomunicaciones.

3.2.4 Objetivos:

Obtenga la solución de telefonía adecuada para su empresa u hogar con un diseño confiable, excelentes funciones para su empresa y soporte de calidad al mejor precio.

3.2.5 Compromiso:

Satisfacer las expectativas de nuestros clientes significa que nos enfocamos en nuestra experiencia laboral, garantía de calidad y disponibilidad de servicios.

3.2.6 Posición de la Empresa:

Kiaratel se ha posicionado con éxito a nivel gerencial, gracias a su capacidad para implementar grandes proyectos dentro de los plazos establecidos y dentro de los presupuestos establecidos. Además, con el conocimiento de los trabajadores de la empresa, Kiaratel está construyendo una organización con una sólida experiencia en el mundo de las telecomunicaciones, lo que marca la diferencia a la hora de elegir un proveedor de soluciones completas. Por eso, nuestras empresas representativas nos dan la confianza de que han tomado la decisión correcta al momento de distribuir sus equipos, lograr metas y objetivos de ventas y conquistar nuevos mercados.

3.3 Diseño Organizacional

Kiaratel Comunicaciones S.A.C es una empresa mediana que cuenta con 100 empleados. La organización está estructurada de la siguiente manera:

Gráfico 1

Estructura de la entidad KIARATEL S.A.C



Nota: Elaboración propia de autor

3.4 Productos y/o Servicios

3.4.1 Productos

- a. Router y Repetidores:** Un dispositivo que amplifica las señales de red. Los repetidores se utilizan cuando la longitud total de los cables de red supera el máximo permitido para el tipo de cable. No se puede utilizar en todos los casos. Un Router con diferentes capacidades hacen lo mismo en el nivel superior, tercer nivel del modelo OSI. Funcionan de tal forma que la dirección de la red depende del protocolo.
- b. Equipos telefónico fijo, móvil:** La telefonía de línea fija es el último servicio de telefonía que proporciona una capacidad de comunicación de voz completa entre los usuarios. Los teléfonos celulares funcionan enviando señales (y señales) a teléfonos celulares (estaciones terrestres) usando ondas de RF.
- c. Decos digitales y satelitales:** Un decodificador de satélite o receptor de satélite es una caja que te permite recibir fácilmente una gran cantidad de canales. Suelen ser cajas delgadas y compactas que funcionan con una antena parabólica para recibir señales de satélite, convertirlas en canales y enviarlas a tu televisor.
- d. Accesorios de equipos móviles:** Los accesorios para equipos móviles son muy útiles. Puede utilizar accesorios para mejorar su experiencia de usuario y para que su teléfono se vea mejor.

3.4.2 Servicios

3.4.2.1 Servicios de soporte técnico. Este departamento se encarga de desarrollar el Soporte dentro de las áreas de Sistemas e Informática, Electrónica,

Redes, Telecomunicaciones, servicio de televisión por cable y Soporte Técnico a nuestros clientes.

Función:

Los estudios se realizan principalmente con el fin de brindar un servicio completo en el campo de las TIC, para satisfacer las necesidades y objetivos de la empresa, y así brindar un servicio de calidad y garantía a los clientes de la entidad.

Las funciones desarrolladas son:

Área de Sistemas e Informática:

Se encarga de gestionar toda la red informática de la empresa, manteniendo la estabilidad de funcionamiento de los equipos de cómputo, proporcionando nuevas tecnologías sobre recursos que se pueden implementar o mejorar para el trabajo cotidiano. Las funciones son:

- ✓ Mantenimiento y conservación de equipos informáticos.
- ✓ Administrar y optimizar el rendimiento de los sistemas operativos.
- ✓ Administrar y mantener la disponibilidad operativa de los servidores (hardware y software).
- ✓ Gestionar cuentas de los usuarios de las altas y bajas.
- ✓ Respaldo de copias de seguridad de datos periódicamente y recuperación de los mismos ante diversas incidencias.
- ✓ Gestión y control de las licencias de software (Antivirus, Microsoft office, etc.).
- ✓ Asegurar y brindar la disponibilidad de las comunicaciones en las áreas de trabajo de la empresa.
- ✓ Evaluar las necesidades de recursos (disco duro, memorias, procesadores, fuentes, otros).

- ✓ Instalar y actualizar utilidades de software que permitan una adecuada funcionalidad a los equipos.
- ✓ Análisis y elaboración de proyectos e informes para la implementación de software y hardware con el propósito de obtener nuevos programas y equipamientos.

Área de Electrónica, Redes, Telecomunicaciones:

Se encarga de gestionar temas de arquitectura de las redes para poder realizar las instalaciones, además revisa los protocolos y programas informáticos para implementar la puesta en marcha de las redes y servicios de telecomunicaciones. Las funciones son:

- ✓ Servicio de Instalación de equipos de la red HFC, ADSL y WIMAX a los clientes de la empresa.
- ✓ Mantenimiento de los servicios de redes HFC, ADSL y otros.

Área de Soporte Técnico:

Se encarga de realizar la instalación y mantenimiento de las redes y servicios de telecomunicaciones (internet, telefonía y televisión por cable) manteniendo un grado de relación con las diferentes áreas de la empresa y los clientes. Las funciones son:

- ✓ Atención al usuario (preguntas, respuestas, preguntas frecuentes, asesoría técnica, información general, etc.)
- ✓ Instalación, configuración y mantenimiento de equipos MODEMS, ROUTERS, DECODIFICADORES. otros.

Las diferentes áreas de trabajo poseen un nivel alto de relación y todos trabajan conjuntamente, de esa manera las operaciones principales y distribuciones de

funciones laborales se cumplen eficaz y eficientemente apuntando a los objetivos de la empresa.

3.4.2.2 Servicios de instalación. Este departamento se encarga de la instalación de todos los equipos tecnológicos que brinda la empresa a sus clientes asociados al servicio de la red de movistar PERU. Cuyos servicios asociados son los oficios de TV por cable digital y satelital, internet de fibra óptica o HFC, telefonía fija y otros servicios adicionales.

Función:

Los estudios se realizan principalmente con el fin de brindar un servicio completo en el campo de las TIC, para satisfacer las necesidades y objetivos de la empresa, y así brindar un servicio de calidad y garantía a los clientes de la entidad.

Las funciones desarrolladas son:

Área de televisión por cable digital y satelital:

Se encarga de gestionar las instalaciones de los oficios de TV por cable digital y satelital a todos los clientes de la empresa, manteniendo la estabilidad de funcionamiento de los equipos de tv, proporcionando nuevas tecnologías sobre recursos que se pueden implementar o mejorar para el trabajo cotidiano.

Área de internet de fibra óptica o HFC:

Se encarga de gestionar las instalaciones de los servicios de internet de fibra óptica o red HFC para brindar una mejor calidad de internet a todos los clientes de la empresa, manteniendo la estabilidad de funcionamiento de los equipos de red adecuados, proporcionando nuevas tecnologías sobre recursos que se pueden implementar o mejorar para el trabajo cotidiano.

Área de telefonía fija y otros servicios adicionales:

Se encarga de gestionar las instalaciones de los servicios de telefonía fija y también de instalar otros servicios menores adicionales relacionados a la red telefónica para brindar una mejor calidad a nuestros clientes debemos mantener una la estabilidad de funcionamiento de los equipos sea adecuada, proporcionando nuevas tecnologías sobre los recursos que se pueden implementar o mejorar para el trabajo cotidiano.

3.5 Diagnóstico Organizacional

El análisis organizacional es lo que nos permite medir la efectividad de la organización, incluido su desempeño y efectividad organizacional, al descubrir la situación actual como fatiga, amenazas, fortalezas y oportunidades de mejora.

Análisis DAFO

Debilidades

- Ofrecer precios más altos que cualquier otro competidor que no es bueno cuando la crisis económica es profunda.
- Préstamos grandes con consecuencias significativas si persiste la contracción del crédito y/o el flujo de caja sigue siendo bueno.
- El mercado está muy fragmentado y es muy tecnológico. Muchos programas no pueden llegar a la audiencia final debido a su alto contenido técnico y al uso de abreviaturas.

Amenazas

- Demanda débil por condiciones macroeconómicas.
- La inestable situación política de varios países latinoamericanos depende del accionar de los pueblos.

- La distribución de su red en Perú si la Comisión del Mercado Telefónico (CMT) decide seguir los lineamientos legales recomendados por la Comisión Sudamericana.
- Nuevas rebajas de precios presentadas por CMT en Perú.
- El endeudamiento sobreexplotado facilita la desestabilización de las empresas extranjeras.

Fortalezas

- El mercado está creciendo debido a las soluciones móviles y servicios de TV.
- América del Sur está haciendo grandes esfuerzos para competir en ciencia y tecnología con programas de investigación y desarrollo para ayudar a los proyectos H2020.
- Gran atracción de eventos internacionales (MWCongress, IoT Congress, Smart City Expo, etc.).
- La adopción de soluciones OTT (Over Top) por parte de los usuarios finales es muy rápida.
- Un amplio catálogo de servicios de comunicación, entretenimiento e información en el móvil y en el móvil para que empresas y familias encuentren nuevas fuentes de ingresos y amplíen su negocio.
- Atención al cliente, investigación y desarrollo, infraestructura, imagen de marca, etc. gran tamaño que le permite lograr economías de escala.
- Orientación al cliente, creando productos y servicios que se ajusten a sus necesidades y valores, y coherencia.

Oportunidades

- Liderar el despliegue de una fibra de próxima generación en la red doméstica, lo que permite entregar una variedad de servicios existentes y futuros en una sola plataforma.
- Crecimiento económico superior a la media en países en vías de desarrollo donde el Grupo Telefónica tiene una importante presencia.
- Reduce los costes de inversión y mantenimiento al combinar empresas fijas y móviles en una única red. +
- Los teléfonos celulares y las estaciones de televisión continúan evolucionando y comunicándose.

MATRIZ DAFO

Tabla 3.

Matriz de Dafo

DEBILIDADES	AMENAZAS
<ul style="list-style-type: none">➤ Ofrecer precios más altos que cualquier otro competidor que no es bueno cuando la crisis económica es profunda.➤ Renovación continua de los empleados que afecta el ambiente de trabajo y la motivación de los empleados.➤ Préstamos grandes con consecuencias significativas si persiste la contracción del crédito y/o el flujo de caja sigue siendo bueno.➤ El mercado está muy fragmentado y es muy tecnológico. Muchos programas no pueden llegar a la audiencia final debido a su alto contenido técnico y al uso de abreviaturas	<ul style="list-style-type: none">➤ Demanda débil por condiciones macroeconómicas.➤ La inestable situación política de varios países latinoamericanos depende del accionar de los pueblos.➤ La distribución de su red en Perú si la Comisión del Mercado Telefónico (CMT) decide seguir los lineamientos legales recomendados por la Comisión Sudamericana.➤ Nuevas rebajas de precios presentadas por CMT en Perú.➤ El endeudamiento sobreexplotado facilita la desestabilización de las empresas extranjeras.
FORTALEZAS	OPORTUNIDADES
<ul style="list-style-type: none">➤ El mercado está creciendo debido a las soluciones móviles y servicios de TV.➤ América del Sur está haciendo grandes esfuerzos para competir en ciencia y tecnología con programas de investigación y desarrollo para ayudar a los proyectos H2020.➤ Gran atracción de eventos internacionales.➤ La adopción de soluciones OTT (Over Top) por parte de los usuarios finales es muy rápida.➤ Un amplio catálogo de servicios de comunicación, entretenimiento e información en el móvil y en el móvil para que empresas y familias encuentren nuevas fuentes de ingresos y amplíen su negocio.➤ Atención al cliente, investigación y desarrollo, infraestructura, imagen de marca, etc. gran tamaño que le permite lograr economías de escala.➤ Orientación al cliente, creando productos y servicios que se ajusten a sus necesidades y valores, y coherencia.	<ul style="list-style-type: none">➤ Liderar el despliegue de una fibra de próxima generación en la red doméstica, lo que permite entregar una variedad de servicios existentes y futuros en una sola plataforma.➤ Crecimiento económico superior a la media en países en vías de desarrollo donde el Grupo Telefónica tiene una importante presencia.➤ Reduce los costes de inversión y mantenimiento al combinar empresas fijas y móviles en una única red.➤ Los teléfonos celulares y las estaciones de televisión continúan evolucionando y comunicándose.

Nota: Elaborado de autoría propia.

Capítulo IV Resultados

4.1 Marco Metodológico

Se realizó un estudio que implica desarrollar la variable independiente y la variable dependiente en el mismo lapso de tiempo.

Primero el enfoque que se utilizó en la investigación fue un enfoque cuantitativo y la metodología seleccionada en este trabajo fue de tipo descriptiva dado que se midió el nivel de relación que existe entre dichas variables en un tiempo determinado y también fue de tipo correlacional ya que cuantifican las variables aparentemente relacionadas y se estudiaron la correlación existente entre ellas. El diseño de la investigación fue no experimental, y tuvo un corte transversal – correlacional.

Nuestra población fue de 100 trabajadores de la empresa KIARATEL S.A.C dado que nuestra población es muy grande y no se dispone de mucho tiempo para el llenado de la encuesta con el total de la población se aplicó una muestra de 40 trabajadores de la empresa KIARATEL S.A.C. El cual se utilizó un instrumento de tipo encuesta ejecutando mediante un cuestionario estructurado de preguntas cerradas, estos serán cuantificados a través de un modelo de cuestionario definido por el método de evaluaciones de la escala de Likert. El tipo de muestreo utilizado en la investigación fue probabilístico para lo cual utilizamos la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N - 1)e^2 + \sigma^2 Z^2}$$

Dónde:

n = el tamaño de la muestra 40.

N = tamaño de la población 100.

σ = Desviación estándar de la población 0,5.

Z = Valor obtenido mediante niveles de confianza 95% que confianza equivale a 1,96

e = Límite aceptable de error 5% (0,1).

4.2 Resultados

4.2.1 Confiabilidad del Instrumento por Alfa de Cronbach

Tabla 4

Estadísticos de fiabilidad de la variable independiente: la ciberseguridad

Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados	N de elementos
80,3%	81.9%	12

Nota: Fue elaborado en el Spss V23

Existe una muy buena consistencia interna entre los ítems de la escala, por lo que la confiabilidad de la recolección de datos de esta tesis es alta, la variable independiente ciberseguridad es de 81.9%.

Tabla 5

Estadísticos de fiabilidad de la variable dependiente: gestión de tecnologías de información

Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados	N de elementos
81,8%	82.3%	12

Nota: Fue elaborado en el Spss V23

Existe una muy buena consistencia interna entre los elementos de la herramienta, por lo que es muy confiable para la tesis de recopilación de información, gestión del cambio de tecnología de la información 82.3%.

4.2.2 Aplicación de la Estadística Inferencial de las Variables

4.2.2.1 Normalización de la Influencia de las Variables 1 y 2.

Ho:” La variable independiente la ciberseguridad y la variable dependiente la gestión de tecnologías de información se distribuyen en forma normal”

H1: “La variable independiente la ciberseguridad y la variable dependiente la gestión de tecnologías de información no se distribuyen en forma normal”

N. S= 0.05

Tabla 6

Pruebas de normalización

Kolmogórov-Smirnov			
	Estadístico	gl	Sig.
V1: LA CIBERSEGURIDAD	0,225	40	0,005
V2: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	0,222	40	0,004

Nota: Se realizó la prueba de normalización con el programa Spss V23

Se introducirá en la siguiente sección. Kolmogorov-Smirnov para todos menos de 0,05 rechazando la hipótesis nula y aceptando la hipótesis alternativa.

Concluimos que la ciberseguridad como variable independiente y la gobernanza de la tecnología de la información como variable dependiente rara vez se comparten. Por lo tanto, utilizamos la prueba estadística ordinal no paramétrica de Spearman.

a) El Planteo de las Hipótesis General.

Ho: “La ciberseguridad no relaciona significativamente con la gestión de tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022”

H1: “La ciberseguridad se relaciona significativamente con la gestión de tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.”

Tabla 7*Correlaciones de hipótesis general*

Matriz de Correlaciones				
			V1: LA CIBERSEGURIDAD	V2: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN
Rho de Spearman	V1: LA CIBERSEGURIDAD	Coefficiente de correlación	1,000	0,825
		Sig. (bilateral)	.	0,019
		N	40	40
	V2: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coefficiente de correlación	0,825	1,000
		Sig. (bilateral)	0,019	.
		N	40	40

Nota: Se aplicó la prueba de Rho de Spearman con el programa Spss V23

Finalmente, se ve que existe una fuerte relación entre la ciberseguridad y la gestión de tecnologías de la información con un 82,5% de confianza.

Conclusión: Se puede concluir que existe una estrecha relación entre la ciberseguridad y la gestión de tecnologías de la información en la empresa Kiaratel SAC, SJL, 2022. Está en un nivel significativo de 0,019% bilateralmente, es decir, menos de 0,5%.

a) El Planteo de las Hipótesis Específicas 1.

Ho: "La eficiencia de la ciberseguridad no se relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022."

H1: "La eficiencia de la ciberseguridad se relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022."

Tabla 8*Correlaciones de hipótesis específica 01*

Matriz de Correlaciones				
Rho de Spearman	Vi d1: EL CICLO DE VIDA DE LA CIBERSEGURIDAD	Coeficiente de correlación	Vi d1: EL CICLO DE VIDA DE LA CIBERSEGURIDAD	Vd.: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN
		Sig. (bilateral)	1,000	0,845
		N	40	40
	Vd.: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coeficiente de correlación	0,845	1,000
		Sig. (bilateral)	0,021	.
		N	40	40

Nota: Se aplicó la prueba de Rho de Spearman con el programa Spss V23

Finalmente, se ve que existe una relación única entre la ciberseguridad de vida y las tecnologías de gestión de la información con un 84,5% de confiabilidad.

Conclusión: Se puede concluir que la efectividad de la ciberseguridad está relacionada con las tecnologías de la información en la empresa Kiaratel SAC, SJL, 2022 y se encuentra en el nivel de significación bidireccional 0,021%, que es inferior a 0,5.

a) El Planteo de las Hipótesis Específicas 2.

Ho: "El mecanismo preventivo, correctivo no relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022"

H1: "El mecanismo preventivo, correctivo si relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022"

Tabla 9*Correlaciones de hipótesis específica 02*

Matriz de Correlaciones				
			Vi d2: SEGURIDAD INFORMÁTICA	Vd.: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN
Rho de Spearman	Vi d2: SEGURIDAD INFORMÁTICA	Coefficiente de correlación	1,000	0,842
		Sig. (bilateral)	.	0,023
		N	40	40
	Vd.: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coefficiente de correlación	0,842	1,000
		Sig. (bilateral)	0,023	.
		N	40	40

Nota: Se aplicó la prueba de Rho de Spearman con el programa Spss V23

Finalmente, se puede apreciar que existe una clara vinculación entre la seguridad informática y la información en salud, lo cual cree el 84,2%.

Conclusión: Se puede concluir que Salvaguarda, un buen método para las tecnologías de la información en la empresa Kiaratel, SJL, 2022, determinó el nivel de significación bidireccional de 0,023%, que es inferior a 0,5%.

a) El Planteo de las Hipótesis Específicas 3.

Ho: "El machine learning no relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022."

H1: "El machine learning si relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022."

Tabla 10*Correlaciones de hipótesis específica 03*

Matriz de Correlaciones				
			Vi d3: CIBERSEGURIDAD Y CIENCIA DE DATOS	Vd.: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN
Rho de Spearman	Vi d3: CIBERSEGURIDAD Y CIENCIA DE DATOS	Coefficiente de correlación	1,000	0,856
		Sig. (bilateral)	.	0,014
	Vd.: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	N	40	40
		Coefficiente de correlación	0,856	1,000
		Sig. (bilateral)	0,014	.
		N	40	40

Nota: Se aplicó la prueba de Rho de Spearman con el programa Spss V23

Finalmente, se aprecia que existe una fuerte relación entre la ciberseguridad y la gestión de la ciencia de datos y tecnologías de la información con un nivel de confianza del 85,6%.

Conclusión: Se puede concluir que el aprendizaje automático en SAC Kiaratel, SJL, 2022 está muy relacionado con las tecnologías de la información. bilateralmente a un nivel significativo del 0,14%, es decir, menos del 0,5%.

a) El Planteo de las Hipótesis Específicas 4.

Ho: "La prevención de los Ciberdelitos no relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022."

H1: "La prevención de los Ciberdelitos si relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022."

Tabla 11*Correlaciones de hipótesis específica 04*

Matriz de Correlaciones				
			Vi d4: PREVENCIÓN Y SANCIÓN DE LOS CIBERDELITOS	Vd.: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN
Rho de Spearman	Vi d4: PREVENCIÓN Y SANCIÓN DE LOS CIBERDELITOS	Coefficiente de correlación	1,000	0,856
		Sig. (bilateral)	.	0,014
		N	40	40
	Vd.: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coefficiente de correlación	0,856	1,000
		Sig. (bilateral)	0,014	.
		N	40	40

Nota: Se aplicó la prueba de Rho de Spearman con el programa Spss V23

Finalmente, existe una clara relación entre la prevención y sanción de delitos informáticos y el manejo de las tecnologías de la información con una confianza del 85,6%.

Conclusión: Se puede concluir que la prevención del ciberdelito en la empresa Kiaratel SAC, SJL, 2022 está muy relacionada con la tecnología. Es una tasa significativa del 0,14% bilateralmente, es decir menos del 0,5%.

4.2.3 Aplicación de la Estadística Descriptiva de las Variables

4.2.3.1 Variable Independiente: La Ciberseguridad.

Tabla 12

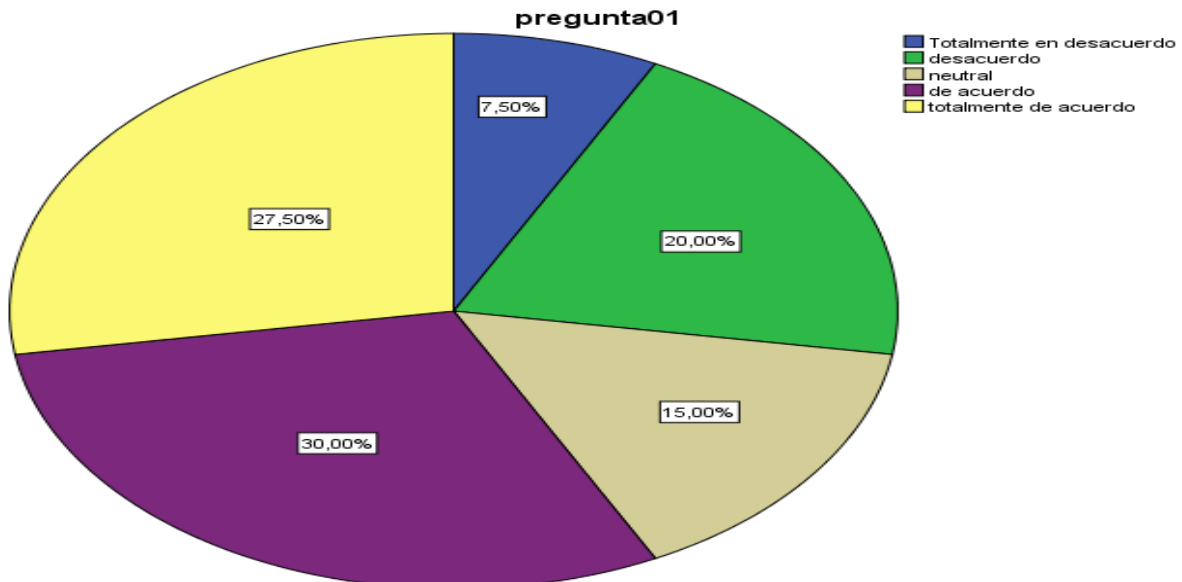
Cuadro de frecuencia de la pregunta ¿Cree que el centro de TI de su empresa tiene programas para aumentar la concienciación sobre las amenazas a la ciberseguridad?

		pregunta01			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	3	7,5	7,5	7,5
	desacuerdo neutral	8	20,0	20,0	27,5
	de acuerdo	6	15,0	15,0	42,5
	totalmente de acuerdo	12	30,0	30,0	72,5
		11	27,5	27,5	100,0
	Total	40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 2

Gráfico circular de la pregunta ¿Cree que el centro de TI de su empresa tiene programas para aumentar la concienciación sobre las amenazas a la ciberseguridad?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN:

De las 40 personas encuestadas, el 30% está de acuerdo con la pregunta: ¿Cree que el departamento de TI de su empresa tiene programas para reportar amenazas de ciberseguridad? El 7,50% dijo estar absolutamente en desacuerdo.

Tabla 13

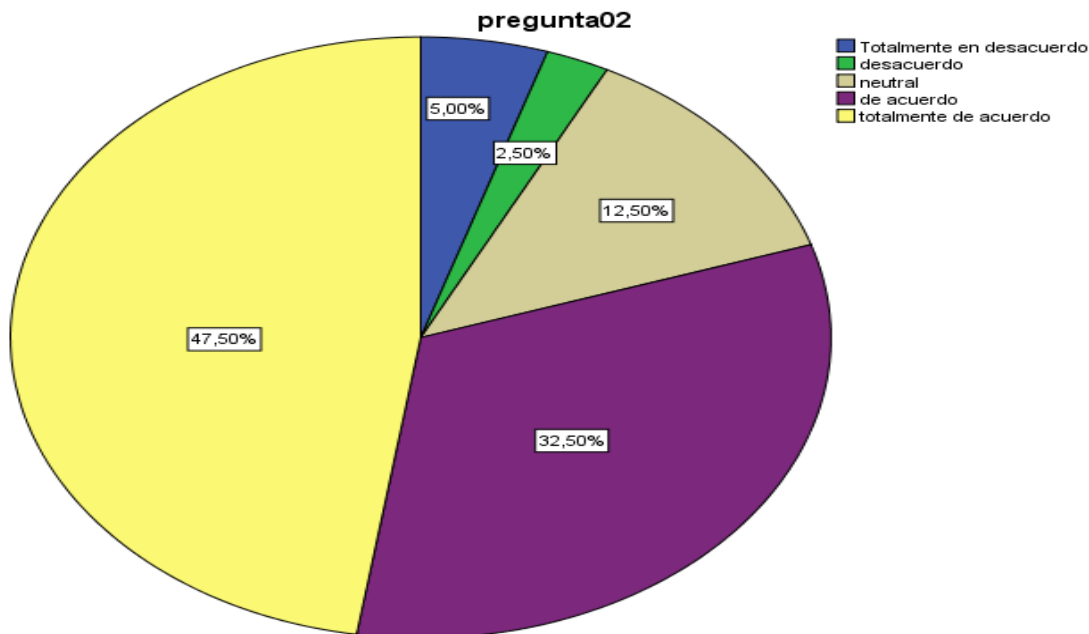
Cuadro de frecuencia de la pregunta ¿Está de acuerdo con la aplicación de un sistema de inventarios?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	5,0	5,0	5,0
	desacuerdo	1	2,5	2,5	7,5
	neutral	5	12,5	12,5	20,0
	de acuerdo	13	32,5	32,5	52,5
	totalmente de acuerdo	19	47,5	47,5	100,0
	Total	40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 3

Gráfico circular de la pregunta ¿Está de acuerdo con la aplicación de un sistema de inventarios?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN:

40 entrevistados el 47.50% expresaron totalmente de acuerdo a la interrogante: ¿Está de acuerdo en la aplicación de un sistema de inventarios? y el 2.50% dijeron desacuerdo.

Tabla 14

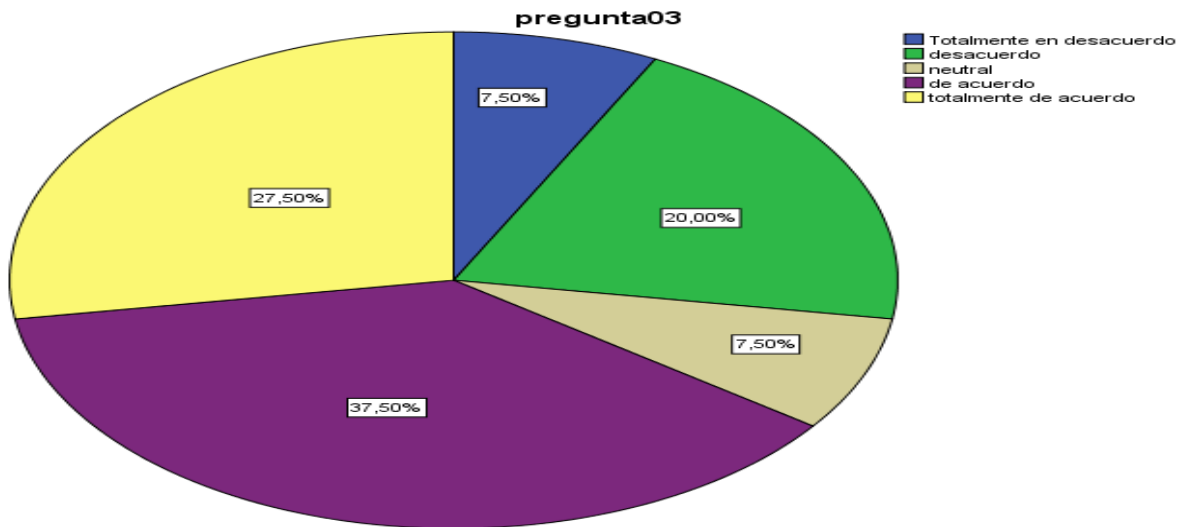
Cuadro de frecuencia de la pregunta ¿Cree que el centro de TI de su empresa mantiene suficientes copias de seguridad de los datos de su empresa?

		pregunta03			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	3	7,5	7,5	7,5
	desacuerdo	8	20,0	20,0	27,5
	neutral	3	7,5	7,5	35,0
	de acuerdo	15	37,5	37,5	72,5
	totalmente de acuerdo	11	27,5	27,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 4

Gráfico circular de la pregunta ¿Cree que el centro de TI de su empresa mantiene suficientes copias de seguridad de los datos de su empresa?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN:

De los 40 encuestados, el 37,50% aprobó la pregunta: ¿Cree que el centro de TI de la empresa almacena suficientes datos de respaldo de la información de la empresa? El 7,50% dijo estar totalmente en desacuerdo.

Tabla 15

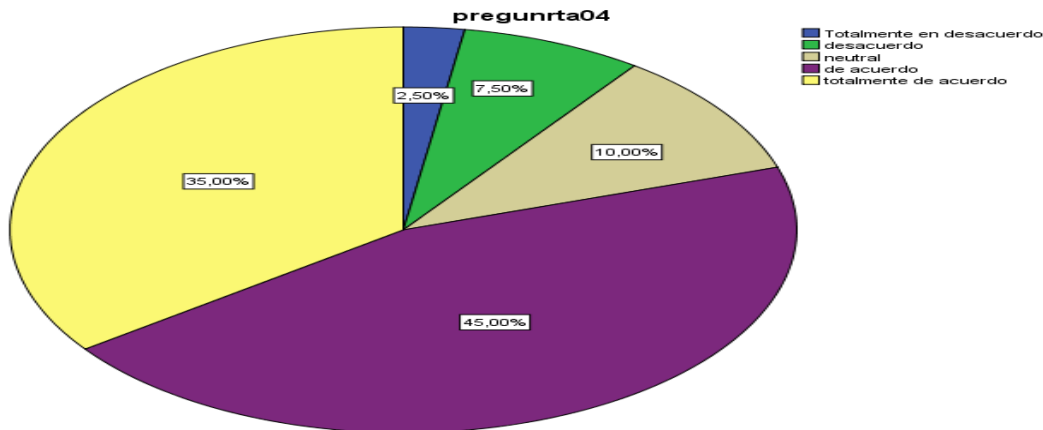
Cuadro de frecuencia de la pregunta ¿Cree que el centro de tecnología de la información de su empresa ha instalado suficiente software para proteger la información de su organización de las actividades ilegales de los ciberdelincuentes?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	2,5	2,5	2,5
	desacuerdo	3	7,5	7,5	10,0
	neutral	4	10,0	10,0	20,0
	de acuerdo	18	45,0	45,0	65,0
	totalmente de acuerdo	14	35,0	35,0	100,0
	Total	40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 5

Gráfico circular de la pregunta ¿Cree que el centro de tecnología de la información de su empresa ha instalado suficiente software para proteger la información de su organización de las actividades ilegales de los ciberdelincuentes?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN:

De los 40 encuestados, el 45 % respondió a la pregunta: ¿Cree que el entorno de TI de su empresa tiene suficiente software de seguridad para proteger la información empresarial de las actividades ilegales de los ciberdelincuentes? El 2,50% dijo no estar completamente satisfecho.

Tabla 16

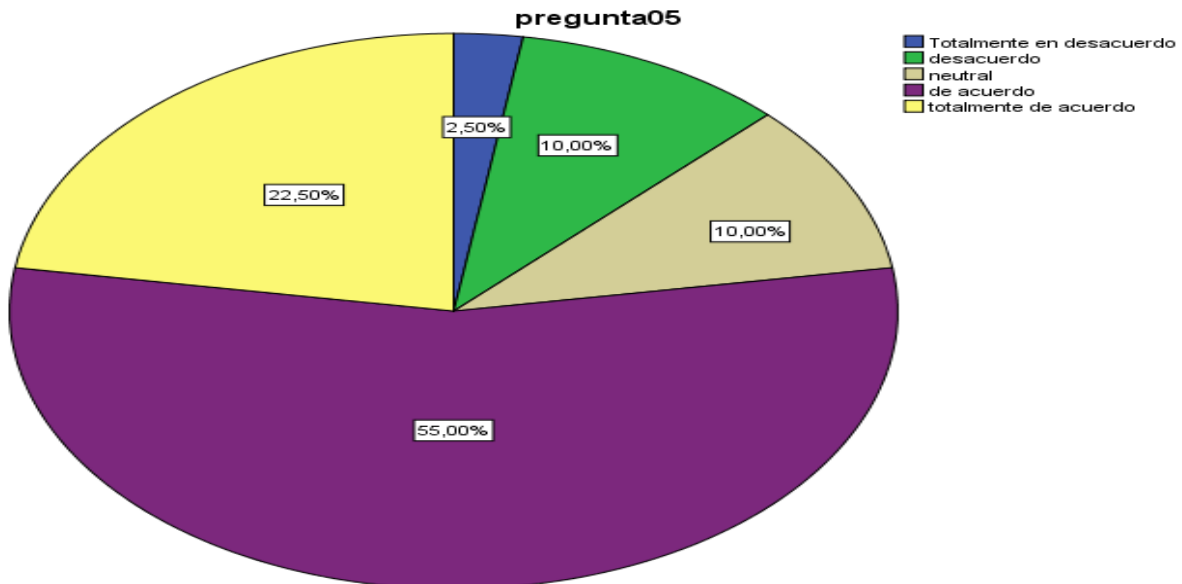
Cuadro de frecuencia de la pregunta ¿Cree que el entorno de TI de la empresa incluye medidas de seguridad física que evitan las actividades ilegales de los ciberdelincuentes?

		pregunta05			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	2,5	2,5	2,5
	desacuerdo	4	10,0	10,0	12,5
	neutral	4	10,0	10,0	22,5
	de acuerdo	22	55,0	55,0	77,5
	totalmente de acuerdo	9	22,5	22,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 6

Gráfico circular de la pregunta ¿Cree que el entorno de TI de la empresa incluye medidas de seguridad física que evitan las actividades ilegales de los ciberdelincuentes?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN:

De los 40 encuestados, el 55% respondió sí a la pregunta: ¿Cree que el entorno de TI de la empresa incluye medidas de seguridad física que previenen las actividades ilegales de los delincuentes? El 2,50% dijo estar totalmente en desacuerdo.

Tabla 17

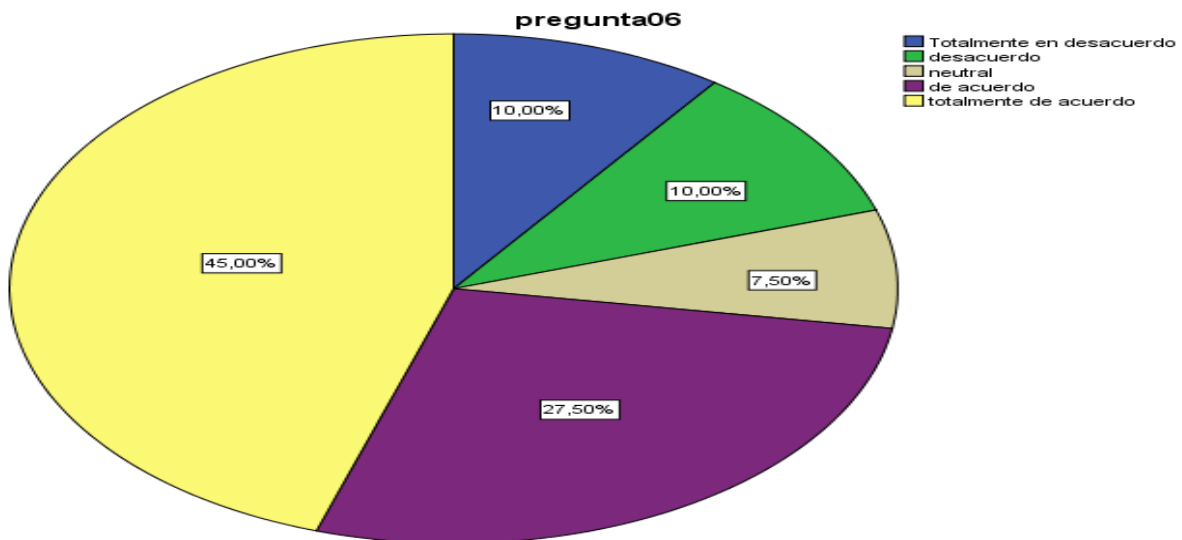
Cuadro de frecuencia de la pregunta ¿Cree que el entorno de TI de su empresa cuenta con programas de seguridad para protegerse contra los ciberdelincuentes?

		pregunta06			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	10,0	10,0	10,0
	desacuerdo	4	10,0	10,0	20,0
	neutral	3	7,5	7,5	27,5
	de acuerdo	11	27,5	27,5	55,0
	totalmente de acuerdo	18	45,0	45,0	100,0
	Total	40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 7

Gráfico circular de la pregunta ¿Cree que el entorno de TI de su empresa cuenta con programas de seguridad para protegerse contra los ciberdelincuentes?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN:

De los 40 encuestados, el 45% dijo estar muy de acuerdo con la pregunta: Muy de acuerdo con la pregunta: ¿Cree que el centro de TI de su empresa tiene planes de seguridad para protegerse contra los ciberdelincuentes? y el 10% dijo que nunca estuvo de acuerdo.

Tabla 18

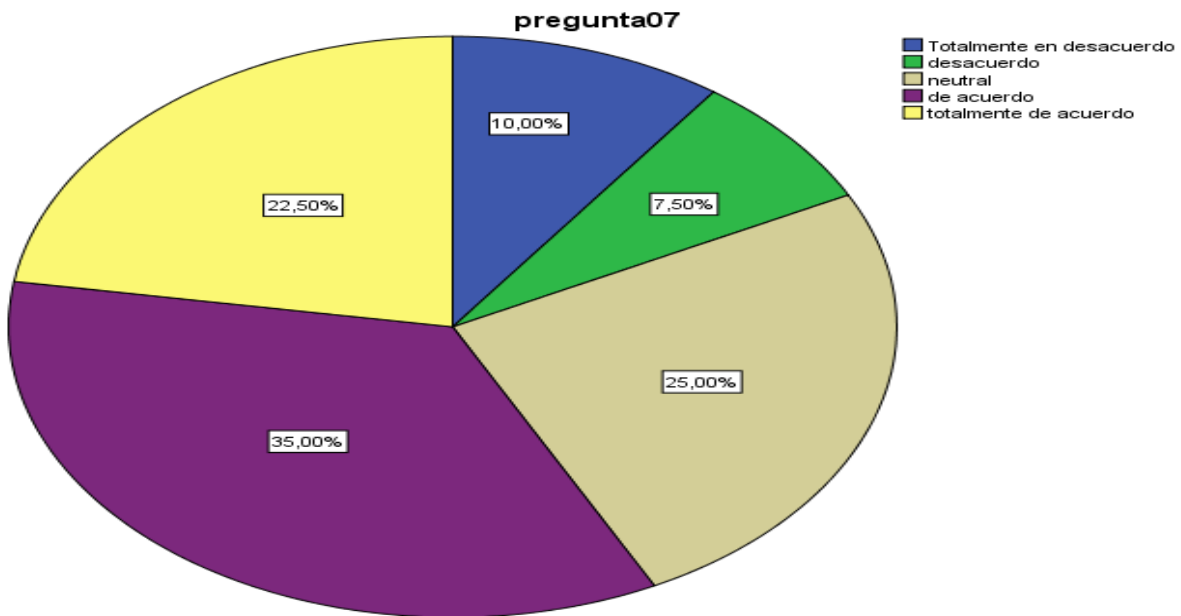
Cuadro de frecuencia de la pregunta ¿Sabe qué hacer cuando ve actividad delictiva cibernética en uno de los dispositivos de su líder empresarial?

		pregunta07			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	10,0	10,0	10,0
	desacuerdo	3	7,5	7,5	17,5
	neutral	10	25,0	25,0	42,5
	de acuerdo	14	35,0	35,0	77,5
	totalmente de acuerdo	9	22,5	22,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 8

Gráfico circular de la pregunta ¿Sabe qué hacer cuando ve actividad delictiva cibernética en uno de los dispositivos de su líder empresarial?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De los 40 encuestados, el 35 % respondió a la pregunta: ¿Sabe qué hacer cuando ve actividad delictiva cibernética en uno de sus dispositivos que más trabaja? y 10% totalmente en desacuerdo.

Tabla 19

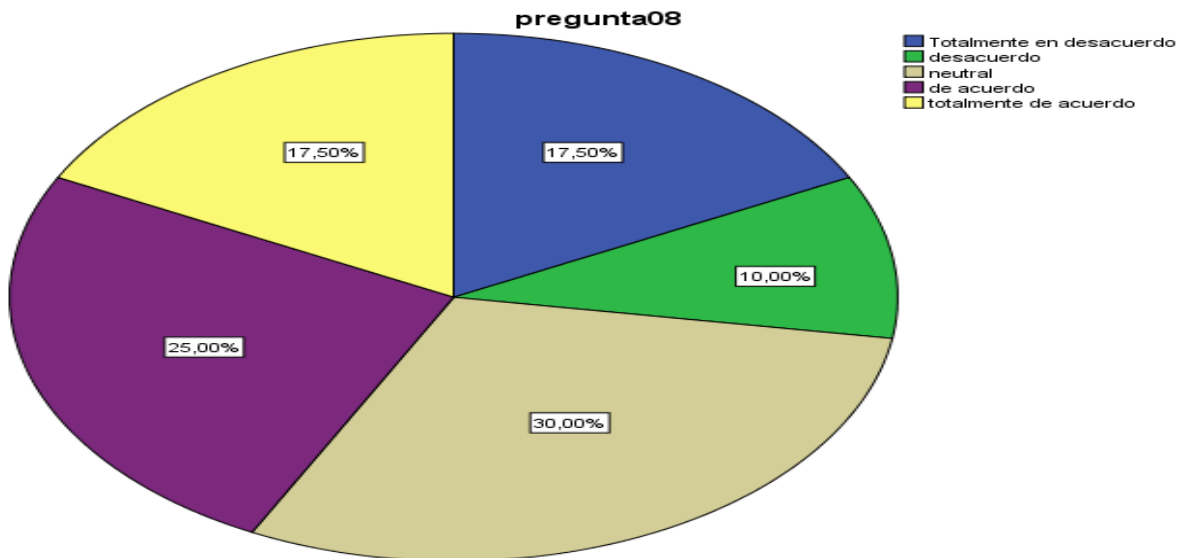
Cuadro de frecuencia de la pregunta ¿Cree usted que el área de TI de la empresa cuenta con personal calificado en ciberseguridad?

		pregunta08			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	7	17,5	17,5	17,5
	desacuerdo	4	10,0	10,0	27,5
	neutral	12	30,0	30,0	57,5
	de acuerdo	10	25,0	25,0	82,5
	totalmente de acuerdo	7	17,5	17,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 9

Gráfico circular de la pregunta ¿Cree usted que el área de TI de la empresa cuenta con personal calificado en ciberseguridad?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De los 40 encuestados, el 30% se declara neutral en esta pregunta: ¿Cree que la empresa cuenta con personal altamente cualificado en ciberseguridad en su centro de tecnologías de la información? y el 10 por ciento no estaba satisfecho.

Tabla 20

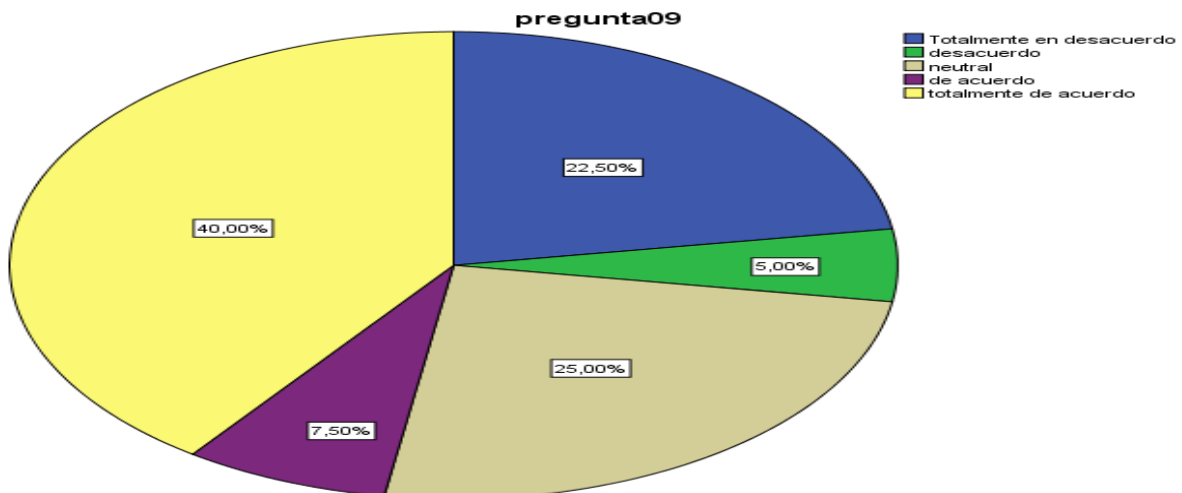
Cuadro de frecuencia de la pregunta ¿Cree usted que los sistemas de seguridad existentes por el área de TI de la empresa utilizan aplicación web que neutralizan los ataques de los ciberdelincuentes?

		pregunta09			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	9	22,5	22,5	22,5
	desacuerdo	2	5,0	5,0	27,5
	neutral	10	25,0	25,0	52,5
	de acuerdo	3	7,5	7,5	60,0
	totalmente de acuerdo	16	40,0	40,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 10

Gráfico circular de la pregunta ¿Cree usted que los sistemas de seguridad existentes por el área de TI de la empresa utilizan aplicación web que neutralizan los ataques de los ciberdelincuentes?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

El 40% de los 40 encuestados está muy de acuerdo con la pregunta: ¿Cree que los sistemas de seguridad existentes en el entorno de TI de la empresa reducirán los ataques cibernéticos mediante el uso de sitios web? y 7.50% aprueba.

Tabla 21

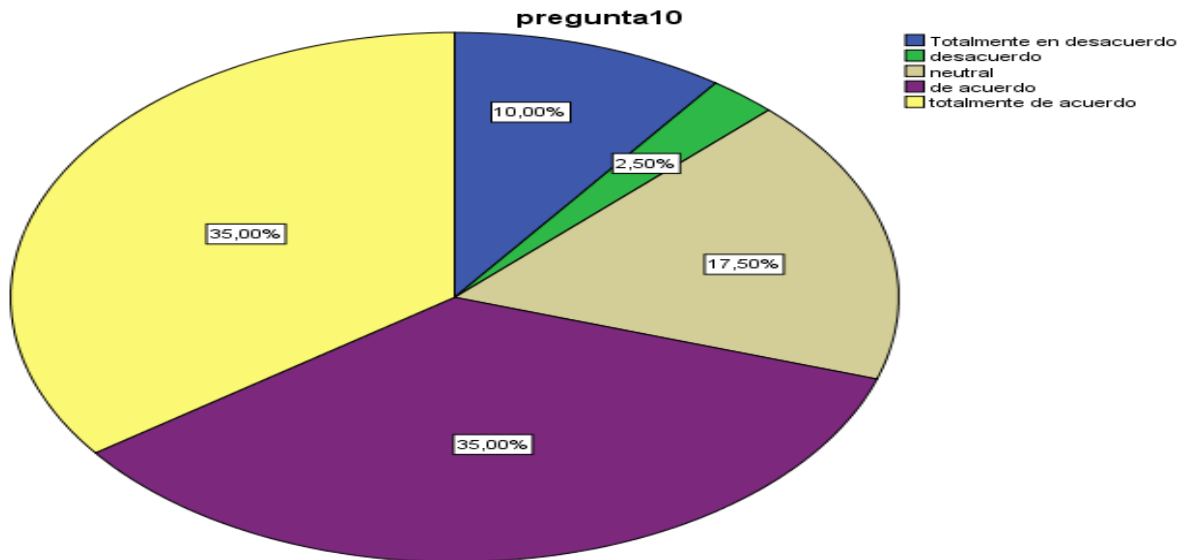
Cuadro de frecuencia de la pregunta ¿Alguna vez ha tenido que detener sus actividades debido a un ataque informático que no fue detectado y bloqueado por los sistemas de seguridad?

		pregunta10			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	10,0	10,0	10,0
	desacuerdo	1	2,5	2,5	12,5
	neutral	7	17,5	17,5	30,0
	de acuerdo	14	35,0	35,0	65,0
	totalmente de acuerdo	14	35,0	35,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 11

Gráfico circular de la pregunta *¿Alguna vez ha tenido que detener sus actividades debido a un ataque informático que no fue detectado y bloqueado por los sistemas de seguridad?*



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De las 40 personas encuestadas, el 35% está muy de acuerdo con la pregunta: *¿Ha tenido que dejar de trabajar por un ataque informático que fue detectado y eliminado por un sistema de seguridad?* y el 2,50 por ciento estaba insatisfecho.

Tabla 22

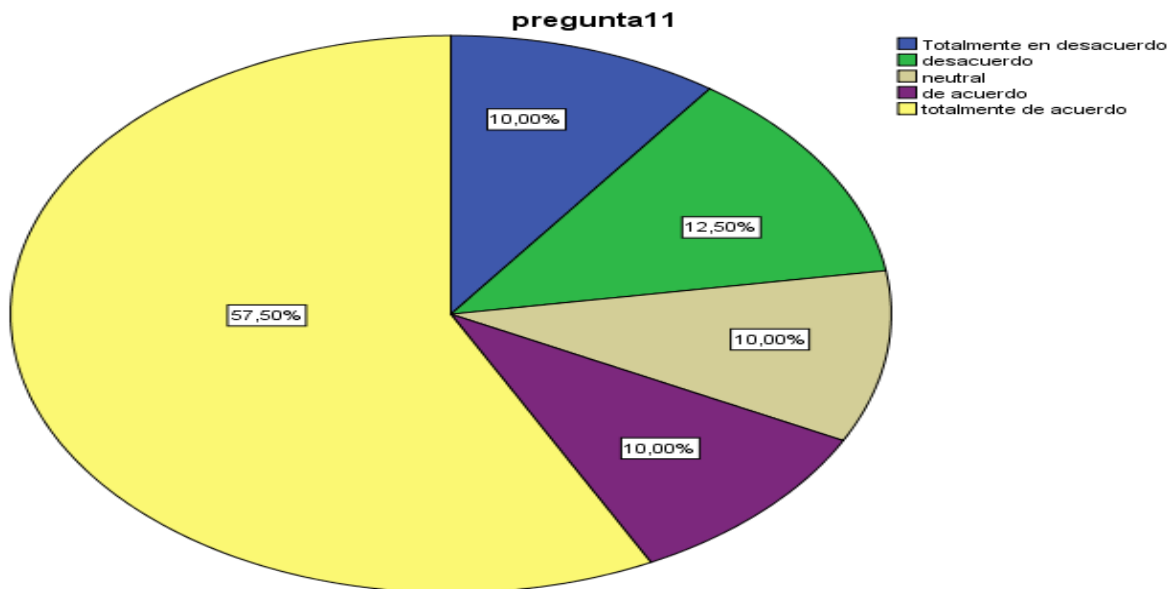
Cuadro de frecuencia de la pregunta *¿Crees que se perdieron datos importantes debido a un virus informático el año pasado?*

		pregunta11			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	10,0	10,0	10,0
	desacuerdo	5	12,5	12,5	22,5
	neutral	4	10,0	10,0	32,5
	de acuerdo	4	10,0	10,0	42,5
	totalmente de acuerdo	23	57,5	57,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 12

Gráfico circular de la pregunta *¿Crees que se perdieron datos importantes debido a un virus informático el año pasado?*



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

El 57,50% de los 40 encuestados está muy de acuerdo con la pregunta: *¿Cree que se perdió información importante por un virus informático en el último año?* y el 10% está de acuerdo.

Tabla 23

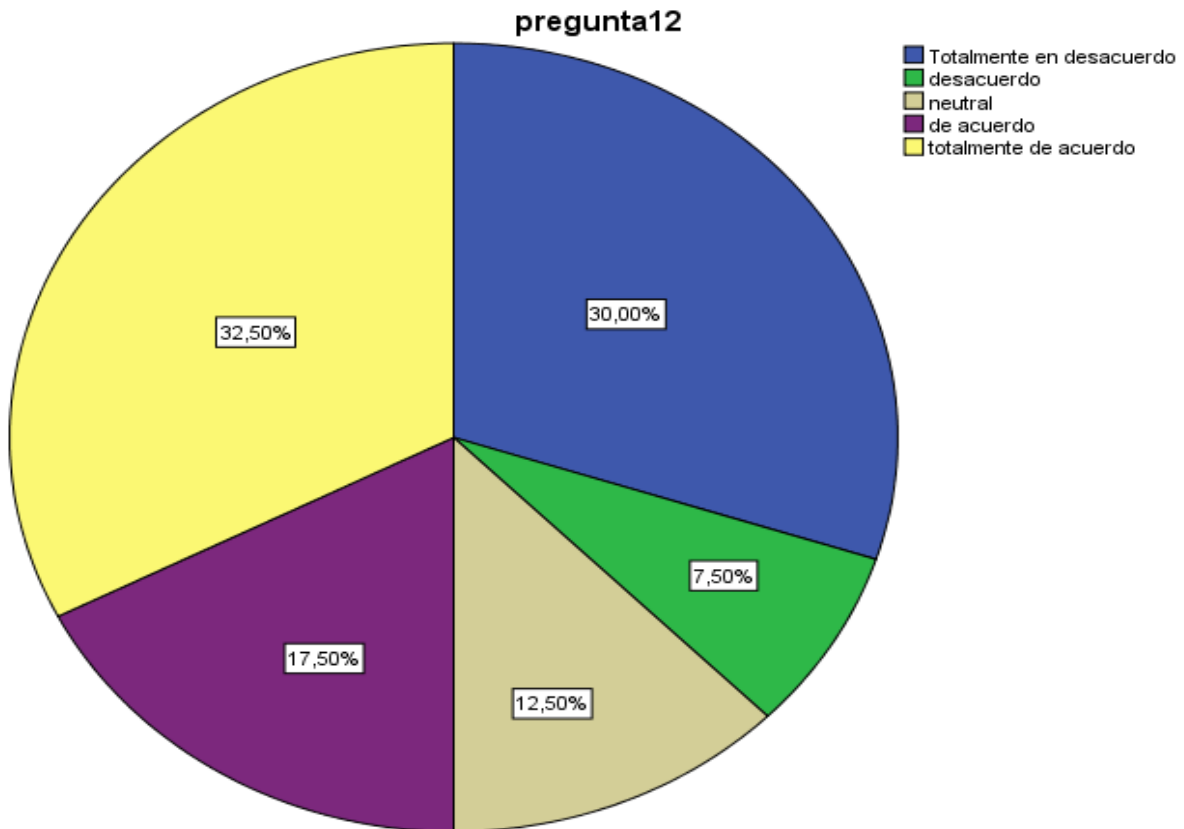
Cuadro de frecuencia de la pregunta *¿El centro de TI de su empresa lo ha capacitado en técnicas comunes utilizadas por los ciberdelincuentes?*

		pregunta12			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	12	30,0	30,0	30,0
	desacuerdo	3	7,5	7,5	37,5
	neutral	5	12,5	12,5	50,0
	de acuerdo	7	17,5	17,5	67,5
	totalmente de acuerdo	13	32,5	32,5	100,0
	Total	40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 13

Gráfico circular de la pregunta ¿El centro de TI de su empresa lo ha capacitado en técnicas comunes utilizadas por los ciberdelincuentes?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

El 32,50% de los 40 encuestados está muy de acuerdo con la pregunta: ¿El departamento de TI de su empresa le ha enseñado las técnicas más comunes que utilizan los delincuentes? y el 7,50 por ciento se mostró insatisfecho.

4.2.3.2 Variable Dependiente: La Gestión de Tecnologías de Información.

Tabla 24

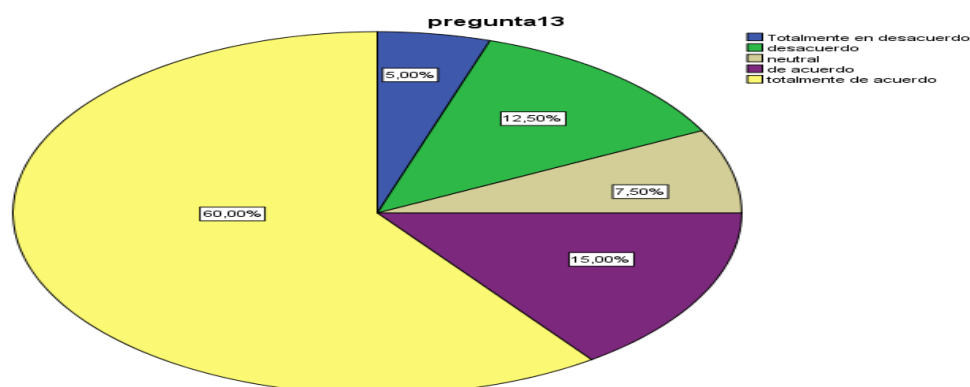
Cuadro de frecuencia de la pregunta ¿Cree que el departamento de tecnología de la información de la empresa tiene tiempo para capacitar a los empleados de la empresa en las prácticas de TI?

		pregunta13			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	5,0	5,0	5,0
	desacuerdo neutral	5	12,5	12,5	17,5
	de acuerdo	3	7,5	7,5	25,0
	totalmente de acuerdo	6	15,0	15,0	40,0
	Total	24	60,0	60,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 14

Gráfico circular de la pregunta ¿Cree que el departamento de tecnología de la información de la empresa tiene tiempo para capacitar a los empleados de la empresa en las prácticas de TI?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De los 40 encuestados, el 60% está muy de acuerdo con la pregunta: ¿Cree que el centro de tecnologías de la información de la empresa cuenta con programas periódicos de capacitación en TI para los empleados de la empresa? y el 5% totalmente de acuerdo.

Tabla 25

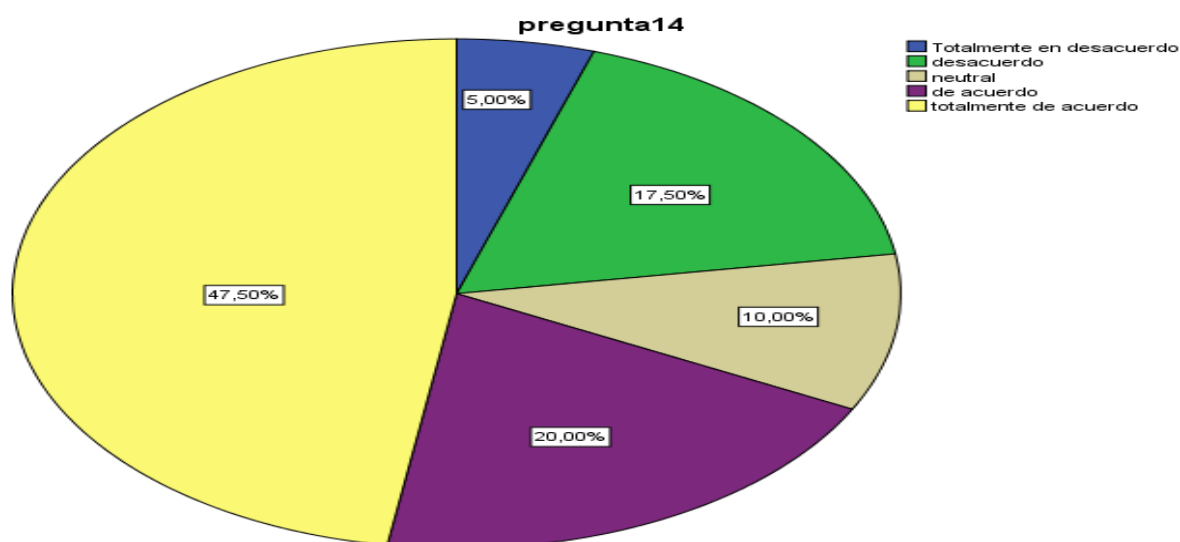
Cuadro de frecuencia de la pregunta ¿Está de acuerdo con la creación de tablas de almacenamiento del sistema?

		pregunta14			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	5,0	5,0	5,0
	desacuerdo	7	17,5	17,5	22,5
	neutral	4	10,0	10,0	32,5
	de acuerdo	8	20,0	20,0	52,5
	totalmente de acuerdo	19	47,5	47,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 15

Gráfico circular de la pregunta ¿Está de acuerdo con la creación de tablas de almacenamiento del sistema?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

El 47,50% de los 40 encuestados está muy de acuerdo con esta pregunta: ¿Está de acuerdo con el diseño de los paneles del sistema de seguridad? y el 5% totalmente de acuerdo.

Tabla 26

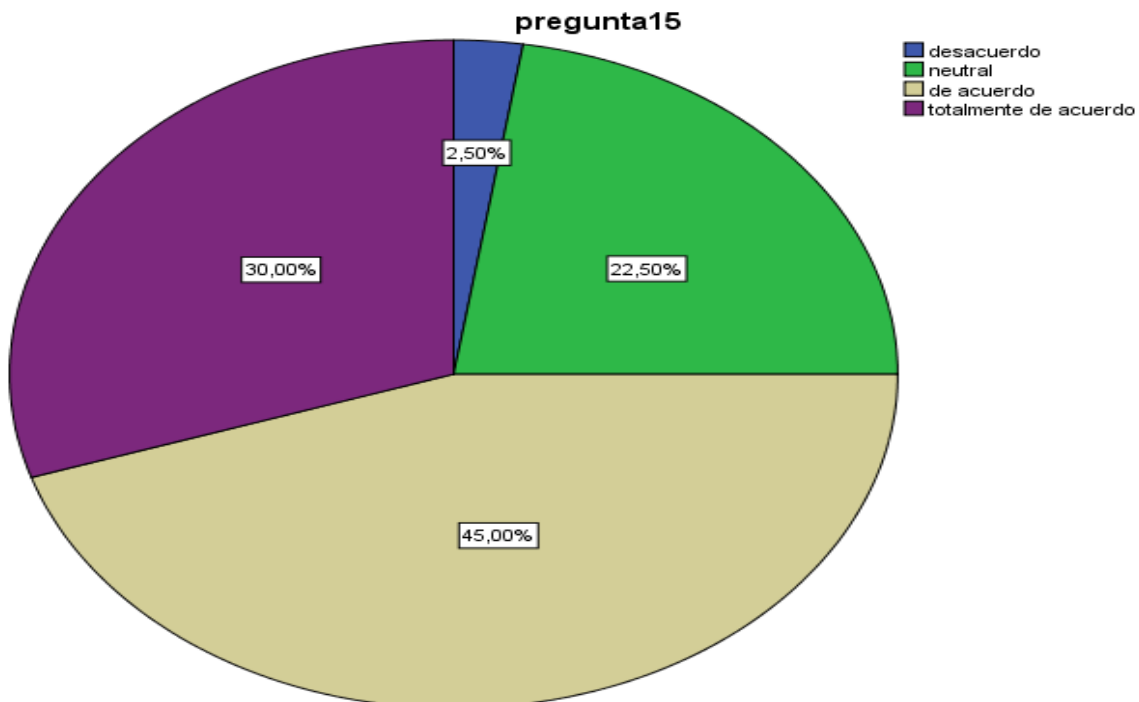
Cuadro de frecuencia de la pregunta ¿Considera usted que el área de TI de la empresa cumple una atención de incidencias de TI?

		pregunta15			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	desacuerdo	1	2,5	2,5	2,5
	neutral	9	22,5	22,5	25,0
	de acuerdo	18	45,0	45,0	70,0
	totalmente de acuerdo	12	30,0	30,0	100,0
	Total	40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 16

Gráfico circular de la pregunta ¿Considera usted que el área de TI de la empresa cumple una atención de incidencias de TI?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De los 40 encuestados, el 45% respondió a la pregunta: ¿Cree que el departamento de TI de la empresa realiza actividades de TI? y el 2,50 por ciento estaba insatisfecho.

Tabla 27

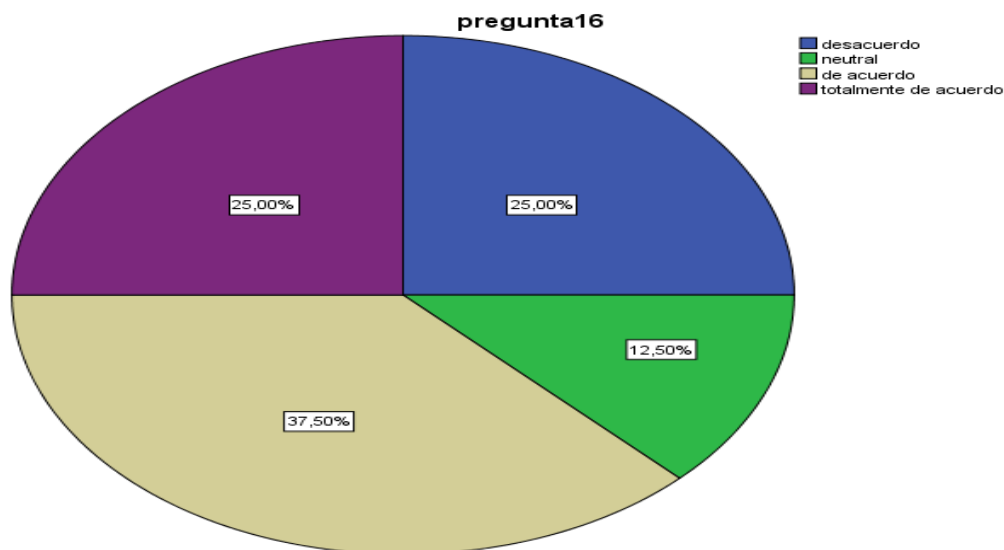
Cuadro de frecuencia de la pregunta ¿Cree usted que el área de TI de la empresa realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?

		pregunta16			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	desacuerdo	10	25,0	25,0	25,0
	neutral	5	12,5	12,5	37,5
	de acuerdo	15	37,5	37,5	75,0
	totalmente de acuerdo	10	25,0	25,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 17

Gráfico circular de la pregunta ¿Cree usted que el área de TI de la empresa realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

Con base en esta pregunta, el 35 % de los 40 encuestados dijo si: ¿Cree que el centro de TI de la empresa mueve el equipo de TI más importante a cualquier lugar dentro de la empresa? y el 12,50% dijo ser neutral.

Tabla 28

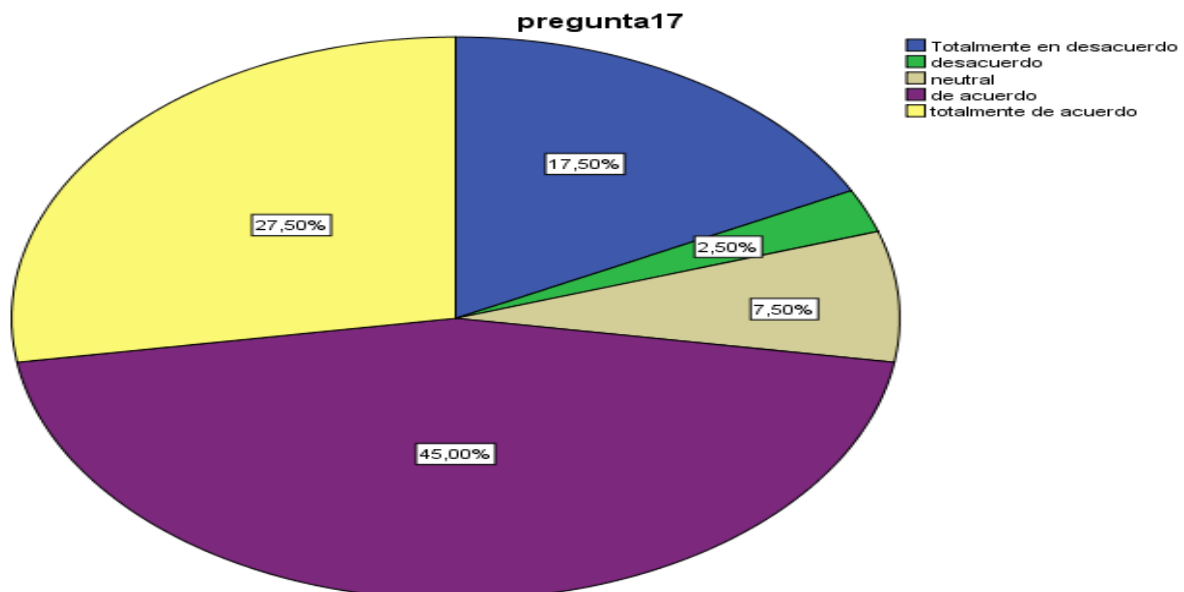
Cuadro de frecuencia de la pregunta ¿Qué tanto está de acuerdo con el lenguaje de C# para la aplicación en el sistema?

		pregunta17			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	7	17,5	17,5	17,5
	desacuerdo	1	2,5	2,5	20,0
	neutral	3	7,5	7,5	27,5
	de acuerdo	18	45,0	45,0	72,5
	totalmente de acuerdo	11	27,5	27,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 18

Gráfico circular de la pregunta ¿Qué tanto está de acuerdo con el lenguaje de C# para la aplicación en el sistema?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De los 40 encuestados, el 45 % respondió a la pregunta sí: ¿Qué tan satisfecho está con el lenguaje C# que se usará en el sistema? y el 2,50 por ciento estaba insatisfecho.

Tabla 29

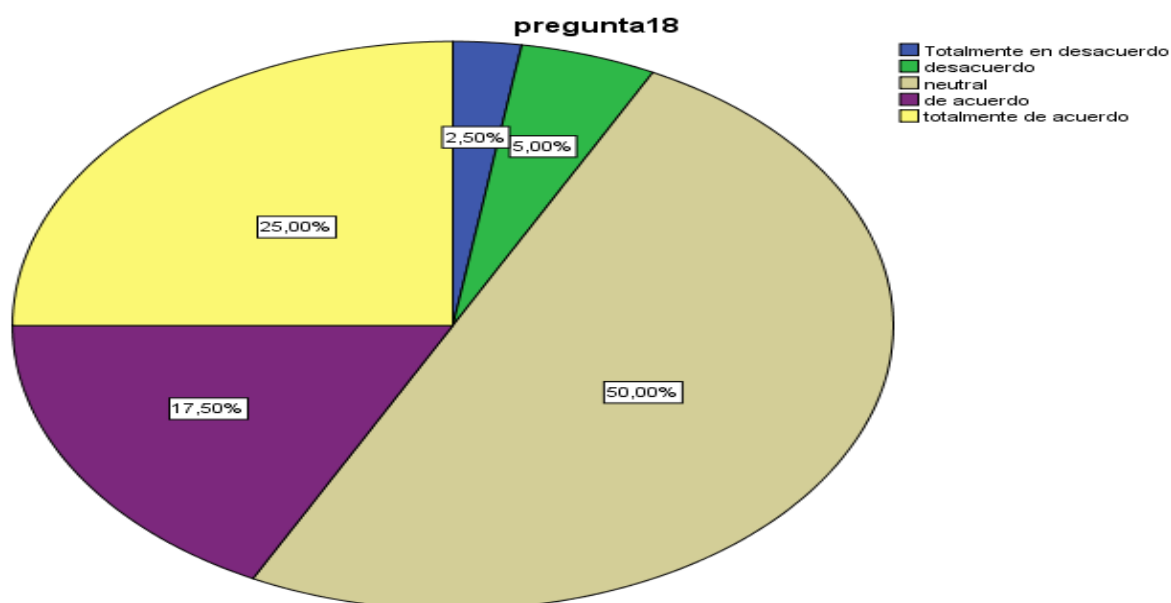
Cuadro de frecuencia de la pregunta ¿Qué tan conforme está usted con la seguridad del internet que cuenta la empresa?

		pregunta18			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	2,5	2,5	2,5
	desacuerdo	2	5,0	5,0	7,5
	neutral	20	50,0	50,0	57,5
	de acuerdo	7	17,5	17,5	75,0
	totalmente de acuerdo	10	25,0	25,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 19

Gráfico circular de la pregunta ¿Qué tan conforme está usted con la seguridad del internet que cuenta la empresa?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De los 40 que respondieron a la encuesta, el 50% dijo que era neutral en la siguiente pregunta: ¿Qué tan satisfecho está con la seguridad en Internet que brinda la empresa? El 2,50% dijo estar totalmente en desacuerdo.

Tabla 30

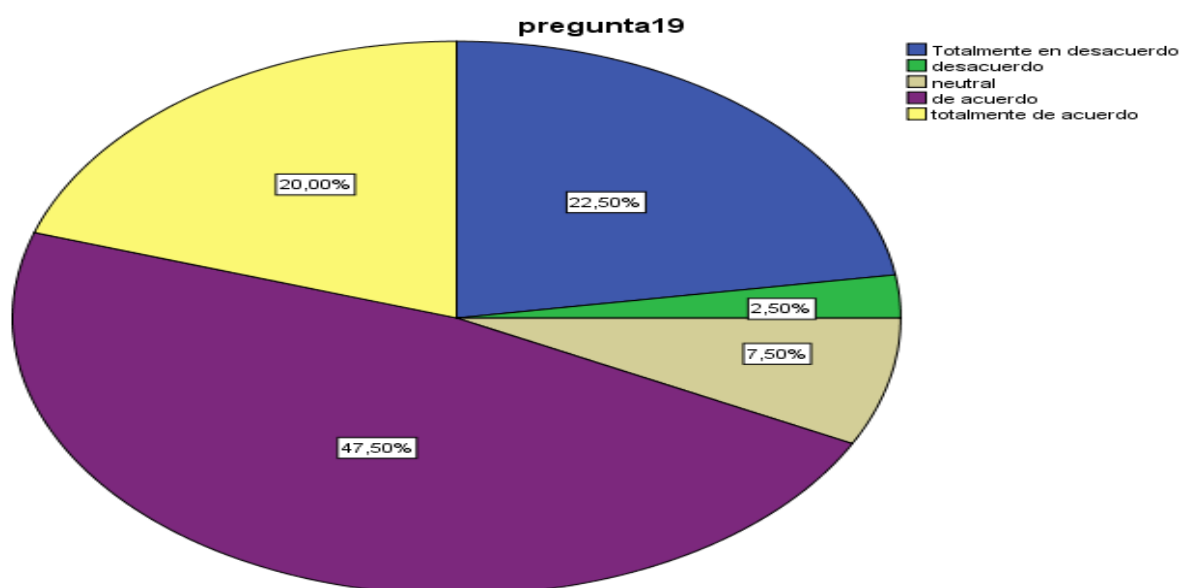
Cuadro de frecuencia de la pregunta ¿Ha recibido capacitación de parte del área de TI de la empresa respecto al uso adecuado de las tecnologías de la empresa?

		pregunta19			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	9	22,5	22,5	22,5
	desacuerdo	1	2,5	2,5	25,0
	neutral	3	7,5	7,5	32,5
	de acuerdo	19	47,5	47,5	80,0
	totalmente de acuerdo	8	20,0	20,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 20

Gráfico circular de la pregunta ¿Ha recibido capacitación de parte del área de TI de la empresa respecto al uso adecuado de las tecnologías de la empresa?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De los 40 encuestados, el 47,50% respondió a la pregunta si: ¿Ha recibido capacitación de la comunidad de TI de la empresa sobre el uso correcto de las tecnologías de la empresa? y el 2,50 por ciento estaba insatisfecho.

Tabla 31

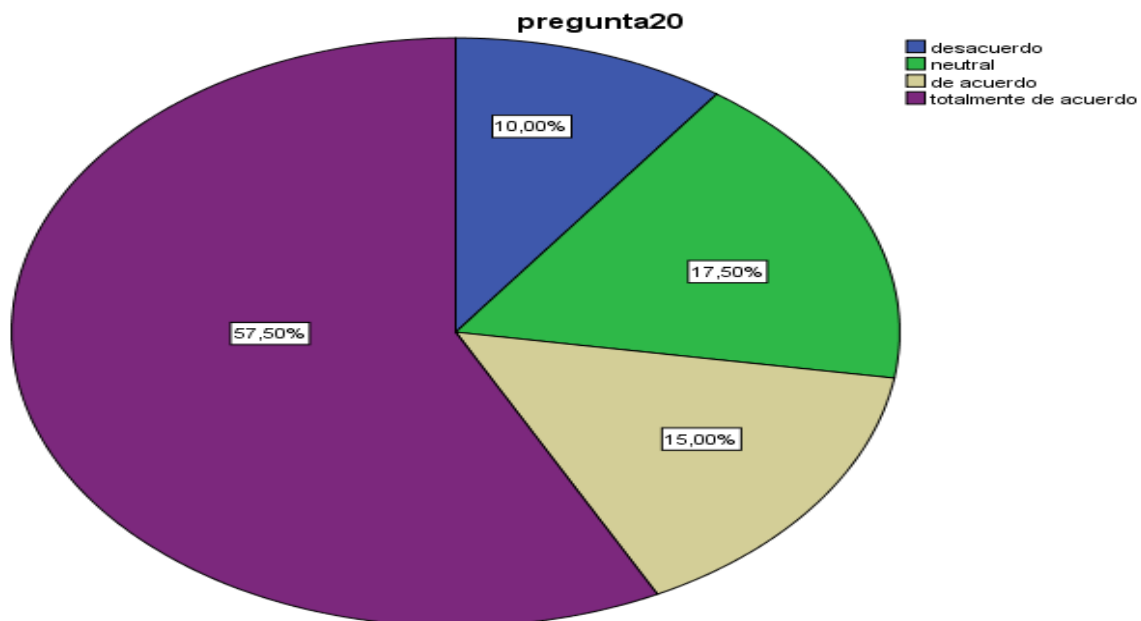
Cuadro de frecuencia de la pregunta ¿Considera que el acceso a la información de los sistemas de información es oportuno y seguro?

		pregunta20			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	desacuerdo	4	10,0	10,0	10,0
	neutral	7	17,5	17,5	27,5
	de acuerdo	6	15,0	15,0	42,5
	totalmente de acuerdo	23	57,5	57,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 21

Gráfico circular de la pregunta ¿Considera que el acceso a la información de los sistemas de información es oportuno y seguro?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

El 57,50% de los 40 participantes está totalmente de acuerdo con la siguiente pregunta: ¿Considera que el acceso a la información de los sistemas de información es oportuno y seguro? y el 10 por ciento no estaba satisfecho.

Tabla 32

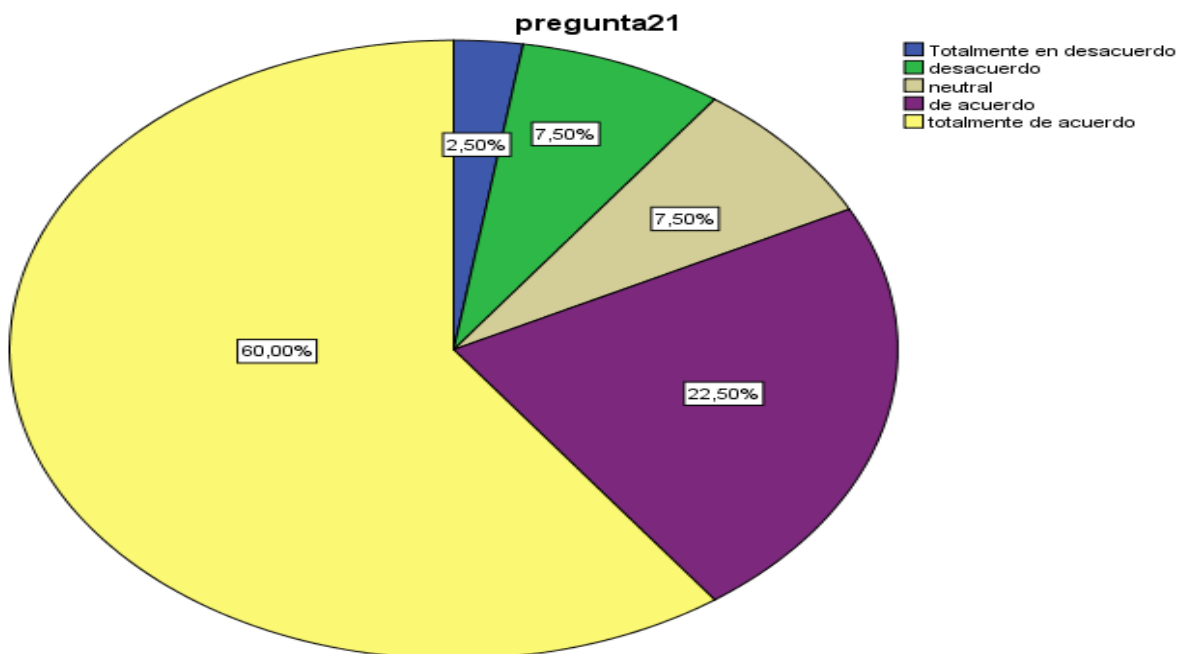
Cuadro de frecuencia de la pregunta ¿Crees que la dirección de la oficina de TI es correcta?

		pregunta21			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	2,5	2,5	2,5
	desacuerdo	3	7,5	7,5	10,0
	neutral	3	7,5	7,5	17,5
	de acuerdo	9	22,5	22,5	40,0
	totalmente de acuerdo	24	60,0	60,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 22

Gráfico circular de la pregunta ¿Crees que la dirección de la oficina de TI es correcta?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

El 60% de los 40 encuestados está totalmente de acuerdo con la pregunta: ¿Tiene una dirección adecuada para su oficina de TI? El 2,50% dijo estar totalmente en desacuerdo.

Tabla 33

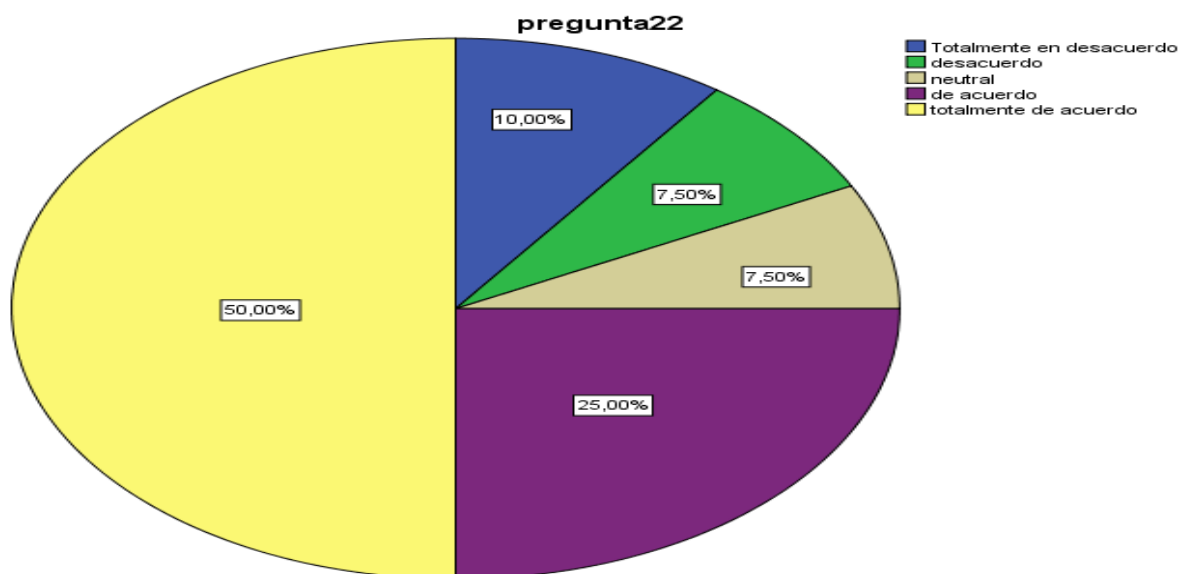
Cuadro de frecuencia de la pregunta ¿Cree usted que el área de TI de la empresa ayuda con las metas trazadas para el área de ventas de la empresa?

		pregunta22			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	4	10,0	10,0	10,0
	desacuerdo	3	7,5	7,5	17,5
	neutral	3	7,5	7,5	25,0
	de acuerdo	10	25,0	25,0	50,0
	totalmente de acuerdo	20	50,0	50,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 23

Gráfico circular de la pregunta ¿Cree usted que el área de TI de la empresa ayuda con las metas trazadas para el área de ventas de la empresa?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

El 50% de los 40 encuestados está totalmente de acuerdo con la pregunta: ¿Cree que el entorno de TI de la empresa es beneficioso para los objetivos de ventas de la empresa? y el 7,50 por ciento se mostró insatisfecho.

Tabla 34

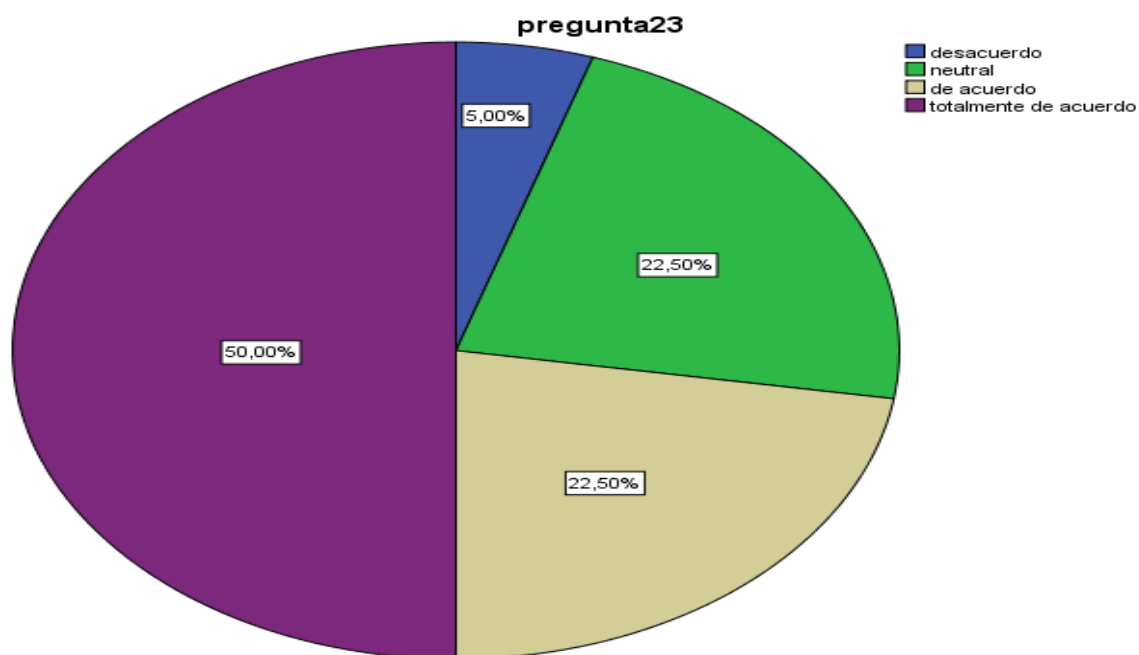
Cuadro de frecuencia de la pregunta ¿Cree que el entorno de TI de la empresa cumple con los requisitos tecnológicos de su sección?

		pregunta23			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	desacuerdo	2	5,0	5,0	5,0
	neutral	9	22,5	22,5	27,5
	de acuerdo	9	22,5	22,5	50,0
	totalmente de acuerdo	20	50,0	50,0	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 24

Gráfico circular de la pregunta ¿Cree que el entorno de TI de la empresa cumple con los requisitos tecnológicos de su sección?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De las 40 personas encuestadas, el 50% está muy de acuerdo con la pregunta: ¿Cree que el entorno de TI de la empresa satisface las necesidades tecnológicas de su comunidad? y el 5 por ciento estaba insatisfecho.

Tabla 35

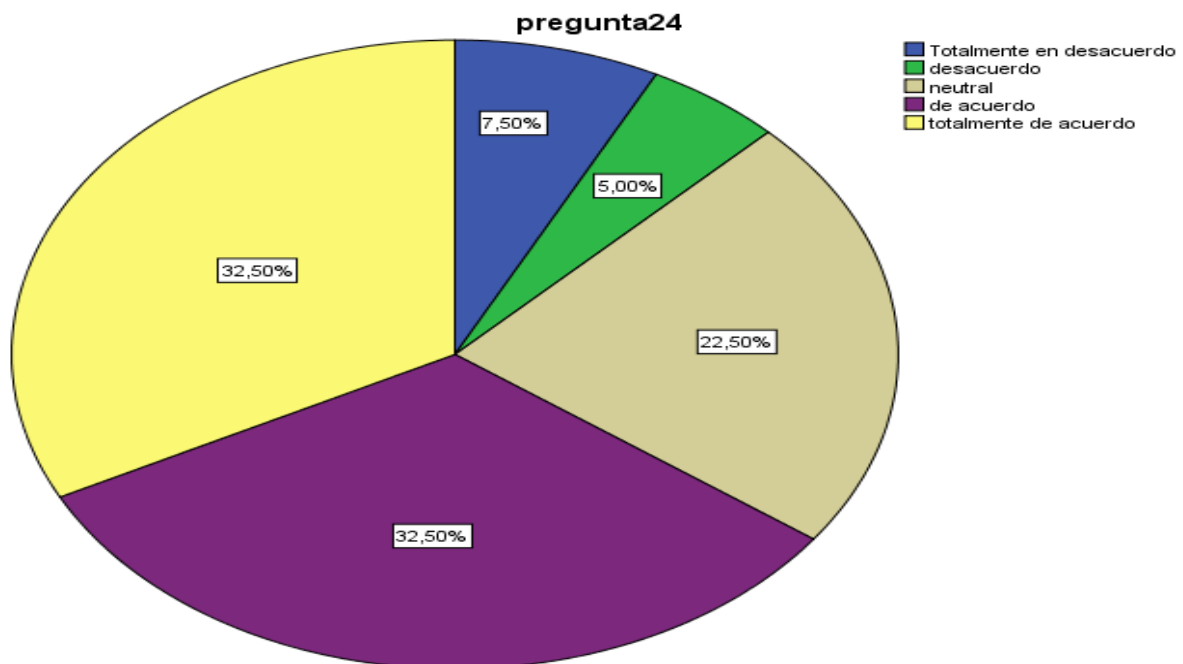
Cuadro de frecuencia de la pregunta ¿Está satisfecho con el nivel establecido por los profesionales del equipo de TI?

		pregunta24			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	3	7,5	7,5	7,5
	desacuerdo	2	5,0	5,0	12,5
	neutral	9	22,5	22,5	35,0
	de acuerdo	13	32,5	32,5	67,5
	totalmente de acuerdo	13	32,5	32,5	100,0
Total		40	100,0	100,0	

Nota: Elaboración propia de autor en spss V23

Gráfico 25

Gráfico circular de la pregunta ¿Está satisfecho con el nivel establecido por los profesionales del equipo de TI?



Nota: Elaboración propia de autor en spss V23

INTERPRETACIÓN

De los 40 que respondieron a la encuesta, el 35 por ciento dijo estar totalmente de acuerdo con la pregunta: ¿Está satisfecho con el nivel de experiencia que ha demostrado su equipo de TI? y el 5 por ciento estaba insatisfecho.

Capítulo V Sugerencias

5.1 Recomendaciones

Recomendación general: Las empresas necesitarán invertir en la seguridad de sus datos para almacenar los datos de manera interna y externa segura. El objetivo principal es contemplar la información después de sufrir un ataque cibernético.

Recomendación específica 01: Proporcionar una base sólida para la relación entre las operaciones de ciberseguridad y las tecnologías de gestión de la información en Kiaratel SAC. Desde el área de SJL se recomienda al director realizar un programa de capacitación anual al personal de todas las industrias para brindar conocimientos técnicos y capacitación interna al centro TIC y al personal técnico; Estas capacitaciones deben planificarse y realizarse con prudencia para mantener y lograr buenos resultados en la empresa.

Recomendación específica 02: La estrategia de gestión de la empresa depende de muchos factores técnicos y humanos y de las normas que la rigen. Es importante tener una política de seguridad cibernética para cada industria para garantizar el cumplimiento de todas las empresas. más gestión que cualquier trabajador comunitario.

Recomendación específica 03: El centro de operaciones de seguridad debe trabajar con políticas de seguridad e implementar todas las medidas tecnológicas, como el uso de aprendizaje automático, y comprometerse a corregir rápidamente los parches de seguridad si se encuentran nuevas vulnerabilidades en el código de desarrollo utilizado.

Recomendación específica 04: Asimismo, realizar auditorías internas y externas para determinar la prevención de delitos cibernéticos en caso de detectarse.

5.2 Conclusiones

Conclusión general: Se ve que existe una fuerte relación entre la ciberseguridad y el gobierno de TI con un nivel de confianza del 82,5%. En este sentido, la ciberseguridad y las tecnologías de la información contribuyen al desarrollo de diversas actividades, haciéndolas dinámicas y accesibles para muchos. Por tanto, se afirma que el desarrollo de las TIC está íntimamente ligado al desarrollo de la economía digital, lo que afecta directamente a la forma tradicional de hacer negocios.

Conclusión específica 01: Se observa que existe una clara relación entre el tiempo de vida de la ciberseguridad y el tiempo de vida de las tecnologías de gestión de la información, con un nivel de confianza del 84,5%. En base a esto, se concluye que la capacidad de ciberseguridad es un factor importante en la creación de valor de la empresa mediante la adopción del marco NIST para mejorar la ciberseguridad en la infraestructura.

Conclusión específica 02: Se aprecia que existe una clara relación entre la seguridad informática y las habilidades de gestión de la información con un nivel de confianza del 84,2%. Por lo tanto, se concluye que existe una completa gestión de riesgos de seguridad de la información que crea estrategias de prevención y control para toda la empresa, aumentando así la confianza de todos los stakeholders (Comité, dueños del sistema y clientes).

Conclusión específica 03: Se ve que existe una clara relación con un 85,6% de confianza entre la ciberseguridad y la gestión de la ciencia de datos y tecnologías de la información. En base a esto, concluí que el uso del aprendizaje automático de ciberseguridad permite la concientización de los empleados para proteger la información de la empresa y de sus clientes.

Conclusión específica 04: Se ve que existe una clara relación con un 85,6% de confianza entre la prevención y sanción del ciberdelito y la gestión de la información. En base a estos resultados, concluyo que la prevención del cibercrimen identifica y clasifica todas las acciones, servicios y métodos de seguridad que necesita una empresa para proteger su ciberespacio, reduciendo el riesgo disruptivo de los hackers.

5.3 Bibliografía

Albiol, J., & Lloveras, J. (2019). PROYECTOS DE INNOVACIÓN A TRAVÉS DE ROADMAPS. *XIII CONGRESO INTERNACIONAL DE INGENIERÍA DE PROYECTOS*.

Ariel. (2016). *CIBERSEGURIDAD, LA PROTECCIÓN DE LA INFORMACIÓN EN UN MUNDO DIGITAL*. Lima: Editorial Ariel. doi:978-84-08-16304-6

Ayala, E., & Gonzales, S. (2015). *Tecnologías de la Información y la Comunicación*. Lima: Fondo Editorial de la UIGV.

Ayala, E., & Gonzales, S. (2015). *Tecnologías de la Información y la Comunicación*. Lima: Fondo Editorial de la UIGV.

Barboza, A., & Alvarado, A. (2010). *Ciberseguridad en Costa Rica*. Costa Rica: Impresión Gráfica del Este S.A.

Caamaño, E., & Gil, R. (2020). Prevención de riesgos por ciberseguridad desde la auditoría forense: conjugando el talento humano organizacional. *NOVUM*, 61-80. doi: 0121-5698

- Camilo, C., García, M., Osorio, J., & Navarro, A. (2018). *Ciberseguridad: un enfoque desde la ciencia de datos*. Colombia: Universidad Icesi. doi:978-958-8936-55-0
- Camilo, C., García, M., Osorio, J., & Navarro, A. (2018). *Ciberseguridad: un enfoque desde la ciencia de datos*. Colombia: Universidad Icesi.
- Casanovas, I. (2014). *Tecnologías de la información y las comunicaciones aplicadas a la administración y gestión editorial*. Buenos aires: Editorial de la Facultad de Filosofía y Letras. doi:978-987-3617-17-1
- Castellanos, O. (2007). *Gestión Tecnológica: de un enfoque tradicional a la inteligencia*. Colombia: GESTIÓN TECNOLÓGICA. doi:958-701-685-8
- castillo, o. (2007). *Gestión Tecnológica: de un enfoque tradicional a la inteligencia*. Colombia: GESTIÓN TECNOLÓGICA.
- Colón, E., & Cuenca, H. (2014). Cómo responder a un delito informático. *Revista Ciencia Unemi*, 43-50.
- Correa, J., Carlos, H., & Velarde, A. (2006). Virus informáticos. *Conciencia Tecnológica*, 54-57.
- del Cid, A., Méndez, R., & Sandoval, F. (2011). *investigacion fundamentos de la investigación*. méxico: PEARSON EDUCACIÓN,. doi:978-607-442-705-9
- Del Cid, A., Méndez, R., & Sandoval, F. (2011). *Investigación fundamentos y metodología*. México : Pearson educación. doi:978-607-442-705-9
- Gómez, I. (2015). Gamificación como recurso de la ingeniería en comunicación social. *Razón y Palabra*.

- Gómez, M. (2006). *Introducción a la metodología de la investigación científica*. Argentina: Editorial Brujas. doi:987-591-026-0
- Hernández, R., Fernández, C., & Baptista, M. d. (2010). *Metodología de la investigación*. México: Mcgraw-hill. doi:978-607-15-0291-9
- Hernández, R., Fernández, C., & Baptista, M. D. (2014). *Metodología de la investigación*. Mcgraw-hill. doi:978-1-4562-2396-0
- Hurtado, F. (2018). *Gestión logística*. Perú: Fondo editorial de la universidad inca garcilaso de la vega. doi:978-612-4340-15-4
- Izar, J., & Ynzunza, C. (2017). El impacto del crédito y la cobranza en las utilidades. *Universidad Tecnológica de Querétaro*, 42-56.
- Lapiedra, R., Devece, C., & Guiral, J. (2011). *Introducción a la gestión de los sistemas de información en las empresas*. España: universidad jaumet. doi:978-84-693-9894-4
- Lapiedra, R., Devece, C., & Guiral, J. (2011). *Introducción a la gestión de sistemas de información en la empresa*. España: Universitat Jaume I. doi:978-84-693-9894-4
- Morillo, R. (2003). Infraestructura tecnológica de vigilancia remota. *Télématique*, 8-16.
- Niño, v. (2011). *metodología de la investigación*. bogotá: ediciones de la U. doi:978-958-8675-94-7
- Niño, V. (2011). *Metodología de la investigación*. Colombia: Ediciones de la u. doi:978-958-8675-94-7

- Nogales, R. (2007). Cambio de concepto de Compras a Cadena de Suministros. *Ciencias Holguín*, 1-22.
- Nolasco, P., & Ojeda, M. (2016). La evaluación de la integración de las TIC en la educación superior: fundamento para una metodología. *RED. Revista de Educación a Distancia*, 1-24.
- Pons, V. (2017). Internet, la nueva era del delito: cibercrimen, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, 80-93.
- Quintero, J. (2013). El uso del valor contable en la gerencia de las PyMES venezolanas. *Revista del Centro de Investigación. Universidad La Salle*, 5-22.
- Quintero, J., & Sánchez, J. (2006). La cadena de valor: Una herramienta del pensamiento estratégico. *Telos*, 377-389.
- Rocha, C. (2011). La Seguridad Informática. *Revista Ciencia Unemi*, 26-33.
- Romero, J. (2018). CONCEPTUALIZACIÓN DE UNA ESTRATEGIA DE CIBERSEGURIDAD PARA LA SEGURIDAD NACIONAL DE MÉXICO. *Revista Internacional de Ciencias Sociales y Humanidades*, 2-25.
- Romero, m. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. Madrid: 3 ciencias.
- Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. ecuador: 3ciencias. doi:978-84-949306-1-4
- Sáinz, R. (2016). *Ciberseguridad, la protección de la información en un mundo digital*. Lima: Editorial Ariel. doi:978-84-08-16304-6

- Sánchez, H., Reyes, C., & Mejía, K. (2018). *Manual de términos en investigación científica, tecnológica y humanística*. lima: universidad Ricardo Palma. doi:978-612-47351-4-1
- Solís, F., Pinto, D., & Solís, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA. *Enfoque UTE*, 160-171.
- Tricoci, G., Corral, P., & Oriolo, M. (2020). Patrones de conducta de las pymes argentinas respecto de las inversiones en TIC. *Tricoci, Guillermo; Corral, Pablo; Oriolo, María*.
- Urbina, A., & de la Calleja, J. (2017). Brief Review of Educational Applications Using Data Mining and Machine Learning. *REDIE. Revista Electrónica de Investigación Educativa*, 84-96.
- Urcuqui, C., García, M., Osorio, J., & Navarro, A. (2018). *Ciberseguridad: un enfoque desde la ciencia de datos*. Colombia: Machine learning. doi:978-958-8936-55-0
- Urretavizcaya, M. (2001). Sistemas inteligentes en el ámbito de la educación. *Inteligencia Artificial. Revista Iberoamericana de Inteligencia Artificial*, 8-12.
- Vargas, R., Recalde, L., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO*, 31-45. doi:http://dx.doi.org/10.17141/urvio.20.2017.2571
- Zevallos, M. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Peruana de Computación y Sistemas*, 43-60. doi:2617-2003

Zunino, A., Berdún, L., & Amandi, A. (2001). JavaLog: un Lenguaje para la Programación de Agentes. *Inteligencia Artificial. Revista Iberoamericana de Inteligencia Artificial*, 94-99.

Zuñá, E., Arce, Á., Romero, W., & Soledispa, C. (2019). ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS PYMES DE LA CIUDAD DE MILAGRO. *UNIVERSIDAD Y SOCIEDAD*, 487-492. doi:2218-3620

Anexos

Anexo 01: Matriz de Consistencia

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS PRINCIPAL	VARIABLES	DISEÑO METODOLÓGICO
¿De qué manera la ciberseguridad se relacionará con la gestión de tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022?	Determinar la relación entre la ciberseguridad y la gestión de tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.	La ciberseguridad si relaciona significativamente con la gestión de tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.	VARIABLE INDEPENDIENTE: LA CIBERSEGURIDAD Según los autores (Camilo, García, Osorio, & Navarro, 2018) Nos describe: "La ciberseguridad es el área de las ciencias de la computación encargada del desarrollo y la implementación de los mecanismos de protección de la información y de la infraestructura tecnológica" (p.25). VARIABLE DEPENDIENTE: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Según los autores (Ayala & Gonzales, 2015) Nos argumentan: "Las Tecnologías de la Información y la Comunicación (TIC) se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones. Es el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido, video)." (p.27).	TIPO DE INVESTIGACIÓN: CORRELACIONAL Según (Hernández, 2014) nos dice: "La investigación correlacional es un tipo de método de investigación no experimental en el cual un investigador mide dos variables. Entiende y evalúa la relación estadística entre ellas sin influencia de ninguna variable extraña". DESCRIPTIVA Según (Niño, 2011) nos dice: "Su propósito es describir la realidad objeto de estudio, un aspecto de ella, sus partes, sus clases, sus categorías o las relaciones que se pueden establecer entre varios objetos, con el fin de esclarecer una verdad, corroborar un enunciado o comprobar una hipótesis" (p. 34). MÉTODO DE INVESTIGACIÓN: Enfoque cuantitativo Según el autor (Niño, 2011) Nos argumenta: "Como la palabra lo indica, la investigación cuantitativa tiene que ver con la "cantidad" y, por tanto, su medio principal es la medición y el cálculo. En general, busca medir variables con referencia a magnitudes" (p.29). DISEÑO DE INVESTIGACIÓN: No experimental Según los autores (Hernández, Fernández, & Baptista, 2010) Nos dicen: "En la investigación no experimental las variables independientes ocurren y no es posible manipularlas, no se tiene control directo sobre dichas variables ni se puede influir sobre ellas, porque ya sucedieron, al igual que sus efectos" (p.149). ÁREA DE ESTUDIO: Empresa KIARATEL S.A.C. POBLACIÓN Y MUESTRA: Población: 100 trabajadores de la empresa KIARATEL S.A.C. Muestra: 40 trabajadores de la empresa KIARATEL S.A.C. Instrumentos: Encuesta. Cuestionario.
PROBLEMAS ESPECÍFICOS	OBJETIVOS ESPECÍFICOS	HIPÓTESIS ESPECÍFICOS		
¿Cómo se relaciona la eficiencia de la ciberseguridad y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022?	Determinar la relación entre la eficiencia de la ciberseguridad y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.	La eficiencia de la ciberseguridad si relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.		
¿Cómo se relaciona el mecanismo preventivo, correctivo y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022?	Determinar la relación entre el mecanismo preventivo, correctivo y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.	El mecanismo preventivo, correctivo si relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.		
¿Cómo se relaciona el machine learning y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022?	Determinar la relación entre el machine learning y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.	El machine learning si relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.		
¿Cómo se relaciona la prevención los Ciberdelitos y las tecnologías de la información con en la empresa KIARATEL SAC, SJL, 2022?	Determinar la relación entre la prevención de los Ciberdelitos y las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.	La prevención de los Ciberdelitos si relaciona significativamente con las tecnologías de la información en la empresa KIARATEL SAC, SJL, 2022.		

Anexo 02: Matriz de Operacionalización de Variables

VARIABLES	DIMENSIONES	INDICADORES	PREGUNTA	ESCALA DE MEDICIÓN	INSTRUMENTO	
VARIABLE INDEPENDIENTE VI.- LA CIBERSEGURIDAD	D.1 EL CICLO DE VIDA DE LA CIBERSEGURIDAD	PREVENCIÓN	¿Cree usted que el área de TI de la empresa cuenta con programas para concientizar las amenazas en la ciberseguridad?	LIKERT: 1. Totalmente en desacuerdo 2. Desacuerdo 3. Neutral 4. De acuerdo 5. Totalmente de acuerdo.	Cuestionario	
		DETECCIÓN				
		RESPUESTA	¿Cree usted que el área de TI de la empresa resguarda los backups de la información de la empresa adecuadamente?			
	D.2 SEGURIDAD INFORMÁTICA	EFICIENCIA A LAS MEDIDAS DE CIBERSEGURIDAD	¿el área de TI de la empresa restringe el uso de los sistemas informáticos de la organización al personal no autorizado?			
		LOS VIRUS INFORMÁTICOS	¿Cree usted que el área de TI de la empresa ha incorporado software de seguridad adecuados para proteger la información de la organización de actividades las ilícitas de los cibercriminales?			
		MECANISMOS PREVENTIVOS	¿Cree usted que el área de TI de la empresa ha incorporado medidas de seguridad físicas que neutralicen las actividades ilícitas de los cibercriminales?			
		MECANISMOS CORRECTIVOS	¿Cree usted que el área de TI de la empresa tiene incorporado planes de protección de detección contra los cibercriminales?			
	D.3 CIBERSEGURIDAD Y CIENCIA DE DATOS	CIENCIA DE DATOS	¿Tiene usted conocimiento de cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?			
		MACHINE LEARNING				
		CIBERSEGURIDAD EN ANDROID	¿Cree usted que el área de TI de la empresa cuenta con personal calificado en ciberseguridad?			
	D.4 PREVENCIÓN Y SANCION DE LOS CIBERDELITOS	CIBERSEGURIDAD EN APLICACIONES WEB	¿Cree usted que los sistemas de seguridad existentes por el área de TI de la empresa utilizan aplicación web que neutralizan los ataques de los cibercriminales?			
		CIBERDELITOS	¿Alguna vez ha tenido que detener sus actividades por causa de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad?			
		LA INGENIERIA SOCIAL	¿el área de TI de la empresa lo ha capacitado a usted sobre las formas más comunes en que los cibercriminales suelen accionar?			
		LOS DELITOS EN LINEA DELITOS DE PI EN EL CIBERESPACIO	¿Considera usted que en el último año se ha perdido información importante por culpa de algún virus informático?			
	VARIABLE DEPENDIENTE VD.- GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	I.1 TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN	FUNDAMENTOS DE LAS TIC			¿Considera usted que el área de TI de la empresa cuenta con planes de capacitaciones de TI oportunas al personal de la empresa?
			EVOLUCION DE LAS TIC			
IMPACTO DE LAS TIC			¿Considera usted que el área de TI de la empresa cumple una atención de incidencias de TI?			
LAS TIC COMO AGENTES DEL CAMBIO			¿Cree usted que el área de TI de la empresa cuenta con herramientas para la protección contra amenazas externas y ambientales respecto a la información?			
INFRAESTRUCTURA DE LAS TIC						
I.2 ASPECTOS FUNDAMENTALES DE LOS SI		COMPONENTES DE LOS SI	¿Cree usted que el área de TI de la empresa realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?			
		FUNCIONES DEL SI				
		EL SI Y LA CADENA DE VALOR. EL SI Y LA INFRAESTRUCTURA DE EMPRESA	¿Considera usted que el área de TI de la empresa realiza mantenimientos oportunos a los dispositivos de la organización? ¿Qué tan conforme está usted con la seguridad del internet que cuenta la empresa			
I.3 SISTEMA DE INTELIGENCIA TECNOLÓGICA		GENERACION DE CONOCIMIENTO.	¿Ha recibido capacitación de parte del área de TI de la empresa respecto al uso adecuado de las tecnologías de la empresa?			
		CASOS DE IMPLEMENTACION	¿Considera usted que la de la oficina dirección de tecnología de información es adecuada?			
		ROADMAPPING TECNOLÓGICO EL CONOCIMIENTO Y LA TECNOLOGIA EN EL DESARROLLO EMPRESARIAL	¿Considera usted que la disponibilidad de la información de los sistemas de información es oportuna y segura?			
I.4 SISTEMAS DE INFORMACION ADMINISTRATIVOS		FUNCION COMERCIALIZACION	¿Cree que usted que el área de TI de la empresa ayuda con las metas trazadas para el área de ventas de la empresa?			
		FUNCION COMPRAS				
		FUNCION COBRANZAS	¿Cree usted que el área de TI de la empresa responde adecuadamente a las necesidades tecnológicas de su área?			
		FUNCION PAGOS				
		FUNCION CONTABLE	¿Está conforme con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?			

Anexo 03: Instrumento

ENCUESTA SOBRE LA CIBERSEGURIDAD

LA CIBERSEGURIDAD Y SU RELACIÓN EN LA GESTIÓN DE
TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA KIARATEL
COMUNICACIONES S.A.C – PERÚ, 2022.

ESTIMADO PARTICIPANTE

INSTRUCCIONES: El siguiente cuestionario tiene como finalidad recolectar información importante para el estudio de “LA CIBERSEGURIDAD Y SU RELACIÓN EN LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA KIARATEL COMUNICACIONES S.A.C – PERÚ, 2022”.

Referente a esto, solicitamos a usted se sirva a responder las preguntas mostradas en los cuadros que a continuación le mostramos, tenga en cuenta que la información obtenida será de mucha importancia para la investigación que se viene realizando. También hacemos de su conocimiento que este instrumento es de carácter anónimo, se le agradece su colaboración.

Donde:

1. Totalmente en desacuerdo
2. Desacuerdo
3. Neutral
4. De acuerdo
5. Totalmente de acuerdo.

N.º	DIMENSIONES /ITEMS	ITEMS				
	DIMENSIÓN 1. EL CICLO DE VIDA DE LA CIBERSEGURIDAD	1	2	3	4	5
1	¿Cree usted que el área de TI de la empresa cuenta con programas para concientizar las amenazas en la ciberseguridad?					
2	¿Está de acuerdo con la aplicación de un sistema de inventarios?					
3	¿Cree usted que el área de TI de la empresa resguarda los backups de la información de la empresa adecuadamente?					
	DIMENSIÓN 2. SEGURIDAD INFORMÁTICA	1	2	3	4	5
4	¿Cree usted que el área de TI de la empresa ha incorporado software de seguridad adecuados para proteger la información de la organización de actividades las ilícitas de los cibercriminales?					
5	¿Cree usted que el área de TI de la empresa ha incorporado medidas de seguridad físicas que neutralicen las actividades ilícitas de los cibercriminales?					
6	¿Cree usted que el área de TI de la empresa tiene incorporado planes de protección de detección contra los cibercriminales?					
	DIMENSIÓN 3. CIBERSEGURIDAD Y CIENCIA DE DATOS	1	2	3	4	5
7	¿Tiene usted conocimiento de cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?					
8	¿Cree usted que el área de TI de la empresa cuenta con personal calificado en ciberseguridad?					
9	¿Cree usted que los sistemas de seguridad existentes por el área de TI de la empresa utilizan aplicación web que neutralizan los ataques de los ciberdelincuentes?					
	DIMENSIÓN 4. PREVENCIÓN Y SANCIÓN DE LOS CIBERDELITOS	1	2	3	4	5
10	¿Alguna vez ha tenido que detener sus actividades por causa de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad?					
11	¿Considera usted que en el último año se ha perdido información importante por acusa de algún virus informático?					
12	¿ <u>el</u> área de TI de la empresa lo ha capacitado a usted sobre las formas más comunes en que los ciberdelincuentes suelen accionar?					

Que tenga un buen día, muchas gracias.

ENCUESTA SOBRE LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

LA CIBERSEGURIDAD Y SU RELACIÓN EN LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA KIARATEL COMUNICACIONES S.A.C – PERÚ, 2022.

ESTIMADO PARTICIPANTE

INSTRUCCIONES: El siguiente cuestionario tiene como finalidad recolectar información importante para el estudio de “LA CIBERSEGURIDAD Y SU RELACIÓN EN LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA KIARATEL COMUNICACIONES S.A.C – PERÚ, 2022”. Referente a esto, solicitamos a usted se sirva a responder las preguntas mostradas en los cuadros que a continuación le mostramos, tenga en cuenta que la información obtenida será de mucha importancia para la investigación que se viene realizando. También hacemos de su conocimiento que este instrumento es de carácter anónimo, se le agradece su colaboración.

- Lea atentamente cada pregunta.
- Sea muy sincero al contestar y marcar las respuestas para obtener una información más sustentada y real.
- La información brindada es anónima y confidencial.

Donde:

1. Totalmente en desacuerdo
2. Desacuerdo
3. Neutral
4. De acuerdo
5. Totalmente de acuerdo.

N.º	DIMENSIONES /ITEMS	ITEMS				
		1	2	3	4	5
	DIMENSIÓN 1. TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN					
1	¿Considera usted que el área de TI de la empresa cuenta con planes de capacitaciones de TI oportunas al personal de la empresa?					
2	¿Está de acuerdo con la creación de tablas de almacenamiento del sistema?					
3	¿Considera usted que el área de TI de la empresa cumple una atención de incidencias de TI?					
	DIMENSIÓN 2. ASPECTOS FUNDAMENTALES DE LOS SI	1	2	3	4	5
4	¿Cree usted que el área de TI de la empresa realiza inventarios pertinentes de los dispositivos de TI que se tiene en cada área de la empresa?					
5	¿Qué tanto está de acuerdo con el lenguaje de C# para la aplicación en el sistema?					
6	¿Qué tan conforme está usted con la seguridad del internet que cuenta la empresa?					
	DIMENSIÓN 3. SISTEMA DE INTELIGENCIA TECNOLÓGICA	1	2	3	4	5
7	¿Ha recibido capacitación de parte del área de TI de la empresa respecto al uso adecuado de las tecnologías de la empresa?					
8	¿Considera usted que la disponibilidad de la información de los sistemas de información es oportuna y segura?					
9	¿Considera usted que la dirección de la oficina de tecnología de información es adecuada?					
	DIMENSIÓN 4. SISTEMAS DE INFORMACIÓN ADMINISTRATIVOS	1	2	3	4	5
10	¿Cree que usted que el área de TI de la empresa ayuda con las metas trazadas para el área de ventas de la empresa?					
11	¿Cree usted que el área de TI de la empresa responde adecuadamente a las necesidades tecnológicas de su área?					
12	¿Está conforme con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?					

Que tenga un buen día, muchas gracias.

Anexo 04: Validación de Instrumento

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- 1.1 Apellidos y nombres del experto: ...**CHRISTIAN OVALLE PAULINO**.....
- 1.2 Grado académico:**MAGISTER**.....
- 1.3 Cargo e institución donde labora:**DOCENTE EN INVESTIGACION**
- 1.4 Título de la Investigación: **LA CIBERSEGURIDAD Y SU RELACIÓN EN LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA KIARATEL COMUNICACIONES S.A.C - PERÚ, 2022**.....
- 1.5 Autor del instrumento:
- 1.6 Licenciatura/Maestría/Doctorado:**LICENCIATURA**.....
- 1.7 Nombre del instrumento:**MATRIZ DE CONSISTENCIA**


INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente 0-20%	Regular 21-40%	Bueno 41-60%	Muy Bueno 61-80%	Excelente 81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado.				X	
2. OBJETIVIDAD	Está expresado en conductas observables.					X
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.				X	
4. ORGANIZACIÓN	Existe una organización lógica.					X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del estudio.					X
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					X
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.					X
9. METODOLOGIA	La estrategia responde al propósito del estudio.				X	
10. CONVENIENCIA	Genera nuevas pautas en la investigación y construcción de teorías.				X	
SUB TOTAL						
TOTAL (PROMEDIO)					4	6

VALORACION CUANTITATIVA (Total x 0.20): **PRESENTA BUENA CONSISTENCIA**

VALORACION CUALITATIVA:

OPINIÓN DE APLICABILIDAD: **ES APLICABLE**

Lugar y fecha: **Lima 20 de junio 2022**



Posfirma Metodologo
DNI 40234320

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- 1.1 Apellidos y nombres del experto: ...**BENAVENTE ORELLANA EDWIN**
- 1.2 Grado académico:**MAGISTER**.....
- 1.3 Cargo e institución donde labora:**DOCENTE EN INVESTIGACION**
- 1.4 Título de la Investigación: **LA CIBERSEGURIDAD Y SU RELACIÓN EN LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA KIARATEL COMUNICACIONES S.A.C - PERÚ, 2022.**.....
- 1.5 Autor del instrumento:
- 1.6 Licenciatura/Maestría/Doctorado:**LICENCIATURA**.....
- 1.7 Nombre del instrumento:**MATRIZ DE CONSISTENCIA**

INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente 0-20%	Regular 21-40%	Bueno 41-60%	Muy Bueno 61-80%	Excelente 81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado.				X	
2. OBJETIVIDAD	Está expresado en conductas observables.					X
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.				X	
4. ORGANIZACIÓN	Existe una organización lógica.					X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del estudio.				X	
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					X
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.				X	
9. METODOLOGIA	La estrategia responde al propósito del estudio.				X	
10. CONVENIENCIA	Genera nuevas pautas en la investigación y construcción de teorías.				X	
SUB TOTAL						
TOTAL (PROMEDIO)					6	4

VALORACION CUANTITATIVA (Total x 0.20): **PRESENTA BUENA CONSISTENCIA**

VALORACION CUALITATIVA:

OPINIÓN DE APLICABILIDAD: **ES APLICABLE**

Lugar y fecha: **Lima 20 de junio 2022**


Posfirma
DNI 10626370

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- 1.1 Apellidos y nombres del experto: **MADELAINE BERNANDO SANTIAGO**
- 1.2 Grado académico:**DOCTOR**.....
- 1.3 Cargo e institución donde labora:**DOCENTE EN INVESTIGACION**
- 1.4 Título de la Investigación: **LA CIBERSEGURIDAD Y SU RELACIÓN EN LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN EN LA EMPRESA KIARATEL COMUNICACIONES S.A.C - PERÚ, 2022**.....
- 1.5 Autor del instrumento:
- 1.6 Licenciatura/Maestría/Doctorado:**LICENCIATURA**.....
- 1.7 Nombre del instrumento:**MATRIZ DE CONSISTENCIA**


INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente 0-20%	Regular 21-40%	Bueno 41-60%	Muy Bueno 61-80%	Excelente 81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado.					X
2. OBJETIVIDAD	Está expresado en conductas observables.					X
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.					X
4. ORGANIZACIÓN	Existe una organización lógica.					X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del estudio.				X	
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					X
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.				X	
9. METODOLOGIA	La estrategia responde al propósito del estudio.					X
10. CONVENIENCIA	Genera nuevas pautas en la investigación y construcción de teorías.				X	
SUB TOTAL						
TOTAL (PROMEDIO)					3	7

VALORACION CUANTITATIVA (Total x 0.20): **PRESENTA BUENA CONSISTENCIA**

VALORACION CUALITATIVA:

OPINIÓN DE APLICABILIDAD: **ES APLICABLE**

Lugar y fecha: **Lima 20 de junio 2022**



Posfirma
DNI 10626370

Anexo 05: Matriz de Datos

N° de Encuestado	VARIABLE INDEPENDIENTE: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN												VARIABLE DEPENDIENTE: LA CIBERSEGURIDAD											
	DIMENSIÓN 1: TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN			DIMENSIÓN 2: ASPECTOS FUNDAMENTALES DE LOS SI			DIMENSIÓN 3: SISTEMA DE INTELIGENCIA TECNOLÓGICA			DIMENSIÓN 4: SISTEMAS DE INFORMACIÓN ADMINISTRATIVOS			DIMENSIÓN 1: EL CICLO DE VIDA DE LA CIBERSEGURIDAD			DIMENSIÓN 2: SEGURIDAD INFORMÁTICA			DIMENSIÓN 3: CIBERSEGURIDAD Y CIENCIA DE DATOS			DIMENSIÓN 4: PREVENCIÓN Y SANCIÓN DE LOS CIBERDELITOS		
	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12	p13	p14	p15	p16	p17	p18	p19	p20	p21	p22	p23	p24
1	1	1	4	3	1	1	4	2	5	5	5	2	5	1	5	5	5	4	1	4	4	4	2	2
2	5	3	3	3	5	3	3	5	5	5	4	4	1	5	5	3	5	4	4	5	5	4	3	3
3	5	3	4	5	5	3	3	5	5	5	5	3	5	2	5	2	5	3	4	3	5	3	5	5
4	5	5	4	3	5	5	3	2	5	5	4	5	3	5	5	5	4	3	4	5	1	5	3	4
5	5	3	1	3	5	1	3	1	5	5	5	3	5	2	5	5	4	4	4	5	2	5	3	4
6	5	4	2	5	5	3	3	4	5	5	5	5	3	5	4	4	4	4	2	2	5	4	5	5
7	5	5	4	5	3	5	4	4	5	5	4	3	4	5	4	5	5	4	4	3	5	4	4	4
8	1	3	2	5	5	4	3	4	3	5	3	5	5	4	4	3	5	4	4	5	4	4	4	4
9	4	4	4	5	5	1	3	4	5	1	5	3	5	5	5	5	4	5	5	4	5	5	4	4
10	4	4	4	5	3	4	4	4	5	1	5	3	4	3	5	5	4	3	5	3	3	5	5	5
11	5	5	4	5	4	5	4	2	2	1	2	5	5	5	4	4	3	5	1	5	5	4	5	5
12	4	4	4	5	4	4	4	4	3	4	5	4	4	5	4	5	5	5	1	5	5	4	4	4
13	4	2	4	5	4	2	4	4	5	1	5	4	3	4	3	4	5	2	1	5	4	3	2	2
14	4	5	3	5	4	4	5	5	4	3	4	4	5	5	5	2	5	5	1	5	5	5	3	3
15	2	5	5	4	3	4	3	5	3	5	5	5	5	4	5	2	5	5	5	4	4	5	5	5
16	5	5	5	1	3	4	5	1	5	3	3	5	5	2	5	3	4	3	5	3	2	5	5	5
17	4	5	3	4	4	4	5	1	5	3	5	4	5	2	5	3	4	5	1	5	2	2	5	5
18	4	5	4	5	4	2	2	1	2	5	3	4	5	3	4	4	4	5	1	5	3	5	4	3
19	5	5	4	4	4	4	3	4	5	4	5	5	5	4	5	4	2	2	1	2	5	5	4	5
20	4	5	4	2	4	4	5	1	5	4	3	1	5	4	4	4	4	3	4	5	4	4	4	4
21	4	4	4	5	4	5	5	3	4	4	5	4	5	4	2	4	4	5	1	5	4	5	5	3
22	1	4	2	5	5	4	3	4	5	5	5	2	5	4	4	5	5	4	3	4	4	3	5	1
23	4	1	4	4	5	4	5	2	3	5	2	5	4	3	4	3	5	3	5	5	5	5	4	5
24	2	3	4	5	2	1	4	4	5	4	5	2	1	3	4	5	1	5	3	3	5	5	4	1
25	5	5	5	2	4	2	2	5	1	4	2	5	4	4	4	5	1	5	3	5	4	4	3	5
26	3	5	5	4	2	5	5	1	3	2	5	5	4	1	3	4	3	1	5	5	4	5	5	5
27	5	5	2	4	2	5	2	3	4	5	2	5	5	2	3	4	4	3	5	4	3	4	5	1
28	4	4	2	2	4	5	5	5	1	4	5	5	2	5	3	4	1	3	4	5	5	2	5	5
29	4	4	5	4	2	2	5	5	3	5	2	5	5	5	4	2	3	3	5	4	5	2	5	5
30	3	5	2	4	4	5	4	3	1	3	5	1	5	5	3	2	1	3	4	2	5	1	3	3
31	3	5	5	4	4	5	1	3	3	4	5	1	2	2	4	2	4	3	4	2	5	5	3	3
32	3	4	2	4	4	5	4	3	1	4	1	1	5	5	3	2	1	3	4	5	5	5	3	4
33	3	4	5	4	4	5	1	3	3	3	5	1	2	2	3	4	4	3	4	3	5	1	3	4
34	2	4	2	4	4	5	4	3	1	4	1	1	5	5	4	2	4	3	4	5	5	5	5	4
35	3	4	5	4	4	5	4	3	3	3	5	1	5	5	3	4	4	3	4	3	5	5	5	4
36	2	5	5	4	4	5	1	3	1	4	1	1	2	5	4	4	1	3	4	5	5	1	5	4
37	2	4	1	4	4	5	4	1	3	3	5	1	5	5	3	2	4	3	4	5	5	5	5	4
38	2	5	5	4	4	5	4	3	1	4	5	1	2	5	4	4	4	3	4	5	5	1	5	3
39	2	5	1	4	4	5	4	3	1	4	1	1	5	5	4	2	1	3	4	5	5	5	5	3
40	2	5	5	4	4	5	1	3	1	4	5	1	5	5	4	4	4	3	4	5	5	5	5	3