UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

VICERRECTORADO DE INVESTIGACIÓN

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

Seguridad de la información y la gestión de riesgos en el Instituto de Educación Superior Tecnológico Privado DETECSUR, Tacna – 2020.

PRESENTADO POR

Edson Buenaventura Huertas Flores

ASESOR

Dr. Anibal Fernando Flores Garcia

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA CON MENCIÓN EN SEGURIDAD Y AUDITORÍA INFORMÁTICA

MOQUEGUA – PERÚ
2022

ÍNDICE DE CONTENIDO

DEDICATORIA ii

AGRADECIMIENTOS iii

ÍNDICE DE CONTENIDO iv

ÍNDICE DE TABLAS vii

ÍNDICE DE FIGURAS viii

RESUMEN ix

ABSTRACT x

INTRODUCCIÓN xi

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN 1

1.1. Descripción de la realidad problemática 1

1.2. Definición del problema 3

1.2.1. Problema general 3

1.2.2. Problemas específicos 3

1.3. Objetivo de la investigación 4

1.3.1. Objetivo general 4

1.3.2. Objetivos específicos 4

1.4. Justificación y limitaciones de la investigación 4

1.4.1. Justificación teórica 4

1.4.2. Justificación metodológica 5

1.4.3. Justificación práctica 5

1.5. Variables 6

1.6. Hipótesis de la investigación 6

1.6.1. Hipótesis general 6

1.6.2. Hipótesis específicas 7

CAPÍTULO II: MARCO TEÓRICO 8

2.1. Antecedentes de la investigación 8

2.1.1. Antecedentes internacionales 8

2.1.2. Antecedentes nacionales 10

2.2. Bases teóricas 12

2.2.1. Gestión de servicios de tecnologías de la información 12

2.2.2. Seguridad informática 14

2.2.3. Gestión de riesgos 16

2.3. Marco conceptual 18

CAPÍTULO III: MÉTODO 20

3.1. Tipo de investigación 20

3.2. Diseño de investigación 20

3.3. Población y muestra 21

3.3.1. Población 21

3.3.2. Muestra 21

3.4. Técnicas e instrumentos de recolección de datos 21

3.5. Técnicas de procesamiento y análisis de datos 22

CAPÍTULO IV: PRESENTACIÓN Y ANÁLISIS DE RESULTADOS 23

4.1. Presentación de resultados por variables..... 23

4.1.1. Seguridad de la información 23

4.1.2. Gestión de riesgos de TI..... 29

4.2. Contrastación de hipótesis 35

4.2.1. Análisis de fiabilidad..... 35

4.2.2. Prueba de normalidad..... 38

4.2.3. Pruebas de hipótesis 39

4.3. Discusión de resultados..... 48

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 51

5.1. Conclusiones 51

5.2. Recomendaciones..... 53

BIBLIOGRAFIA 55

ANEXOS 59

Anexo 01: Matriz de consistencia 59

Anexo 02: Base de datos 60

Anexo 03: Instrumento de medición variable 1 61

Anexo 04: Instrumento de medición variable 2 62

ÍNDICE DE TABLAS

Tabla 1 Operacionalización de la variable independiente 6

Tabla 2 Operacionalización de la variable dependiente 6

Tabla 3 Nivel de variable independiente 23

Tabla 4 Nivel de Disponibilidad 25

Tabla 5 Nivel de Confidencialidad 26

Tabla 6 Nivel de Integridad de datos 28

Tabla 7 Nivel de variable dependiente 29

Tabla 8 Nivel de Cultura consciente sobre riesgos 31

Tabla 9 Nivel de Proceso de gobernanza del riesgo 32

Tabla 10 Nivel de Implantación eficaz de tecnologías de la información 34

Tabla 11 Magnitud de los rangos de confiabilidad 36

Tabla 12 Resumen de casos - Variable independiente 36

Tabla 13 Alfa de Cronbach - Variable independiente 36

Tabla 14 Resumen de casos - Variable dependiente 37

Tabla 15 Alfa de Cronbach – Variable dependiente 37

Tabla 16 Evaluación de normalidad de la variable independiente 38

Tabla 17 Evaluación de normalidad de la variable dependiente 38

Tabla 18 Correlación disponibilidad vs gestión de riesgos 40

Tabla 19 Correlación confidencialidad vs gestión de riesgos 42

Tabla 20 Correlación integridad de datos vs gestión de riesgos 44

Tabla 21 Correlación seguridad de la información vs gestión de riesgos 46

ÍNDICE DE FIGURAS

Figura 1. Nivel de variable independiente 24

Figura 2. Nivel de Disponibilidad 25

Figura 3. Nivel de Confidencialidad 27

Figura 4. Nivel de Integridad de datos 28

Figura 5. Nivel de variable dependiente 30

Figura 6. Nivel de Cultura consciente sobre riesgos 31

Figura 7. Nivel de Proceso de gobernanza del riesgo 33

Figura 8. Nivel de Implantación eficaz de tecnologías de la información 34

Figura 9. Diagrama de dispersión disponibilidad vs gestión de riesgos 41

Figura 10. Diagrama de dispersión confidencialidad vs gestión de riesgos 43

Figura 11. Diagrama de dispersión integridad de datos vs gestión de riesgos 45

Figura 12. Diagrama de dispersión general 47

RESUMEN

El presente trabajo tiene como finalidad establecer la relación que existe entre la seguridad de la información y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna. Se desarrolló un estudio básico, descriptivo-correlacional, no experimental-transversal, a través de un cuestionario aplicado a 15 colaboradores de la empresa. Se recurrió al estadístico de normalidad Shapiro-Wilk y correlación Rho de Spearman para el establecimiento del nivel de relación entre dichas variables estudiadas y sus respectivas dimensiones. Los resultados denotaron la existencia de una correlación significativa alta ($R=.709$; $p<.05$) entre la Seguridad de la información y la gestión de riesgos, de igual manera entres esta última y las dimensiones Disponibilidad ($R = .697$; $p<.05$), Confidencialidad ($R = .664$; $p<.05$) e Integridad de datos ($R = .785$; $p<.05$).

Palabras clave: Seguridad de información, Gestión de riesgos, Instituto.

ABSTRACT

The purpose of this paper is to establish the relationship between information security and risk management at the IESTP Detecsur in the city of Tacna. A basic, descriptive-correlational, non-experimental-cross-sectional study was developed through a questionnaire applied to 15 company employees. The Shapiro-Wilk normality statistic and Spearman's Rho correlation were used to establish the level of relationship between the variables studied and their respective dimensions. The results denoted the existence of a significant high correlation (R=.709; p<.05) between Information Security and risk management, in the same way between the latter and the Availability dimensions (R = .697; p <.05), Confidentiality (R = .664; p<.05) and Data Integrity (R = .785; p<.05).

Keywords: Information security, Risk management, Institute.

INTRODUCCIÓN

Relación existente entre la seguridad de la información y la gestión de riesgos en el Instituto de Educación Superior Tecnológico Privado DETECSUR de la ciudad de Tacna. El estudio se encuentra compuesto por los subsiguientes capítulos: En el capítulo I se mencionan los antecedentes de la investigación, además de la problemática, la justificación y los objetivos trazados para la investigación. En el capítulo II se desarrolla el marco teórico y la revisión de investigaciones relacionadas al tema de investigación. En el capítulo III se detalla el aspecto metodológico, se establece las hipótesis, variables, tipo y nivel de estudio, población y muestra, técnicas e instrumentos, además de las metodologías empleadas para el estudio de los datos. En el capítulo IV se detallan los resultados logrados en la exploración personificados mediante tablas y gráficos estadísticos. En el capítulo V, se realiza la discusión de los resultados obtenidos. Finalmente se muestran las conclusiones y recomendaciones, además de la bibliografía y los anexos.

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción de la realidad problemática

La información, sea en formato digital o en formato físico, desarrolla un rol preponderante en cualquier tipo de entidad, puesto que ejerce como principal activo y genera valores económicos para las instituciones. Si no se administra, protege o asegura de forma adecuada la información se encontrará expuesta a riesgos que puede perjudicar la continuidad de sus operaciones. Por ello es necesario que toda la información deba ser protegida y accesible en tiempo y forma, o preservar sus peculiaridades de integridad, confidencialidad y disponibilidad.

A nivel internacional la mayor cantidad de incidentes concernientes a la seguridad informática se presentan gracias a diversos elementos que hacen incrementar los niveles de riesgo en el menoscabo de la información. Según el Doctor Almanza se identifican cuatro principales incidentes, el primero de ellos relacionado con la instalación no autorizada de software representado por el 55.56%, el segundo factor son los Virus/Caballos de Troya con el 46.3%, el tercer factor es el acceso de personal no autorizado al sitio web, por ello la pérdida de información se relaciona con las escalas de lo observado (19,14%), lo cual denota la actual situación latente de los peligros que existen (Palacios, 2015)

El acceso sin autorización a la información se ha tornado más rápido de realizar, gracias a los varios y nuevos métodos existentes actualmente para la extracción de la información, permitiendo que sea más compleja la protección de la información, así como sus formas de transmitirla; sin distinción de cómo son comunicados, pudiendo ser verbales, documentos, verbales, base de datos, etc. (Huanca, 2019).

En enero del 2016, se realizó la publicación de la R. M. N°246-2007-PCM divulgado a través del diario oficial El Peruano, resolución que aprobó la obligatoriedad de aplicación de las Normas Técnicas Peruanas NTP ISO/IEC 27001:2014 en todas las organizaciones que conforman el Sistema Nacional de Informática, siendo la ONGEI la encargada de proporcionar ayuda técnica a las organizaciones que la soliciten, a excepción de las entidades que posean certificación ISO 27001.

La gestión de las operaciones que realiza los diferentes estamentos de la Asociación Educativa Desarrollo y Tecnología del Sur se lleva a cabo a través de medios automatizados, desde el registro de información hasta su procesamiento y entrega a los clientes internos y externos. A pesar que las operaciones se mantienen estables, nace la necesidad de empezar a gestionar todos los controles correspondientes a la seguridad, para garantizar que los activos correspondientes de información no sean alteradas o manipuladas por individuos no autorizados, sean estos internos o externos a la institución. Actualmente no se dispone de un plan de seguridad informática, por lo cual no se han realizado ninguna acción para la mitigación de temas relacionados. La falta de lineamientos de seguridad impide la creación de medios de control adecuados para la manipulación y la accesibilidad de

los sistemas gestores de información, permitiendo la posibilidad de que la información sea empleada para fines que puedan perjudicar a la institución y/o directamente a los clientes externos. De continuar bajo la misma línea de gestión, la institución puede ser susceptible a la presencia de incidentes de seguridad que perjudiquen las operaciones e información.

La institución a pesar de contar con más de diez años de operación en la ciudad de Tacna, brindando programas de educación técnica en las carreras de Administración de Negocios Internacionales, Computación e Informática y Contabilidad, además de encontrarse actualmente en el proceso de transición al empleo de las TIC's para la automatización de los procesos y para el otorgamiento del licenciamiento por parte del Ministerio de Educación para brindar nuevos programas de formación técnica profesional, requiere establecer la actual situación de la seguridad informática y la gestión de riesgos, para de acuerdo a los resultados derivados formular estrategias como parte de un plan de mejora continua en pro de los estudiantes que depositan su confianza en la institución.

1.2. Definición del problema

1.2.1. Problema general

¿Cómo es la relación existente entre la seguridad de la información y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna?

1.2.2. Problemas específicos

- ¿Cómo es la relación existente entre la dimensión disponibilidad y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna?

- ¿Cómo es la relación existente entre la dimensión confidencialidad y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna?
- ¿Cómo es la relación existente entre la dimensión integridad de datos y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna?

1.3. Objetivo de la investigación

1.3.1. Objetivo general

Especificar la relación existente entre la seguridad de la información y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

1.3.2. Objetivos específicos

- Especificar la relación entre la dimensión disponibilidad y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.
- Especificar la relación entre la dimensión confidencialidad y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.
- Especificar la relación entre la dimensión integridad de datos y la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

1.4. Justificación y limitaciones de la investigación

1.4.1. Justificación teórica

El proceso de investigación permitió recopilar y ampliar las conceptualizaciones y definiciones actuales respecto a la seguridad informática, con el significativo aporte de diferentes reconocidos estudiosos e investigadores del tema, además de establecer la asociación entre dicha variable con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna, generándose información

actualizada y relevante para estudiantes y especialistas que estudian o buscan estudiar las mencionadas variables.

1.4.2. Justificación metodológica

La metodología usada podrá estar sujeto a reutilización para realización de futuras investigaciones, debido a que en la presente se recurrió al uso de metodologías que consideran el desarrollo de técnicas e instrumentos para la recolección y procesamiento de información que será de utilidad para investigaciones con parámetros símiles, puesto que en una sociedad que se basa en el uso de TIC's, la seguridad informática desempeña un rol preponderante en la dirección de cualquiera sea el tipo de organización.

1.4.3. Justificación práctica

Los resultados estadísticos que se lograron obtener en la investigación permitirán a las organizaciones mejorar sus estrategias de seguridad informática, como en el caso de los Institutos de Educación Superior Tecnológico Privado de la ciudad de Tacna, ya que con el presente estudio se logrará mejorar los aspectos que sean determinados como endebles y optimizar aquellos que muestren indicadores favorables al interior de la institución donde se realizará el estudio.

1.5. Variables

Tabla 1
Operacionalización de la variable independiente

Variable independiente	Dimensión	Indicador	Escala	Niveles y rangos
Seguridad de la información	a) Disponibilidad	Tiempo en obtener la información	Likert	1) Malo 2) Regular 3) Bueno
		Copias de respaldo de bases de datos		
	b) Confidencialidad	Categorización de los activos de información		
		Políticas de seguridad informática		
	c) Integridad de datos	Encriptación de la información		
		Número de incidentes por manejo de datos		

Fuente: Elaboración propia

Tabla 2
Operacionalización de la variable dependiente

Variable dependiente	Dimensión	Indicador	Escala	Niveles y rangos
Gestión de riesgos de TI	a) Proceso de gobernanza del riesgo	Nivel de compromiso del trabajador hacia la institución.	Likert	1) Malo 2) Regular 3) Bueno
	b) Cultura consecuente sobre riesgos	Nivel de productividad		
	c) Implantación eficaz de tecnologías de la información	Nivel de satisfacción del trabajador.		

Fuente: Elaboración propia

1.6. Hipótesis de la investigación

1.6.1. Hipótesis general

La seguridad de la información se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

1.6.2. Hipótesis específicas

- H1: La dimensión disponibilidad se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.
- H2: La dimensión confidencialidad se relación directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.
- H3: La dimensión integridad de datos se relación directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Parada, Flórez y Gómez (2018) en la investigación desarrollada en Bucaramanga, realiza el análisis sistémico de los componentes de la seguridad a través de los lenguajes de la dinámica de sistemas, haciendo uso de diagramas de influencias, flujo-nivel, ecuaciones y comportamientos, permitiendo analizar la complejidad de los elementos mediante la caracterización de los ciclos de retroalimentación. Como parte del estudio se realizó una simulación, observando que los controles cumplen un papel significativo en la valoración de los activos, en uno de los dos escenarios estudiados.

Crespo (2016) en el estudio desarrollado en la ciudad de Cuenca, planteó un estudio básico, diseño no experimental - transversal, considerando una población de 50 MPYMES, se realizó la evaluación de la situación actual en cuanto a los niveles de gestión de la seguridad de la información, analizando comparativamente las metodologías CRAMM, Microsoft Risk Guide , OCTAVE-S, COSO III y COBIT 5, concluyendo que es de vital importancia una conveniente gestión de riesgos en el interior de cualquier tipo de empresa u organización de acuerdo a sus

indicadores de análisis y procedimientos de acción ante riesgos para lograr una solución eficaz y eficiente.

Muñoz (2016) en el estudio desarrollado en la ciudad de Cuenca, a través de una investigación básica de diseño no experimental - transeccional, considerando una población correspondiente a los 11 dominios de seguridad que se establecen en la norma ISO 27002, Manual de Políticas de Seguridad Informática – Mejores prácticas internacionales, entre otra documentación relativa al tema de seguridad informática, se observó un cumplimiento de 52% de los once (11) dominios de seguridad considerados en la normativa ISO 27002, denotando puntos débiles referentes al establecimiento de políticas de seguridad, llegando a la conclusión de que los indicadores de integridad, confiabilidad y disponibilidad de la información son de especial necesidad para lograr optimizar el cumplimiento de las normativas de seguridad y disminución de los niveles de riesgo al interior de la organización.

Miranda, Valdés, Pérez, Portelles y Sánchez (2016) en la investigación desarrollada en Cuba, plantean que la administración de la seguridad informática tiene que ser establecida como el conjunto de procedimientos correctamente definidos, por ello como parte del resultado del estudio se establece un método para realizar la administración automatizada de exámenes de los mecanismos de control de la seguridad informática, como la composición de cada uno de los métodos encaminados a la administración óptima de peligros con la automatización de los procedimientos de manipulación, seguimiento y control de un SGSI. Considerando que en promedio la tercera parte de los mencionados controles establecidos en la norma ISO/IEC 27002 son posibles ser automatizadas, la metodología planteada se presenta como una atractiva vía para alcanzar que la administración de la seguridad

informática logre ser un procedimiento de menor complejidad y más efectiva, liberando a los expertos a cargo de una menor proporción del trabajo que les corresponde. El análisis estadístico de los indicadores de complejidad y eficiencia confirmaron la reducción de la complicación y la acentuación de la eficiencia luego de la implantación de controles automáticos de seguridad informática.

Guerrero y Gómez (2012) en la investigación desarrollada en Cali, muestra el resultado de un procedimiento de análisis desde la perspectiva correspondiente a la tendencia de SSM (Sistemas blandos) como soporte para la GRCSI de las instituciones, detallando los sistemas de actividad humana, la evolución organizacional que se necesita y el establecimiento de las acciones y metodologías formuladas. La propuesta presentada por los autores muestra una composición de las actividades afines a los estándares de GRCSI y métodos que pueden emplear para que los implicados en la institución las puedan llevar a cabo, la GRCSI necesita del compromiso y el esfuerzo de los miembros de la unidad de Tecnologías de la Información, los responsables de gerencia y los sectores estratégicos de la organización. La propuesta de la GRCSI propone diversos métodos para la gestión de riesgos y controles que posteriormente permitirán la construcción de herramientas de software para lograr sistematizarlos, para que su utilización sea más amplia.

2.1.2. Antecedentes nacionales

Coaguila (2020) en la investigación desarrollada en Moquegua, a través de un estudio de tipo aplicado, diseño no experimental – transeccional, mediante la aplicación de cuestionarios, determinando la idoneidad de la norma debido a su versatilidad y compatibilidad de la aplicación de los lineamientos, además de la

propuesta de los planes de seguridad de información que validado previamente de forma satisfactoria por 03 especialistas, obteniendo elevados niveles de validez en cada uno de los aspectos analizados, quedando demostrada la hipótesis general.

Calderón (2019) en la investigación desarrollada en la ciudad de Lima, mediante un estudio correspondiente al tipo básico, con diseño no experimental - transversa, relacional, y un universo conformado por 106 colaboradores pertenecientes a la oficina de Gestión de Recursos Humanos del MINEDU, se estableció que existe evidencias suficientes para concluir la presencia de una correlación directa y significativa entre las variables seguridad de la información y la variable administración de riesgos (Rho=0.886, $p < 0.05$), así como la dimensión disponibilidad (Rho=0.866, $p < 0.05$), dimensión confidencialidad (Rho=0.866, $p<0.05$) y la dimensión integridad de datos (Rho=0.866, $p < 0.05$) con la gestión de riesgos, denotando una clara dependencia entre ambas variables.

Calderon (2019) en la investigación desarrollada en el distrito de Lima (cercado), a partir de una investigación de tipo básico, nivel correlacional descriptivo, no experimental - transeccional y método hipotético - deductivo, se determinó la existencia de evidencia estadística suficiente para inferir la presencia de una asociación directa y significativa de nivel regular entre las variables gestión de riesgos y seguridad de la información en el programa denominado Fortalece Perú 2019, con un índice de correlación de 0.661, motivando el planteamiento de uso de metodologías para cada una de las variables para certificar la continuación del proyecto.

Niño (2018) en la investigación realizada en la ciudad de Lambayeque, en base a un análisis documental, revisión bibliográfica y observación directa de los

hechos se concluyó que un SGSI brinda apoyo a las instituciones en temas referentes al proceso de gestión conformado por la dirección, operación y control sistemático y transparente de cada una de sus actividades, con la finalidad de obtener el éxito de los mismos, por ello como parte de la propuesta de SGSI se planteó la norma NTP ISO/IEC 27001:2014 ante la ausencia de gestión de seguridad de la información, a través de la metodología PDCA para la autoevaluación de la institución y la metodología MAGERIT para el análisis de riesgos.

Maquera y Serpa (2017) en la investigación realizada en la ciudad de Tacna, se concluyó que: A) La ejecución y uso de dispositivos para el control de la administración de los activos permite incrementar las tasas de seguridad de la información. B) La administración de los inventarios, pertenencia y uso admisible de activos, normas de codificación, rotulado y administración de la información según la norma ISO/IEC 27002 permitió incrementar los niveles de implantación y uso de los medios de control, sirviendo de catalizador para una adecuada toma de decisiones. C) La normativa ISO/IEC 27002 facilita el modelado y el conglomerado de prácticas para el establecimiento de relaciones, compromisos y dispositivos para lograr resguardar cada uno de los activos de información a los requerimientos del área de proyectos digitales.

2.2. Bases teóricas

2.2.1. Gestión de servicios de tecnologías de la información

La gestión de los servicios proporcionados por las tecnologías de la información (GSTI), también reconocida a través de las siglas en inglés ITSM - IT Service Management es un método basado en procedimientos, enfocados en

enderezar los servicios de TI establecidos por los proveedores de TI, con los requerimientos de las organizaciones, con mayor énfasis en todo lo beneficioso que pueda llegar a percibir los clientes finales. ITSM, o GSTI plantea la modificación de los paradigmas de la Administración de TI, por la recopilación de módulos encauzados para proporcionar servicios de “punta a punta”, o “fin a fin”, utilizando diferentes métodos de trabajo que se encuentran fundados en las "mejores prácticas", como pueden ser por ejemplo el eSCM (enabled Service Capability Model), ITIL o MOF, entre otras (Oltra, 2016).

Según Velázquez (2016), la gestión de servicios TI se determina en un inicio como el proyecto encaminado al proceso y al servicio de los que en su momento fue la Administración de Tecnologías de la Información. Una de las más importantes finalidades de los métodos de Administración de Servicios TI es favorecer a la calidad de los servicios facilitados por las Tecnología de la Información, procurando satisfacer un requerimiento sin asumir de forma directa las capacidades y recursos que sean necesarios para tal fin. La administración de calidad y de los procesos constituyen parte de la institución y de sus políticas.

Una adecuada gestión de los servicios necesita (Bon, 2008):

- Reconocer los requerimientos del cliente.
- Determinar la capacidad y recursos necesarios para el desarrollo del servicio.
- Identificar los niveles de calidad de los servicios.
- Controlar el desarrollo y ejecución del servicio.
- Instaurar dispositivos de mejora y perfeccionamiento del servicio.

Los fines de una buena gestión de servicios de Tecnologías de Información deberán ser (Osorio & Reascos, 2015):

- Facilitar una apropiada dirección de la calidad.
- Incrementar la eficiencia en el uso de recursos de Tecnologías de Información.
- Orientar los procedimientos del negocio y la infraestructura de TIC.
- Disminuir los peligros vinculados a los Servicios de TIC.
- Formar negocio.

En la actualidad las áreas responsables de la gestión de TI sólo desarrollan tareas concretas para la gestión y configuración de servidores, redes, cableado estructurado, soporte técnico, actualización de software, instalación y desarrollo de software, etcétera, actividades que son consideradas poco suficientes para las instituciones. Las necesidades presentes exigen un trabajo eficaz, labores predecibles y fiables, eficiente en cuestión de recursos (tiempo y dinero).

El incremento del uso de modelos y estándares plantean diferentes retos y requerimientos, identificar la finalidad del negocio y las ventajas de estos modelos para los procedimientos de toma de decisiones, haciendo uso de las principales prácticas y complementando en ellas las políticas interinas, operaciones, la conciliación de los modelos y el grado de los requerimientos específicos de la institución (Féliz & Calvo, 2014)

2.2.2. Seguridad informática

Los SGSI se determinan como el acumulado de compromisos, procedimientos, ordenamientos y activos que constituye la alta gerencia con la intención de regir, además de vigilar los niveles de seguridad de los intangibles de información y certificar la continuación de las sistematizaciones de la institución. (Kuna, 2006)

Se comprende por el término “seguridad de la información” a todo el conglomerado de todas las orientaciones de carácter preventivo y reactivo realizados por el hombre, en las instituciones y de los sistemas informáticos que les faciliten el cuidado y protección de la información procurando conservar niveles aceptables de privacidad, disponibilidad e integridad de los mismos (Díaz, 2018).

Es imperativo mencionar que, para el manejo de la seguridad de la información, esta se fundamenta en el uso de las tecnologías y de carácter confidencial. La información puede ser pública, mal empleada, hurtada, eliminada, estropeada, etc., la información es indicativo de poder, y de acuerdo a las variedades de carácter estratégico que proporciona poseer fácil acceso a determinada calidad de información, ésta es clasificado como importante, inapreciable y sensible. Los conceptos de seguridad informática, seguridad de la información y protección de la información son generalmente empleados como semejantes debido a que persiguen el mismo objetivo al brindar protección a las características de confidencia, correctitud, completitud y disponibilidad de la información (Robledo, Loinaz, Lozano, & Sánchez, 2017).

La seguridad de la información incluye diferentes características entre los que se ubican la comunicación, disponibilidad, caracterización de problemas, integridad, observación de los peligros, privacidad, reparación de los riesgos. La disminución o supresión de inseguridades vinculados a determinado tipo de información, es la finalidad que persigue la SGSI, además de la seguridad informática; tienen como objetos los sistemas, accesibilidad, usabilidad, propalación, entorpecimiento o eliminación no facultada de la información. Los conceptos de seguridad de la información, protección de la información y seguridad

informática son empleados generalmente de formas semejantes gracias a que todos estos buscan lograr una misma finalidad con el resguardo de la privacidad, entereza y accesibilidad de la información, en cambio, existen diversos sutiles, las cuales residen primordialmente en el enfoque, los métodos usados y las áreas de concentración. (Galindo, Bladimir, & Santizo, 2014)

2.2.3. Gestión de riesgos

Se entiende por riesgo de seguridad informática a todas aquellas amenazas que exploten alguna o varias vulnerabilidades de alguno o varios activos y que proporcionalmente afecten el trabajo de un sistema, considerado la posibilidad de que acontezca el incidente y el efecto en caso de concretarse, en algunas de las posibles tres particularidades de la seguridad de la información (integridad, confidencialidad, disponibilidad).

Según Gavino (2018) es un instrumento de apoyo para la seguridad de la información porque indican las posibles causas de riesgo en las dimensiones referentes a ala correctitud y completitud, accesibilidad y confiabilidad de la información concerniente a la institución, y además gestiona y controla que se cumplan los requerimientos reglamentados en la medida que son exhibidas y perturba concisamente a su persistencia.

La gestión de riesgos implica la apropiada gestión de los riesgos, siendo el objetivo primordial la minimización hasta la obtención de un riesgo admisible, siendo esta no solo compromiso del área de seguridad, sino de varias áreas, quienes desempeñan roles muy significativos entre los que se pueden mencionar (Pinzón, 2014):

- Alta dirección.

- Jefatura de informática.
- Gerencia.
- Responsables de seguridad.
- Profesionales de TI.
- Creadores de conciencia en temas de seguridad.

El planteamiento de las directrices en temas de seguridad y la adecuada gestión del riesgo deben comenzar desde la alta gerencia, a través de la concientización a todos los elementos de la entidad, sobre su importancia y el buen rol que desempeñan cada uno de los colaboradores.

La gestión de riesgos también es el autoconocimiento de las amenazas y vulnerabilidades, por ello la gestión involucrará el reconocimiento del origen de los peligros con la finalidad de ponderar los efectos producidos sobre las organizaciones, siendo de esta manera manejados con mayor eficiencia.

El procedimiento de evaluación de los riesgos se compone de la identificación, análisis y valoración. En este punto se determinan los grados de las amenazas potenciales y los riesgos asociados, se debe plantear el alcance y el resultado de estos procesos para apoyar en la identificación de los controles apropiados, dicho proceso debe ser realizado por lo menos una vez cada año, siendo no únicamente por el acatamiento de las normas sino por ser considerado una buena práctica, contribuyendo de manera constante a la mejora continua. Es importante que la evaluación que se realice debe ser flexible para permitir cambios justificables.

2.3. Marco conceptual

A. Activos: Son todos aquellos que se encuentran relacionados con los sistemas de información.

B. Amenazas: Acciones que probablemente ocasionen consecuencias desfavorables en las operaciones de la empresa.

C. Delito informático: Actividades que se realizan haciendo uso de medios informáticos con el objetivo de hurtar, dañar o modificar información y que afecta a las instituciones y personas.

D. Gestión de los riesgos: Acciones conjuntas para gestionar y fiscalizar las características vinculadas a los riesgos al interior de una institución.

E. Impacto: Resultados originados a partir de las ocurrencias de las diferentes amenazas, que generan pérdidas, tanto financieras como no financieras para el corto plazo o largo plazo.

F. Incidente: Un suceso o conjunto de sucesos imprevistos de seguridad de la información que poseen probabilidad significativa para complicar las acciones comerciales y perjudicar los niveles aceptables de seguridad de la información.

G. Normas: Son reglas, leyes o parámetros diseñadas para gestionar, preservar y promover el orden en las acciones al interior de una comunidad u organización.

H. Seguridad informática: Acumulado de pautas y reglas trazadas para velar por la confidencialidad, integridad y disposición de la infraestructura tecnológica comprendiendo tanto hardware como software.

I. Tecnología de la información: Instrumentos que son usadas para manejar o distribuir información, es decir son el software y hardware maniobrado por una organización.

J. Vulnerabilidad: Debilidad del sistema de información que puede ser empleada para generar daño. Las debilidades aparecen en cualquier elemento de una computadora, en el hardware o el software.

CAPÍTULO III: MÉTODO

3.1. Tipo de investigación

Según Hernández et al. (2014) la investigación de tipo básica, también denominadas puras, son aquellas en los cuales el principal objetivo es ampliar el conocimiento entorno a determinadas variables para un mejor entendimiento de la realidad.

Es un estudio descriptivo – correlacional; cuya característica principal es el establecimiento de niveles de asociación entre diversas variables, a través de estas asociaciones se buscan obtener información para la realización de inferencias estadísticas sobre el nivel y/o grado de influencia o relación entre las variables planteadas (Vara, 2012).

3.2. Diseño de investigación

Se optó por un diseño no experimental, debido a que no se efectuará manejo intencional alguna de las variables y sólo serán observados los acontecimientos en su entorno de desarrollo natural (Hernández et al., 2014). Transversal gracias a que se analizaran las relaciones entre las variables en un lapso de tiempo específico.

3.3. Población y muestra

3.3.1. Población

Cualquier investigación, sea cualesquiera su naturaleza, necesita que se determinen los parámetros entre los cuales será desarrollada la investigación, concretamente respecto a las unidades de análisis, considerando ser personas, grupos o fenómenos. Hernández et al (2014) indica que la población se determina como el grupo de entidades que conservan peculiaridades similares.

La población se establece como la totalidad de trabajadores administrativos de la Asociación Educativa Desarrollo y Tecnología del Sur, estimado en quince (15) prestadores de servicios.

3.3.2. Muestra

De acuerdo a Hernández et. al (2014), la muestra de una investigación es la proporción representativa de la población. Es una porción de la población total, a partir del cual se lograrán obtener información respecto a las variables de estudio. Hernández et al (2014), establece que si la población estudiada es una cantidad inferior a cincuenta (50) entidades, la muestra es igual a la totalidad de la población. En base a lo referido previamente, en la presente investigación se considera un tipo de muestreo no probabilístico de carácter censal.

3.4. Técnicas e instrumentos de recolección de datos

Un instrumento es la recapitulación de los indicadores escogidos de forma vinculada con la técnica de recolección de datos (Sabino, 1992). Un estudio carece de confiabilidad si no se hace uso de técnicas determinadas para la recolección de datos que permitan respaldar la respuesta de los problemas formulados en el

estudio; de acuerdo al método y tipo de investigación, se necesitará la aplicación de determinadas técnicas (Bernal, 2010).

Se menciona la presencia de dos (2) tipos de instrumentos para medir variables que pueden ser usados al instante de desarrollar un estudio: a) Instrumento ya estructurado y listo para su ejecución. b) Nuevo instrumento de medición que deberá de pasar por un proceso de validez y confiabilidad previo a su ejecución (Hernández et al, 2014).

La técnica a emplear es la encuesta, haciendo uso del cuestionario como instrumento, el cual estará constituido por preguntas ordinales referentes a las dos variables de investigación, considerando un rango de respuesta medidas mediante la escala de Likert. Dicho instrumento deberá ser sometido previamente a la validación mediante el procedimiento de juicio de expertos y evaluación de nivel de confianza haciendo uso del coeficiente Alfa de Cronbach.

3.5. Técnicas de procesamiento y análisis de datos

La técnica de distribución de frecuencia se empleará para la tabulación de los datos obtenidos en tablas de frecuencia que representarán los datos en forma breve y concisa. Además, permitió la representación de forma gráfica de los valores o frecuencias que se generan en el estudio. Para realizar el tratamiento estadístico de los datos se empleará el software estadístico SPSS, el cual permitirá obtener los porcentajes y frecuencias.

A través de las pruebas estadísticas de normalidad de la distribución de datos se determinará la prueba estadística paramétrica o no paramétrica que se empleará para la afirmación o rechazo de las hipótesis planteadas en la investigación y para observar el grado de correlación entre ambas variables.

CAPÍTULO IV: PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

4.1. Presentación de resultados por variables

Para el análisis estadístico descriptivo se asumirán las puntuaciones de la variable Seguridad de la información y la Gestión de riesgos según los colaboradores del Instituto de Educación Superior Tecnológico Privado DETECSUR de Tacna, se procederá a presentar mediante niveles y/o rangos para el correspondiente análisis de resultados.

4.1.1. Seguridad de la información

4.1.1.1. Nivel de la Seguridad de la información

Tabla 3
Nivel de variable independiente

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	26.7	26.7	26.7
	Regular	7	46.7	46.7	73.3
	Bueno	4	26.7	26.7	100.0
	Total	15	100.0	100.0	

Fuente: Resultados SPSS

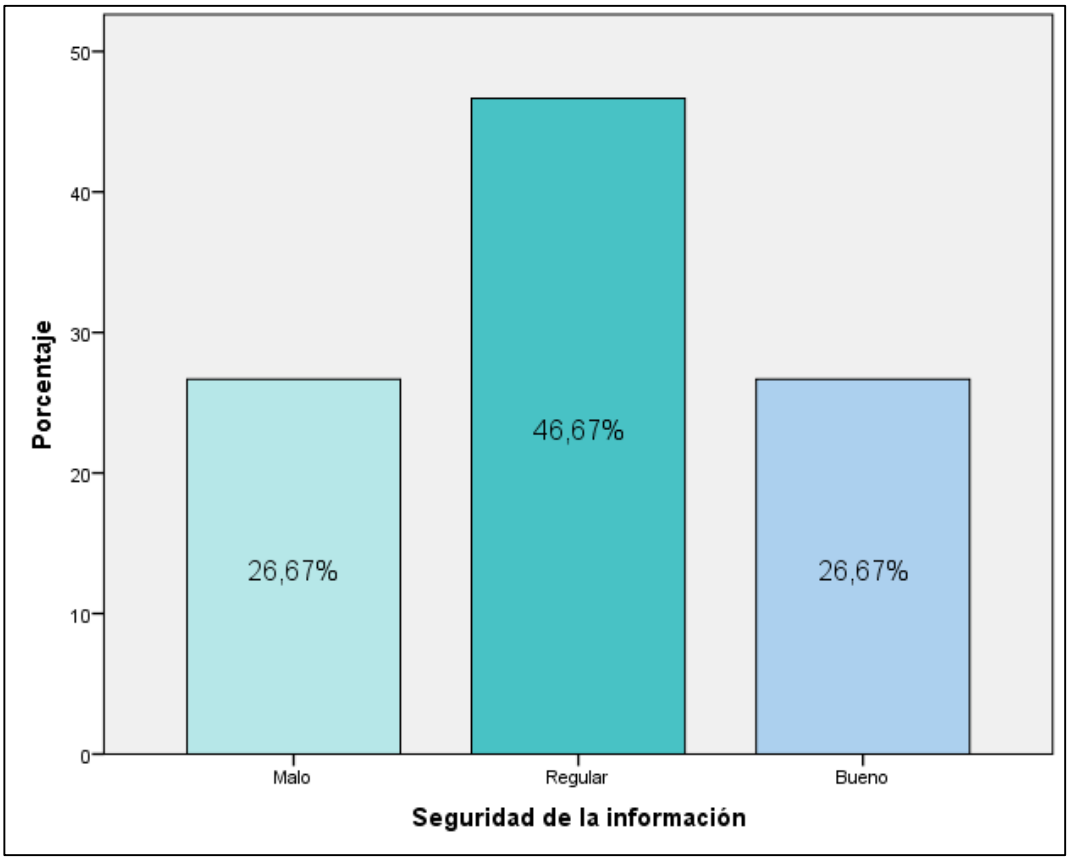

Figura 1. Nivel de variable independiente
Fuente: Tabla N° 08

ANÁLISIS E INTERPRETACIÓN:

Los resultados que se logran apreciar en la Tabla 8 y Figura 1 respecto a los niveles de la variable Seguridad de la Información de acuerdo a los colaboradores del IESTP Detecsur de Tacna, se observa que el 46.67% de los colaboradores perciben que el nivel es regular, el 26.67% bueno y el 26.67% malo. Los niveles de Seguridad de la Información se ven más influenciados por las dimensiones de disponibilidad e integridad de datos, siendo estos los que tienen mayor percepción con tendencia negativa en los resultados analizados en la investigación, factores como la disponibilidad de la información requerida, el tiempo de recuperación del sistema ante un incidente, la calidad de los antivirus y capacitaciones respecto a ataques de virus.

4.1.1.2. Análisis por dimensiones

Tabla 4
Nivel de Disponibilidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	6	40.0	40.0	40.0
	Regular	8	53.3	53.3	93.3
	Bueno	1	6.7	6.7	100.0
	Total	15	100.0	100.0	

Fuente: Resultados SPSS

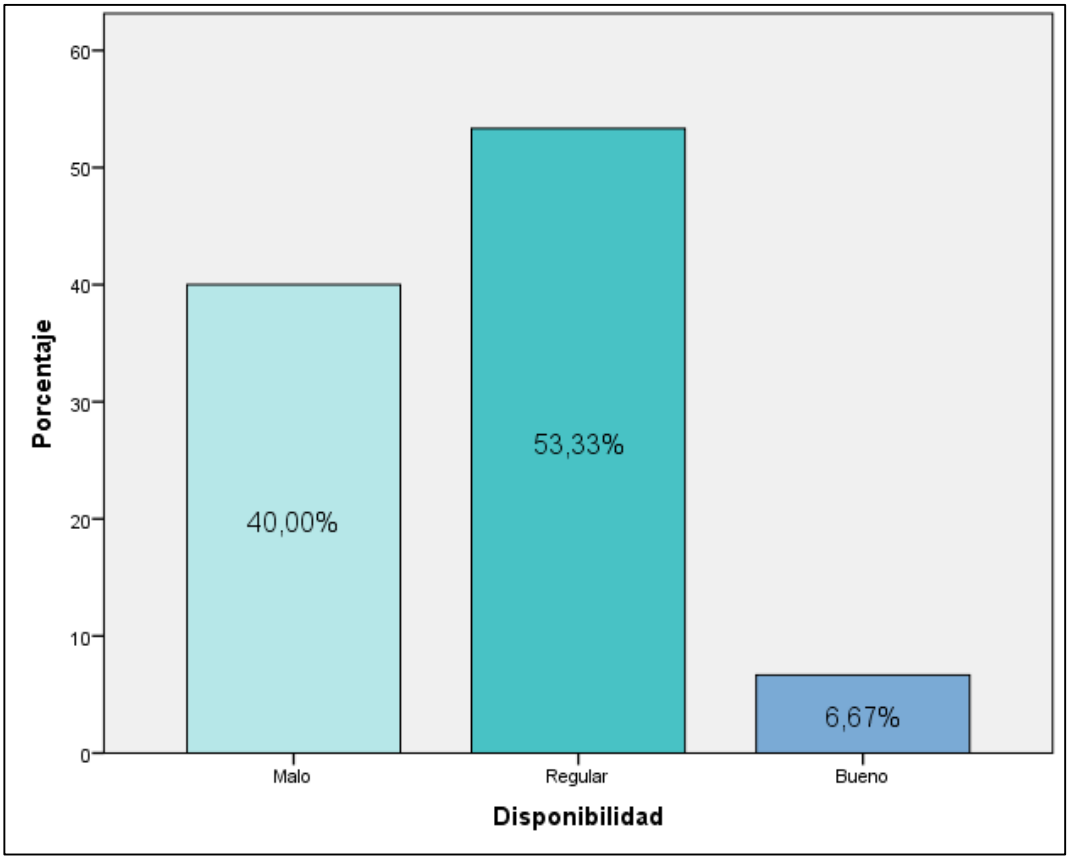

Figura 2. Nivel de Disponibilidad
Fuente: Tabla N° 09

ANÁLISIS E INTERPRETACIÓN:

Los resultados que se logran apreciar en la Tabla 9 y Figura 2 respecto al nivel de la dimensión Disponibilidad de la variable Seguridad de la Información de acuerdo a los colaboradores del IESTP Detecsur de Tacna, se observa que el 53.33% de los colaboradores perciben que el nivel es regular, el 40.00% es malo y el 6.67% es bueno. Las mayores percepciones negativas son referentes al tiempo en el cual se logra recuperar los sistemas de la institución ante un incidente, seguido de la poca disponibilidad de la información en el momento que este se requiere.

Tabla 5
Nivel de Confidencialidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	26.7	26.7	26.7
	Regular	7	46.7	46.7	73.3
	Bueno	4	26.7	26.7	100.0
	Total	15	100.0	100.0	

Fuente: Resultados SPSS

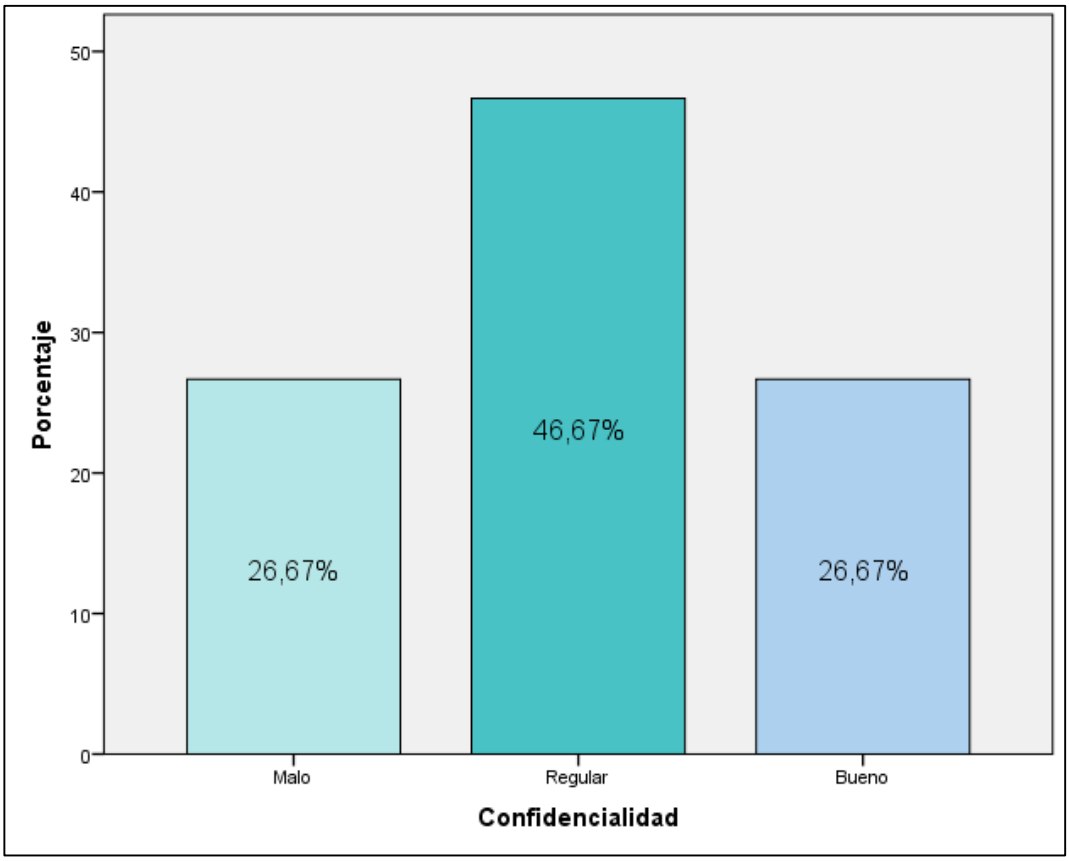

Figura 3. Nivel de Confidencialidad
Fuente: Tabla N° 10

ANÁLISIS E INTERPRETACIÓN:

Los resultados que se logran apreciar en la Tabla 10 y Figura 3 respecto al nivel de la dimensión Confidencialidad de la variable Seguridad de la Información de acuerdo a los colaboradores del IESTP Detecsur de Tacna, se observa que el 46.67% de los colaboradores perciben que el nivel es regular, el 26.67% es bueno y el 26.67% es malo. Las mayores percepciones negativas son referentes al resguardo de la información en medios seguros y los permisos que se otorgan a las carpetas que son compartidas a través de la red interna de la institución.

Tabla 6
Nivel de Integridad de datos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	33.3	33.3	33.3
	Regular	9	60.0	60.0	93.3
	Bueno	1	6.7	6.7	100.0
	Total	15	100.0	100.0	

Fuente: Resultados SPSS

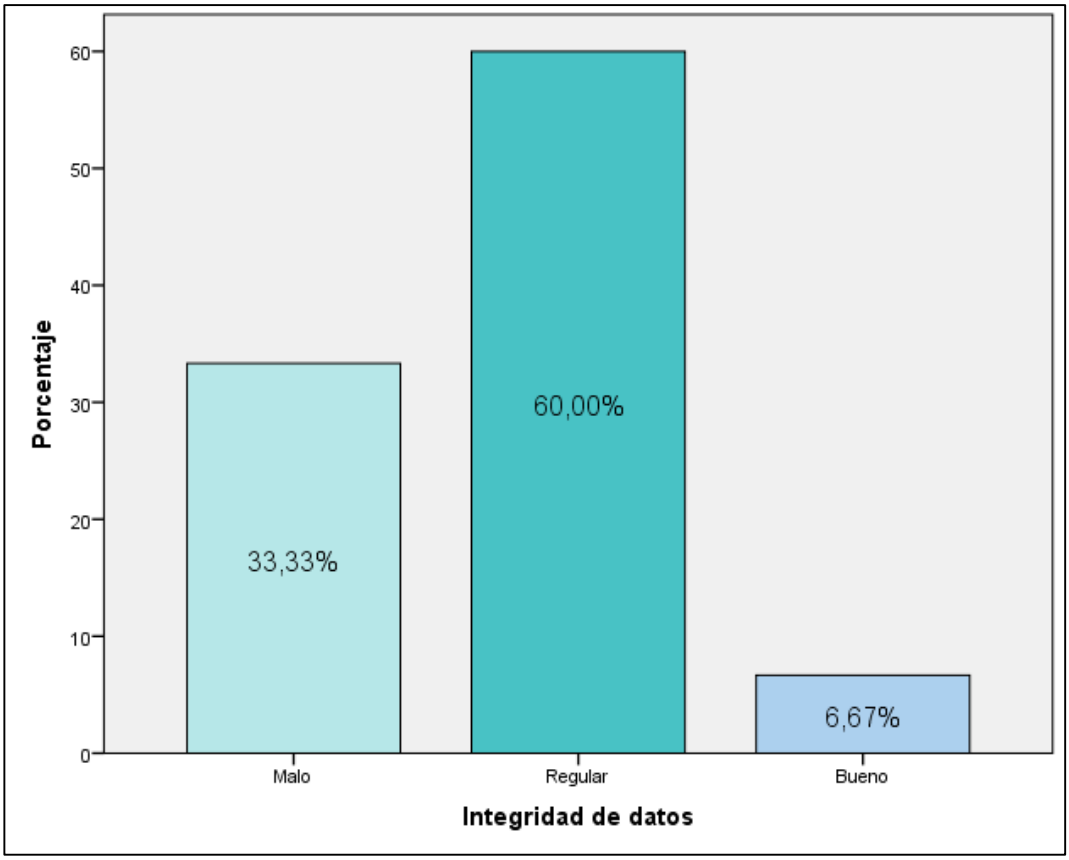

Figura 4. Nivel de Integridad de datos
Fuente: Tabla N° 11

ANÁLISIS E INTERPRETACIÓN:

Los resultados que se logran apreciar en la Tabla 11 y Figura 4 respecto al nivel de la dimensión Integridad de datos de la variable Seguridad de la Información de acuerdo a los colaboradores del IESTP Detecsur de Tacna, se observa que el 60.00% de los colaboradores perciben que el nivel es regular, el 33.33% es malo y el 6.67% es bueno. Las mayores percepciones negativas son referentes la actualización de los antivirus instalados en los equipos y las capacitaciones recibidas por los trabajadores sobre los niveles de ataques de los virus y sus respectivas modalidades.

4.1.2. Gestión de riesgos de TI

4.1.2.1. Nivel de la Gestión de riesgos de TI

Tabla 7
Nivel de variable dependiente

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	26.7	26.7	26.7
	Regular	9	60.0	60.0	86.7
	Bueno	2	13.3	13.3	100.0
	Total	15	100.0	100.0	

Fuente: Resultados SPSS

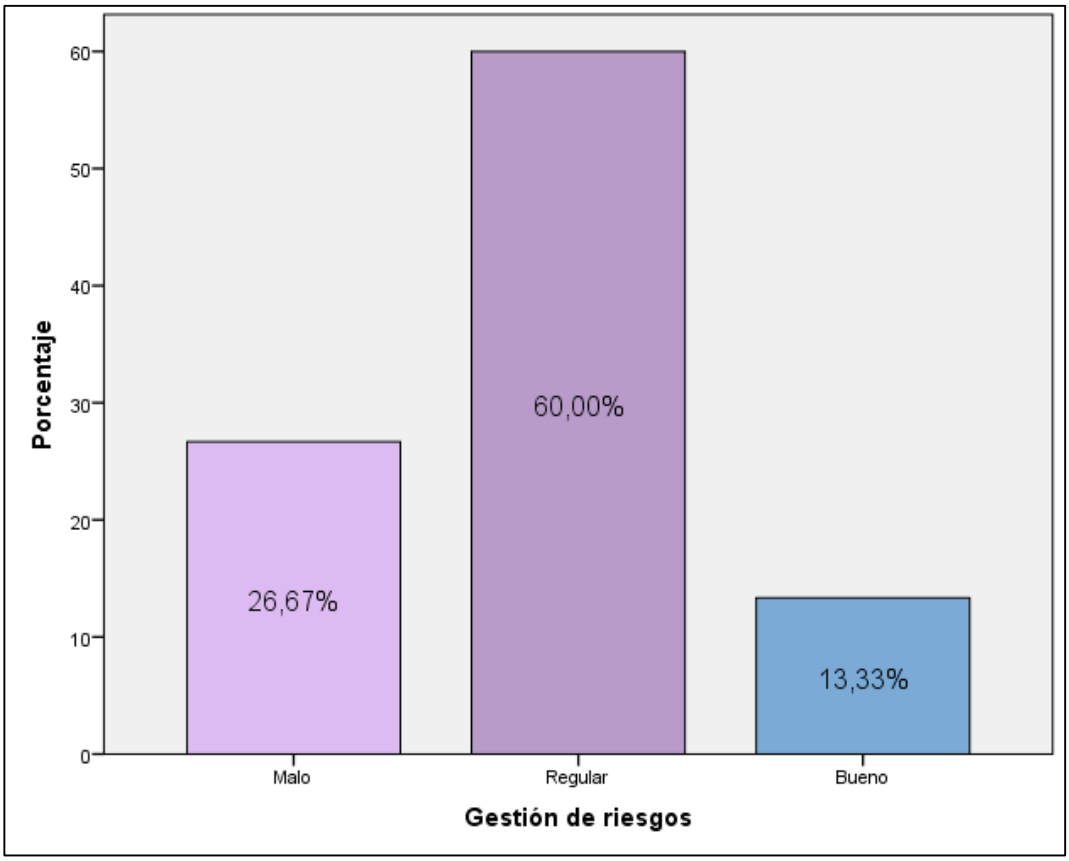

Figura 5. Nivel de variable dependiente
Fuente: Tabla N° 12

ANÁLISIS E INTERPRETACIÓN:

Los resultados que se logran apreciar en la Tabla 12 y Figura 5 respecto a los niveles de la variable Gestión de riesgos de TI de acuerdo a los colaboradores del IESTP Detecsur de Tacna, se observa que el 60.00% de los colaboradores perciben que el nivel es regular, el 26.67% es malo y el 13.33% es bueno. Los niveles de Gestión de riesgos se ven más influenciados por las dimensiones cultura consecuente sobre riesgos e implantación eficaz de las tecnologías de la información, siendo estos los que tienen mayor percepción con tendencia negativa en los resultados analizados en la investigación, factores como la cuantificación de las posibilidades de que ocurran riesgos evaluados y el seguimiento a las brechas de seguridad.

4.1.2.2. Análisis por dimensiones

Tabla 8
Nivel de Cultura consciente sobre riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	53.3	53.3	53.3
	Regular	4	26.7	26.7	80.0
	Bueno	3	20.0	20.0	100.0
	Total	15	100.0	100.0	

Fuente: Resultados SPSS

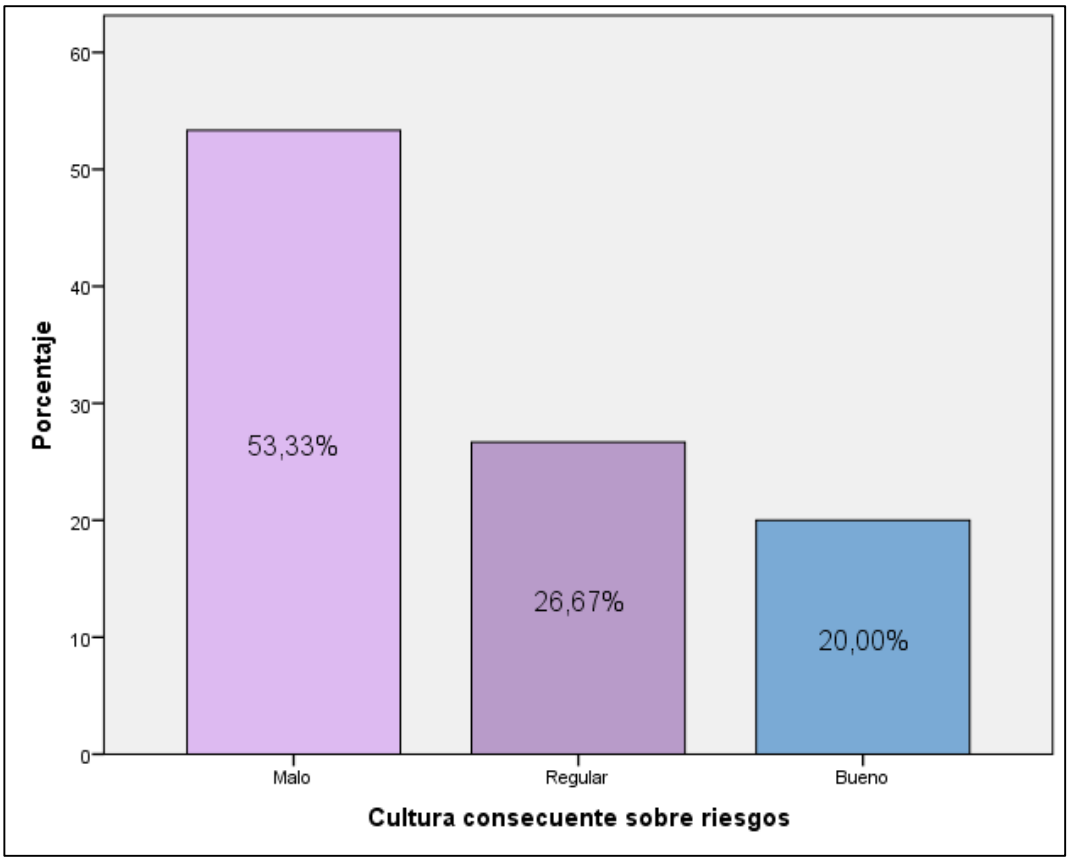

Figura 6. Nivel de Cultura consciente sobre riesgos
Fuente: Tabla N° 13

ANÁLISIS E INTERPRETACIÓN:

Los resultados que se logran apreciar en la Tabla 13 y Figura 6 respecto al nivel de la dimensión Cultura consciente sobre riesgos de la variable Gestión de riesgos de acuerdo a los colaboradores del IESTP Detecsur de Tacna, se observa que el 53.33% de los colaboradores perciben que el nivel es malo, el 26.67% es regular y el 20.00% es bueno. Las mayores percepciones negativas son referentes a la sensibilización en la gestión de riesgos y el compromiso con las acciones vinculadas a brindar protección y seguridad a los datos de los sistemas informático que se emplean en la institución.

Tabla 9
Nivel de Proceso de gobernanza del riesgo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	9	60.0	60.0	60.0
	Regular	6	40.0	40.0	100.0
	Bueno	0	0.0	0.0	100.0
	Total	15	100.0	100.0	

Fuente: Resultados SPSS

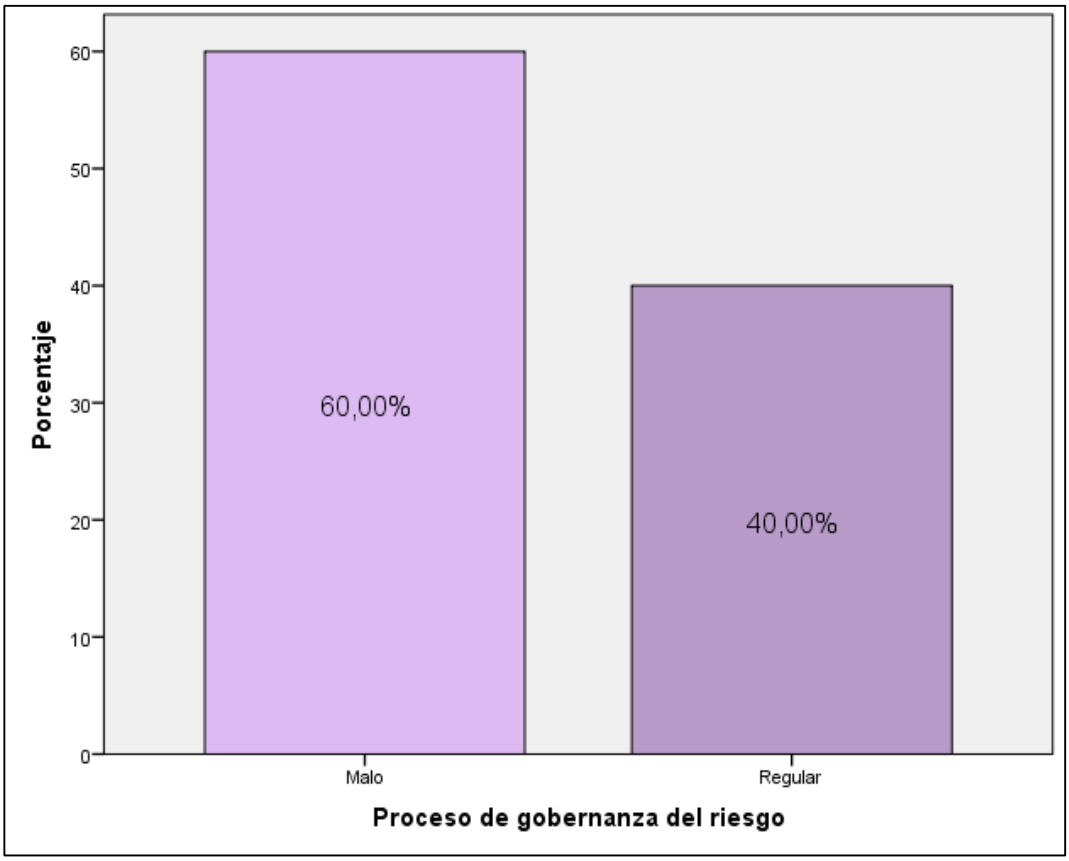

Figura 7. Nivel de Proceso de gobernanza del riesgo
Fuente: Tabla N° 14

ANÁLISIS E INTERPRETACIÓN:

Los resultados que se logran apreciar en la Tabla 14 y Figura 7 respecto al nivel de la dimensión Proceso de gobernanza del riesgo de la variable Gestión de riesgos de acuerdo a los colaboradores del IESTP Detecsur de Tacna, se observa que el 60.00% de los colaboradores perciben que el nivel es malo y el 40.00% es regular. Las mayores percepciones negativas son referentes a la falta de participación del personal en los procesos de identificación de los riesgos a los cuales se encuentra expuesto la información en cada área y la cuantificación de las posibilidades de ocurrencia de los riesgos identificados previamente.

Tabla 10
Nivel de Implantación eficaz de tecnologías de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	4	26.7	26.7	26.7
	Regular	7	46.7	46.7	73.3
	Bueno	4	26.7	26.7	100.0
	Total	15	100.0	100.0	

Fuente: Resultados SPSS

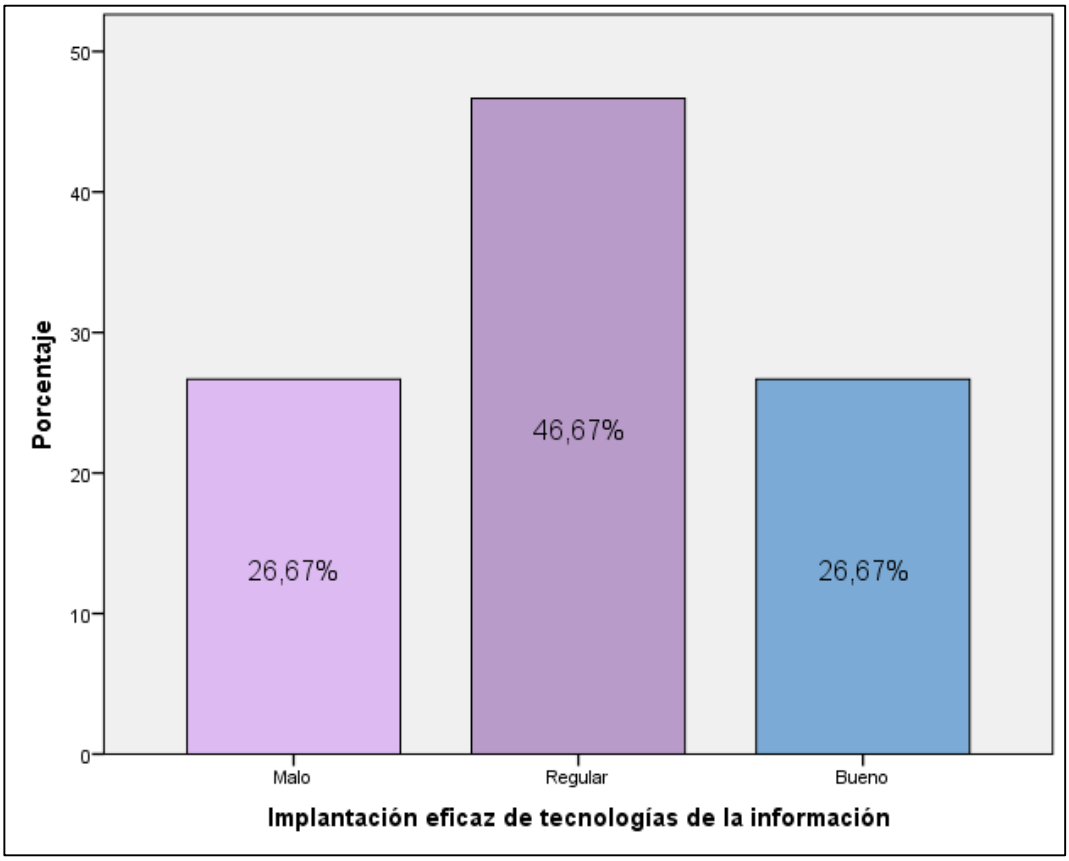

Figura 8. Nivel de Implantación eficaz de tecnologías de la información
Fuente: Tabla N° 15

ANÁLISIS E INTERPRETACIÓN:

Los resultados que se logran apreciar en la Tabla 15 y Figura 8 respecto al nivel de la dimensión Implantación eficaz de tecnologías de la información de la variable Gestión de riesgos de acuerdo a los colaboradores del IESTP Detecsur de Tacna, se observa que el 46.67% de los colaboradores perciben que el nivel es regular, el 26.67% es bueno y el 26.67% es malo. Las mayores percepciones negativas son referentes al seguimiento de las brechas de seguridad de información y la renovación de los equipos informáticos de la institución.

4.2. Contrastación de hipótesis

4.2.1. Análisis de fiabilidad

Hernández (2014) establece que la confiabilidad es el nivel en el cual un instrumento llega a producir resultados consistentes, además señala que el principal procedimiento usado para la determinación de la confiabilidad es el estadístico Alfa de Cronbach, indicador que oscila entre 0 y 1, en cual el valor de cero manifiesta una confiabilidad nula y el valor de uno una confiabilidad superior.

Para la determinación del índice de confiabilidad de los instrumentos empleados, se realizó la prueba Alfa de Cronbach a una muestra conformada por 15 prestadores de servicios de la institución educativa. Para la interpretación del nivel de confiabilidad se tomó en cuenta el conjunto de rangos formulados por Ruiz (2002).

Tabla 11
Magnitud de los rangos de confiabilidad

Rangos	**Magnitud**
0,81 a 1,00	Muy alta
0,61 a 0,80	Moderada
0,41 a 0,60	Baja
0,01 a 0,20	Muy baja

Fuente: Ruiz (2002)

4.2.1.1. Confiabilidad de la variable Seguridad de la información

Tabla 12
Resumen de casos - Variable independiente

		N	%
Casos	Válido	15	100.0
	Excluido	0	0.0
	Total	**15**	**100.0**

Fuente: Resultados SPSS

Tabla 13
Alfa de Cronbach - Variable independiente

Alfa de Cronbach	N de elementos
0.908	18

Fuente: Resultados SPSS

INTERPRETACIÓN:

El coeficiente Alfa de Cronbach del cuestionario realizado para medir la variable Seguridad de la información, conformado por 18 ítems y 3 dimensiones, dispone de un nivel de fiabilidad muy alta, gracias a un $\propto=0.908$.

4.2.1.2. Confiabilidad de la variable Gestión de riesgos de TI

Tabla 14
Resumen de casos - Variable dependiente

		N	%
Casos	Válido	15	100.0
	Excluido	0	0.0
	Total	**15**	**100.0**

Fuente: Resultados SPSS

Tabla 15
Alfa de Cronbach – Variable dependiente

Alfa de Cronbach	N de elementos
0.868	18

Fuente: Resultados SPSS

INTERPRETACIÓN:

El coeficiente Alfa de Cronbach del cuestionario realizado para medir la variable Gestión de riesgos de TI, conformado por 18 ítems y 3 dimensiones, dispone de una fiabilidad muy alta, gracias a un $\propto = 0.868$

4.2.2. Prueba de normalidad

Tabla 16
Evaluación de normalidad de la variable independiente

	Kolmogorov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad de la información	.155	15	.200	.940	15	.387
Disponibilidad	.192	15	.143	.931	15	.279
Confidencialidad	.190	15	.150	.882	15	.051
Integridad de datos	.189	15	.156	.913	15	.152

Fuente: Resultados SPSS

Tabla 17
Evaluación de normalidad de la variable dependiente

	Kolmogorov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Gestión de riesgos	.319	15	.000	.823	15	.007
Cultura consecuente sobre riesgos	.313	15	.000	.806	15	.004
Proceso de gobernanza del riesgo	.364	15	.000	.723	15	.000
Implantación eficaz de tecnologías de la información	.294	15	.001	.844	15	.014

Fuente: Resultados SPSS

ANÁLISIS INTERPRETACIÓN

En las dos (2) tablas anteriores se detallan los resultados de la aplicación de las pruebas estadísticas de distribución de normalidad, tanto el de Kolmogorov-Smirnov y Shapiro-Wilk, correspondiente a cada variable estudiada y sus correspondientes dimensiones, dado que la muestra es menor a treinta (30) unidades de estudio, se analizarán la significancia estadística obtenida de la prueba de Shapiro-Wilk. Los resultados que corresponden a la seguridad de la información la mayor parte de sus componentes denotan un nivel de significancia superior a 0.05, por tanto, se puede afirmar que la distribución de los datos sigue una tendencia normal. En cuanto a la Gestión de riesgos, la distribución de los datos es no normal, debido a niveles de significancia inferiores a 0.05. Dado que ambas variables demuestran una distribución de datos diferente, se aplicaron pruebas estadísticas de correlación no paramétricas para la comprobación de las hipótesis.

4.2.3. Pruebas de hipótesis

4.2.3.1. Hipótesis específica 1

Para la demostración de la hipótesis se formulan los siguientes elementos:

a) Nivel de significación: $\propto$ =0.05=5% de margen de error.

b) Regla de aceptación:

   $p \geq \propto \rightarrow$ se rechaza la H1.

   $p < \propto \rightarrow$ se acepta la H1.

c) Planteamiento de las hipótesis:

   H0: La dimensión disponibilidad no se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

H1: La dimensión disponibilidad se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

d) Resultados estadísticos:

Tabla 18
Correlación disponibilidad vs gestión de riesgos

			Disponibilidad	Gestión de riesgos
Rho de Spearman	Disponibilidad	Coeficiente de correlación	1.000	.697
		Sig. (bilateral)		.004
		N	15	15
	Gestión de riesgos	Coeficiente de correlación	.697	1.000
		Sig. (bilateral)	.004	
		N	15	15

Fuente: Resultados SPSS

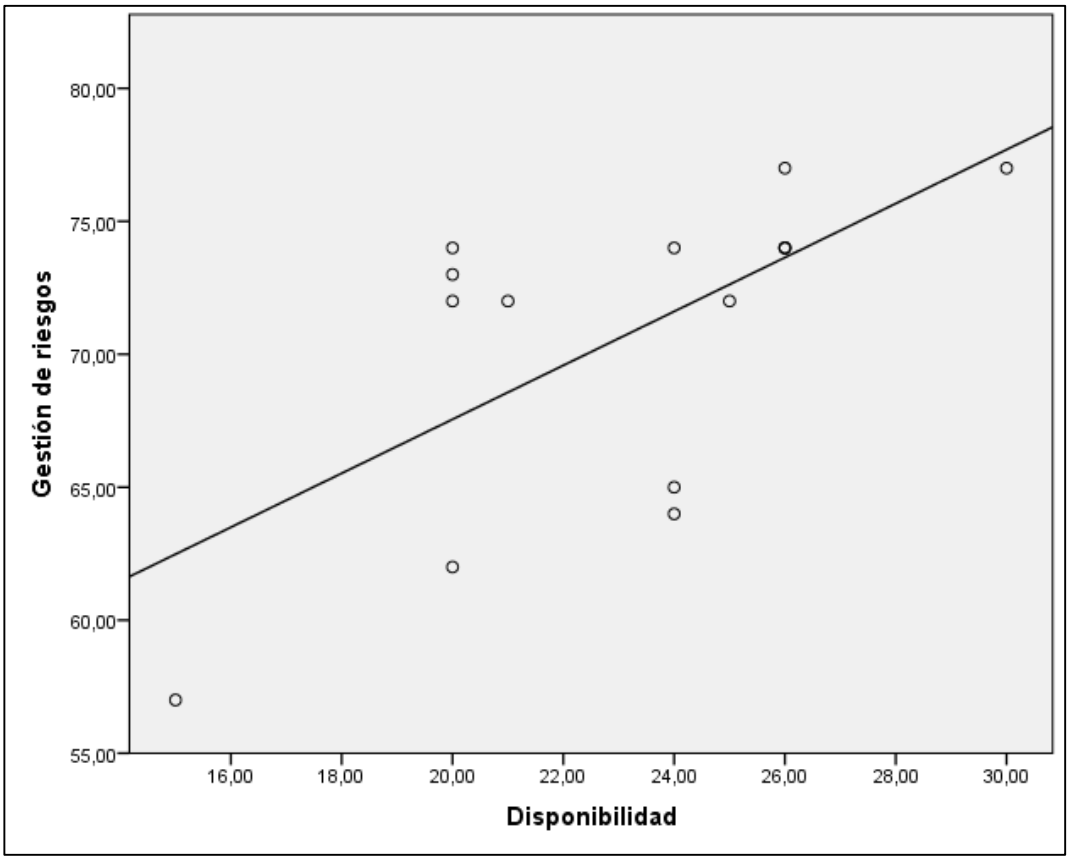

Figura 9. Diagrama de dispersión disponibilidad vs gestión de riesgos
Fuente: Resultados SPSS

e) Interpretación:

A través de los resultados de la prueba estadística de correlación y el diagrama de dispersión correspondiente, se observa que existe una relación directa y significativa entre la Disponibilidad y la Gestión de riesgos, representado por un p=.004 con un nivel de significación de .05 y el valor de correlación de .697, indicando que se relacionan de forma positiva alta. Concluyendo que la dimensión disponibilidad se relaciona directa y significativamente con la gestión de riesgos en el IESTP DETECSUR de la ciudad de Tacna.

4.2.3.2. Hipótesis específica 2

Para la demostración de la hipótesis se formulan los siguientes elementos:

a) Nivel de significación: $\propto$ =0.05=5% de margen de error.

b) Regla de aceptación:

   $p \geq \propto \rightarrow$ se rechaza la H1.

   $p < \propto \rightarrow$ se acepta la H1.

c) Planteamiento de las hipótesis:

   H0: La dimensión confidencialidad no se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

   H1: La dimensión confidencialidad se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

d) Resultados estadísticos:

Tabla 19
Correlación confidencialidad vs gestión de riesgos

			Confidencialidad	Gestión de riesgos
Rho de Spearman	Confidencialidad	Coeficiente de correlación	1.000	.664
		Sig. (bilateral)		.007
		N	15	15
	Gestión de riesgos	Coeficiente de correlación	.664	1.000
		Sig. (bilateral)	.007	
		N	15	15

Fuente: Resultados SPSS

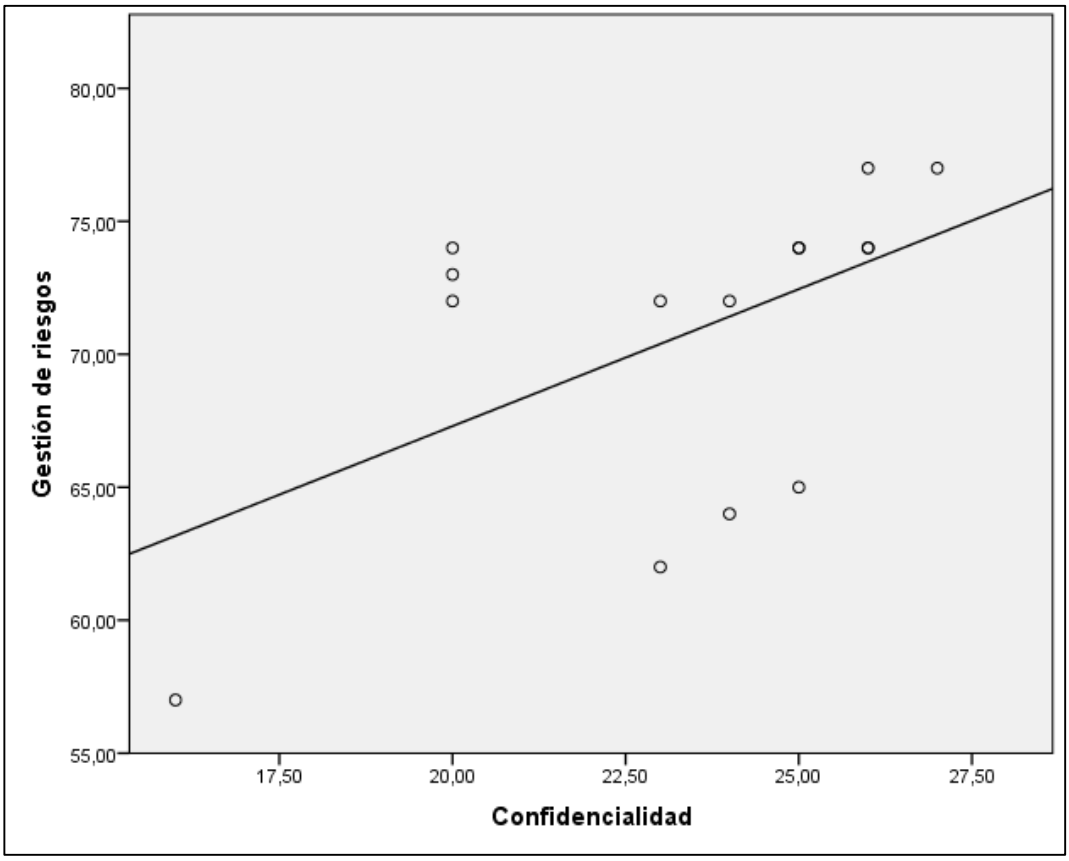

Figura 10. Diagrama de dispersión confidencialidad vs gestión de riesgos
Fuente: Resultados SPSS

e) Interpretación:

A través de los resultados de la prueba estadística de correlación y el diagrama de dispersión correspondiente, se observa que existe una relación directa y significativa entre la Confidencialidad y la Gestión de riesgos, representado por un p=.007 con un nivel de significación de .05 y el valor de correlación de .664, indicando que se relacionan de forma positiva alta. Concluyendo que la dimensión confidencialidad se relaciona directa y significativamente con la gestión de riesgos en el IESTP DETECSUR de la ciudad de Tacna.

4.2.3.3. Hipótesis específica 3

Para la demostración de la hipótesis se formulan los siguientes elementos:

a) Nivel de significación: $\propto$ =0.05=5% de margen de error.

b) Regla de aceptación:

   $p \geq \propto \rightarrow$ se rechaza la H1.

   $p < \propto \rightarrow$ se acepta la H1.

c) Planteamiento de las hipótesis:

   H0: La dimensión integridad de datos no se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

   H1: La dimensión integridad de datos se relación directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

d) Resultados estadísticos:

Tabla 20
Correlación integridad de datos vs gestión de riesgos

			Integridad de datos	Gestión de riesgos
Rho de Spearman	Integridad de datos	Coeficiente de correlación	1.000	.785
		Sig. (bilateral)		.001
		N	15	15
	Gestión de riesgos	Coeficiente de correlación	.785	1.000
		Sig. (bilateral)	.001	
		N	15	15

Fuente: Resultados SPSS

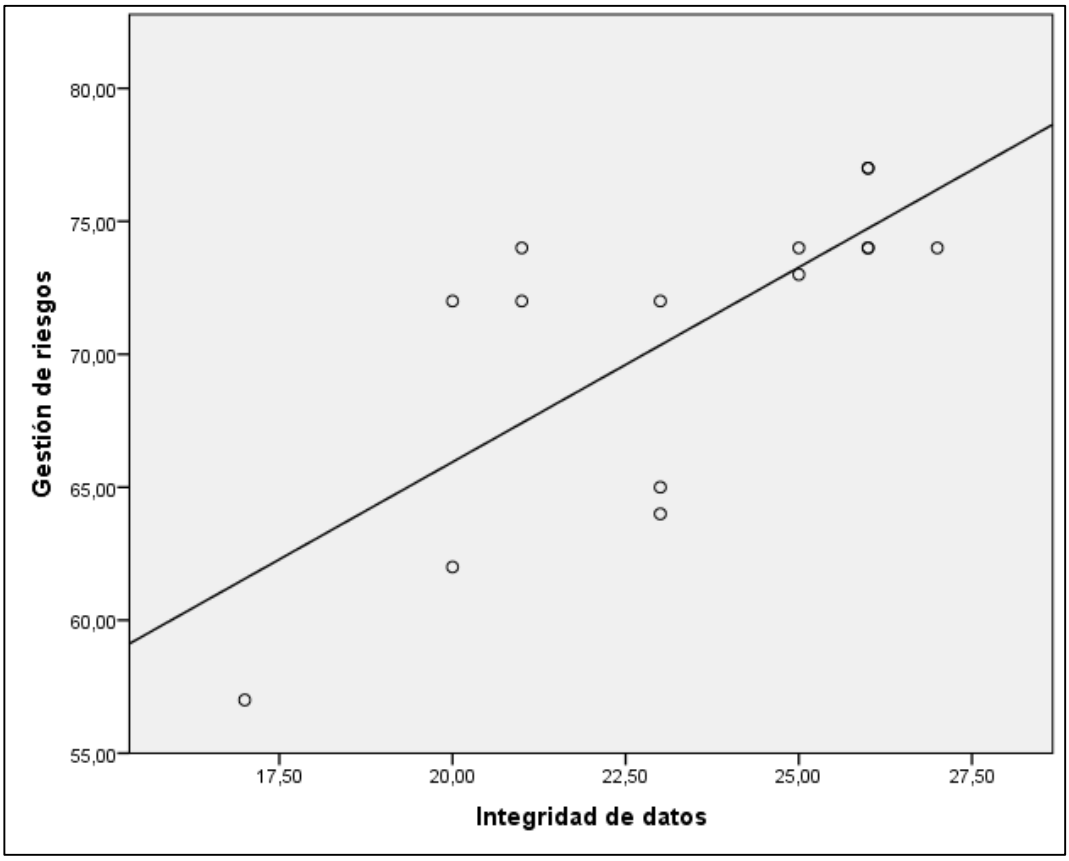

Figura 11. Diagrama de dispersión integridad de datos vs gestión de riesgos
Fuente: Resultados SPSS

e) Interpretación:

A través de los resultados de la prueba estadística de correlación y el diagrama de dispersión correspondiente, se observa que existe una relación directa y significativa entre la Integridad de datos y la Gestión de riesgos, representado por un p=.001 con un nivel de significación de .05 y el valor de correlación de .785, indicando que se relacionan de forma positiva alta. Concluyendo que la dimensión integridad de datos se relación directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

4.2.3.4. Hipótesis general

Para la demostración de la hipótesis se formulan los siguientes elementos:

a) Nivel de significación: $\propto$ =0.05=5% de margen de error.

b) Regla de aceptación:

   $p \geq \propto \rightarrow$ se rechaza la H1.

   $p < \propto \rightarrow$ se acepta la H1.

c) Planteamiento de las hipótesis:

   H0: La seguridad de la información no se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

   H1: La seguridad de la información se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

d) Resultados estadísticos:

Tabla 21
Correlación seguridad de la información vs gestión de riesgos

			Seguridad de la información	Gestión de riesgos
Rho de Spearman	Seguridad de la información	Coeficiente de correlación	1.000	.709
		Sig. (bilateral)		.003
		N	15	15
	Gestión de riesgos	Coeficiente de correlación	.709	1.000
		Sig. (bilateral)	.003	
		N	15	15

Fuente: Resultados SPSS

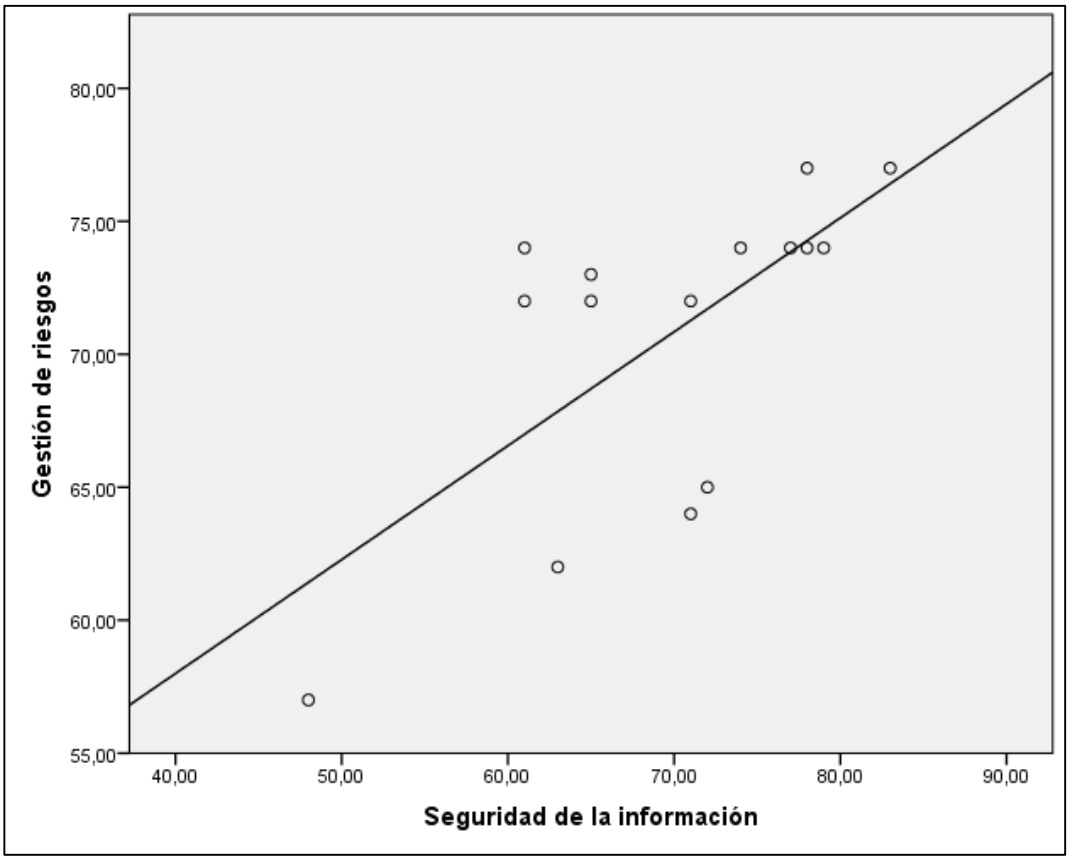

Figura 12. Diagrama de dispersión general
Fuente: Resultados SPSS

e) Interpretación:

A través de los resultados de la prueba estadística de correlación y el diagrama de dispersión correspondiente, se observa que existe una relación directa y significativa entre la Seguridad de la Información y la Gestión de riesgos, representado por un p=.003 con un nivel de significación de .05 y el valor de correlación de .709, indicando que se relacionan de forma positiva alta. Concluyendo que la seguridad de la información se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

4.3. Discusión de resultados

Los resultados logrados a través de la investigación denotaron, a través de la aplicación de encuestas para medir las variables Seguridad de la información y Gestión de riesgos, previamente validados mediante un coeficiente de fiabilidad Alfa de Cronbach de .908 y .868 de forma respectiva, que los colaboradores del IESTP Detecsur de Tacna, califican la seguridad de la información como malo (26.7%), regular (46.7%) y bueno (26.7%) y el nivel de la gestión de riesgos como malo (26.7%), regular (60.0%) y bueno (13.3%). Se observa que, en la institución educativa, la percepción de los colaboradores posee una tendencia negativa, mostrando valores negativos con mayor representatividad.

Respecto a las dimensiones, en el caso de la variable seguridad de la información, la dimensión disponibilidad el 6.7% señalaron que es bueno, el 53.3% regular y el 40.0% como malo; la dimensión confidencialidad es bueno (26.7%), regular (46.7%) y malo (26.7%); y en cuanto a la dimensión integridad de datos el 6.7% lo indica como bueno, el 60.0% como regular y 33.3% como malo.

En cuanto a las dimensiones de la variable gestión de riesgos, la dimensión cultura consecuente sobre riesgos, según la percepción de los colaboradores es bueno representado por un 20.0%, regular con un 26.7% y malo con un 53.3%; la dimensión proceso de gobernanza del riesgo posee un nivel regular con 40.0% y malo con 60.0%; y la dimensión implantación eficaz de tecnologías de la información fue calificado con un nivel bueno (26.7%), nivel regular (46.7%) y nivel malo (26.7%).

Debido a que la muestra de colaboradores es de 15 unidades de estudio, se eligió la prueba estadística de normalidad de Shapiro-Wilk para las dos variables,

indicando que su distribución de datos sigue una tendencia normal, significando la aplicación de pruebas estadísticas de correlación no paramétricas, el cuál a través un nivel de significancia bilateral menor a .05 (p = .003) demostraron la existencia de correlación significativa positiva alta (R = .709) entre las variables Seguridad de la información y gestión de riesgos. Resultado similar al obtenido por Calderón (2019), que estudio el caso de la oficina de Gestión de Recursos Humanos del Ministerio de Educación, en el cual obtuvo una relación significativa entre ambas variables con un R = .886, al igual que esta última variable y las dimensiones de la gestión de riesgos, tales como la disponibilidad (r = .866), confidencialidad (r = .866) e integridad de datos (r = .866).

Se observa a través de los resultados de la investigación, y su correspondiente comparación con los resultados logrados de otros estudios realizados con similares características, que la percepción de los propios trabajadores hacia la gestión de riesgos que realiza la institución y el trabajo que desarrollan poseen opiniones divididas con tendencias negativas, encontrándose trabajadores que consideran la gobernanza como mala y una proporción relativamente menor como regular.

Estas opiniones se validan estadísticamente a través de una prueba de correlación, siendo el caso del presente estudio, la relación entre dichas variables denota una relación positiva alta, indicando que existen otros factores que no son motivos de estudio del presente documento que afectan a la gestión de riesgos de las instituciones educativas de Tacna, pudiendo ser uno de estos factores la falta de conocimiento y áreas especializadas por parte de las entidades.

En el presente estudio también se determinó la relación entre la gestión de riesgos y las dimensiones que representan a la seguridad de la información, respecto a la dimensión disponibilidad se demostró una relación directa alta ($R=0.697$, $p < 0.05$). En cuanto a la dimensión confidencialidad, se demostró en el presente estudio la presencia de una relación directa y proporcionalmente significativa con la gestión de riesgos ($R=0.667$, $p<0.05$). Finalmente, la dimensión integridad de datos posee una relación directa con la gestión de riesgos, representando por un $R=0.785$ y un $p=0.001$.

Considerando que la seguridad de la información tiene relación directa con la gestión de los riesgos, en cualquier tipo de institución, las entidades tienen que reforzar y/o concientizar a los trabajadores sobre la importancia de un adecuado manejo de las tecnologías y de la información, para apoyar al logro de los objetivos estratégicos de la institución, así también el apoyo de la gerencia para destinar los recursos necesarios al área competente para reforzar y actualizar las medidas de seguridad.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Luego de la evaluación de los resultados conseguidos del procesamiento de los datos y en concordancia con los objetivos planteados inicialmente, se llegó a las subsiguientes terminaciones:

PRIMERO: Se ha determinado la correlación de Spearman entre las variables Seguridad de la información y Gestión de riesgos es de .709 que de acuerdo a los niveles de evaluación denota la existencia de una relación positiva alta, determinando que son variables directamente proporcionales. Además se estableció que el grado de significancia calculado es de .003, determinando que existe certeza suficiente para aseverar que la seguridad de la información se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

SEGUNDO: Se ha establecido la correlación de Spearman entre las variable Gestión de riesgos y la dimensión Disponibilidad es de .697 que de acuerdo a los niveles de evaluación denota la existencia de una relación positiva alta,

determinando que son variables directamente proporcionales. Además se estableció que el grado de significancia calculado es de .004, determinando que existe certeza suficiente para aseverar que la dimensión disponibilidad se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

TERCERO: Se ha establecido la correlación de Spearman entre las variable Gestión de riesgos y la dimensión Confidencialidad es de .664 que de acuerdo a los niveles de evaluación denota la existencia de una relación positiva alta, determinando que son variables directamente proporcionales. Además se estableció que el grado de significancia calculado es de .007, determinando que existe certeza suficiente para aseverar que la dimensión confidencialidad se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

CUARTO: Se ha establecido la correlación de Spearman entre las variable Gestión de riesgos y la dimensión Integridad de datos es de .785 que de acuerdo a los niveles de evaluación denota la existencia de una relación positiva alta, determinando que son variables directamente proporcionales. Además se estableció que el grado de significancia calculado es de .001, determinando que existe certeza suficiente para aseverar que la dimensión Integridad de datos se relaciona directa y significativamente con la gestión de riesgos en el IESTP Detecsur de la ciudad de Tacna.

5.2. Recomendaciones

1. De acuerdo a los resultados se observa que el nivel de seguridad de la información y gestión de riesgos es aceptable, empero se sugiere implementar estrategias, representado a través de proyectos de capacitación y sensibilización, así como la mejora e implementación de indicadores de seguridad de la información.

2. Se recomienda a la institución educativa que para mejorar sus operaciones, se debe de adquirir nuevos equipos informáticos, dado que los que poseen son obsoletos y excedieron el tiempo de vida útil como activo de la empresa; mediante esta optimización de sus recursos se logrará mejorar los tiempos de obtención de información, además de mejorar el almacenamiento de las copias de seguridad de la base de datos.

3. Diversas instituciones poseen políticas de seguridad, pero son pocas las que implantan una cultura de conciencia de seguridad para fomentar la identificación del trabajador con la información que gestiona, por ello es necesario y recomendable el desarrollo de un marketing efectivo sobre seguridad de la información a todos los colaboradores de las instituciones, desde los niveles inferiores a los superiores.

4. Se recomienda rediseñar las redes informáticas de la institución, separando el área académica del área administrativa, debido a que tienen sistemas de administración críticos, además se deberá de consolidar sus

redes aplicando tecnologías para la prevención y detección de potenciales intrusos, observando el tráfico de red, permitiendo únicamente el ingreso de tráfico legítimo e identificar los comportamientos maliciosos.

BIBLIOGRAFIA

Barrantes, C. (2012). *Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos.* Tesis de grado, Universidad de San Martín Porres, Lima.

Bernal, C. (2010). *Metodología de la investigación.* Colombia: Pearson Educación.

Bon, V. (2008). *Estrategia de Servicio Basado en ITIL V3.* Reino Unido: Editorial del Gobierno Británico.

Calderón, J. (2019). *Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018.* Tesis de maestría, Escuela de Posgrado, Lima.

Calderon, L. (2019). *Gestión de riesgos y seguridad de la información del Programa Fortalece Perú del MTPE, 2019.* Tesis de maestría, Universidad César Vallejo, Lima.

Castro, F. (2003). *El proyecto de investigación y su esquema de elaboración.* Caracas: Uyapal.

Coaguila, M. (2020). *Diseño de un plan de gestión de seguridad de información alineado a la Norma ISO/IEC 27001: Caso Universidad nacional de Moquegua.* Tesis de maestría, Universidad José Carlos Mariátegui, Moquegua.

Crespo, P. (2016). *Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPymes.* Tesis de maestría, Universidad de Cuenca, Cuenca.

Díaz, R. (2018). *La auditoría informática y la seguridad de la información en el áreade sistemas de la Caja del Santa, Chimbote - 2018.* Tesis de maestría, Universidad Privada del Norte, Trujillo.

Féliz, A., & Calvo, J. (2014). *Comparison of models and standars for implementing IT service capacity management.* Artículo Científico, Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros Informáticos, Madrid.

Galindo, C., Bladimir, A., & Santizo, W. (2014). *Seguridad de la información.* Guatemala: Universidad San Carlos de Guatemala.

Gavino, A. (2018). *Auditoria en seguridad informática y gestión de riesgo en el Hospital Regional de Huacho, 2018.* Tesis de maestría, Universidad Nacional José Faustino Sánchez Carrión, Huacho.

Guerrero, M., & Gómez, L. (2012). Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. *Estudio gerenciales, 28*(125), 87-95.

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

Huanca, J. (2019). *Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud*

Virgen de Cocharcas - Chincheros. Tesis de grado, Universidad Nacional José María Arguedas, Facultad de Ingeniería, Apurímac.

Kuna, H. (2006). *Asistente para la realización de auditoría de sistemas en organismos públicos o privados.* Tesis de maestría, Universidad Politécnica de Madrid, Madrid.

Maquera, H., & Serpa, P. (2017). Gestión de activos basado en ISO/IEC 27002 para garantizar seguridad de la información. *Ciencia & Desarrollo, 16*(21), 100 - 112.

Miranda, M., Valdés, O., Pérez, I., Portelles, R., & Sánchez, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas, 10*(2).

Muñoz, J. (2016). *Diseño de políticas de seguridad informática para la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad de Cuenca.* Tesis de maestría, Universidad de Cuenca, Cuenca.

Niño, N. (2018). *Modelo de un sistema de gestión de seguridad de información - SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI Filial Lambayeque.* Tesis de maestría, Universidad Nacional Pedro Ruiz Gallo, Lambayeque.

Oltra, R. (2016). *Gestión de Servicios de TI (ITSM).* Valencia: Universitat Politécnica de Valéncia.

Osorio, E., & Reascos, A. (2015). *Desarrollar e implementar un sistema gestor de incidentes en el área PS&I - GDO para la empresa Xeros del Ecuador S.A.* Tesis de grado, Universidad de las Fuerzas Armadas, Departamento de las Ciencias de la Computación, Sangolquí.

Palacios, A. (2015). *Diseño de un modelo de políticas de seguridad informática para la Superintendencia de Industria y Comercio de Bogotá.* Tesis de posgrado, Universidad Libre de Colombia, Facultad de Ingeniería, Bogotá.

Parada, D., Flórez, A., & Gómez, U. (2018). Análisis de los componentes de la seguridad de una perspectiva sistémica de la Dinámica de Sistemas. *Información tecnológica, 29*(1).

Pinzón, I. (2014). *Gestión del riesgo en Seguridad Informática.* Artículo científico, Universidad Piloto de Colombia.

Robledo, T., Loinaz, B., Lozano, G., & Sánchez, J. (2017). *Grupo auxiliar de la Función Administrativa.* Sevilla: Ediciones Rodio.

Vara, A. (2012). *Desde la idea hasta la sustentación: Siete pasos para una tesis exitosa. Un método efectivo para las ciencias empresariales.* Universidad de San Martín de Porres, Instituto de Investigación de la Facultad de Ciencias Administrativas y Recursos Humanos, Lima.