UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Ciberseguridad y su incidencia en la gestión de seguridad de la información en una entidad pública, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información

AUTOR:

Rivera Lazaro, Wilfredo Elias (orcid.org/0000-0002-6289-5642)

ASESOR:

Dr. Acuña Benites, Marlon Frank (orcid.org/0000-0001-5207-9353)

CO-ASESOR:

Mtro. Aliaga Cerna, Dante (orcid.org/0000-0002-5775-3885)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

Dedicatoria

A Dios, mis padres, mi esposa y mis hijos quienes han sido apoyo e impulso para seguir reinventándome y evolucionando

Agradecimiento

Al ser supremo, fuente infinita de sabiduría y amor.

A mis padres, por sus enseñanzas y apoyo hasta el último día que pudieron.

A mi esposa e hijos por su paciencia y cariño en todo este tiempo.

A mi asesor por su paciencia, orientación y sugerencias, volcadas en el presente.

Declaratoria de autenticidad del asesor

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis Completa titulada: "Ciberseguridad y su incidencia en la Gestión de Seguridad de la Información en una entidad pública, Lima 2023", cuyo autor es RIVERA LAZARO WILFREDO ELIAS, constato que la investigación tiene un índice de similitud de 12.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis Completa cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 31 de Julio del 2023

Apellidos y Nombres del Asesor:	Firma
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 31-07-2023 22:59:20

Código documento Trilce: TRI - 0632274

INVESTIGA UCV

Declaratoria de originalidad del autor

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Originalidad del Autor

Yo, RIVERA LAZARO WILFREDO ELIAS estudiante de la ESCUELA DE POSGRADO del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Ciberseguridad y su incidencia en la Gestión de Seguridad de la Información en una entidad pública, Lima 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	Firma
RIVERA LAZARO WILFREDO ELIAS **DNI:** 10057591 **ORCID:** 0000-0002-6289-5642	Firmado electrónicamente por: WRIVERAL el 14-08-2023 08:53:39

Código documento Trilce: INV - 1241250

INVESTIGA UCV

Índice de contenidos

Pág.

Índice de tablas

Índice de figuras

Resumen

La presente investigación tuvo como objetivo general determinar la incidencia de la Ciberseguridad en la Gestión de Seguridad de la Información de una entidad pública, Lima 2023. El tipo de investigación que se empleo fue de tipo básica, con un diseño no experimental de tipo transversal de nivel correlacional; con el propósito de comprobar la incidencia de las variables estudiadas en un momento especifico. Asimismo, la población y muestra en esta investigación estuvo compuesta por 75 trabajadores de la entidad pública.

En el análisis descriptivo se utilizó tablas cruzadas e histogramas, del cual se evidencia que la ciberseguridad tendrá un nivel adecuado ante la incidencia satisfactorio de la Gestión de Seguridad de la Información; mientras que en análisis inferencial se usó la regresión logística ordinal, de cual se pudo concluir que existe incidencia significativa de la Ciberseguridad en la Gestión de Seguridad de la Información; lo cual se fundamentó al obtener un valor de significancia de 0.000 menor a 0.05 el cual confirma la anterior conclusión. Además, se obtuvo un valor de R2 de Nagelkerke igual a 0.609, el cual representa el grado de incidencia entre las variables en un 60.9%.

Palabras clave: Ciberseguridad, Gestión de Seguridad de la Información, Gestión de Tecnologías de información, Ciberespacio, Ataque cibernético.

Abstract

The present investigation had as general objective to determine the incidence of Cybersecurity in the Information Security Management of a public entity, Lima 2023. The type of investigation that was used was of a basic type, with a non-experimental design of a transversal type of correlational level; with the purpose of verifying the incidence of the variables studied at a specific moment. Likewise, the population and sample in this investigation consisted of 75 workers of the public entity.

In the descriptive analysis, cross tables and histograms were used, from which it is evident that cybersecurity will have an adequate level given the satisfactory incidence of Information Security Management; while in inferential analysis ordinal logistic regression was used, from which it was possible to conclude that there is a significant incidence of Cybersecurity in Information Security Management; which was based on obtaining a significance value of 0.000 less than 0.05 which confirms the previous conclusion. In addition, a Nagelkerke R2 value equal to 0.609 was obtained, which represents the degree of incidence between the variables by 60.9%.

Keywords: Cybersecurity, Information Security Management, Information Technology Management, Cyberspace, Cyber attack.

I. INTRODUCCIÓN

La seguridad informática es importante para la sociedad porque la cantidad de ataques continúa aumentando y estas amenazas continúan volviéndose más sofisticadas, afectando a las organizaciones y a las personas Infoguard (2019).

La ciberseguridad es un tema importante para las organizaciones. A medida que continúa la digitalización y se adoptan nuevas tecnologías a un ritmo acelerado, las organizaciones dependen de las tecnologías de la información, por lo tanto, la protección contra los riesgos de ciberseguridad es importante para muchas organizaciones Wang et al. (2020).

Hoy en día, ninguna organización puede sobrevivir sin las medidas de ciberseguridad adecuadas. La educación, el gobierno, la salud, las finanzas y las redes sociales son solo algunos de los muchos sectores verticales de la industria que han sido afectados por los ataques cibernéticos.

A nivel internacional, Tesco, una cadena de supermercados británica, se enfrentó a una interrupción de dos días debido a un intento de ciberataque, lo que provocó que tanto su sitio web como su aplicación quedaran inaccesibles para los clientes. Esto dejó frustrados a muchos de sus 6,6 millones de usuarios de la aplicación, lo que provocó que cancelaran pedidos y llevaran sus negocios a otra parte. El proveedor de servicios de Internet Yahoo fue víctima de tres violaciones de datos separadas entre 2013 y 2016, que afectaron hasta tres mil millones de cuentas. Esto provocó un acuerdo de demanda colectiva de un estimado de $ 117,5 millones. Además de la evidente mella financiera, la lenta divulgación de estas infracciones al público por parte de Yahoo provocó daños a la reputación. La seguridad cibernética ha estado bajo el foco de atención durante mucho tiempo debido al rápido ritmo del crecimiento tecnológico. La pandemia y la automatización resultante de casi todos los aspectos de la vida han acelerado el mercado de la ciberseguridad incluso más de lo esperado. Asimismo, Fortinet (2023) en su informe de investigación de brecha de competencias en ciberseguridad 2023 menciona que el 84% de las organizaciones experimentaron una o más violaciones de seguridad

en el año 2022, en esa misma línea CyberedgeGroup (2022) reporta que el 85%de las organizaciones sufrieron un ciberataque exitoso durante el año 2022.

En nuestro país, en el año 2018, el Banco de la Nación de Perú sufrió un ciberataque que resultó en el robo de más de 2 millones de soles de cuentas bancarias; en el año 2019, la Bolsa de Valores de Lima fue hackeado, lo que resultó en la publicación de un mensaje en el que se criticaba la falta de seguridad del sitio web; en el año 2020, la UNMSM sufrió un ciberataque que resultó en la filtración de información confidencial, incluidos nombres, fechas de nacimiento y números de DNI de estudiantes y docentes y en el año 2021, la aerolínea peruana Aero Perú sufrió un ciberataque que afectó a su sitio web y a su sistema de reservas en línea, lo que resultó en la filtración de información de los clientes, finalmente el 19 de septiembre de 2022, el grupo de hacker denominado “Guacamaya Roja”, publicó un comunicado donde señala que habían hackeado los sistemas militares y policiales de Perú. Asimismo, Fortinet anunció que Perú recibió 15 mil millones de ciberataques en el año 2022, un crecimiento del 35% frente al año 2021, según datos de FortiGuard Labs.

Teniendo en cuenta lo anterior, algunas instituciones públicas nacionales han introducido nuevas herramientas tecnológicas, que deben ser funcionales para la implementación de los servicios de gestión de TI, asimismo deben cumplir de manera integral y sistemática con los estándares de seguridad. La entidad pública no es ajena al problema, ya que la entidad ha tenido intentos de ataques cibernéticos. Por ello, es importante esta investigación, con el fin de proponer medidas preventivas y correctivas que permitan fortalecer su sistema de información.

Teniendo en cuenta los aspectos mencionados anteriormente, esta investigación tiene como formulación general del problema: ¿De qué manera la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023?; con los subsiguientes problemas: (a) ¿De qué manera la prevención de la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023?, (b) ¿De qué manera la detección de la

ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023?, (c) ¿De qué manera la recuperación de la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023?.

Este estudio se justifica por varias razones. En términos epistemológicos, se busca encontrar los factores clave que influyen las relaciones entre la seguridad cibernética y la administración del SGSI, con el objetivo de mejorar el entorno informático y la protección de los sistemas en las organizaciones. Además, la investigación empírica puede ayudar a generar nuevos conocimientos y comprensión en los campos de la ciberseguridad y las administraciones de SGI en las empresas.

En términos prácticos el tema de estudio es significativo dado que la digitalización se ha apoderado de todas las empresas, la tecnología se integra en todo y las empresas deben pensar en la ciberseguridad desde un punto de vista completamente nuevo. La ciberseguridad debe abordarse de manera integral y holística. Asumir la responsabilidad, mostrar el compromiso e incorporar la ciberseguridad a todo lo que se enciende desde la alta dirección, se conecta a través de ella para desarrollarse en toda la empresa.

Finalmente, la justificación metodológica del presente estudio tiene como base la necesidad de utilizar un enfoque metodológico riguroso y adecuado para abordar la complejidad y la multidisciplinariedad del tema. Es necesario desarrollar un método para recopilar, analizar y sintetizar información de varias fuentes para comprender la gestión de la ciberseguridad y su correspondencia con la gestión del SGSI.

Por lo tanto, el objetivo general es: Determinar la incidencia de la ciberseguridad en la gestión de seguridad de la información en una entidad pública, Lima 2023. Y teniendo en cuenta los problemas específicos, se plantearon los objetivos: (a) Determinar la incidencia de la prevención de la ciberseguridad en la gestión de seguridad de la información en una entidad pública, Lima 2023, (b)

Determinar la incidencia de la detección de la ciberseguridad en la gestión de seguridad de la información en una entidad pública, Lima 2023, (c) Determinar la incidencia de la recuperación de la ciberseguridad en la gestión de seguridad de la información en una entidad pública, Lima 2023.

Finalmente, para dar respuesta a la pregunta general se tiene la hipótesis principal: La ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023. Igualmente, se establecen las hipótesis especificas: (a) La prevención de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023, (b) La detección de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023, (c) La recuperación de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

II. MARCO TEÓRICO

Según Calderón (2019) quien realizó un trabajo que, establecido la relación entre la seguridad informática y la administración de riesgos, el diseño fue transversal, correlacional, no experimental y se enmarca en la categoría de investigación básica. La población estuvo conformada por 106 colaboradores quienes fueron escogidos mediante muestreo probabilístico simple y aleatorio; Se utilizó SPSS para trabajar con los datos; Se aplicó la prueba de rango de correlación no paramétrica Rho de Spearman. Los hallazgos del estudio indicaron una correlación directa entre la administración de riesgos de los trabajadores y la SGSI. Teniendo como resultado que existe una correlación directa entre ambas variables.

Ñañez (2021) realizó un trabajo de investigación cuyo propósito fue establecer un diseño de trámite de riesgos de TI. La perspectiva que utilizó fue cuantitativo de tipo básico; con una muestra de 40 trabajadores, utilizando una encuesta. Entre las conclusiones se confirmó que el SGSI se encuentra un nivel regular 69%, 65.5% y 58.6%.

Risco (2021), en su investigación utilizó el diseño del tipo preexperimental, metodología cuantitativa y buscó conocer el impacto de un SGSI. Adicionalmente, se utilizó 20 registros por cada indicador para obtener un resultado favorable en las dimensiones. Las conclusiones obtenidas muestran que la confidencialidad de la vulnerabilidad de la información disminuyó de 68.85% a 15.40%, la integridad de la vulnerabilidad de la información disminuyó de 52.60% a 11.40% y la disponibilidad de la vulnerabilidad de la información podría reducirse de 47.15% a 15.40%. El SGSI tiene un impacto positivo en el negocio.

También Mallqui (2022) en su trabajo tiene el propósito de establecer cómo la ciberseguridad afecta la administración de TI. El enfoque fue básico, del tipo no experimental, un estudio transversal de nivel correlacional-causal. Se seleccionó una muestra de 175 servidores, de una población total de 321 servidores, utilizando un muestreo probabilístico simple, utilizando una encuesta y un cuestionario como

instrumento. Las conclusiones indican que la ciberseguridad influye en la administración de TI en un 53,7%, lo que indica una correlación positiva importante.

Asimismo, Bohorquez (2020) en su estudio se pretendía establecer la correspondencia entre la ciberseguridad con la administración de tecnologías. Su enfoque fue de tipo básico, correlacional - no experimental con 71 trabajadores como muestra, utilizando una encuesta y un cuestionario como instrumento, teniendo como resultado que existe una correlación fuerte de 0,832.

También, Correa (2022) en su análisis cuyo propósito fue averiguar el estado de la ciberseguridad cuando se trata de información personal, desarrollo un trabajo con diseño no experimental, utilizo a 1046 personas, aplicando como instrumento una encuesta, las conclusiones indican que el procesamiento de los datos personales se ven afectado por la ciberseguridad.

Asimismo, Flores (2023) en su estudio que pretende establecer una relación que existe entre la ciberseguridad y la administración de riesgos de TI, utilizó una investigación aplicada, un diseño preexperimental, para este estudio la población fue de 30 empleados del departamento de TI, esta investigación obtuvo un Rho de Spearman de 0.833, datos que indican que existe una dependencia entre las variables.

Por otro lado, Marín (2022) en su trabajo que tuvo como fin establecer la influencia de la ciberseguridad en el teletrabajo, realizó un estudio no experimental con una población de 150 personas, concluyendo que existe un grado de significancia de 76.4% entre las variables.

Bustamante et al. (2021), en su análisis, tuvieron como propósito la mejora de la administración del SGSI en una municipalidad aplicando políticas de la ISO 270001, el enfoque fue preexperimental con una muestra de 30 trabajadores de un total de 90 trabajadores, utilizando un cuestionario como instrumento. Los resultados indicaron que más del 90 % reconoció mejoras en la institución, se concluye que el modelo de políticas mejoró la gestión del SGSI.

Igualmente, E. D. León et al. (2020), en el trabajo que tiene como objetivo revisar los avances y cambios en materia de ciberseguridad en el Perú. La metodología utilizada en esta revisión incluyó la revisión de información sobre seguridad cibernética en el país, así como la identificación de políticas y estrategias gubernamentales y de la industria en esta área. El grupo objetivo de esta revisión es el país fueron los sectores público y privado. Los hallazgos muestran que, si bien se ha logrado avances en seguridad cibernética en los últimos años, aún se enfrenta desafíos importantes. Estos incluyen la falta de inversión en seguridad cibernética, la falta de conciencia y educación sobre seguridad cibernética y la falta de una regulación efectiva.

De igual importancia Quevedo (2023) en su artículo que tiene como objetivo analizar las Fuerzas Armadas con relación a su capacidad para atender ciberataques, utiliza una metodología de análisis de documentos oficiales, entrevistas a expertos en ciberseguridad y defensa nacional, así como la revisión de estudios y estadísticas relacionados. La población objetivo son las Fuerzas Armadas del Perú y su capacidad para enfrentar ciberataques que puedan comprometer la seguridad nacional. Los resultados de este artículo indican que, si bien ha habido avances en la implementación de medidas de ciberdefensa y ciberseguridad en las Fuerzas Armadas, aún existen retos importantes a enfrentar.

En las referencias internacionales mencionamos a Choejey et al. (2017) quien evaluó el impacto de la percepción de la ciberseguridad en entidades del gobierno, fue un estudio explicativo de enfoque cuantitativo, El estudio indica que la ciberseguridad se está desarrollando en las empresas de forma no adecuada, creando una brecha de seguridad, por lo tanto, se determina que la implementación de esquemas de ciberseguridad influye en un 40% sobre las políticas relacionadas a ciberseguridad en las empresas.

Según Razikin & Soewito (2022) en la investigación presenta un modelo de apoyo en ciberseguridad para el diseño de sistemas de seguridad, sistemas que evaluaran riesgos en un determinado marco de ciberseguridad, utiliza una metodología que incluye la revisión de literatura, un cuestionario y entrevistas con

expertos en ciberseguridad. El público objetivo son las organizaciones que desean configurar un SGSI. Los resultados concluyen que la propuesta puede ayudar a tomar decisiones sobre el SGSI y reducir los riesgos de ciberseguridad.

Según Guillermo (2020) en el artículo analiza el papel del personal de una organización como una fuente potencial de riesgo en la ciberseguridad, utiliza la metodología de revisión bibliográfica y análisis de estudios de caso relacionados con incidentes de seguridad causados por el personal de una organización. La población objetivo fueron las organizaciones que dependen de las tecnologías. Las conclusiones del estudio muestran que el personal de una organización puede ser una fuente potencial de riesgo para la ciberseguridad debido a factores como el desconocimiento en cuestiones de TI, el uso inadecuado de dispositivos y la falta de conciencia sobre las políticas del SGSI.

Asimismo, Velecela (2020) elaboró un artículo que tiene como propósito presentar un plan de administración del SGSI para el Gobierno Provincial del Cañar en Ecuador. La metodología utilizada fue un estudio de caso en el Gobierno Provincial del Cañar, donde se realizó una evaluación de riesgos y se propuso un proyecto de administración del SGSI alineado en la norma ISO 27001. Tuvo como población objetivo los empleados y usuarios del sistema de la organización. Las conclusiones señalan que la ejecución de un plan de administración del SGSI ayudó a mejorar el SGSI en la organización.

Alzahrani (2021) elaboro una investigación que busco examinar y analizar los problemas de seguridad cibernética, incluido el riesgo cibernético, la seguridad cibernética, la conciencia de seguridad cibernética y la confianza cibernética, entre los estudiantes de educación superior en Arabia Saudita. Basado en un análisis de los datos recopilados utilizando SPSS, los hallazgos de este estudio resaltan la falta de conocimiento de la información básica relacionada con la seguridad cibernética entre los estudiantes saudíes. Además, el número de estudiantes que asistían a programas de formación era muy bajo. Teniendo en cuenta otros problemas de seguridad, este estudio revela que, si bien los estudiantes saudíes son conscientes del riesgo cibernético, no son conscientes de la seguridad cibernética. La meta de

esta investigación fue analizar los problemas de seguridad cibernética en Arabia Saudita. Según las conclusiones de esta encuesta, los estudiantes saudíes desconocen la importancia de la ciberseguridad. Esta investigación indicó un puntaje bajo en capacitación y concientización, ya que el 92 por ciento de los encuestados nunca recibió ningún tipo de capacitación en seguridad cibernética. De acuerdo con los hallazgos de este estudio, las instituciones saudíes deberían enseñar a sus estudiantes sobre la legislación contra el ciberdelito y los problemas clave de concienciación en materia de seguridad informática.

En cuanto al desarrollo teórico que avalan la presente investigación se consideró la teoría general de sistema (TGS) desarrollada por Ludwig von Bertalanffy. La TGS propone un enfoque interdisciplinario para la comprensión de los sistemas en su totalidad, más allá de sus partes individuales. En su libro, Buckley (2017) define a la TGS como un esfuerzo para desarrollar teorías y principios que puedan ser aplicados a todos los niveles de sistemas en todas las disciplinas de la ciencia. La TGS se construye con la idea de que todos los sistemas, sean físicos, biológicos, sociales o abstractos, comparten ciertos principios y características comunes. Según Buckley, estos principios incluyen la organización jerárquica de los sistemas, la equifinalidad, la entropía y la retroalimentación.

En relación a ello, Stroh (2015) indica que la TGS proporciona un marco conceptual y herramientas útiles para comprender la complejidad de los sistemas sociales y para diseñar estrategias efectivas para el cambio y la mejora social. Asimismo, Senge (1990) argumenta que la TGS proporciona un marco conceptual para entender la complejidad de las organizaciones y para diseñar estrategias efectivas de aprendizaje y mejora continua. Por su parte, Adam et al. (2013) argumenta que la TGS sigue siendo una herramienta valiosa para entender la complejidad de los sistemas y para diseñar soluciones efectivas y finalmente Mitroff & Sagasti (1973) concluyen que la TGS ofrece una forma de comprender cómo las diferentes partes de un determinado sistema interactúan entre sí, y el conocimiento de estas interacciones puede ser utilizado para tomar decisiones efectivas, argumenta que la TGS puede ser aplicada para diseñar experimentos que simulen

sistemas complejos y permitan a los participantes tomar decisiones en situaciones realistas.

De la misma forma, identificamos la teoría de restricciones - TOC, sustentado por Elyahu Goldratt, que es una metodología de gestión que se enfoca en identificar y superar las restricciones que limitan la eficiencia y efectividad de un sistema o proceso, en relación a ello Rahman (1998) explora cómo la TOC puede aplicarse a una variedad de industrias, incluyendo la manufactura, la logística y los servicios. La TOC se centra en identificar y superar las restricciones que limitan la eficiencia y efectividad de un sistema o proceso. Asimismo, Trojanowska & Dostatni (2017) mencionan que aplicación de la TOC ayuda a mejorar la gestión de proyectos y lograr resultados más efectivos y eficientes.

Asimismo, se considera la teoría de la resiliencia propuesta por Hollnagel (2017), el desempeño resiliente denota que una organización es capaz de continuar sus operaciones requeridas en condiciones previstas e imprevistas modificando sus actividades antes, durante y después de eventos particulares. Según Hollnagel (2017), para que las empresas logren un desempeño resiliente, deben desarrollar cuatro capacidades: la capacidad de anticipar, monitorear, responder y aprender de sus experiencias. La capacidad de ver lo que ocurrirá en el futuro se denomina capacidad de anticipación. Ejemplos de esto incluyen la posibilidad de interrupciones, la introducción de nuevos requisitos o límites, o la introducción de oportunidades innovadoras. La capacidad de monitorear tiene en cuenta qué tan bien una organización puede reconocer los cambios en las condiciones de trabajo, además de los indicadores que se utilizan para realizar un seguimiento de lo que sucede tanto dentro como fuera del edificio. Para tener la capacidad de responder, uno debe saber qué acciones tomar y ser capaz de ejecutar esas acciones de manera rápida y efectiva en respuesta a los eventos.

Esto incluye adaptarse a los cambios, las interrupciones y las oportunidades que ocurren tanto de manera regular como irregular mediante la realización de actividades que han sido planificadas previamente, la modificación de los métodos de trabajo existentes y/o la creación de nuevos modos de operación Chuang et al.,

(2020). En conclusión, tener la capacidad de aprender requiere tener conciencia de lo que ha sucedido, así como la capacidad de aplicar lo aprendido. En particular, Hollnagel (2017) reconoce que cultivar los cuatro potenciales no implica necesariamente un desempeño resiliente cuando se requiere, como durante una crisis. Este es un punto importante a destacar. Según él, es más probable que una empresa que los ha construido se ejecute de manera resiliente que una empresa que no los ha construido. Continúa afirmando que una organización no podrá mantener el rendimiento si no se encuentran potenciales en ninguna parte de toda la entidad. Esta idea sirve como base para nuestra investigación porque incorpora estrategias para la gestión del riesgo de ciberseguridad que, cuando se llevan a cabo de manera eficiente, pueden ayudar a una organización a lograr un desempeño resiliente.

En consecuencia, tenemos las definiciones de la variable ciberseguridad, Rea-Guaman (2017) menciona que la ciberseguridad es un proceso que incluye prevención, detección y reacción. Compartiendo este punto de vista, Dunn (2005) afirma que no existe una definición generalmente aceptada de ciberseguridad, y sugiere el uso de varios términos diferentes que tienen significados relacionados, como garantía de información, seguridad de información o datos, protección de infraestructura crítica. Por otro lado, Craigen et al. (2014) encontraron que la definición de ciberseguridad es altamente variable, a menudo subjetiva y, en ocasiones, poco informativa. Asimismo, Perwej et al. (2021) menciona que la ciberseguridad se refiere a mecanismos y procedimientos destinados a proteger la información digital y además estrategias para proteger computadoras, redes, bases de datos y aplicaciones contra ataques, accesos no autorizados, alteración o destrucción.

En contraste a estas definiciones, el marco de ciberseguridad del NIST incluye claramente definidas cinco funciones básicas de ciberseguridad: identificación, protección, detección, respuesta y recuperación (NIST, 2018). La literatura también reconoce algunos modelos simplificados, que incluyen prevención, detección y respuesta/recuperación Jalali (2018). De esta manera y con el fin de presentar un marco determinado para la variable Ciberseguridad, las

dimensiones que se utilizarán en esta investigación serán: prevención, detección y recuperación.

Por lo tanto, comenzamos a identificar las dimensiones de la variable independiente. Como primera dimensión se tiene prevención. Sobre este punto, Ahsan et al. (2022) menciona que prevenir ataques de ciberseguridad -más allá de un conjunto de necesidades funcionales fundamentales y conocimiento sobre riesgos, amenazas o vulnerabilidades- requiere el análisis de los datos de ciberseguridad y construir las herramientas adecuadas para procesarlos con éxito. Asimismo, Vega & Ramos (2017) mencionan que es importante proteger y asegurar la infraestructura tecnológica para prevenir y reducir los ataques. Aseguran que esto puede lograrse mediante la ejecución de normativas de seguridad. De la misma forma, Reigada (2018), señala que los mecanismos de protección deben garantizar la confidencialidad, integridad y disponibilidad. Por último, Fernández (2020) menciona que, con el fin de evitar los peligros de seguridad informática, es esencial que estas adopten medidas preventivas como políticas, procedimientos y controles, gestionándolos de manera efectiva y tomando conciencia de su importancia.

Como segunda dimensión se tiene detección, que es una dimensión clave en la ciberseguridad, debido a que al realizarse de manera correcta y a tiempo, permite identificar y responder rápidamente a posibles amenazas en los sistemas. Jacob & Wanjala (2017) mencionan que la fase de detección permite la identificación de actividades que comprometen la integridad y confidencialidad. De la misma manera, Castro et al. (2018) puntualiza la detección como un desarrollo que permite identificar las actividades ilícitas contra los sistemas y elaborar una respuesta adecuada. De otra parte, Florez & Valderrama (2022) aclara que la detección es la búsqueda de amenazas en sistemas donde ya se ha producido una intrusión. Por el contrario, Coyac-Torres et al. (2020) mencionan que la detección tiene como meta descubrir amenazas que puedan existir en el ciberespacio, es decir, previamente a la ejecución de una brecha o intrusión, por lo que la detección cumple la función de avisar o alertar del hallazgo de diversas formas de amenazas.

Como tercera dimensión se tiene recuperación. La dimensión de recuperación en ciberseguridad se refiere a la capacidad para restaurar sus sistemas, datos y servicios después de un incidente de seguridad, dicho de otra manera, es la capacidad de una organización para recuperarse y volver a la normalidad después de un ataque o una interrupción. La importancia de esta dimensión radica en la certeza que los incidentes de seguridad cibernética son inevitables, y la capacidad de recuperación es importante para minimizar los daños. Bartock et al. (2016) mencionan que la recuperación es una parte del proceso de administración de riesgos. En un nivel más fundamental, las capacidades de la función recuperar tienen un efecto significativo en toda la organización al proporcionar datos realistas para mejorar otras capacidades.

Por ejemplo, Hutschenreuter et al. (2021) precisa que la fase de recuperación es el objetivo final de resiliencia de restablecer el sistema a su estado original o incluso a un mejor estado, en el que las lecciones aprendidas de incidentes pasados se documenten y contribuyan a la resiliencia futura. En esa misma línea, Padilla & Freire (2019) considera que la fase de recuperación es considerada como de vuelta a la normalidad, considerando los siguientes aspectos tras la mitigación de un ataque: reunión con el equipo de contingencia, evaluación de daños, priorización de actividades, evaluación y valoración de resultados. Por último. Barker et al. (2021), mencionan que la recuperación se refiere al diseño de acciones para mantener los servicios afectados por un determinado incidente de seguridad, por lo se puede concluir en que las capacidades de recuperación permiten restaurar las operaciones normales de manera oportuna, asimismo reduce el impacto del incidente.

Dentro de las definiciones consideradas para la segunda variable, la Gestión de Seguridad de la Información (GSI) engloba una serie de actividades orientadas a proteger los sistemas. Esta gestión implica elaborar controles de seguridad, gestionar riesgos y administrar incidentes de seguridad Di Luca (2019). La importancia de la GSI se debe a que la información es un producto valioso y su pérdida o compromiso puede tener consecuencias graves. Por lo tanto, la GSI es una parte importante de una empresa. Ko & Dorantes (2006) menciona que las

brechas del SGSI impactan en el trabajo financiero de las organizaciones, por lo que se concluye en que se debe primar una adecuada gestión y una respuesta eficiente a los incidentes de seguridad. Es en ese sentido que Soomro et al. (2016) destaca la necesidad de un enfoque más holístico en la administración de la GSI y argumenta que debe considerarse como un aspecto crítico de la estrategia empresarial.

Esto implica proteger los sistemas y administrar los riesgos e incidentes, la educación y la concienciación del personal, y la colaboración con otras áreas de la empresa. Ampliando esta idea, Nanda (2020) destacó lo importante que es la administración de la seguridad de TI en el entorno comercial actual y afirmó que la adecuada administración de este acápite puede proteger los activos organizacionales y brindar continuidad de las actividades cuando se presente una brecha de seguridad. Por último, Farid et al. (2023) destaca el valor del SGSI, asimismo resaltan los riesgos de seguridad que son la pérdida de datos, la violación de la privacidad y el acceso sin autorizado, destacando el uso de normativas de seguridad efectivas.

Como primera dimensión se tiene controles de seguridad, que son acciones preventivas y de mitigación que se implementan para reducir los riesgos de seguridad y garantizar la confidencialidad, integridad y disponibilidad de los patrimonios de una entidad. Estos controles pueden incluir políticas, procedimientos, tecnologías y medidas físicas que se aplican para proteger los sistemas. Shojaie (2018) menciona que la defensa de la información privada y el aseguramiento de la red interna son posibles motivaciones para implementar la norma ISO 27001, que brindan un entorno de mejores prácticas para identificar e implementar controles de seguridad mínimos. Agregando a lo anterior, Kim et al. (2017) mencionan que los fines de un control de seguridad de la información son mantener (disponibilidad) funcionando los sistemas informáticos en una organización (empresa, banco, etc.), prevenir (confidencialidad) la divulgación o fuga de información pertenecientes a una institución y preservar (integridad) la exactitud de la información importante en poder de la organización.

Del mismo modo, Otero et al. (2010) indica que, para las organizaciones, la información es importante y se encuentra relacionada directamente con la implementación de protocolos de seguridad apropiados y efectivos que permitirán asegurar la información. Igualmente, Ključnikov et al. (2019) menciona que los mecanismos de seguridad se pueden desarrollar eficazmente, lo que lleva al éxito de la gestión del SGSI.

La segunda dimensión es evaluación de riesgos, proceso importante que sirve para identificar y posterior evaluación de los riesgos potenciales que se presentara en una organización. En este proceso se identificarán los principales activos de la información de una empresa, identificar y estimar las amenazas y vulnerabilidades y determinar el impacto potencial de las brechas de seguridad en la organización. Con base en los resultados, se pueden implementar acciones de seguridad determinadas para reducir los riesgos. Mora (2018) menciona que es importante evaluar los riesgos que permitirán identificar las amenazas que pueden causar incidentes o interrupciones que afectan la continuidad del negocio, es importante identificar los principales peligros que afronta la organización y así asegurar que no existan amenazas que atenten contra la organización.

Agregando a esta idea, Li & Li (2018) indica que la observación e identificación de los peligros de seguridad requiere conciencia de los patrimonios de la tarea, el impacto clave de las pérdidas de activos de la tarea, así como las amenazas potenciales que podrían socavar la capacidad de una misión. Además, Di Luca (2019) menciona que el nivel de seguridad determinado debe ser consistente con el análisis de riesgo anterior, teniendo en cuenta el impacto de dicho acceso no deseado sobre la probabilidad de su ocurrencia. Al respecto, De Freitas (2009) menciona que la valoración de riesgos se basa en el reconocimiento de los principales activos de TI, la verificación de amenazas y vulnerabilidades, la determinación del efecto de los incidentes de seguridad y la ejecución de medidas de seguridad adecuadas.

Como tercera dimensión se tiene la gestión de incidentes de seguridad, proceso importante en el SGSI que busca prevenir, detectar, responder y

recuperarse ante incidentes que puedan afectar a una organización. Esta gestión involucra la planificación, implementación, monitoreo y mejora de las tareas y normativas de gestión de incidentes, con el objetivo de minimizar el impacto. Al respecto, Tøndel et al. (2014) menciona que la gestión de incidentes incluye rutinas establecidas, manuales de gestión de incidentes, procesos bien estructurados y planes de comunicación durante los incidentes, que incluyan la identificación, clasificación, respuesta, resolución y monitoreo, los planes de contingencia deberán cubrir los principales incidentes de TI. Por otro lado, Bartnes et al. (2016) describe que la capacitación es importante para responder a incidentes, asimismo recomienda crear equipos multifuncionales para garantizar una visión holística para atender los incidentes. De la misma manera, Cichonski et al. (2012) recomiendan recopilar y analizar información sobre incidentes que amenacen la información, informar sobre las amenazas y vulnerabilidades actuales y potenciales. Por consiguiente, se puede afirmar que la administración de incidentes de seguridad es un aspecto clave en el SGSI, que requiere de un enfoque sistemático y bien definido, y permite prevenir, detectar y recuperarse ante eventuales incidentes.

III. METODOLOGÍA

3.1. Enfoque, tipo y diseño de investigación

Enfoque de investigación

Con respecto a la metodología, en este trabajo se consideró el enfoque cuantitativo, pues busca comprobar hipótesis asistiéndose de la estadística, Trochim (2007).

Tipo de investigación

Este estudio es del tipo de básico, porque centra su investigación a un cuerpo organizado de conocimientos en base a teorías existentes, es decir no tienen resultados de utilidad práctica inmediata, Valderrama (2013).

Diseño de investigación

El nivel es correlacional porque permitirá determinar la relación entre dos variables sin intervenir en ellas; estas variables medidas corresponderán al mismo sujeto. Será no experimental porque no se aplicará ningún experimento; es decir, no existirá manipulación de variables, además es transaccional pues tiene como objetivo describir su incidencia en un tiempo determinado, Hernández & Mendoza (2018).

3.2. Variables y Operacionalización

Variable: Ciberseguridad

Según Rea-Guaman (2017) menciona que la ciberseguridad es un desarrollo que incorpora los siguientes parámetros: prevención, detección y reacción.

Definición Operacional de la variable ciberseguridad

La definición operacional de la ciberseguridad se refiere a implementar medidas y prácticas que protejan los sistemas informáticos y redes de computadoras contra ataques cibernéticos, al respecto Rea-Guaman (2017) menciona que la ciberseguridad es un proceso que incluye prevención, detección y reacción. En ese sentido, la variable se medirá a través de un cuestionario de 18 ítems que consta

de tres dimensiones: prevención, detección y recuperación con los siguientes indicadores: anticipación, confiabilidad, integridad; anticipación, confiabilidad, mejora; revisión disponibilidad y mejora.

Variable: Gestión de Seguridad de la Información

Involucra actividades que tienen como objetivo asegurar los sistemas. Esta tarea implica desarrollar controles de seguridad, evaluación de riesgos y la gestión de incidentes de seguridad, entre otras actividades. La importancia de la GSI se debe a que la información es valiosa para cualquier organización y su pérdida o compromiso puede tener consecuencias graves. Por lo tanto, la GSI es importante para la gestión empresarial, según Di Luca (2019) la GSI son actividades orientadas a proteger los sistemas de una organización. Esto implica elaborar controles de seguridad, gestionar los riesgos y administrar incidentes de seguridad.

Definición Operacional de la variable Gestión de Seguridad de la Información

La definición operacional implica la aplicación de medidas técnicas, organizacionales y administrativas para proteger la información. Según Di Luca (2019) son actividades orientadas a proteger los sistemas de una empresa. La variable se medirá a través de un cuestionario de 18 ítems, el cual se divide en tres dimensiones: controles de seguridad, evaluación de riesgos y gestión de incidentes de seguridad, con los siguientes indicadores: revisión, disponibilidad, verificación; revisión, disponibilidad, verificación; confiabilidad, verificación y mejora.

3.3. Población, muestra, muestreo y unidad de análisis

Población

Según Wyer (2014) es el grupo completo de personas, objetos o eventos que se desean investigar y se adaptan a normas específicos, y las que al obtener resultados se pretenderá generalizar a la población. Sánchez & Reyes (2015). Esta investigación tuvo como población a 75 participantes del Departamento de TI en el Perú al año 2023.

Muestra

Tabachnick (2013) define la muestra como un subgrupo de la población que se usara para buscar información adecuada para la investigación, estas pueden ser probabilísticas o no probabilísticas, Sánchez & Reyes (2015), el presente estudio tuvo la participación de 75 empleados.

Muestreo

Se define como un subconjunto de la población, o también como una parte de la población, representa el tamaño de la muestra que se considerará como representación de la población. Estas pueden ser probabilísticas o no probabilísticas, Sánchez & Reyes (2015). Para este estudio se consideró el total de la población como muestra.

Unidad de Análisis

Colaborador del Departamento de TI de la institución pública.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

Son métodos para recoger información de un fenómeno o realidad de acuerdo a los objetivos de la investigación. Existen diferentes técnicas y estas se emplean de acuerdo a lo que requiera la investigación, Sánchez & Reyes (2015). Asimismo, Groves (2011) define la encuesta como una técnica de medición en la que se obtienen datos mediante la selección y el interrogatorio de una muestra de elementos de la población, herramienta que se utilizara en este estudio.

Instrumentos de recolección de datos

De acuerdo a Hernández & Mendoza (2018) Lo definen como herramientas que se emplean en el proceso del trabajo de campo, de acuerdo a la técnica seleccionada o elegida será el cuestionario.

3.5. Procedimientos

Se solicito permiso de uso de nombre de la institución, se solicitó el permiso para el consentimiento del instrumento, se envió a validar los instrumentos a expertos, luego se utilizó el instrumento para el recojo de la información y el vaciado de datos obtenidos en las planillas de Excel.

3.6. Método de análisis de datos

Se considerará la estadística descriptiva representará de manera resumida los datos obtenidos a través de tablas de frecuencia y porcentajes o figuras de los resultados obtenidos, y la estadística inferencial, que buscará encontrar significatividad en sus resultados, es decir, comprobar las hipótesis planteadas.

3.7. Aspectos éticos

El presente trabajo fue escrito por el investigador asegurando que la información sea veraz, autentica y transparente. El investigador reconoció las contribuciones de otros autores cuyos trabajos fueron utilizados como fuentes de información y fueron citados correctamente de acuerdo con los estándares de la 7 edición de la Asociación Americana de Psicología. El centro de estudios requiere que todos los proyectos de investigación se subordinen a una valoración obligatoria a través del programa Turnitin para garantizar la autenticidad de los proyectos, por lo que la investigación también se evaluó mediante el programa Turnitin un sistema de detección de plagio. El investigador se aseguró de que el porcentaje de similitud no excedería el nivel mínimo aceptado según las pautas de investigación. Asimismo, se consideraron las siguientes resoluciones: Resolución de Consejo Universitario n° 0340-2021/UCV y la Resolución de Vicerrectorado de Investigación n°281-2022-VI-UCV.

IV. RESULTADOS

Evaluación descriptiva de la Ciberseguridad y la GSI

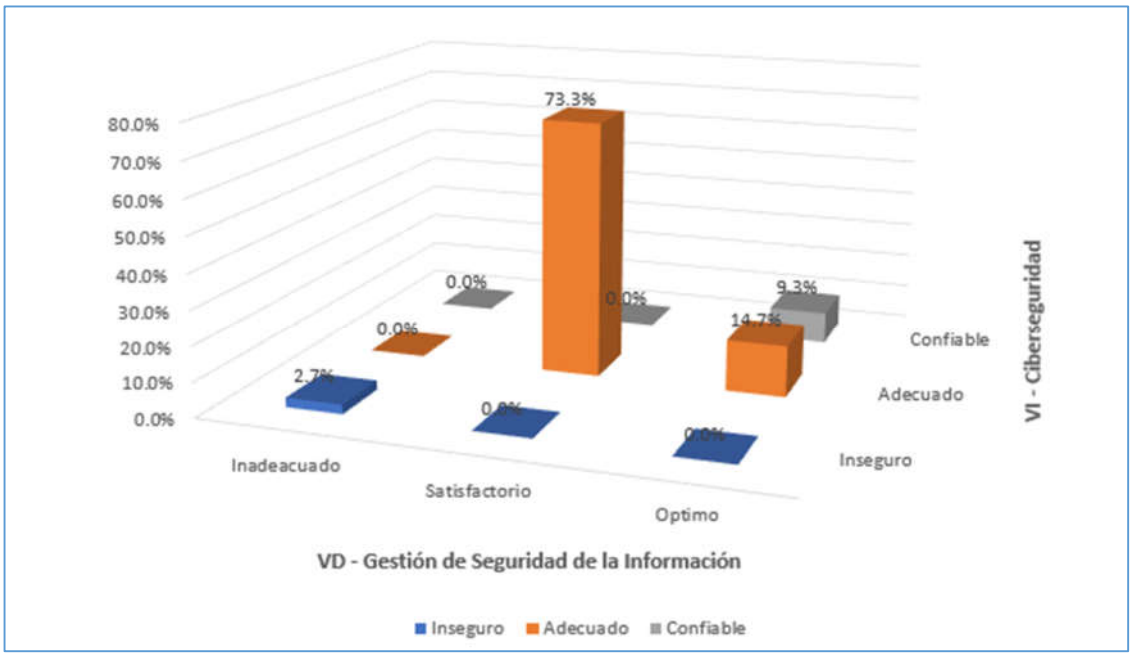
Tabla 1

*Tabla cruzada Ciberseguridad * GSI*

		VD-Gestión de Seguridad de la Información			
		Inadecuado	Satisfactorio	Optimo	Total
VI-Ciberseguridad	Inseguro	2(2.7%)	0(0.0%)	0(0.0%)	2(2.7%)
	Adecuado	0(0.0%)	55(73.3%)	11(14.7%)	66(88.0%)
	Confiable	0(0.0%)	0(0.0%)	7(9.3%)	7(9.3%)
	Total	2(2.7%)	55(73.3%)	18(24.0%)	75(100%)

Figura 1

Histograma Ciberseguridad * GSI



Del histograma, identificamos el mayor valor de frecuencia ocurre con los niveles “Adecuado” de la Ciberseguridad y “Satisfactorio” de la GSI, se obtuvieron 55 respuestas que equivalen al 73.3% de la totalidad de preguntas realizadas.

Asimismo, tenemos frecuencias intermedias, como ocurre con los niveles “Adecuado” de la Ciberseguridad y “Óptimo” de la GSI, se obtuvieron 11 respuestas que equivalen al 14.7% de la totalidad de preguntas realizadas.

Por último, mencionar que la mayor frecuencia se identifica en el nivel “Adecuado” de la Ciberseguridad, donde se obtuvieron 66 respuestas que equivalen al 88.0% del total de preguntas realizadas. Asimismo, la frecuencia mayor se identifica en el nivel “Satisfactorio” de la GSI, donde se obtuvieron 55 respuestas que equivalen al 73.3% del total de preguntas realizadas.

Evaluación descriptiva de la prevención de la Ciberseguridad y GSI

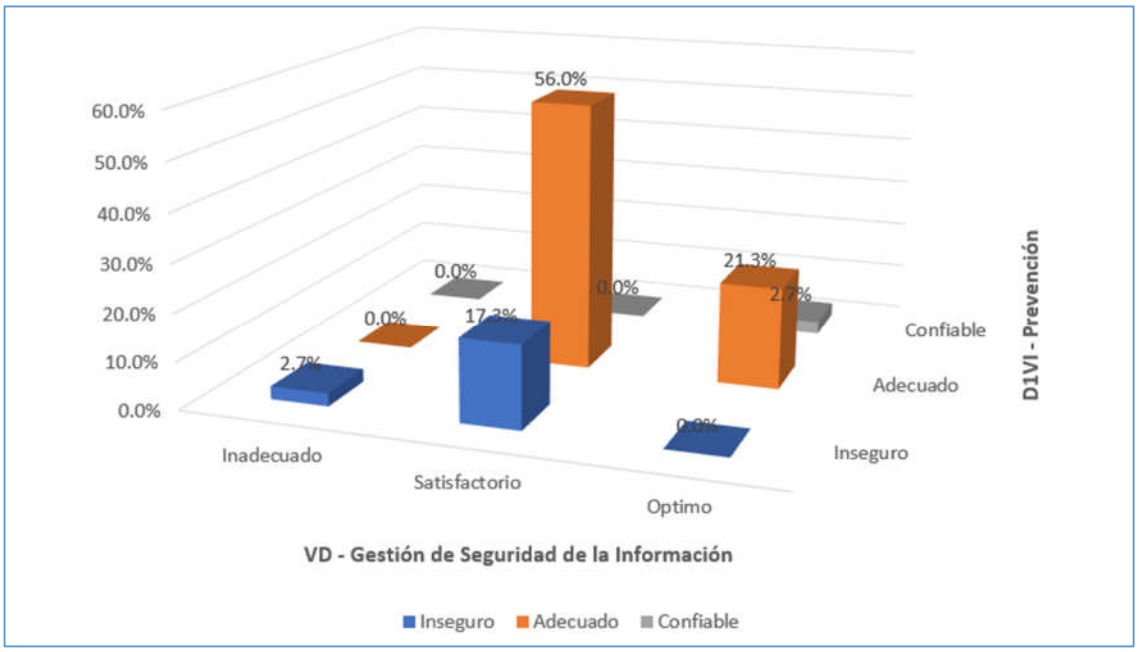
Tabla 2

*Tabla cruzada prevención de la Ciberseguridad * GSI*

		VD-Gestión de Seguridad de la Información			Total
		Inadecuado	Satisfactorio	Optimo	
D1VI-Prevencion	Inseguro	2(2.7%)	13(17.3%)	0(0.0%)	15(20.0%)
	Adecuado	0(0.0%)	42(56.0%)	16(21.3%)	58(77.3%)
	Confiable	0(0.0%)	0(0.0%)	2(2.7%)	2(2.7%)
	Total	2(2.7%)	55(73.3%)	18(24.0%)	75(100%)

Figura 2

*Histograma dimensión prevención de la Ciberseguridad * GSI*



Del histograma, identificamos el mayor valor de frecuencia ocurre con los niveles “Adecuado” de la Prevención de la Ciberseguridad y “Satisfactorio” de la GSI, se obtuvieron 42 respuestas que equivalen al 56.0% de la totalidad de preguntas realizadas.

Asimismo, tenemos frecuencias intermedias, como ocurre con los niveles “Adecuado” y “Optimo” de la Prevención de la Ciberseguridad y de la GSI respectivamente, se obtuvieron 16 respuestas que equivalen al 21.3% de la totalidad de preguntas realizadas.

Por último, mencionar que la mayor asiduidad se identifica en el nivel “Adecuado” de la prevención de la Ciberseguridad, donde se obtuvieron 58 respuestas que equivalen al 77.3% del total de preguntas realizadas. Asimismo, la mayor frecuencia de identifica en el nivel “Satisfactorio” de la GSI, donde se obtuvieron 55 respuestas que equivalen al 73.3% del total de preguntas realizadas.

Evaluación descriptiva de la detección de la Ciberseguridad y GSI

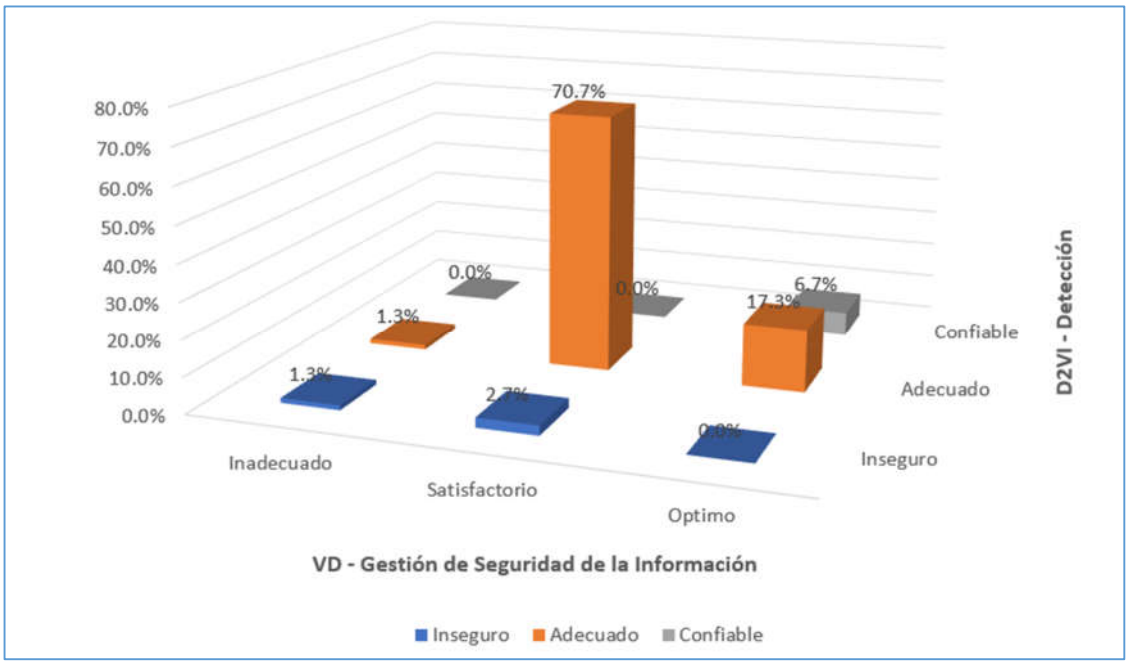
Tabla 3

*Tabla cruzada detección de la Ciberseguridad * GSI*

		VD-Gestión de Seguridad de la Información			
		Inadecuado	Satisfactorio	Optimo	Total
D2VI-Deteccion	Inseguro	1(1.3%)	2(2.7%)	0(0.0%)	3(4.0%)
	Adecuado	1(1.3%)	53(70.7%)	13(17.3%)	67(89.3%)
	Confiable	0(0.0%)	0(0.0%)	5(6.7%)	5(6.7%)
	Total	2(2.7%)	55(73.3%)	18(24.0%)	75(100%)

Figura 3

*Histograma dimensión detección de la Ciberseguridad * GSI*



Del histograma, identificamos el mayor valor de frecuencia ocurre con los niveles “Adecuado” de la detección de la Ciberseguridad y “Satisfactorio” de la GSI, se obtuvieron 53 respuestas que equivalen al 70.7% de la totalidad de preguntas realizadas.

Asimismo, tenemos frecuencias intermedias, como ocurre con los niveles “Adecuado” y “Optimo” de la detección de la Ciberseguridad y de la GSI respectivamente, se obtuvieron 13 respuestas que equivalen al 17.3% de la totalidad de preguntas realizadas.

Por último, mencionar que la mayor asiduidad se identifica en el nivel “Adecuado” de la detección de la Ciberseguridad, donde se obtuvieron 67 respuestas que equivalen al 89.3% del total de preguntas realizadas. Asimismo, la mayor frecuencia de identifica en el nivel “Satisfactorio” de la GSI, donde se obtuvieron 55 respuestas que equivalen al 73.3% del total de preguntas realizadas.

Evaluación descriptiva de la recuperación de la Ciberseguridad y GSI

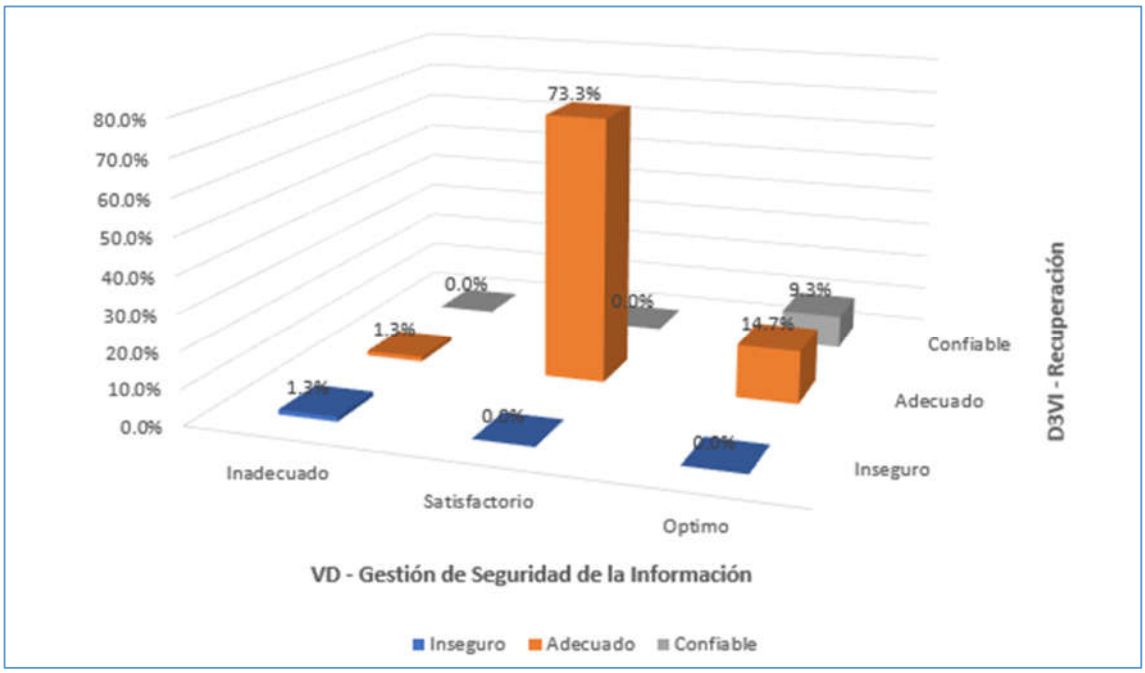
Tabla 4

*Tabla cruzada dimensión Recuperación de la Ciberseguridad * GSI*

		VD-Gestión de Seguridad de la Información			
		Inadecuado	Satisfactorio	Optimo	Total
D3VI-Recuperacion	Inseguro	1(1.3%)	0(0.0%)	0(0.0%)	1(1.3%)
	Adecuado	1(1.3%)	55(73.3%)	11(14.7%)	67(89.3%)
	Confiable	0(0.0%)	0(0.0%)	7(9.3%)	7(9.3%)
	Total	2(2.7%)	55(73.3%)	18(24.0%)	75(100%)

Figura 4

*Histograma dimensión recuperación de la Ciberseguridad * GSI*



Del histograma, identificamos el mayor valor de frecuencia ocurre con los niveles “Adecuado” de la recuperación de la Ciberseguridad y “Satisfactorio” de la GSI, se obtuvieron 55 respuestas que equivalen al 73.3% de la totalidad de preguntas realizadas.

Asimismo, tenemos frecuencias intermedias, como ocurre con los niveles “Adecuado” y “Optimo” de la recuperación de la Ciberseguridad y de la GSI respectivamente, se obtuvieron 11 respuestas que equivalen al 14.7% de la totalidad de preguntas realizadas.

Por último, mencionar que la mayor asiduidad se identifica en el nivel “Adecuado” de la recuperación de la Ciberseguridad, donde se obtuvieron 67 respuestas que equivalen al 89.3% del total de preguntas realizadas. Asimismo, la mayor frecuencia de identifica en el nivel “Satisfactorio” de la GSI, donde se obtuvieron 55 respuestas que equivalen al 73.3% del total de preguntas realizadas.

Prueba de la Hipótesis General

Formulación de la hipótesis estadística:

H_0: La Ciberseguridad no incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

H_1: La Ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

Contrastación de Hipótesis estadística:

Tabla 5

Datos de la regla que demuestra la influencia de la Ciberseguridad en la GSI

	Logaritmo de la verosimilitud -2	X^2	gl	Sig.
Sólo intersección	44.586			
Final	0.000	44.586	2	0.000

De la tabla 5 podemos concluir que se identifica una significancia estadística de 0.000, valor menor a 0.05; que permite establecer que la hipótesis nula (H_0) es desestimada, considerando como valida la hipótesis alterna (H_1). Por lo tanto, la Ciberseguridad si incide sobre la GSI.

Tabla 6

Pseudo R^2 de la influencia de la Ciberseguridad en la GSI

Pseudo R cuadrado	
Cox y Snell	0.448
Nagelkerke	0.609
McFadden	0.446

De los datos de la tabla 6, se verifica que el estadístico de Nagelkerke es igual a 0.609, entonces deducimos que tenemos un modelo adecuado que grafica el nivel de influencia de la Ciberseguridad sobre la GSI, esta influencia equivale a un 60.9%.

Tabla 7

Cálculos de los indicadores de la influencia de la Ciberseguridad en la GSI

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VD = 1]	-39,799	1995,385	0,000	1	0,984	-3950,681	3871,084
	[VD = 2]	-18,803	,330	3240,776	1	0,000	-19,450	-18,155
Ubicación	[VI=1]	-57,509	5342,014	0,000	1	0,991	-10527,664	10412,647
	[VI=2]	-20,412	,000	.	1	.	-20,412	-20,412
	[VI=3]	0[a]	.	.	0	.	.	.

De acuerdo a los datos de la tabla 7, se verifica que el coeficiente de regresión de la variable GSI fue de -18.803, con un valor de significancia igual a 0.000. Por lo tanto, considerando que tenemos un valor de significancia inferior a 0.05; se concluye que debemos rechazar la hipótesis nula (H_0), dando como valida la hipótesis alterna (H_1). En ese sentido, se afirma que la Ciberseguridad incide significativamente en la GSI.

Prueba de Hipótesis especifica 1:

Formulación de la hipótesis estadística:

H_0: La prevención de la ciberseguridad no incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

H_1: La prevención de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

Contrastación de Hipótesis estadística:

Tabla 8

Datos de la regla que demuestra la influencia de la Prevención de la Ciberseguridad en la GSI

	Logaritmo de la verosimilitud -2	X^2	gl	Sig.
Sólo intersección	26.658			
Final	6.772	19.886	2	0.000

De la tabla 8 podemos concluir que se identifica una significancia estadística de 0.000, valor menor a 0.05; que permite establecer que la hipótesis nula (H_0) es desestimada, considerando como valida la hipótesis alterna (H_1). Por lo tanto, la prevención de la Ciberseguridad si incide sobre la GSI.

Tabla 9

Pseudo R^2 de la influencia de la Prevención de la Ciberseguridad en la GSI

Pseudo R cuadrado	
Cox y Snell	0.233
Nagelkerke	0.316
McFadden	0.199

De los datos de la tabla 9, se verifica que el estadístico de Nagelkerke es igual a 0.316, entonces deducimos que tenemos un modelo adecuado que grafica el nivel de influencia de la prevención de la Ciberseguridad sobre la GSI, esta influencia equivale a un 31.6%.

Tabla 10

Cálculos de los indicadores de la influencia de la Prevención de la Ciberseguridad en la GSI

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VD = 1]	-35.609	767.135	0.002	1	0.963	-1539.166	1467.949
	[VD = 2]	-16.803	0.294	3271.153	1	0.000	-17.379	-16.227
Ubicación	[D1VI=1]	-33.737	767.135	0.002	1	0.965	-1537.294	1469.821
	[D1VI=2]	-17.768	0.000		1		-17.768	-17.768
	[D1VI=3]	0a			0			

De acuerdo a los datos de la tabla 10, se verifica que el coeficiente de regresión de la variable GSI fue de -16.803, con un valor de significancia igual a 0.000. Por lo tanto, considerando que tenemos un valor de significancia inferior a 0.05; se concluye que debemos rechazar la hipótesis nula (H_0), dando como valida la hipótesis alterna (H_1). En ese sentido, se afirma que la dimensión prevención de la Ciberseguridad incide significativamente en la GSI.

Prueba de Hipótesis especifica 2:

Formulación de la hipótesis estadística:

H_0: La detección de la ciberseguridad no incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

H_1: La detección de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

Contrastación de Hipótesis estadística:

Tabla 11

Datos de la regla que demuestra la influencia de la Detección de la Ciberseguridad en la GSI

	Logaritmo de la verosimilitud -2	X^2	gl	Sig.
Sólo intersección	28.086			
Final	7.847	20.239	2	0.000

De la tabla 11 podemos concluir que se identifica una significancia estadística de 0.000, valor menor a 0.05; que permite establecer que la hipótesis nula (H_0) es desestimada, considerando como valida la hipótesis alterna (H_1). Por lo tanto, la detección de la Ciberseguridad si incide sobre la GSI.

Tabla 12

Pseudo R^2 de la influencia de la detección de la Ciberseguridad en la GSI

Pseudo R cuadrado	
Cox y Snell	0.237
Nagelkerke	0.321
McFadden	0.202

De los datos de la tabla 12, se verifica que el estadístico de Nagelkerke es igual a 0.321, entonces deducimos que tenemos un modelo adecuado que grafica el nivel de influencia de la prevención de la Ciberseguridad sobre la GSI, esta influencia equivale a un 32.1%.

Tabla 13

Cálculos de los indicadores de la influencia de la detección de la Ciberseguridad en la GSI

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VD = 1]	-23.440	1.008	541.019	1	0.000	-25.415	-21.464
	[VD = 2]	-17.803	0.309	3321.679	1	0.000	-18.408	-17.198
Ubicación	[D2VI=1]	-22.767	1.564	211.917	1	0.000	-25.832	-19.702
	[D2VI=2]	-19.229	0.000		1		-19.229	-19.229
	[D2VI=3]	0[a]			0			

De acuerdo a los datos de la tabla 13, se verifica que el coeficiente de regresión de la variable GSI fue de -17.803, con un valor de significancia igual a 0. Por lo tanto, considerando que tenemos un valor de significancia inferior a 0.05; se concluye que debemos rechazar la hipótesis nula (H_0), dando como valida la hipótesis alterna (H_1). En ese sentido, se afirma que la dimensión detección de la Ciberseguridad incide significativamente en la GSI.

Prueba de Hipótesis especifica 3:

Formulación de la hipótesis estadística:

H_0: La recuperación de la ciberseguridad no incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

H_1: La recuperación de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023.

Contrastación de Hipótesis estadística:

Tabla 14

Datos de la regla que demuestra la influencia de la recuperación de la Ciberseguridad en la GSI

	Logaritmo de la verosimilitud -2	X^2	gl	Sig.
Sólo intersección	36.176			
Final	6.054	30.122	2	0.000

De la tabla 14 podemos concluir que se identifica significancia estadística de 0.000, valor menor a 0.05; que permite establecer que la hipótesis nula (H_0) es desestimada, considerando como valida la hipótesis alterna (H_1). Por lo tanto, la recuperación de la Ciberseguridad si incide sobre la GSI.

Tabla 15

Pseudo R^2 de la influencia de la Recuperación de la Ciberseguridad en la GSI

Pseudo R cuadrado	
Cox y Snell	0.331
Nagelkerke	0.449
McFadden	0.301

De los datos de la tabla 15, se verifica que el estadístico de Nagelkerke es igual a 0.449, entonces deducimos que tenemos un modelo adecuado que grafica el nivel de influencia de la recuperación de la Ciberseguridad sobre la GSI, esta influencia equivale a un 44.9%.

Tabla 16

Cálculos de los indicadores de la influencia de la Recuperación de la Ciberseguridad en la GSI

							Intervalo de confianza al 95%	
		Estimación	Desv. Error	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VD = 1]	-24.620	1.008	597.101	1	0.000	-26.595	-22.645
	[VD = 2]	-18.803	0.330	3250.560	1	0.000	-19.449	-18.157
Ubicación	[D3VI=1]	-42.331	7012.509	0.000	1	0.995	-13786.596	13701.934
	[D3VI=2]	-20.430	0.000		1		-20.430	-20.430
	[D3VI=3]	0[a]			0			

De acuerdo a los datos de la tabla 16, se verifica que el coeficiente de regresión de la variable GSI fue de -18.803, con un valor de significancia igual a 0.000. Por lo tanto, considerando que tenemos un valor de significancia inferior a 0.05; se concluye que debemos rechazar la hipótesis nula (H_0), dando como valida la hipótesis alterna (H_1). En ese sentido, se afirma que la dimensión detección de la Ciberseguridad incide significativamente en la GSI.

V. DISCUSIÓN

Con relación al objetivo general; considerando los datos obtenidos de la evaluación estadística descriptiva, donde se indica que la asiduidad más alta ocurre con la convergencia del nivel adecuado de la Ciberseguridad con el nivel satisfactorio de la Gestión de Seguridad de la Información.

Asimismo, de la evaluación inferencial se alcanzó un valor estadístico de Nagelkerke de 0.609, entonces deducimos que tenemos un modelo conveniente que grafica el nivel de influencia de la ciberseguridad sobre la GSI, dicha influencia equivale a un 60.9%.

Los resultados que se obtuvieron coinciden con los resultados hallados por Mallqui (2022) quien realizó una investigación que tuvo como propósito determinar cómo la ciberseguridad afecta la administración de tecnologías de información, investigación con enfoque básica, del tipo no experimental, de nivel correlacional-causal, con un grupo de 175 servidores concluyendo que los resultados obtenidos indican que la ciberseguridad influye significativamente en la administración de tecnologías de información en un 53,7%, lo que indica una correlación positiva importante. También se precisa lo mencionado por Bohorquez (2020) quien realizó una investigación que tuvo como propósito establecer la correspondencia entre la ciberseguridad con la administración de tecnologías, investigación con un enfoque de tipo básico, correlacional - no experimental con 71 trabajadores como muestra, obtuvo como resultado que existe una correlación fuerte de 0,832 entre ambas variables.

Por otro lado, estos resultados están relacionados con las definiciones de Ciberseguridad, los cuales según Rea-Guaman (2017) menciona que la ciberseguridad es un proceso que incluye prevención, detección y reacción. Compartiendo este punto de vista, Dunn (2005) afirma que no existe una definición generalmente aceptada de ciberseguridad, y sugiere el uso de varios términos diferentes que tienen significados relacionados, como garantía de información, seguridad de información o datos, protección de infraestructura crítica. Asimismo,

Perwej et al. (2021) menciona que ciberseguridad se refiere a tratamientos y procedimientos para proteger la información digital y además estrategias para proteger computadoras, redes, bases de datos y aplicaciones contra ataques, accesos no autorizados, alteración o destrucción. En contraste a estas definiciones, el marco de ciberseguridad del NIST incluye claramente definidas cinco funciones básicas de ciberseguridad: identificación, protección, detección, respuesta y recuperación (NIST, 2018).

Con relación al objetivo específico 1; considerando los datos obtenidos de la evaluación estadística descriptiva, donde se indica que la asiduidad más alta ocurre con la convergencia del nivel adecuado de la Prevención de la Ciberseguridad con el nivel satisfactorio de la Gestión de Seguridad de la Información.

Asimismo, de la evaluación inferencial se alcanzó un valor estadístico de Nagelkerke de 0.316, entonces deducimos que tenemos un modelo conveniente que grafica el nivel de influencia de la prevención de la ciberseguridad sobre la GSI, dicha influencia equivale a un 31.6%.

Los resultados que se obtuvieron coinciden con los resultados hallados por Bustamante et al. (2021), quienes, en su estudio, que tuvo como propósito la mejora de la administración del SGSI en una municipalidad aplicando políticas de la ISO 270001, el enfoque fue preexperimental con una muestra de 30 trabajadores de un total de 90 trabajadores, utilizando un cuestionario como instrumento. Los resultados indicaron que más del 90 % reconoció mejoras en la institución, se concluye que el modelo de políticas mejoró la gestión del SGSI. Por otro lado, se contrasta con la investigación de Razikin & Soewito (2022) en su investigación presenta un modelo de apoyo en ciberseguridad para el diseño de sistemas de seguridad, sistemas que evaluaran riesgos en un determinado marco de ciberseguridad, utiliza una metodología que incluye la revisión de literatura, un cuestionario y entrevistas con expertos en ciberseguridad. El público objetivo son las organizaciones que desean configurar un SGSI. Los resultados concluyen que la propuesta puede ayudar a tomar decisiones sobre los sistemas de seguridad, prevenir y reducir los riesgos de seguridad.

Por otro lado, estos resultados están relacionados con las definiciones de la dimensión prevención, sobre este punto, Ahsan et al. (2022) menciona que prevenir ataques de ciberseguridad -más allá de un conjunto de necesidades funcionales fundamentales y conocimiento sobre riesgos, amenazas o vulnerabilidades- requiere el análisis de los datos de ciberseguridad y construir las herramientas adecuadas para procesarlos con éxito. Asimismo, Vega & Ramos (2017) mencionan que es importante proteger y asegurar la infraestructura tecnológica para prevenir y reducir los ataques. Aseguran que esto puede lograrse mediante la adopción de políticas de seguridad.

Con relación al objetivo específico 2; considerando los datos obtenidos de la evaluación estadística descriptiva, donde se indica que la asiduidad más alta ocurre con la convergencia del nivel adecuado de la Detección de la Ciberseguridad con el nivel satisfactorio de la Gestión de Seguridad de la Información.

Asimismo, de la evaluación inferencial se alcanzó un valor estadístico de Nagelkerke de 0.321, entonces deducimos que tenemos un modelo conveniente que grafica el nivel de influencia de la detección de la ciberseguridad sobre la GSI, dicha influencia equivale a un 32.1%.

Los resultados que se obtuvieron coinciden con los resultados hallados por Choejey et al. (2017) quien evaluó el impacto de la percepción de la ciberseguridad en entidades del gobierno, elaboro un estudio explicativo de enfoque cuantitativo, este estudio indico que la ciberseguridad se está desarrollando en las empresas de forma no adecuada, creando una brecha de seguridad, por lo tanto, se determina que la implementación de esquemas de ciberseguridad, como la detección influyen en un 40% sobre las políticas relacionadas a ciberseguridad en las empresas. En esa misma línea, se coteja con Alzahrani (2021) que realizó una investigación que busco examinar y evaluar los problemas de seguridad cibernética, incluido el riesgo cibernético, la seguridad cibernética, la conciencia de seguridad cibernética y la confianza cibernética, entre los estudiantes de educación superior en Arabia Saudita. Teniendo en cuenta otros problemas de seguridad, este estudio revela que, si bien los estudiantes saudíes son conscientes del riesgo cibernético, no son

conscientes de la seguridad cibernética por lo tanto tampoco consideran la prevención. Esta investigación indicó un puntaje bajo en capacitación y concientización, ya que el 92% de los encuestados nunca recibió ningún tipo de capacitación en seguridad cibernética. De acuerdo con los hallazgos de este estudio, las instituciones saudíes deberían enseñar a sus estudiantes sobre la legislación contra el ciberdelito y los problemas clave de concienciación y prevención.

Por otro lado, los datos obtenidos están relacionados con las definiciones de la dimensión detección que es una dimensión clave en la ciberseguridad, debido a que al realizarse de manera correcta y a tiempo, permite identificar y responder rápidamente a posibles amenazas en los sistemas. Misiko & Yusuf (2017) mencionan que la fase de detección permite la identificación de actividades que comprometen la integridad y confidencialidad. De la misma manera, Romero et al. (2018) define la detección como una actividad que permite identificar las actividades ilícitas contra los sistemas y elaborar una respuesta adecuada. Por el contrario, Coyac-Torres (2020) menciona que la detección tiene como meta descubrir amenazas que puedan existir en el ciberespacio, es decir, previamente a la ejecución de una brecha o intrusión, por lo que la detección cumple la función de avisar o alertar del hallazgo de diversas formas de amenazas.

Con relación al objetivo específico 3; considerando los datos obtenidos de la evaluación estadística descriptiva, donde se indica que la asiduidad más alta ocurre con la convergencia del nivel adecuado de la Recuperación de la Ciberseguridad con el nivel satisfactorio de la Gestión de Seguridad de la Información.

Asimismo, de la evaluación inferencial se alcanzó un valor estadístico de Nagelkerke igual a 0.449, entonces deducimos que tenemos un modelo conveniente que grafica el grado de influencia de la recuperación de la Ciberseguridad sobre la GSI, dicha influencia equivale a un 44.9%.

Los resultados obtenidos coinciden con los resultados hallados por Velecela (2020) en el artículo que tiene como propósito presentar un plan de administración

del SGSI para el Gobierno Provincial del Cañar en Ecuador, donde se realizó una evaluación de riesgos y se propuso un plan de administración basado en el standard ISO 27001. La población objetivo fueron los empleados y usuarios del sistema de la organización. Los resultados indican que la implementación de un plan de administración del SGSI ayudo a mejorar la seguridad de la información en la organización, reduciendo el riesgo de pérdida o fuga de información confidencial y estableciendo parámetros adecuados parala recuperación. De igual forma, se confronta con Calderón (2019) quien elaboró un trabajo para identificar la relación entre la seguridad informática y la administración de riesgos, el diseño que utilizo fue transversal, correlacional, no experimental y se enmarca en la categoría de investigación básica. La población estuvo conformada por 106 colaboradores quienes fueron escogidos mediante muestreo probabilístico simple y aleatorio; se aplicó la prueba de rango de correlación no paramétrica Rho de Spearman. Los hallazgos del estudio indicaron una correlación directa entre los riesgos de TI, la información y la recuperación. Teniendo como resultado que existe una correlación directa entre ambas variables.

Por otro lado, estos resultados están relacionados con las definiciones de la dimensión recuperación en ciberseguridad que se refiere a la capacidad para restaurar los sistemas, datos y servicios después de un incidente de seguridad, dicho de otra manera, es la capacidad de una organización para recuperarse y volver a la normalidad después de un ataque o una interrupción. La importancia de esta dimensión radica en la certeza que los incidentes de seguridad cibernética son inevitables, y la capacidad de recuperación es importante para minimizar los daños. Bartock et al. (2016) mencionan que la recuperación es una parte del proceso de administración de riesgos. En un nivel más fundamental, las capacidades de la función recuperar tienen un efecto significativo en toda la organización al proporcionar datos realistas para mejorar otras capacidades. Por ejemplo, Hutschenreuter et al. (2021) precisa que la fase de recuperación es el objetivo final de resiliencia de restablecer el sistema a su estado original o incluso a un mejor estado, en el que las lecciones aprendidas de incidentes pasados se documenten y contribuyan a la resiliencia futura.

Los análisis descriptivos e inferenciales son dos enfoques fundamentales en el análisis estadístico. En ese sentido un análisis descriptivo permite al investigador resumir y presentar las características y patrones clave de los datos, la estadística descriptiva suelen ser a menudo sencillas e intuitivas, lo que facilita que el investigador y los no expertos comprendan e interpreten los resultados, asimismo se utiliza como un paso inicial para explorar y obtener información de los datos, lo que ayuda a los investigadores a identificar tendencias, valores atípicos y posibles relaciones para una mayor investigación. En contraste a lo indicado, el análisis descriptivo se enfoca en resumir los datos observados y no brinda información directa sobre las características o relaciones de la población, esto permite tener información específica de la muestra o conjunto de datos en estudio y no permiten generalizaciones a una población más grande, pasando por alto interacciones o asociaciones complejas entre variables, ya que se centra principalmente en resúmenes de variables individuales.

Por otro lado, el análisis inferencial permite al investigador hacer inferencias y sacar conclusiones de una población teniendo en cuenta una muestra, se utiliza para realizar pruebas de hipótesis y responder las preguntas de investigación empleando para este caso pruebas estadísticas para examinar relaciones, diferencias y asociaciones entre variables, lo que ayuda a los investigadores a evaluar hipótesis y responder preguntas de investigación específicas, asimismo el análisis inferencial proporciona medidas de incertidumbre, como intervalos de confianza y valores p, que ayudan a evaluar la confiabilidad y la importancia de los hallazgos.

Sin embargo, el análisis inferencial a menudo se basa en ciertas suposiciones sobre los datos, como la distribución normal, la independencia y la homogeneidad de la varianza, las violaciones de estas suposiciones pueden conducir a resultados inexactos o sesgados. Asimismo, se basa en un muestreo representativo para que las inferencias sean válidas, la muestra utilizada en el análisis inferencial debe ser representativa de la población objetivo, si el muestreo es sesgado o no representativo puede conducir a conclusiones incorrectas, por otro lado la estadística inferencial utiliza el análisis inferencial que involucra técnicas

estadísticas más avanzadas, que pueden ser complejas y requieren experiencia para implementarlas correctamente, la mala interpretación de los resultados o la mala aplicación de las pruebas estadísticas pueden conducir a conclusiones erróneas.

En resumen, el análisis descriptivo es valioso para resumir y explorar datos, mientras que el análisis inferencial permite generalizaciones y pruebas de hipótesis. En esta investigación se utilizó ambos enfoques en combinación para obtener una comprensión integral de los datos y sacar conclusiones significativas.

VI. CONCLUSIONES

1. Se concluyó que la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023, obteniéndose el valor de R2 de Nagelkerke de 0.609 que significa un 60.9% de incidencia entre las variables.

2. Se concluyó que la prevención de la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023, obteniéndose el valor de R2 de Nagelkerke de 0.316 que significa un 31.6% de incidencia entre las variables.

3. Se concluyó que la detección de la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023, obteniéndose el valor de R2 de Nagelkerke de 0.321 que significa un 32.1% de incidencia entre las variables.

4. Se concluyó que la recuperación de la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023, obteniéndose el valor de R2 de Nagelkerke de 0.449 que significa un 44.9% de incidencia entre las variables.

VII. RECOMENDACIONES

1. Se recomienda al Encargado de la Administración General la implementación de buenas prácticas en ciberseguridad establecidas en marcos de trabajo robustos y exitosos.

2. Se recomienda al Encargado de Tecnologías implementar programas y/o capacitaciones que permitan prevenir ataques externos.

3. Se recomienda al Encargado de Tecnologías desarrollar un plan para revisar y mejorar los controles y procedimientos tecnológicos para identificar riesgos y/o vulnerabilidades.

4. Se recomienda al Encargado de Tecnologías ejecutar un plan de valorización y manejo de la gestión de incidentes, se debe considerar desde el reporte, la investigación de los incidentes de seguridad.

REFERENCIAS

Adams, K. M., Hester, P. T., & Bradley, J. M. (2013). *A historical perspective of systems theory. ResearchGate.* https://www.researchgate.net/publication/288782223_A_historical_perspective_of_systems_theory

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M., Rifat, N. I., & Connolly, J. F. (2022). *Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. Journal of Cybersecurity and Privacy*, *2*(3), 527–555. https://doi.org/10.3390/jcp2030027

Alzahrani, L. (2021). Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes. International Journal of Advanced Computer Science and Applications, 12(11).

Barker, W. C., Scarfone, K., Fisher, W., & Souppaya, M. (2021). *Cybersecurity Framework Profile for Ransomware Risk Management.* National Institute of Standards and Technology. https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8374-draft.pdf

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). *The future of information security incident management training: A case study of electrical power companies*. Computers & Security, 61, 32-45. https://www.sciencedirect.com/science/article/abs/pii/S0167404816300530

Bartock, M., Cichonski, J., Souppaya, M., Witte, G., & Scarfone, K. (2016). *Guide for cybersecurity event recovery.*

Bohorquez, S. A. (2021). *Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020*. https://repositorio.ucv.edu.pe/handle/20.500.12692/63128

Buckley, W. (2017). *General System Theory—a Critical Review*. https://www.semanticscholar.org/paper/General-System-

Theory%E2%80%94a-Critical-Review-Buckley-Bertalanffy/b0e54bd91d695e0c3a7ce8f0ee06b2c72f41b16f

Bustamante García, S., Valles Coral, M. Á., Cuellar Rodríguez, I. E., & Lévano Rodríguez, D. (2021). Políticas basadas en la ISO 27001: 2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE*, *12*(2), 69-79. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-65422021000200069&script=sci_arttext

Calderón, S. J. A. (2019). *Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018*. https://repositorio.ucv.edu.pe/handle/20.500.12692/30014

Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades (*Vol. 46). 3Ciencias. https://books.google.es/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=Introducci%C3%B3n+a+la+seguridad+inform%C3%A1tica+y+el+an%C3%A1lisis+de+vulnerabilidades&ots=ymzOBZh6Qx&sig=GED6v5A1SIH8EozxHnWNZKfH-Ms#v=onepage&q=Introducci%C3%B3n%20a%20la%20seguridad%20inform%C3%A1tica%20y%20el%20an%C3%A1lisis%20de%20vulnerabilidades&f=false

Choejey, P., Murray, D. y Che, Ch. (2017). *Perceptions of Cybersecurity in Government Organizations: Case Study of Bhutan. World Academy of Science,* Engineering and Technology, Open Science Index 121, International Journal of Computer and Information Engineering, 11(1), 152-155. https://publications.waset.org/10007724/perceptions-of-cybersecurity-ingovernment-organizations-case-study-of-bhutan

Chuang, S., Ou, J. C., Hollnagel, E., & Hou, S. K. (2020). Measurement of resilience potential-development of a resilience assessment grid for emergency departments. Plos one, 15(9), e0239472.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide*. NIST Special Publication, 800(61), 1-147.

Correa Coronel, M. M. (2022). Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021. https://repositorio.ucv.edu.pe/handle/20.500.12692/85975

Coyac-Torres, J. E., Sidorov, G., & Anaya, E. A. (2020). *Detección de ciberataques a través del análisis de mensajes de redes sociales: revisión del estado del arte*. Res. Comput. Sci., 149(8), 1031-1041. https://rcs.cic.ipn.mx/2020_149_8/Deteccion%20de%20ciberataques%20a%20traves%20del%20analisis%20de%20mensajes%20de%20redes%20sociales_%20revision%20del%20estado.pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Defining cybersecurity. Technology Innovation Management Review*, 4(10).

Cyberthreat Defense Report 2022 - CyberEdge Group. (2022, March 31). CyberEdge Group. https://cyber-edge.com/cyberthreat-defense-report-2022/

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Enlace*, *6*(1), 43-55 http://ve.scielo.org/scielo.php?pid=S1690-75152009000100004&script=sci_arttext

Di Luca, M. A. (2019). *Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso*. https://www.redalyc.org/journal/6378/637869113010/html/

Dunn Myriam, “A Comparative Analysis of Cyber security Initiatives Worldwide”, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June-1 July 2005. - References - Scientific Research Publishing. (s. f.). https://scirp.org/reference/referencespapers.aspx?referenceid=112322

E. D. León Gutierrez, C. M. Tesillo Gomez, Y. A. Escobar Arcaya, y L. A. Godoy Montoya, *Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital*, Innov. softw., vol. 3, n.º 2, pp. 109-120, sep. 2022. https://revistas.ulasalle.edu.pe/innosoft/article/view/62

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). *Digital information security management policy in academic libraries: A systematic review* (2010–2022). *Journal of Information Science*, 016555152311600. https://doi.org/10.1177/01655515231160026

Fernández, E. E. C. (2020). *Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional*. https://www.redalyc.org/journal/5713/571361695004/html/

Flores Cortez, R. A. (2023). Ciberseguridad para el proceso de gestión de riesgos de TI en una empresa transnacional, Lima 2023. https://repositorio.ucv.edu.pe/handle/20.500.12692/107946

Flórez-Tunaroza, D. J., & Valderrama-Coronado, S. (2022). Detección de vulnerabilidades y emulación de adversarios en los activos críticos de la empresa WEXLER SAS. https://repository.ucatolica.edu.co/entities/publication/70e7daee-e668-4897-bd0a-f8c27a27e17c

Groves, R. M., Fowler Jr, F. J., Couper, M. P., Lepkowski, J. M., Singer, E., & Tourangeau, R. (2011). *Survey methodology*. John Wiley & Sons. https://books.google.es/books?hl=es&lr=&id=ctow8zWdyFgC&oi=fnd&pg=PR15&dq=Survey+methodology&ots=fglEbG3fZb&sig=41tcsbCobExUrmvm5EVgTOyLdaA#v=onepage&q=Survey%20methodology&f=false

Guillermo, G. F. L. F. (2020). *Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo.* http://repository.unipiloto.edu.co/handle/20.500.12277/9545

Hernández, R. y Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. Ciudad de México, México: Editorial Mc Graw Hill Education. ISBN: 978-1-4562-6096-5

Hollnagel, E. (2017) Resilience Engineering and the Future of Safety Management. In: Moller, N., et al., Eds., Handbook of Safety Principles, John Wiley & Sons, Inc., Hoboken, NJ. https://doi.org/10.1002/9781119443070.ch3

Hutschenreuter, H., Çakmakçi, S. D., Maeder, C., & Kemmerich, T. (2021). *Ontology-based Cybersecurity and Resilience* Framework. In ICISSP (pp. 458-466). https://www.scitepress.org/PublishedPapers/2021/102336/102336.pdf

Infoguard. (2019). *3 Reasons Why Cybersecurity is More Important Than Ever. Cyber Security Solutions, Compliance, and Consulting Services - IT Security*. http://www.infoguardsecurity.com/3-reasons-why-cybersecurity-is-more-important-than-ever/

Informe anual de Fortinet revela un aumento en las brechas, atribuido a la falta de habilidades en ciberseguridad. (n.d.-b). Fortinet. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortinet-annual-skills-gap-report-uncovers-increase-breaches-attributed-to-lack-of-cybersecurity-skills

Jacob, N. M., & Wanjala, M. Y. (2018). *A Review of Intrusion Detection Systems. Global Journal of Computer Science and Technology.* https://computerresearch.org/index.php/computer/article/download/1610/1594

Jalali, M. S. (2018, September 1). *Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment*. https://dspace.mit.edu/handle/1721.1/120555

Kim, H., Lee, K., & Lim, J. (2017). *A study on the impact analysis of security flaws between security controls: An empirical analysis of K-ISMS using case-control study. KSII Transactions on Internet and Information Systems* (TIIS), 11(9), 4588-4608. itiis.org/digital-library/manuscript/file/21560/TIISVol11No9-22.pdf

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081. https://www.researchgate.net/profile/Aleksandr-Kljucnikov/publication/333885503_Information_security_management_in_SMEs_factors_of_success/links/5d0c8010458515c11ceaf543/Information-security-management-in-SMEs-factors-of-success.pdf

Ko, M., Osei-Bryson, K., & Dorantes, C. (2009). *Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms*. *Information Resources Management Journal*, *22*(2), 1–21. https://doi.org/10.4018/irmj.2009040101

Li, X., & Li, H. (2018). A visual analysis of research on information security risk by using CiteSpace. Ieee Access, 6, 63243-63257. https://ieeexplore.ieee.org/abstract/document/8481339/

Mallqui, M. A. (2022). *Ciberseguridad y su incidencia en la gestión de tecnologías de información en una institución administradora de fondos de aseguramiento en salud, Lima 2022.* https://repositorio.ucv.edu.pe/handle/20.500.12692/96925

Marin Puris, L. E. (2023). Ciberseguridad y su incidencia en el teletrabajo en una entidad pública, Lima 2022. https://repositorio.ucv.edu.pe/handle/20.500.12692/106398

Mitroff, I. I., & Sagasti, F. R. (1973). *Epistemology as General Systems Theory: An Approach to the Design of Complex Decision-Making Experiments. Philosophy of the Social Sciences*, 3(2), 117–134. https://doi.org/10.1177/004839317300300202

Mora Yomayuza, D. F. (2018). Plan de continuidad de negocio como base del éxito organizacional. http://repository.unipiloto.edu.co/handle/20.500.12277/4635

Nanda, M. K. (2020, November 1). A Review Article on Information Security Management. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3878639

Ñañez, C. O. (2021). *Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas*. https://repositorio.ucv.edu.pe/handle/20.500.12692/67841

Otero, A. R., Otero, C. E., & Qureshi, A. (2010). A multi-criteria evaluation of information security controls using boolean features. International Journal of Network Security & Its Applications, 2(4), 1-11.

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6b6aa4ee434eb7104f4c00c2ef80e146e3f48645

Padilla, V. S., & Freire, F. F. (2019). *A contingency plan framework for cyber-attacks. Journal of Information Systems Engineering & Management*, 4(2), 2-7. https://www.jisem-journal.com/download/a-contingency-plan-framework-for-cyber-attacks-5898.pdf

Perwej, Dr. Yusuf & Abbas, Qamar & Dixit, Jai & Akhtar, Nikhat & Jaiswal, Anurag. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management. Volume 9. Pages 669 - 710. 10.18535/ijsrm/v9i12.ec04. https://hal.science/hal-03509116/

Quevedo Lezama, C. R. (2023). *Ciberdefensa y ciberseguridad en el Perú: realidad y retos en torno a la capacidad de las FF. AA. para neutralizar ciberataques que atenten contra la seguridad nacional*. Revista De Ciencia E Investigación En Defensa - CAEN, 4(1), 55–76. https://doi.org/10.58211/recide.v4i1.99

Rahman, S. U. (1998). *Theory of constraints: a review of the philosophy and its applications. International journal of operations & production management*. https://www.emerald.com/insight/content/doi/10.1108/01443579810199720/full/html

Razikin, K., & Soewito, B. (2022). *Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework.* Egyptian Informatics Journal, 23(3), 383–404. https://doi.org/10.1016/j.eij.2022.03.001

Rea-Guaman, Á. M., Sánchez-García, I. D., San Feliu Gilabert, T., & Calvo-Manzano Villalón, J. A. (2017). *Modelos de Madurez en Ciberseguridad: una revisión sistemática.* https://oa.upm.es/48746/

Reigada, A. T. (2018). *Del principio de seguridad de los datos al derecho a la seguridad digital. Economía* https://dialnet.unirioja.es/servlet/articulo?codigo=6815107

Risco, V. E. (2021). *Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021.* https://repositorio.ucv.edu.pe/handle/20.500.12692/63424?show=full

Sánchez, H. y Reyes, C. (2015). *Metodología y Diseños en la Investigación Científica*. Lima: Business Support.

Senge, P. M. (1990). The art and practice of the learning organization. www.seeing-everything-in-a-new-way.com/uploads/2/8/5/1/28516163/peter-senge-the-fifth-discipline.pdf

Shojaie, B. (2018). *Implementation of information security management systems based on the ISOIEC 27001 standard in different cultures* (Doctoral dissertation, Staats-und Universitätsbibliothek Hamburg Carl von Ossietzky). https://ediss.sub.uni-hamburg.de/handle/ediss/7572

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). *Information security management needs more holistic approach: A literature review. International journal of information management*, 36(2), 215-225. https://www.sciencedirect.com/science/article/abs/pii/S0268401215001103

Stroh, D. (2015). *Systems Thinking For Social Change: A Practical Guide to Solving Complex Problems, Avoiding Unintended Consequences, and Achieving Lasting Results.* https://openlibrary.org/books/OL29728316M/Systems_Thinking_for_Social_Change

Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2013). *Using multivariate statistics* (Vol. 6, pp. 497-516). Boston, MA: pearson. https://www.pearsonhighered.com/assets/preface/0/1/3/4/0134790545.pdf

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). *Information security incident management: Current practice as reported in the literature. Computers & Security,* 45, 42-57. https://www.sciencedirect.com/science/article/abs/pii/S0167404814000819

Trochim, W. M. (2007). *The Research Methods Knowledge Base. ResearchGate*. https://www.researchgate.net/publication/243783609_The_Research_Methods_Knowledge_Base

Trojanowska, Justyna & Dostatni, Ewa. (2017). *Application of the Theory of Constraints for Project Management.* https://www.researchgate.net/publication/320284452_Application_of_the_Theory_of_Constraints_for_Project_Management

Valderrama, S. (2013). *Pasos para elaborar proyectos de investigación científica cualitativa, cuantitativa y mixta*. *Lima. 2da Edición. Editorial San Marcos*.

Vega, G., y Ramos, R. A. (2017). *Vulnerabilidades y amenazas a los servicios web de la intranet de la Universidad Técnica de Babahoyo*. 3C Tecnología.Glosas de innovación aplicadas a la pyme, 6(1), 53-66. https://dialnet.unirioja.es/descarga/articulo/6031033.pdf

Velecela, C. L. (2020). *Plan de gestión de seguridad de la información: caso de estudio: Gobierno Provincial del Cañar.* Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=7634599

Wang, J., Neil, M., & Fenton, N. (2020). *A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model*. Computers & Security, 89, 101659. https://doi.org/10.1016/j.cose.2019.101659

Wyer Jr, R. S., & Srull, T. K. (Eds.). (2014). *Handbook of social cognition: Volume 2: Applications*. Psychology Press. https://books.google.es/books?hl=es&lr=&id=9czsAgAAQBAJ&oi=fnd&pg=PP6&dq=Handbook+of+social+cognition&ots=JTwlf1oRTR&sig=h9NpvdEmv1AldA-8TpzcwqB67bY#v=onepage&q=Handbook%20of%20social%20cognition&f=false

ANEXOS

Anexo 1: Matriz de Operacionalización de Variables

VARIABLE	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA DE MEDICION	NIVEL O RANGO
CIBERSEGURIDAD	Rea-Guaman (2017) menciona que la ciberseguridad es un proceso que incluye prevención, detección y reacción.	Se refiere a la implementación de medidas y prácticas que protejan los sistemas informáticos y redes de computadoras contra ataques cibernéticos, al respecto Rea-Guaman (2017) menciona que la ciberseguridad es un proceso que incluye prevención, detección y reacción. La variable se medirá a través de un cuestionario de 18 ítems que consta de tres dimensiones: prevención, detección y recuperación con los siguientes indicadores: anticipación, confiabilidad, integridad; anticipación, confiabilidad, mejora; revisión disponibilidad, mejora.	Prevención	Anticipación	1, 2	Escala Ordinal, de tipo Likert. Alternativas: 1=Totalmente en desacuerdo 2=En desacuerdo 3=Ni en acuerdo, ni en desacuerdo 4=De acuerdo 5=Totalmente de acuerdo	Confiable [68-90] Adecuado [43-67] Inseguro [18-42]
				Confiabilidad	3, 4		
				Integridad	5, 6		
			Detección	Anticipación	7, 8		
				Confiabilidad	9, 10		
				Mejora	11, 12		
			Recuperación	Revisión	13, 14		
				Disponibilidad	15, 16		
				Mejora	17, 18		

VARIABLE	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA DE MEDICION	NIVEL O RANGO
GESTION DE SEGURIDAD DE LA INFORMACION	Son actividades que tienen como objetivo proteger los sistemas de información. Esta gestión implica la implementación de controles de seguridad, la evaluación de riesgos y la gestión de incidentes de seguridad, entre otras actividades.	Implica la aplicación de medidas técnicas, organizacionales y administrativas para proteger los activos de información, incluyendo la identificación de riesgos, evaluación de vulnerabilidades, implementación de controles de seguridad, la monitorización y la mejora continua del sistema de gestión de seguridad de la información. La variable se medirá a través de un cuestionario de 18 ítems que consta de tres dimensiones: controles de seguridad, evaluación de riesgos y gestión de incidentes de seguridad con los siguientes indicadores: revisión, disponibilidad, mejora, revisión, confiabilidad, verificación, revisión, verificación y mejora.	Controles de seguridad	Revisión	19, 20	Escala Ordinal, de tipo Likert. Alternativas: 1=Totalmente en desacuerdo 2=En desacuerdo 3=Ni en acuerdo, ni en desacuerdo 4=De acuerdo 5 =Totalmente de acuerdo	Óptimo [68-90] Satisfactorio [43-67] Inadecuado [18-42]
				Disponibilidad	21, 22		
				Mejora	23, 24		
			Evaluación de riesgos	Revisión	25, 26		
				Confiabilidad	27, 28		
				Verificación	29, 30		
			Gestión de incidentes de seguridad	Revisión	31, 32		
				Verificación	33, 34		
				Mejora	35, 36		

Anexo 2: Certificado de Validación del Instrumento de Recolección de Datos

Validación del Experto N°1

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE:

VARIABLE: Ciberseguridad

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	PREVENCION	Si	No	Si	No	Si	No	
1	¿En qué medida considera usted que la oficina de tecnología de información cuenta con programas para concientizar sobre las amenazas en la ciberseguridad?	X		X		X		
2	¿Está satisfecho con la capacitación recibida por la oficina de tecnología de información sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	X		X		X		
3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?	X		X		X		
4	¿Considera que se realizan adecuadamente los respaldos y/o backups de la información de la institución por parte de la oficina de tecnología de información?	X		X		X		
5	¿En qué medida cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la institución de las actividades ilícitas de los cibercriminales?	X		X		X		
6	¿Considera usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas eficientes para neutralizar las actividades ilícitas de los cibercriminales?	X		X		X		
	DETECCION	Si	No	Si	No	Si	No	
7	¿Cuán de acuerdo se encuentra con la afirmación que la oficina de tecnología de información ha incorporado planes de protección de detección contra los cibercriminales en los servicios informáticos?	X		X		X		
8	¿Considera que usted sabría cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?	X		X		X		
9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la institución para evitar acciones desleales que conlleven a pérdida o robo de información?	X		X		X		
10	¿Está de acuerdo con el despliegue de cámaras de seguridad por parte de la oficina de tecnología de información para detectar acciones de personas no autorizadas con la información?	X		X		X		
11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?	X		X		X		
12	¿Está satisfecho con los medios de seguridad tecnológicos para que los empleados se identifiquen al ingresar a la institución?	X		X		X		
	RECUPERACION	Si	No	Si	No	Si	No	
13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?	X		X		X		
14	¿Considera que los planes de contingencia en caso de un ciberataque establecidos por la oficina de tecnología de información son idóneos para la institución?	X		X		X		
15	En su experiencia ¿el impacto de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad ha afectado la disponibilidad de los servicios que usa diariamente?	X		X		X		

16	¿Considera usted que en el último año se ha perdido información importante por causa de algún virus informático?	X		X		X		
17	¿Las incidencias de ciberseguridad son atendidas en orden por parte de la oficina de tecnología de información?	X		X		X		
18	¿En qué medida puede afirmar que la oficina de tecnología busca mejoras para la ciberseguridad?	X		X		X		

VARIABLE: Gestión de Seguridad de la Información

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CONTROLES DE SEGURIDAD	Si	No	Si	No	Si	No	
1	¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?	X		X		X		
2	¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?	X		X		X		
3	¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?	X		X		X		
4	¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?	X		X		X		
5	¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?	X		X		X		
6	¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?	X		X		X		
	EVALUACION DE RIESGOS	Si	No	Si	No	Si	No	
7	¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?	X		X		X		
8	¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?	X		X		X		
9	¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?	X		X		X		
10	¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?	X		X		X		
11	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad implementadas para reducir o mitigar los riesgos de seguridad de la información?	X		X		X		
12	¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?	X		X		X		
	GESTION DE INCIDENTES DE SEGURIDAD	Si	No	Si	No	Si	No	
13	¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?	X		X		X		
14	¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?	X		X		X		
15	¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?	X		X		X		
16	¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?	X		X		X		

17	¿Está usted satisfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	X		X		X		
18	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos de gestión de incidentes de seguridad de la información?	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr. ACUÑA BENITES MARLON FRANK **DNI: 42097456**

Especialidad del validador: Metodólogo **[X]** Temático [ ]

13 de mayo del 2023

[1]**Pertinencia**:El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto Informante.

Validación del Experto N°2

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE:

VARIABLE: Ciberseguridad

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	PREVENCION	Si	No	Si	No	Si	No	
1	¿En qué medida considera usted que la oficina de tecnología de información cuenta con programas para concientizar sobre las amenazas en la ciberseguridad?	X		X		X		
2	¿Está satisfecho con la capacitación recibida por la oficina de tecnología de información sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	X		X		X		
3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?	X		X		X		
4	¿Considera que se realizan adecuadamente los respaldos y/o backups de la información de la institución por parte de la oficina de tecnología de información?	X		X		X		
5	¿En qué medida cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la institución de las actividades ilícitas de los cibercriminales?	X		X		X		
6	¿Considera usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas eficientes para neutralizar las actividades ilícitas de los cibercriminales?	X		X		X		
	DETECCION	Si	No	Si	No	Si	No	
7	¿Cuán de acuerdo se encuentra con la afirmación que la oficina de tecnología de información ha incorporado planes de protección de detección contra los cibercriminales en los servicios informáticos?	X		X		X		
8	¿Considera que usted sabría cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?	X		X		X		
9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la institución para evitar acciones desleales que conlleven a pérdida o robo de información?	X		X		X		
10	¿Está de acuerdo con el despliegue de cámaras de seguridad por parte de la oficina de tecnología de información para detectar acciones de personas no autorizadas con la información?	X		X		X		
11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?	X		X		X		
12	¿Está satisfecho con los medios de seguridad tecnológicos para que los empleados se identifiquen al ingresar a la institución?	X		X		X		
	RECUPERACION	Si	No	Si	No	Si	No	
13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?	X		X		X		
14	¿Considera que los planes de contingencia en caso de un ciberataque establecidos por la oficina de tecnología de información son idóneos para la institución?	X		X		X		
15	En su experiencia ¿el impacto de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad ha afectado la disponibilidad de los servicios que usa diariamente?	X		X		X		

16	¿Considera usted que en el último año se ha perdido información importante por causa de algún virus informático?	X		X		X		
17	¿Las incidencias de ciberseguridad son atendidas en orden por parte de la oficina de tecnología de información?	X		X		X		
18	¿En qué medida puede afirmar que la oficina de tecnología busca mejoras para la ciberseguridad?	X		X		X		

VARIABLE: Gestión de Seguridad de la Información

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CONTROLES DE SEGURIDAD	Si	No	Si	No	Si	No	
1	¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?	X		X		X		
2	¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?	X		X		X		
3	¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?	X		X		X		
4	¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?	X		X		X		
5	¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?	X		X		X		
6	¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?	X		X		X		
	EVALUACIÓN DE RIESGOS	Si	No	Si	No	Si	No	
7	¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?	X		X		X		
8	¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?	X		X		X		
9	¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?	X		X		X		
10	¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?	X		X		X		
11	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad implementadas para reducir o mitigar los riesgos de seguridad de la información?	X		X		X		
12	¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?	X		X		X		
	GESTIÓN DE INCIDENTES DE SEGURIDAD	Si	No	Si	No	Si	No	
13	¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?	X		X		X		
14	¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?	X		X		X		
15	¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?	X		X		X		
16	¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?	X		X		X		

17	¿Está usted satisfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	X		X		X		
18	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos de gestión de incidentes de seguridad de la información?	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Mg. RÍOS CASSANA OSCAR EDGARDO **DNI: 08468430**

Especialidad del validador: Metodólogo **[X]** Temático **[ ]**

15 de mayo del 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Firma del Experto Informante.

08468430

Validación del Experto N°3

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

VARIABLE: Ciberseguridad

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	PREVENCION	Si	No	Si	No	Si	No	
1	¿En qué medida considera usted que la oficina de tecnología de información cuenta con programas para concientizar sobre las amenazas en la ciberseguridad?	X		X		X		
2	¿Está satisfecho con la capacitación recibida por la oficina de tecnología de información sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	X		X		X		
3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?	X		X		X		
4	¿Considera que se realizan adecuadamente los respaldos y/o backups de la información de la institución por parte de la oficina de tecnología de información?	X		X		X		
5	¿En qué medida cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la institución de las actividades ilícitas de los cibercriminales?	X		X		X		
6	¿Considera usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas eficientes para neutralizar las actividades ilícitas de los cibercriminales?	X		X		X		
	DETECCION	Si	No	Si	No	Si	No	
7	¿Cuán de acuerdo se encuentra con la afirmación que la oficina de tecnología de información ha incorporado planes de protección de detección contra los cibercriminales en los servicios informáticos?	X		X		X		
8	¿Considera que usted sabría cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?	X		X		X		
9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la institución para evitar acciones desleales que conlleven a pérdida o robo de información?	X		X		X		
10	¿Está de acuerdo con el despliegue de cámaras de seguridad por parte de la oficina de tecnología de información para detectar acciones de personas no autorizadas con la información?	X		X		X		
11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?	X		X		X		
12	¿Está satisfecho con los medios de seguridad tecnológicos para que los empleados se identifiquen al ingresar a la institución?	X		X		X		

	RECUPERACION	Si	No	Si	No	Si	No	
13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?	X		X		X		
14	¿Considera que los planes de contingencia en caso de un ciberataque establecidos por la oficina de tecnología de información son idóneos para la institución?	X		X		X		
15	En su experiencia ¿el impacto de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad ha afectado la disponibilidad de los servicios que usa diariamente?	X		X		X		
16	¿Considera usted que en el último año se ha perdido información importante por causa de algún virus informático?	X		X		X		
17	¿Las incidencias de ciberseguridad son atendidas en orden por parte de la oficina de tecnología de información?	X		X		X		
18	¿En qué medida puede afirmar que la oficina de tecnología busca mejoras para la ciberseguridad?	X		X		X		

VARIABLE: Gestión de Seguridad de la Información

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CONTROLES DE SEGURIDAD	Si	No	Si	No	Si	No	
1	¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?	X		X		X		
2	¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?	X		X		X		
3	¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?	X		X		X		
4	¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?	X		X		X		
5	¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?	X		X		X		
6	¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?	X		X		X		
	EVALUACION DE RIESGOS	Si	No	Si	No	Si	No	
7	¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?	X		X		X		
8	¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?	X		X		X		
9	¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?	X		X		X		
10	¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?	X		X		X		

11	¿Cuando se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad implementadas para reducir o mitigar los riesgos de seguridad de la información?	X		X		X		
12	¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?	X		X		X		
	GESTION DE INCIDENTES DE SEGURIDAD	Si	No	Si	No	Si	No	
13	¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?	X		X		X		
14	¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?	X		X		X		
15	¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?	X		X		X		
16	¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?	X		X		X		
17	¿Está usted satisfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	X		X		X		
18	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos de gestión de incidentes de seguridad de la información?	X		X		X		

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr. CARLOS MANUEL RECUAY CÓNDOR **DNI: 09365798**

Especialidad del validador: Metodólogo **[X]** Temático **[ ]** **Doctor en Gestión Pública y Gobernabilidad, Magister en Economía**

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

25 de mayo del 2023.

Firma del Experto Informante.

Anexo 3: Instrumento de Recolección de Datos

Cuestionario para trabajadores de la entidad publica

Fecha: [/ /]

Sexo: Femenino[ ] Masculino[ ]

Autor: Mallqui (2022) adaptado para la investigación

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo al siguiente ejemplo: Totalmente en desacuerdo (1), En desacuerdo (2), Ni de acuerdo ni en desacuerdo (3), De acuerdo (4) y Totalmente de acuerdo (5).

No	Pregunta	Valoración				
		1	2	3	4	5
	Sobre ciberseguridad					
1	¿En qué medida considera usted que la oficina de tecnología de información cuenta con programas para concientizar sobre las amenazas en la ciberseguridad?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
2	¿Está satisfecho con la capacitación recibida por la oficina de tecnología de información sobre las formas más comunes en que los ciberdelincuentes suelen accionar?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
3	¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
4	¿Considera que se realizan adecuadamente los respaldos y/o backups de la información de la institución por parte de la oficina de tecnología de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
5	¿En qué medida cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información de la institución de las actividades ilícitas de los cibercriminales?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
6	¿Considera usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas eficientes para neutralizar las actividades ilícitas de los cibercriminales?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
7	¿Cuán de acuerdo se encuentra con la afirmación que la oficina de tecnología de información ha incorporado planes de protección de detección contra los cibercriminales en los servicios informáticos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
8	¿Considera que usted sabría cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
9	¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la institución para evitar acciones desleales que conlleven a pérdida o robo de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
10	¿Está de acuerdo con el despliegue de cámaras de seguridad por parte de la oficina de tecnología de información para detectar acciones de personas no autorizadas con la información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

No	Pregunta	Valoración				
		1	2	3	4	5
11	¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
12	¿Está satisfecho con los medios de seguridad tecnológicos para que los empleados se identifiquen al ingresar a la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
13	¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
14	¿Considera que los planes de contingencia en caso de un ciberataque establecidos por la oficina de tecnología de información son idóneos para la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
15	En su experiencia ¿el impacto de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad ha afectado la disponibilidad de los servicios que usa diariamente?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
16	¿Considera usted que en el último año se ha perdido información importante por causa de algún virus informático?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
17	¿Las incidencias de ciberseguridad son atendidas en orden de prioridad de riesgo por parte de la oficina de tecnología de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
18	¿En qué medida puede afirmar que la oficina de tecnología busca mejoras para la ciberseguridad?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
	Sobre Gestión de Seguridad de la Información					
19	¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
20	¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
21	¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
22	¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
23	¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
24	¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
25	¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
26	¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

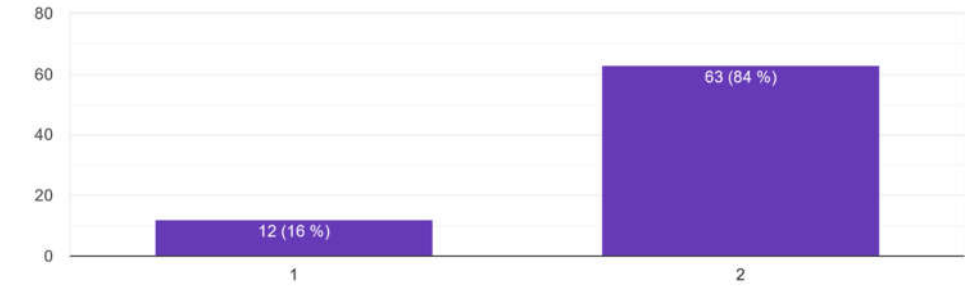
No	Pregunta	Valoración				
		1	2	3	4	5
27	¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
28	¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
29	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad implementadas para reducir o mitigar los riesgos de seguridad de la información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
30	¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
31	¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
32	¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
33	¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
34	¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
35	¿Está usted satisfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
36	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos de gestión de incidentes de seguridad de la información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

¡Gracias por su tiempo!

Anexo 4: Resumen de encuestas realizadas

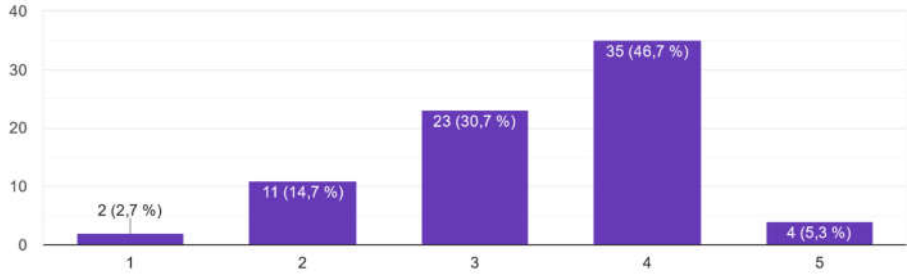
Sexo

75 respuestas



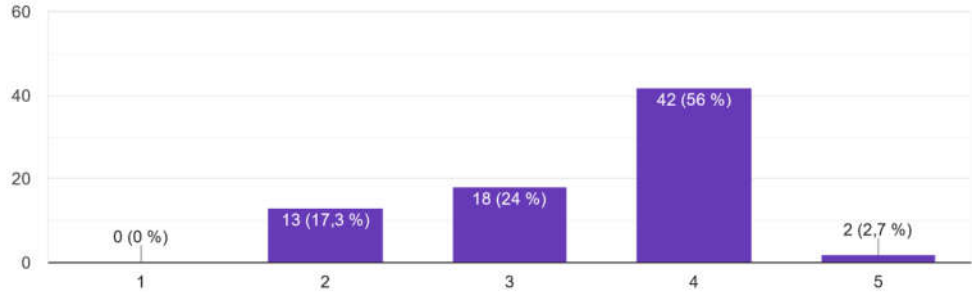
1. ¿En qué medida considera usted que la oficina de tecnología de información cuenta con programas para concientizar sobre las amenazas en la ciberseguridad?

75 respuestas



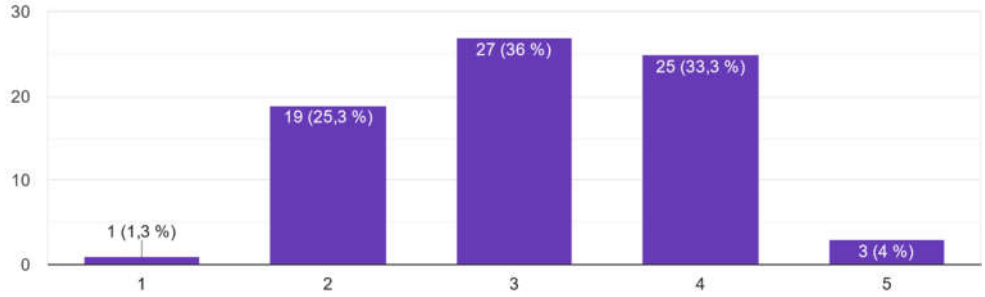
2. ¿Está satisfecho con la capacitación recibida por la oficina de tecnología de información sobre las formas más comunes en que los ciberdelincuentes suelen accionar?

75 respuestas



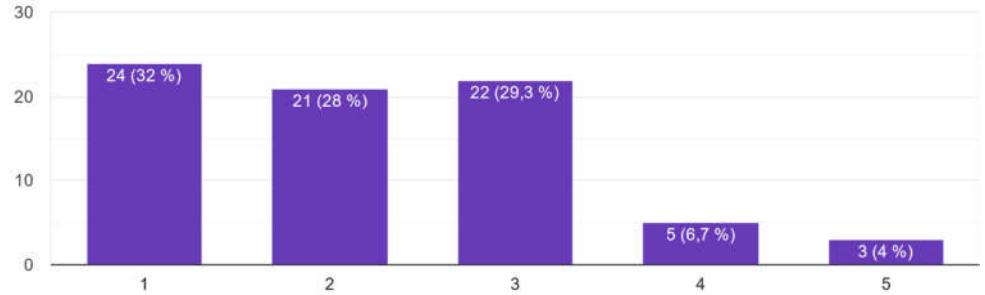
3. ¿La oficina de tecnología de información restringe el uso de los sistemas informáticos de la organización al personal no autorizado?

75 respuestas



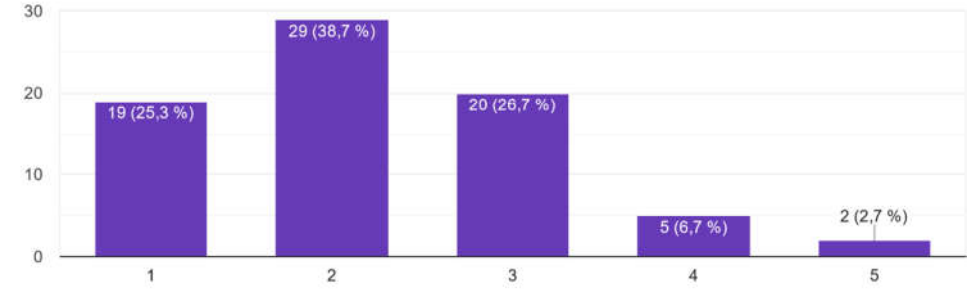
4. ¿Considera que se realizan adecuadamente los respaldos y/o backups de la información de la institución por parte de la oficina de tecnología de información?

75 respuestas



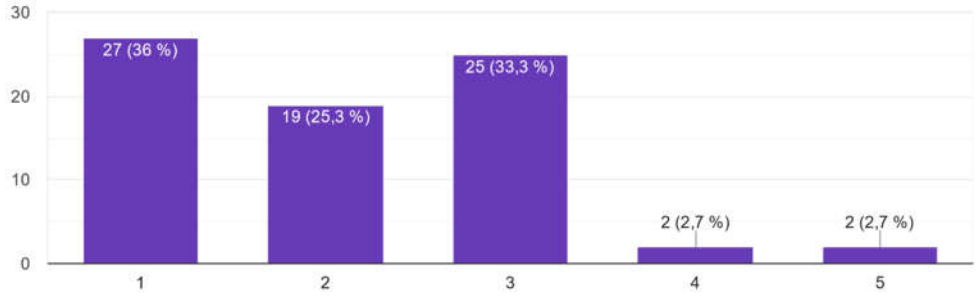
5. ¿En qué medida cree usted que la oficina de tecnología de información ha incorporado software de seguridad adecuados para proteger la información...e las actividades ilícitas de los cibercriminales?

75 respuestas



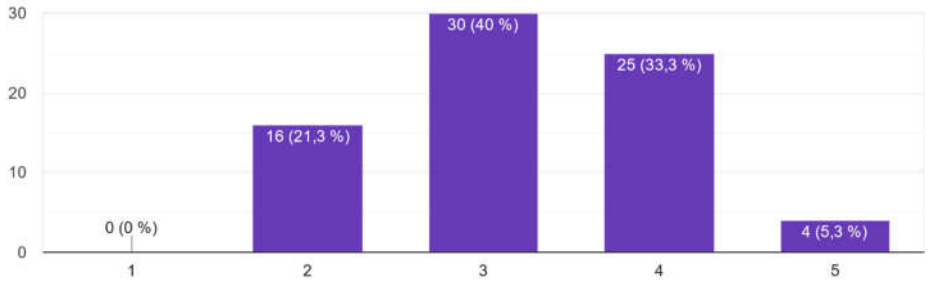
6. ¿Considera usted que la oficina de tecnología de información ha incorporado medidas de seguridad físicas eficientes para neutralizar las actividades ilícitas de los cibercriminales?

75 respuestas



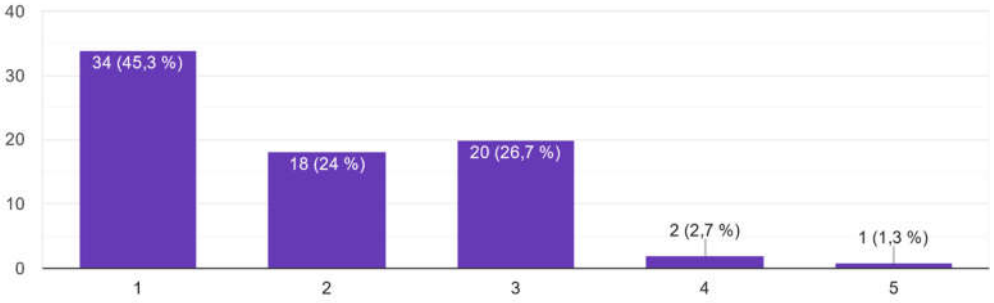
7. ¿Cuán de acuerdo se encuentra con la afirmación que la oficina de tecnología de información ha incorporado planes de protección de detección cont...los cibercriminales en los servicios informáticos?

75 respuestas



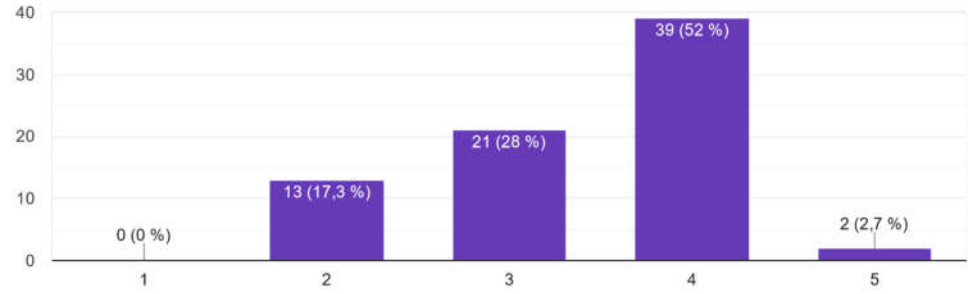
8. ¿Considera que usted sabría cómo actuar en caso de detectar actividades de cibercriminales en unos de los dispositivos a cargo dentro de sus funciones?

75 respuestas



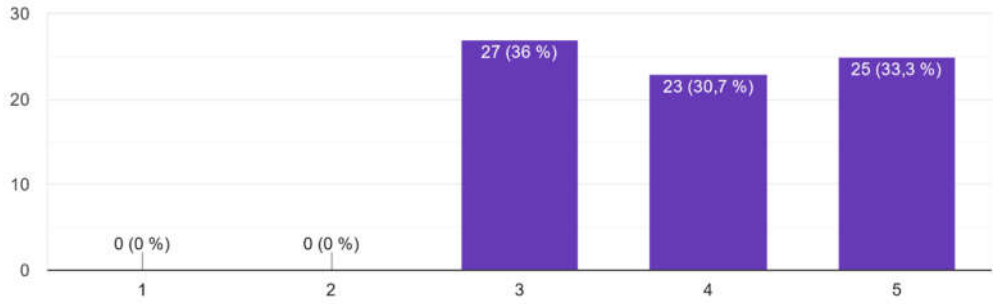
9. ¿Cree usted que la oficina de tecnología de información supervisa y previene las actividades de los colaboradores de la institución para evitar acc...les que conlleven a pérdida o robo de información?

75 respuestas



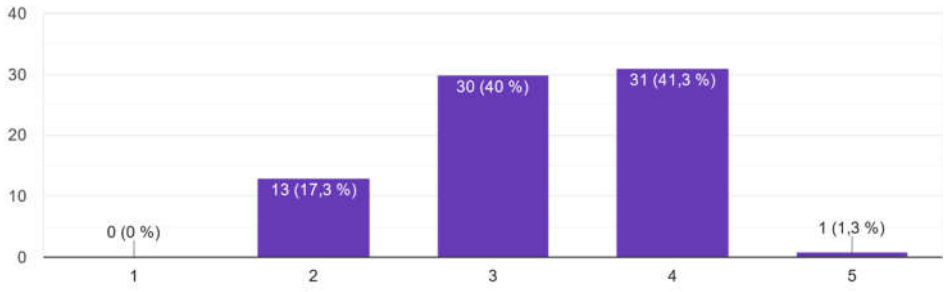
10. ¿Está de acuerdo con el despliegue de cámaras de seguridad por parte de la oficina de tecnología de información para detectar acciones de personas no autorizadas con la información?

75 respuestas



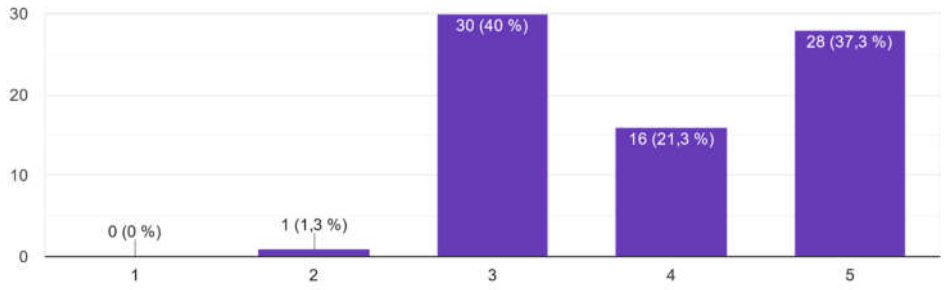
11. ¿Cree usted que la oficina de tecnología de información cuenta con personal calificado en ciberseguridad?

75 respuestas



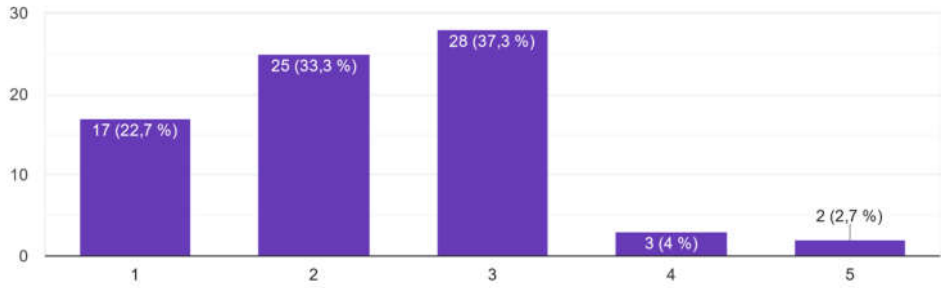
12. ¿Está satisfecho con los medios de seguridad tecnológicos para que los empleados se identifiquen al ingresar a la institución?

75 respuestas



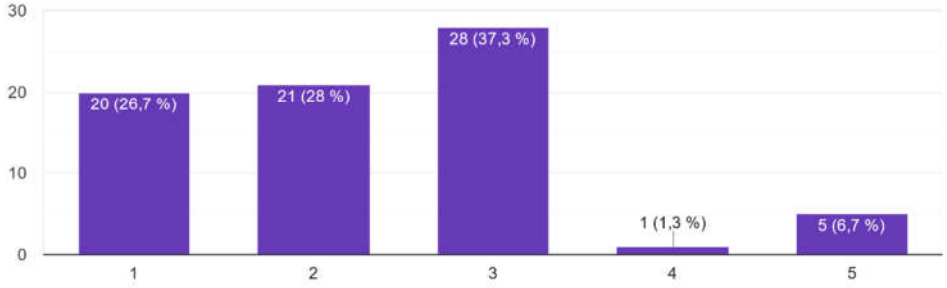
13. ¿Cree usted que los sistemas de seguridad existentes gestionados por la oficina de tecnología de información neutralizan los ataques de los ciberdelincuentes?

75 respuestas



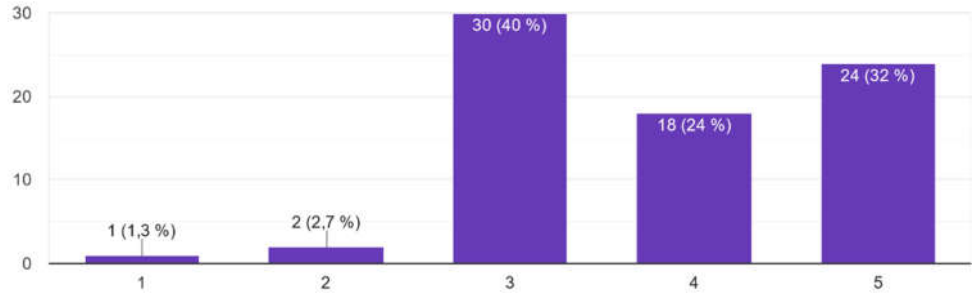
14. ¿Considera que los planes de contingencia en caso de un ciberataque establecidos por la oficina de tecnología de información son idóneos para la institución?

75 respuestas



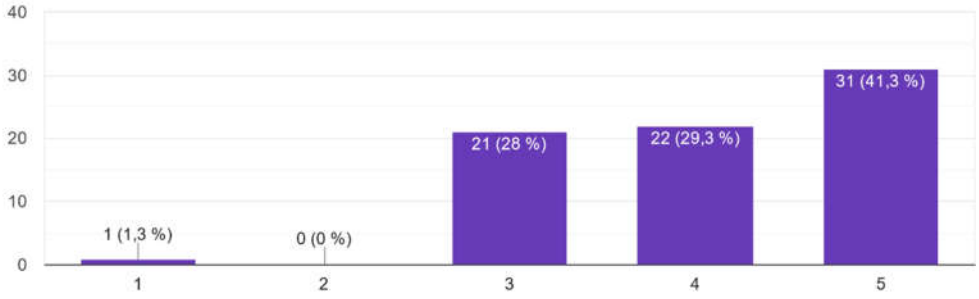
15. En su experiencia ¿el impacto de algún ataque informático que no pudo ser detectado y anulado por los sistemas de seguridad ha afectado la disponibilidad de los servicios que usa diariamente?

75 respuestas



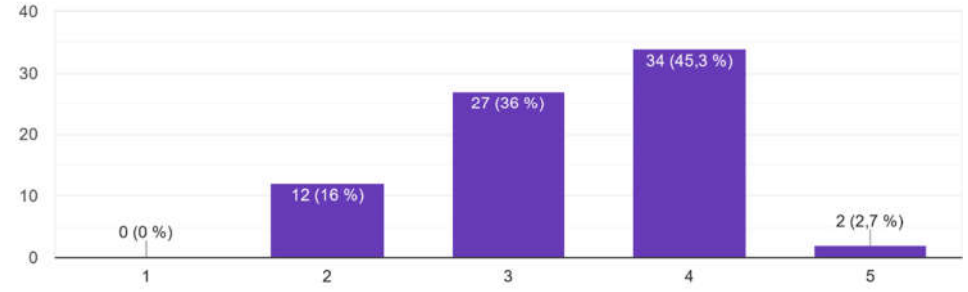
16. ¿Considera usted que en el último año se ha perdido información importante por causa de algún virus informático?

75 respuestas



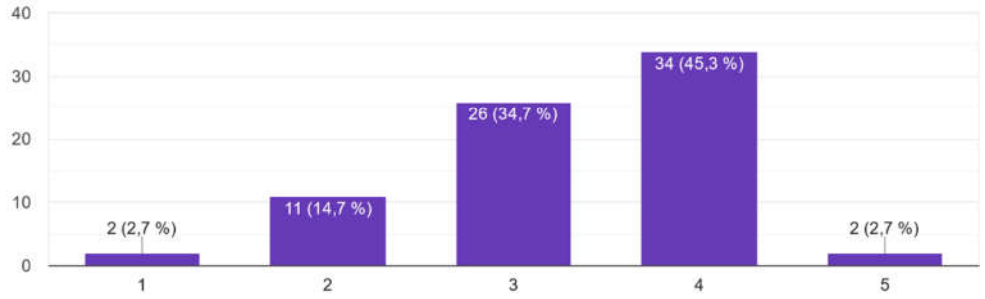
17. ¿Las incidencias de ciberseguridad son atendidas en orden de prioridad de riesgo por parte de la oficina de tecnología de información?

75 respuestas



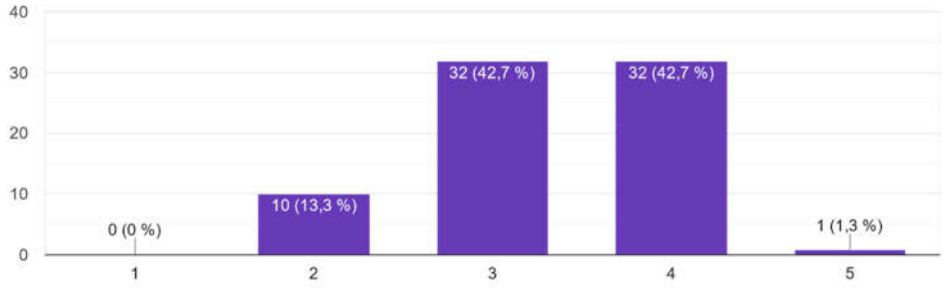
18. ¿En qué medida puede afirmar que la oficina de tecnología busca mejoras para la ciberseguridad?

75 respuestas



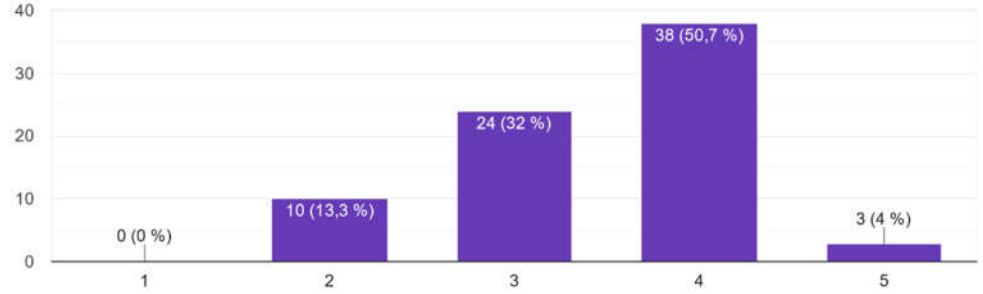
19. ¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?

75 respuestas



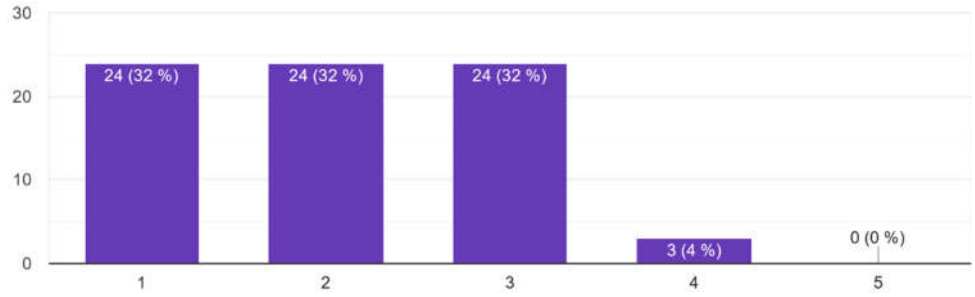
20. ¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?

75 respuestas



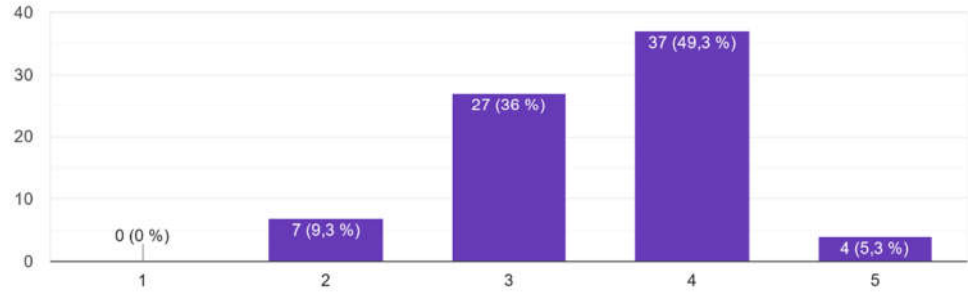
21. ¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?

75 respuestas



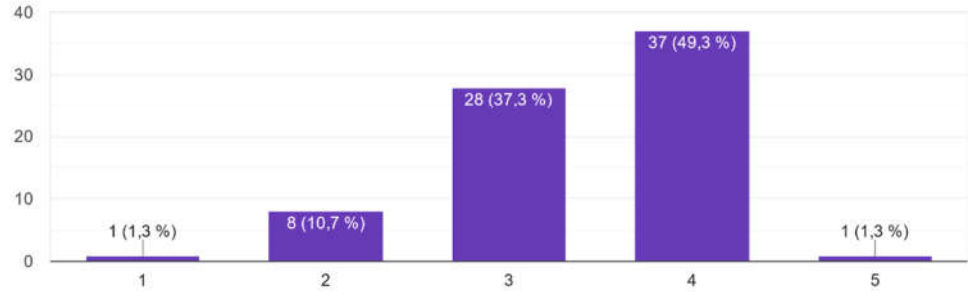
22. ¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?

75 respuestas



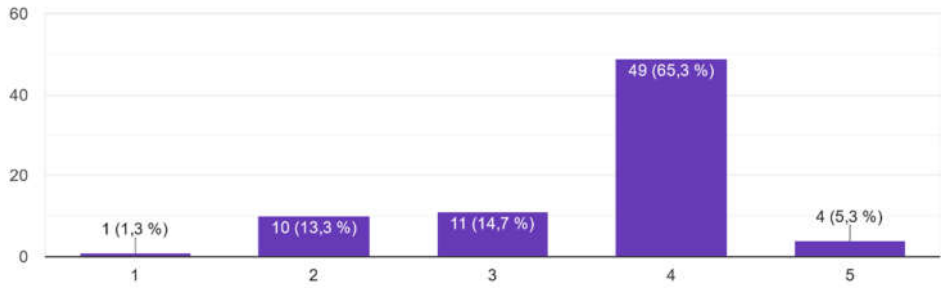
23. ¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?

75 respuestas



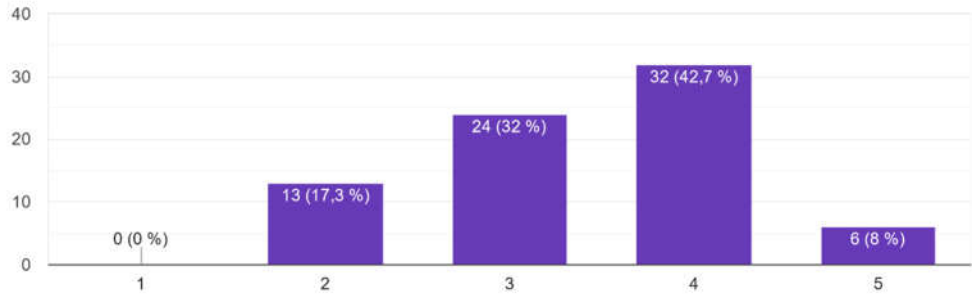
24. ¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?

75 respuestas



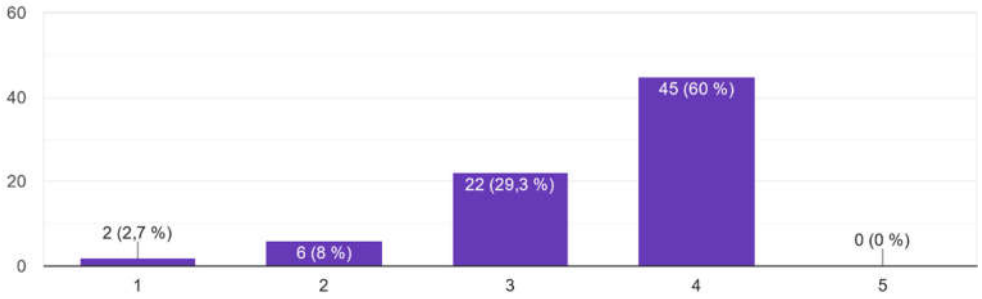
25. ¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?

75 respuestas



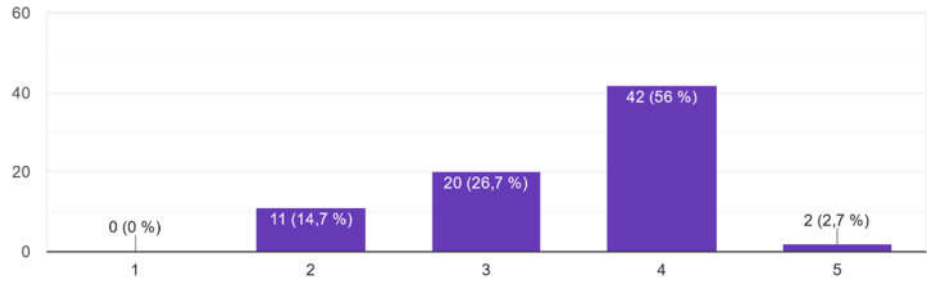
26. ¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?

75 respuestas



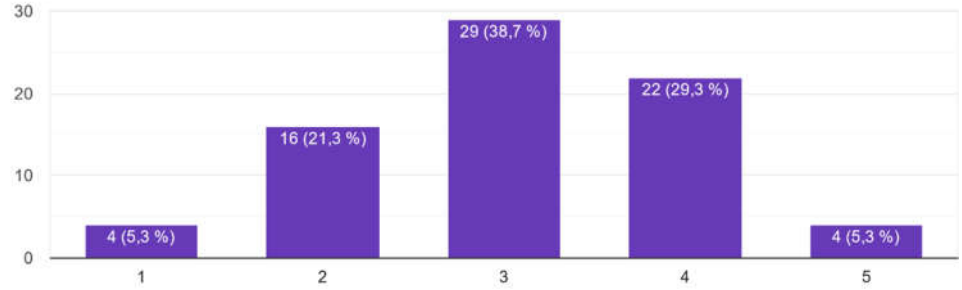
27. ¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?

75 respuestas



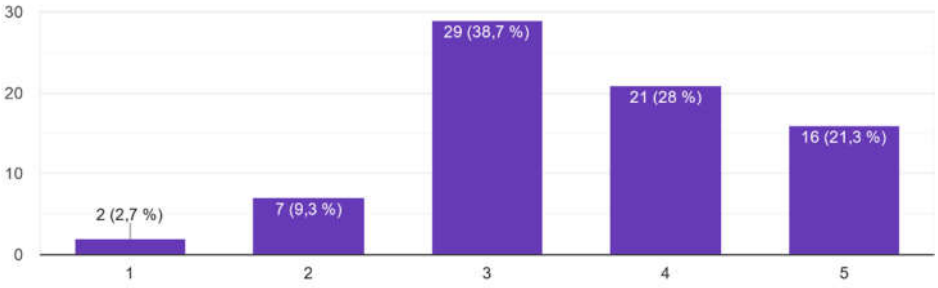
28. ¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?

75 respuestas



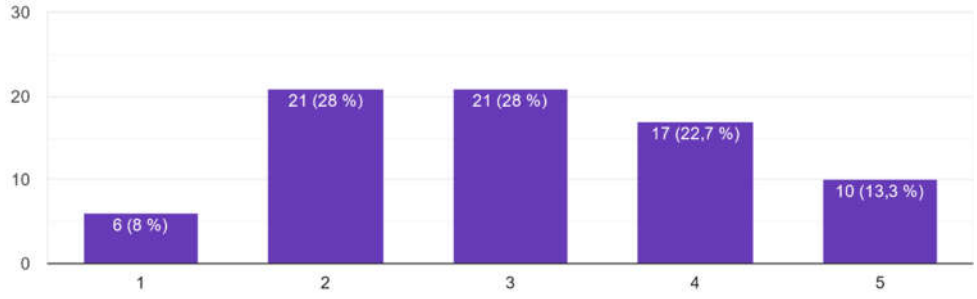
29. ¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad...itigar los riesgos de seguridad de la información?

75 respuestas



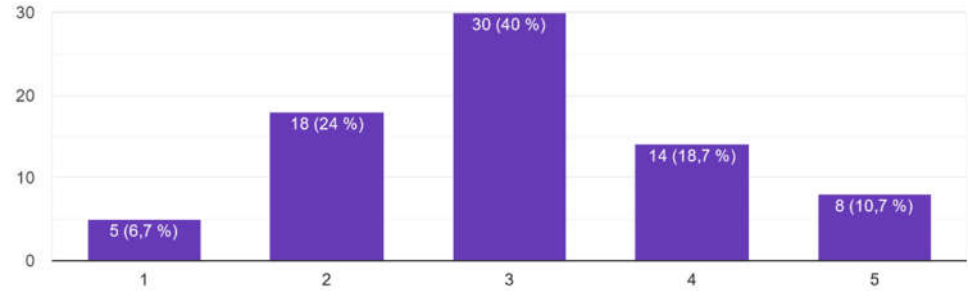
30. ¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?

75 respuestas



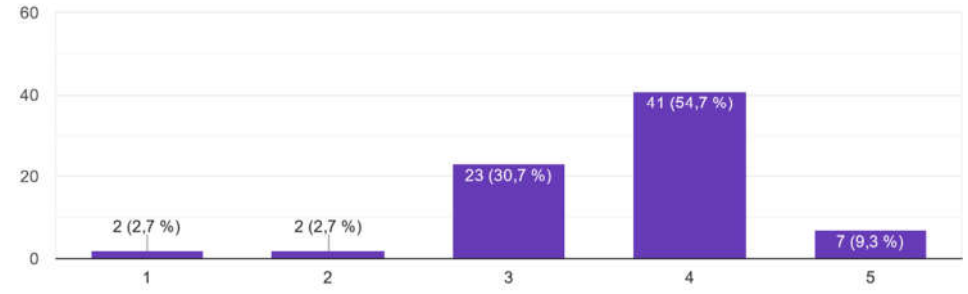
31. ¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?

75 respuestas



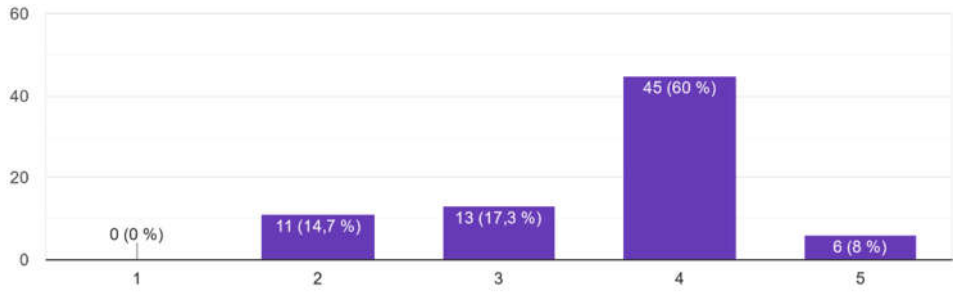
32. ¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?

75 respuestas



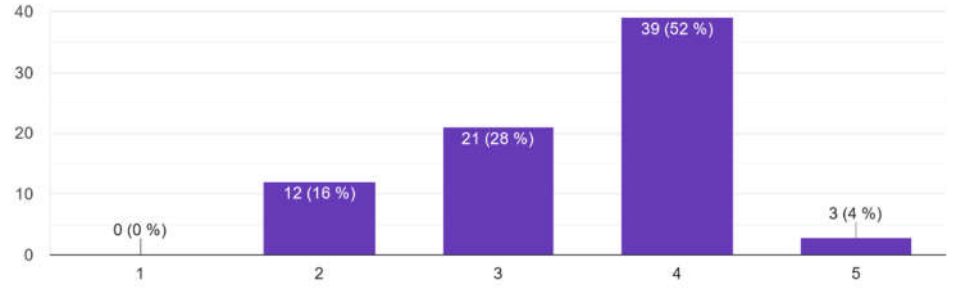
33. ¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?

75 respuestas



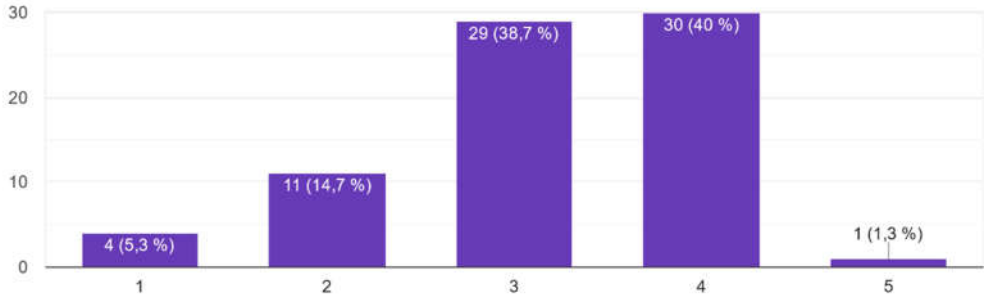
34 ¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?

75 respuestas



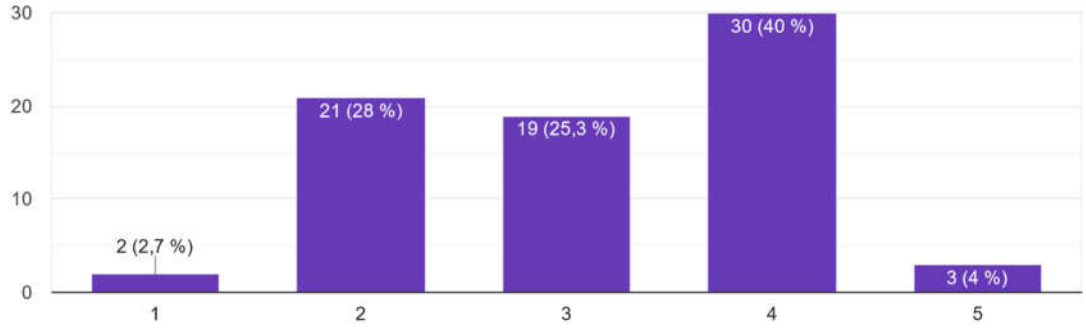
35. ¿Está usted satisfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?

75 respuestas



36. ¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos d...tión de incidentes de seguridad de la información?

75 respuestas



Anexo 5: Carta de Presentación

UNIVERSIDAD CÉSAR VALLEJO

"Año de la unidad, la paz y el desarrollo"

Lima, 10 de mayo de 2023
Carta P. 0055-2023-UCV-VA-EPG-FDL/J

ING.
GALA TATIANA BRICEÑO DIAZ
JEFE DEL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION
CONGRESO DE LA REPUBLICA

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a RIVERA LAZARO, WILFREDO ELIAS; identificado con DNI N° 10057581 y con código de matrícula N° 6000140519; estudiante del programa de MAESTRIA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

Obberseguridad y su incidencia en la Gestión de Seguridad de la Información en una entidad pública, Lima 2023

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador RIVERA LAZARO, WILFREDO ELIAS asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

Dra. Helga R. Mejo Marrufo
Jefe
Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

Ing. GALA TATIANA BRICEÑO DIAZ
Jefe del Departamento de Tecnología de la Información
CONGRESO DE LA REPUBLICA

Anexo 6: Aspectos Administrativos

Recursos y Presupuesto

Recursos Humanos

La Tabla 1 detalla el presupuesto de recursos humanos o mano de obra esperado para el desarrollo de este estudio, que comprende parte del presupuesto de inversión en las actividades de revisión bibliográfica, recolección y procesamiento de información, interpretación de resultados y la gestión del proyecto de investigación.

Tabla 1

Presupuesto en Recursos Humanos

Cantidad	Recurso Humano	Valor Unitario S/.	Sub total S/.
09	Gastos mensuales para el desarrollo de la tesis	S/. 450.00	S/. 4050.00
01	Asesor de tesis	S/. 500.00	S/. 500.00
	Total		S/. 4550.00

Recursos Hardware

En la tabla 2 se detalla el presupuesto de los recursos de hardware y equipos informáticos para el desarrollo de este estudio, los cuales también forman parte del presupuesto de inversión en las actividades de revisión bibliográfica, recolección y procesamiento de información, interpretación de resultados y la gestión del proyecto de investigación.

Tabla 2

Presupuesto en Recursos Hardware

Cantidad	Descripción del Recurso	Valor Unitario S/.	Sub total S/.
01	Notebook DELL Alienware x17 R2 Core i9-12900HK	S/. 4500.00	S/. 4500.00
01	Multifuncional HP Smart Tank 720	S/. 920.00	S/. 920.00
	Total		S/. 5420.00

Recursos Software

En la tabla 3 se detalla el presupuesto de los recursos de software a utilizar en el desarrollo de la presente investigación, que también forman parte del presupuesto de inversión en las actividades de revisión bibliográfica, recolección y procesamiento de información, interpretación de resultados y la gestión del proyecto de investigación.

Tabla 3

Presupuesto en Recursos Software

Cantidad	Descripción del Recurso	Valor Unitario S/.	Sub total S/.
01	Licencia anual Office 365	S/. 200.00	S/. 200.00
01	Licencia anual antivirus	S/. 120.00	S/. 120.00
	Total		S/. 320.00

Presupuesto

El presupuesto asignado para esta investigación es la suma de todos los presupuestos mencionados anteriormente, la misma que se detalla a continuación:

Tabla 4

Presupuesto

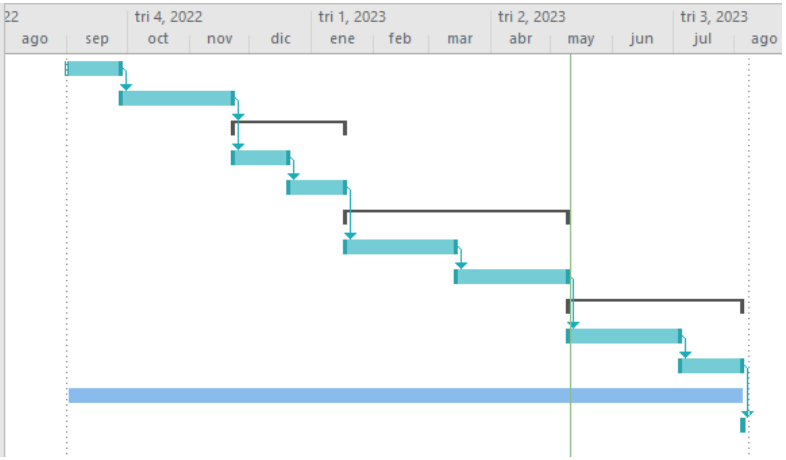
Costos	Monto
Recursos humanos	S/. 4550.00
Recursos hardware	S/. 5420.00
Recursos software	S/. 320.00
Presupuesto total	S/. 10290.00

Financiamiento

Este proyecto de investigación tiene un presupuesto de S/. 10,290.00 (diez mil doscientos noventa soles y 00/100) que será asumido por el investigador.

Cronograma de ejecución

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	Determinacion del problema de investigacion	1 ms	jue 1/09/22	mar 27/09/22	
2	Marco teorico	2 mss	mar 27/09/22	mar 22/11/22	1
3	**Antecedentes**	**40 días**	**mar 22/11/22**	**mar 17/01/23**	**2**
4	Nacionales	1 ms	mar 22/11/22	mar 20/12/22	2
5	Internacionales	1 ms	mar 20/12/22	mar 17/01/23	4
6	**Aplicación instrumentos**	**80 días**	**mar 17/01/23**	**mar 9/05/23**	
7	Coordinacion con el personal de la entidad	2 mss	mar 17/01/23	mar 14/03/23	5
8	Recoleccion de datos	2 mss	mar 14/03/23	mar 9/05/23	7
9	**Resultados**	**63.13 días**	**mar 9/05/23**	**vie 4/08/23**	
10	Procesamiento de datos	2 mss	mar 9/05/23	mar 4/07/23	8
11	Interpretacion de datos	1.18 mss	mar 4/07/23	vie 4/08/23	10
12	Redaccion del trabajo de investigacion	242 días	jue 1/09/22	vie 4/08/23	
13	Sustentacion de tesis	1 día	sáb 5/08/23	sáb 5/08/23	11

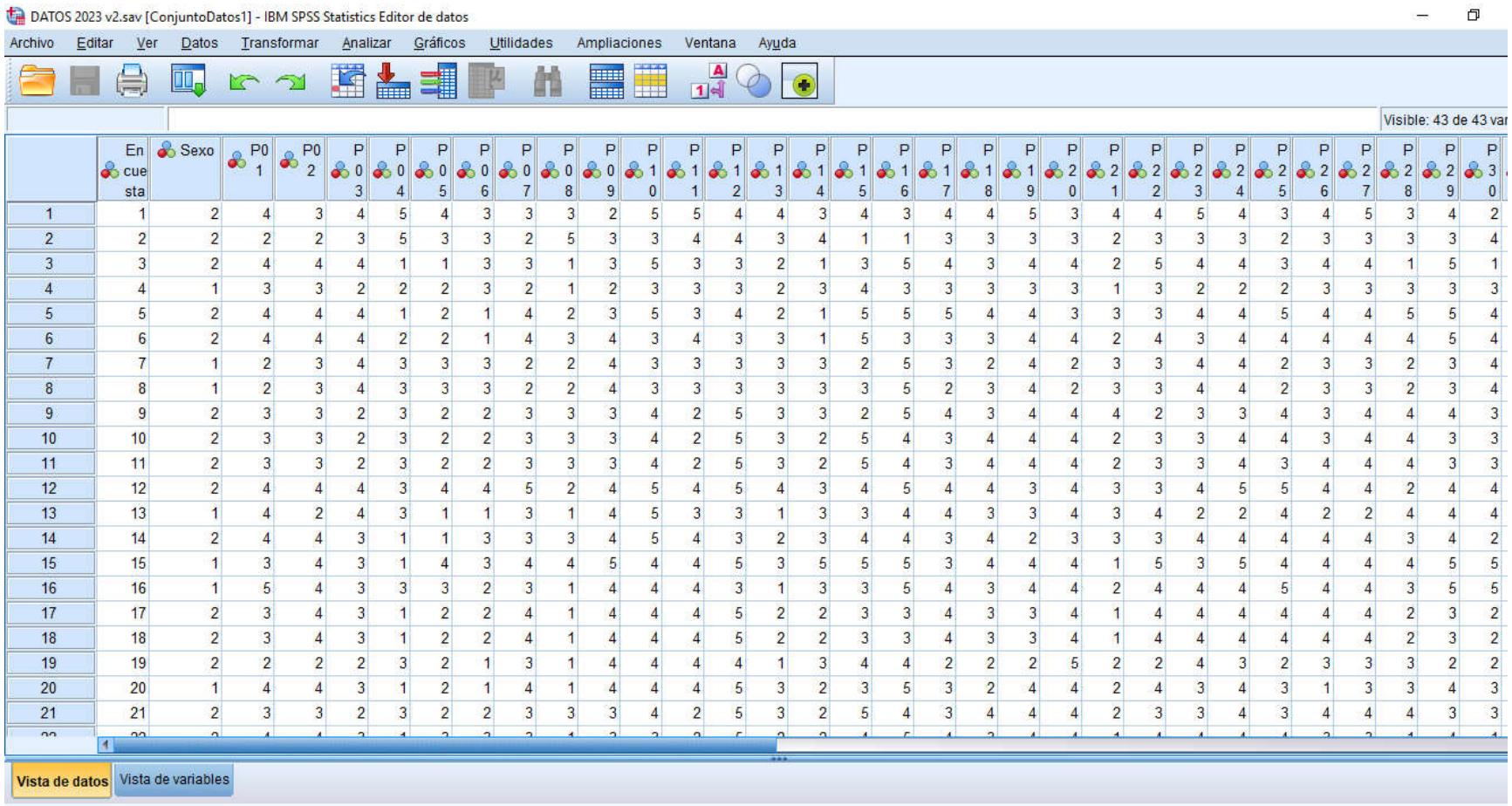


Anexo 7: Base de datos

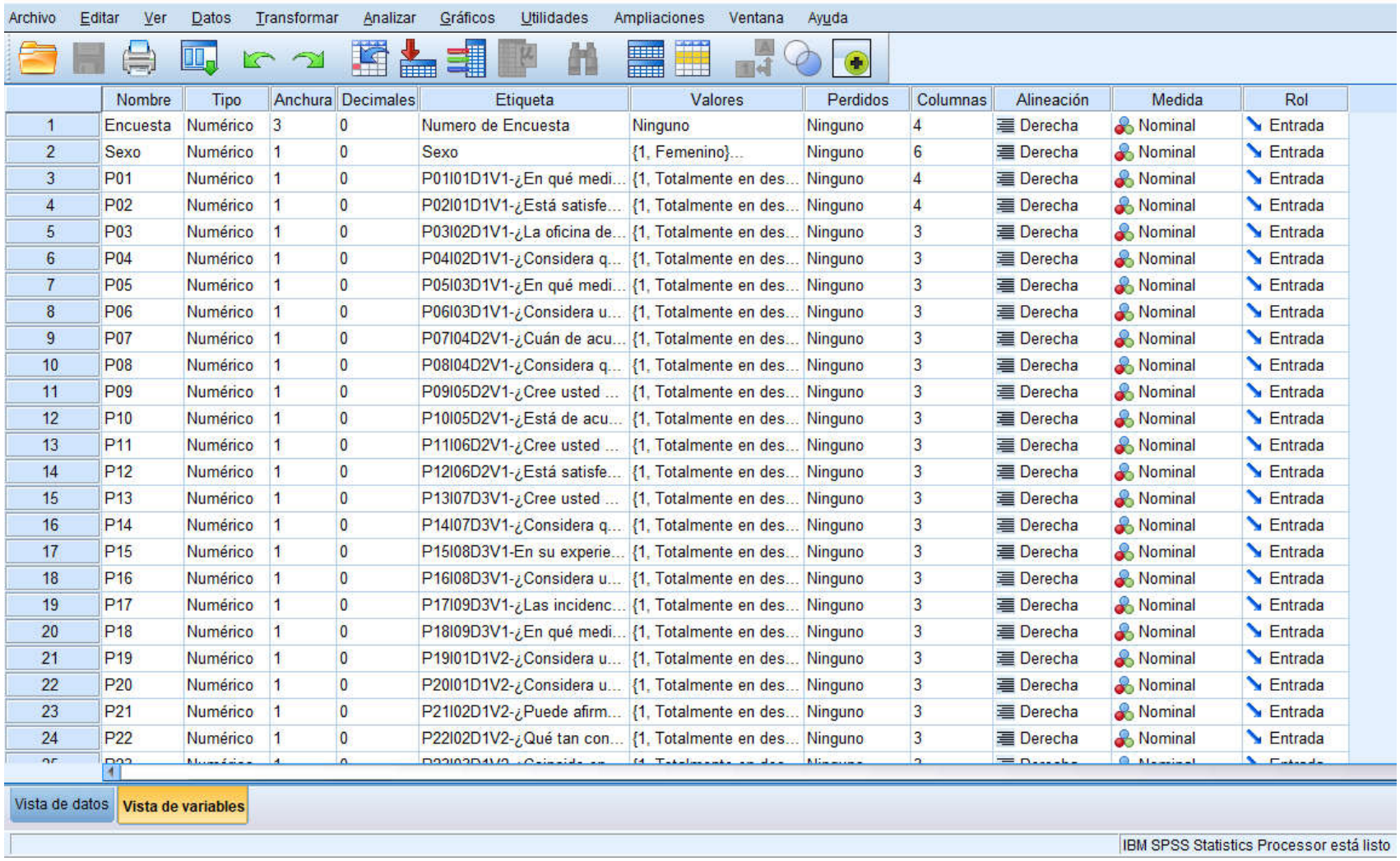
Encuesta	Sexo	V1																		V2																	
		D1						D2						D3						D1						D2						D3					
		I1		I2		I3		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	2	4	3	4	5	4	3	3	3	2	5	5	4	4	3	4	3	4	4	5	3	4	4	5	4	3	4	5	3	4	2	4	4	5	3	5	3
2	2	2	2	3	5	3	3	2	5	3	3	4	4	3	4	1	1	3	3	3	3	2	3	3	3	2	3	3	3	3	4	2	2	2	2	3	2
3	2	4	4	4	1	1	3	3	1	3	5	3	3	2	1	3	5	4	3	4	4	2	5	4	4	3	4	4	1	5	1	2	4	4	4	4	2
4	1	3	3	2	2	2	3	2	1	2	3	3	3	2	3	4	3	3	3	3	3	1	3	2	2	2	3	3	3	3	3	2	3	3	3	3	3
5	2	4	4	4	1	2	1	4	2	3	5	3	4	2	1	5	5	5	4	4	3	3	3	4	4	5	4	4	5	5	4	4	4	4	4	4	5
6	2	4	4	4	2	2	1	4	3	4	3	4	3	3	1	5	3	3	3	4	4	2	4	3	4	4	4	4	4	5	4	4	4	4	4	4	2
7	1	2	3	4	3	3	3	2	2	4	3	3	3	3	3	2	5	3	2	4	2	3	3	4	4	2	3	3	2	3	4	3	4	4	2	3	2
8	1	2	3	4	3	3	3	2	2	4	3	3	3	3	3	3	5	2	3	4	2	3	3	4	4	2	3	3	2	3	4	3	4	4	2	3	2
9	2	3	3	2	3	2	2	3	3	3	4	2	5	3	3	2	5	4	3	4	4	4	2	3	3	4	3	4	4	4	3	3	3	3	4	3	4
10	2	3	3	2	3	2	2	3	3	3	4	2	5	3	2	5	4	3	4	4	4	2	3	3	4	4	3	4	4	3	3	3	3	3	4	3	4
11	2	3	3	2	3	2	2	3	3	3	4	2	5	3	2	5	4	3	4	4	4	2	3	3	4	3	4	4	4	3	3	3	3	3	4	3	4
12	2	4	4	4	3	4	4	5	2	4	5	4	5	4	3	4	5	4	4	3	4	3	3	4	5	5	4	4	2	4	4	5	4	4	4	3	5
13	1	4	2	4	3	1	1	3	1	4	5	3	3	1	3	3	4	4	3	3	4	3	4	2	2	4	2	2	4	4	4	2	4	2	2	2	3
14	2	4	4	3	1	1	3	3	3	4	5	4	3	2	3	4	4	3	4	2	3	3	3	4	4	4	4	4	3	4	2	3	3	4	3	3	2
15	1	3	4	3	1	4	3	4	4	5	4	4	5	3	5	5	5	3	4	4	4	1	5	3	5	4	4	4	4	5	5	5	3	4	3	4	4
16	1	5	4	3	3	3	2	3	1	4	4	4	3	1	3	3	5	4	3	4	4	2	4	4	4	5	4	4	3	5	5	4	5	4	4	4	4
17	2	3	4	3	1	2	2	4	1	4	4	4	5	2	2	3	3	4	3	3	4	1	4	4	4	4	4	4	2	3	2	2	4	4	3	3	2
18	2	3	4	3	1	2	2	4	1	4	4	4	5	2	2	3	3	4	3	3	4	1	4	4	4	4	4	4	2	3	2	2	4	4	3	3	2
19	2	2	2	2	3	2	1	3	1	4	4	4	4	1	3	4	4	2	2	2	5	2	2	4	3	2	3	3	3	2	2	3	3	4	2	2	2
20	1	4	4	3	1	2	1	4	1	4	4	4	5	3	2	3	5	3	2	4	4	2	4	3	4	3	1	3	3	4	3	1	4	4	4	1	3

21	2	3	3	2	3	2	2	3	3	3	4	2	5	3	2	5	4	3	4	4	4	2	3	3	4	3	4	4	4	3	3	3	3	3	4	3	4
22	2	4	4	3	1	3	3	3	1	3	3	2	5	2	2	4	5	4	3	4	4	1	4	4	4	4	3	3	1	4	1	2	4	4	4	4	2
23	2	3	4	3	1	2	2	4	1	4	4	4	5	2	2	3	3	4	3	3	4	1	4	4	4	4	4	4	2	3	2	2	4	4	3	3	2
24	1	4	4	3	1	3	2	3	3	3	5	3	5	2	1	5	5	4	4	4	4	2	4	4	4	4	4	4	3	3	3	3	4	4	4	3	4
25	2	4	4	4	3	4	4	5	2	4	5	4	5	4	3	4	5	4	4	3	4	3	3	4	5	5	4	4	2	4	4	5	4	4	4	3	4
26	1	5	4	4	2	1	3	3	3	3	3	3	4	3	2	4	4	3	4	3	5	1	4	4	4	3	4	4	4	4	5	5	5	4	4	4	3
27	1	4	4	4	2	2	1	4	2	4	3	3	5	3	2	3	4	4	3	4	4	3	4	4	4	4	4	4	4	5	5	4	5	5	4	4	4
28	1	4	4	4	2	2	1	4	3	4	3	4	3	3	1	5	3	3	3	4	4	2	4	3	4	4	4	4	4	5	4	4	4	4	4	4	2
29	2	4	4	3	2	3	2	4	1	4	3	4	5	2	2	3	3	3	3	3	3	3	3	3	3	4	3	4	4	3	3	3	3	4	4	3	3	3
30	2	4	4	3	1	1	3	3	3	4	5	4	3	2	3	4	4	3	4	2	3	3	3	4	4	4	4	4	3	4	2	3	3	4	3	3	2
31	2	3	3	2	2	2	3	2	1	2	3	3	3	2	3	4	3	3	3	3	3	1	3	2	2	2	3	3	3	3	3	2	3	3	3	3	3
32	2	3	4	3	1	4	3	4	4	5	4	4	5	3	5	5	5	3	4	4	4	1	5	3	5	4	4	4	4	5	5	5	3	4	3	4	4
33	2	3	4	3	1	2	1	4	1	4	4	4	5	3	3	3	4	4	4	3	4	1	4	3	4	4	3	4	3	4	4	3	4	4	4	4	4
34	2	4	4	3	3	2	3	4	2	4	3	4	4	3	3	3	4	3	2	3	3	3	4	4	4	4	3	3	2	4	2	3	4	4	4	3	3
35	2	2	3	3	3	1	2	2	2	4	4	3	3	1	1	3	5	2	4	4	4	2	4	3	3	2	3	4	3	2	3	2	4	4	4	4	2
36	2	3	2	4	4	3	1	3	2	4	5	2	4	2	1	5	4	2	4	4	2	1	4	2	4	3	4	4	2	2	2	2	4	2	4	2	2
37	2	4	5	5	4	5	5	5	3	2	5	4	3	5	5	5	5	4	5	2	3	3	3	3	3	4	3	3	5	5	5	5	4	5	5	4	4
38	2	3	4	2	2	1	1	4	3	4	3	3	3	2	1	5	4	4	4	4	4	2	4	4	4	4	4	4	2	4	2	4	4	4	4	4	4
39	2	1	2	3	1	2	1	2	2	2	4	4	5	2	3	5	3	4	1	3	2	3	4	3	3	3	4	3	4	5	1	1	1	2	2	1	1
40	2	2	3	4	3	1	3	3	1	3	5	3	4	1	3	4	3	4	4	3	2	2	2	3	3	4	4	4	3	4	2	3	3	2	2	2	2
41	2	4	3	4	4	2	3	3	1	4	3	4	4	2	2	4	4	2	2	4	3	1	2	4	2	4	4	3	4	4	2	3	2	2	4	2	2
42	2	4	4	3	3	3	1	3	1	3	5	3	3	1	1	3	3	4	4	3	3	1	4	3	4	3	4	4	4	3	3	3	4	3	3	3	4
43	2	4	4	4	1	1	3	3	1	3	5	3	3	2	1	3	5	4	3	4	4	2	5	4	4	3	4	4	1	5	1	2	4	4	4	4	2
44	2	2	3	4	3	3	3	2	2	4	3	3	3	3	3	3	5	2	3	4	2	3	3	4	4	2	3	3	2	3	4	3	4	4	2	3	2
45	2	4	2	2	5	1	3	3	2	3	5	3	3	1	1	4	5	4	4	3	4	2	4	4	2	2	4	2	2	2	4	2	4	2	3	4	4
46	2	4	3	5	2	3	3	4	3	4	5	4	5	3	5	5	5	4	3	4	4	4	3	4	4	4	3	3	4	4	4	3	5	5	4	4	4
47	2	2	2	4	2	3	1	3	2	3	3	2	3	2	2	5	3	3	2	3	4	1	3	2	3	3	2	2	2	3	4	3	4	4	3	2	3
48	2	3	2	2	3	1	1	2	1	2	5	4	4	1	3	3	3	4	4	3	4	1	3	4	4	2	2	4	4	3	2	3	4	4	5	4	3

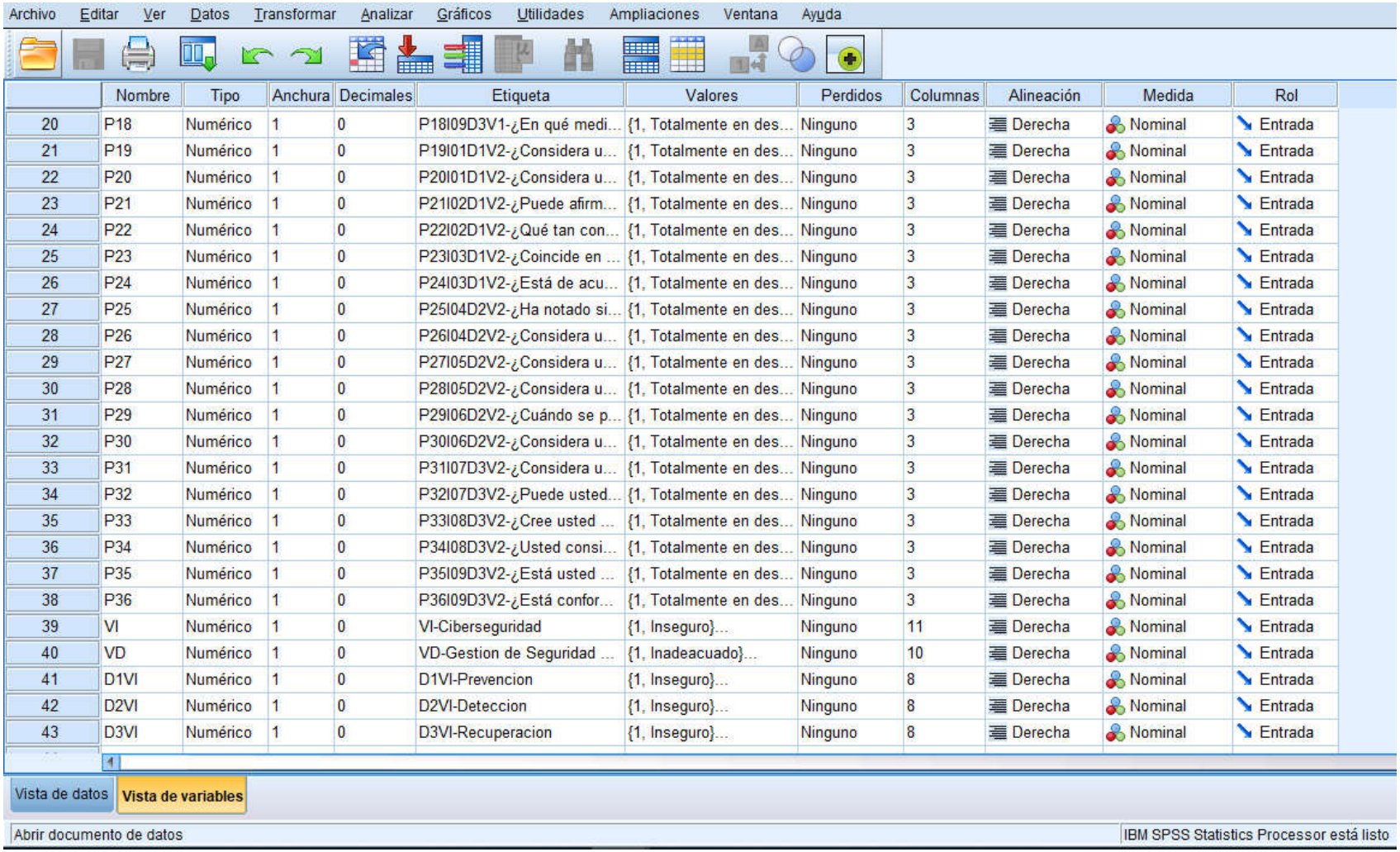
49	2	2	2	2	3	1	1	3	1	2	5	3	3	3	2	5	5	4	4	4	3	2	4	4	4	3	4	5	3	2	4	2	3	3	4	2	4
50	2	4	4	4	1	2	1	4	2	3	5	3	4	2	1	5	5	5	4	4	3	3	3	4	4	5	4	4	5	5	4	4	4	4	4	4	5
51	2	2	2	2	1	2	3	3	1	2	5	2	4	1	3	4	5	3	4	4	4	2	4	3	2	2	3	2	3	4	3	3	3	2	4	4	3
52	2	4	3	2	3	3	2	3	1	4	4	2	5	3	2	3	4	2	2	2	4	2	3	4	2	3	3	2	3	1	2	4	4	3	4	4	2
53	2	4	4	1	1	2	1	3	1	3	3	3	2	1	1	3	3	3	2	3	3	1	3	1	1	3	2	3	1	3	1	2	3	2	3	2	3
54	2	5	4	4	2	1	3	3	3	3	3	3	4	3	2	4	4	3	4	3	5	1	4	4	4	3	4	4	4	4	5	5	5	4	4	4	3
55	2	5	4	3	3	3	2	3	1	4	4	4	3	1	3	3	5	4	3	4	4	2	4	4	4	5	4	4	3	5	5	4	5	4	4	4	4
56	2	3	4	2	2	1	3	2	1	2	4	3	3	3	2	5	5	2	4	3	2	1	4	4	2	2	4	2	4	2	3	2	3	4	3	3	4
57	1	3	4	4	1	1	3	4	1	4	3	3	3	1	3	3	4	4	4	3	3	3	4	2	4	4	4	2	3	3	2	3	3	4	4	4	3
58	2	3	3	3	4	2	1	2	1	3	5	2	3	3	1	4	4	3	3	3	2	1	2	4	2	4	3	4	3	3	3	3	3	3	4	3	4
59	2	4	3	2	2	2	2	2	3	4	3	4	3	3	3	4	3	3	4	2	4	1	3	3	4	2	4	2	2	3	3	4	3	4	3	2	4
60	2	3	2	4	2	3	2	3	2	2	4	3	4	1	1	3	5	2	3	2	3	1	2	4	2	3	4	2	4	2	2	4	4	2	2	2	4
61	2	2	2	2	2	1	1	2	1	2	4	2	3	1	1	5	5	2	4	2	2	1	2	2	4	4	2	2	3	1	2	1	3	3	3	3	2
62	2	4	4	4	2	1	1	2	3	4	3	2	4	2	3	5	3	2	2	3	3	3	3	4	3	3	3	3	3	3	2	3	3	4	4	4	4
63	2	4	4	3	1	3	2	3	3	3	5	3	5	2	1	5	5	4	4	4	4	2	4	4	4	4	4	4	3	3	3	3	4	4	4	3	4
64	2	4	3	2	3	3	2	2	1	4	3	2	5	3	3	3	5	3	3	2	4	3	4	3	4	3	2	4	3	3	3	2	4	3	2	2	3
65	2	3	4	4	1	1	3	4	1	4	3	3	3	1	3	3	4	4	4	3	3	3	4	2	4	4	4	2	3	3	2	3	3	4	4	4	3
66	2	4	4	3	1	2	1	4	1	4	4	4	5	3	2	3	5	3	2	4	4	2	4	3	4	3	1	3	3	4	3	1	4	4	4	1	3
67	2	4	4	3	3	3	1	3	1	3	5	3	3	1	1	3	3	4	4	3	3	1	4	3	4	3	4	4	4	3	3	3	4	3	3	3	4
68	2	3	4	2	2	2	1	4	2	4	5	3	4	1	1	4	5	2	2	3	3	2	4	3	4	4	3	3	2	3	2	2	3	4	2	3	4
69	2	1	2	3	1	2	1	2	2	2	4	4	5	2	3	5	3	4	1	3	2	3	4	3	3	3	4	3	4	5	1	1	1	2	2	1	1
70	2	4	4	4	2	2	1	4	2	4	3	3	5	3	2	3	4	4	3	4	4	3	4	4	4	4	4	4	4	5	5	4	5	5	4	4	4
71	2	3	4	3	1	2	1	4	1	4	4	4	5	3	3	3	4	4	4	3	4	1	4	3	4	4	3	4	3	4	4	3	4	4	4	4	4
72	2	4	4	3	2	3	2	4	1	4	3	4	5	2	2	3	3	3	3	3	3	3	3	3	3	4	3	4	4	3	3	3	3	4	4	3	3	3
73	2	4	4	3	2	3	2	4	1	4	3	4	5	2	2	3	3	3	3	3	3	3	3	3	3	4	3	4	4	3	3	3	3	4	4	3	3	3
74	2	4	5	5	4	5	5	5	3	2	5	4	3	5	5	5	5	4	5	2	3	3	3	3	3	4	3	3	5	5	5	5	4	5	5	4	4
75	2	3	4	2	2	1	1	4	3	4	3	3	3	2	1	5	4	4	4	4	4	2	4	4	4	4	4	4	2	4	2	4	4	4	4	4	4



	Encuesta	Sexo	P01	P02	P03	P04	P05	P06	P07	P08	P09	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30
1	1	2	4	3	4	5	4	3	3	3	2	5	5	4	4	3	4	3	4	4	5	3	4	4	5	4	3	4	5	3	4	2
2	2	2	2	2	3	5	3	3	2	5	3	3	4	4	3	4	1	1	3	3	3	3	2	3	3	3	2	3	3	3	3	4
3	3	2	4	4	4	1	1	3	3	1	3	5	3	3	2	1	3	5	4	3	4	4	2	5	4	4	3	4	4	1	5	1
4	4	1	3	3	2	2	2	3	2	1	2	3	3	3	2	3	4	3	3	3	3	3	1	3	2	2	2	3	3	3	3	3
5	5	2	4	4	4	1	2	1	4	2	3	5	3	4	2	1	5	5	5	4	4	3	3	3	4	4	5	4	4	5	5	4
6	6	2	4	4	4	2	2	1	4	3	4	3	4	3	3	1	5	3	3	3	4	4	2	4	3	4	4	4	4	4	5	4
7	7	1	2	3	4	3	3	3	2	2	4	3	3	3	3	3	2	5	3	2	4	2	3	3	4	4	2	3	3	2	3	4
8	8	1	2	3	4	3	3	3	2	2	4	3	3	3	3	3	3	5	2	3	4	2	3	3	4	4	2	3	3	2	3	4
9	9	2	3	3	2	3	2	2	3	3	3	4	2	5	3	3	2	5	4	3	4	4	4	2	3	3	4	3	4	4	4	3
10	10	2	3	3	2	3	2	2	3	3	3	4	2	5	3	2	5	4	3	4	4	4	2	3	3	4	4	3	4	4	3	3
11	11	2	3	3	2	3	2	2	3	3	3	4	2	5	3	2	5	4	3	4	4	4	2	3	3	4	3	4	4	4	3	3
12	12	2	4	4	4	3	4	4	5	2	4	5	4	5	4	3	4	5	4	4	3	4	3	3	4	5	5	4	4	2	4	4
13	13	1	4	2	4	3	1	1	3	1	4	5	3	3	1	3	3	4	4	3	3	4	3	4	2	2	4	2	2	4	4	4
14	14	2	4	4	3	1	1	3	3	3	4	5	4	3	2	3	4	4	3	4	2	3	3	3	4	4	4	4	4	3	4	2
15	15	1	3	4	3	1	4	3	4	4	5	4	4	5	3	5	5	5	3	4	4	4	1	5	3	5	4	4	4	4	5	5
16	16	1	5	4	3	3	3	2	3	1	4	4	4	3	1	3	3	5	4	3	4	4	2	4	4	4	5	4	4	3	5	5
17	17	2	3	4	3	1	2	2	4	1	4	4	4	5	2	2	3	3	4	3	3	4	1	4	4	4	4	4	4	2	3	2
18	18	2	3	4	3	1	2	2	4	1	4	4	4	5	2	2	3	3	4	3	3	4	1	4	4	4	4	4	4	2	3	2
19	19	2	2	2	2	3	2	1	3	1	4	4	4	4	1	3	4	4	2	2	2	5	2	2	4	3	2	3	3	3	2	2
20	20	1	4	4	3	1	2	1	4	1	4	4	4	5	3	2	3	5	3	2	4	4	2	4	3	4	3	1	3	3	4	3
21	21	2	3	3	2	3	2	2	3	3	3	4	2	5	3	2	5	4	3	4	4	4	2	3	3	4	3	4	4	4	3	3



	Nombre	Tipo	Anchura	Decimales	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida	Rol
1	Encuesta	Numérico	3	0	Numero de Encuesta	Ninguno	Ninguno	4	Derecha	Nominal	Entrada
2	Sexo	Numérico	1	0	Sexo	{1, Femenino}...	Ninguno	6	Derecha	Nominal	Entrada
3	P01	Numérico	1	0	P01I01D1V1-¿En qué medi...	{1, Totalmente en des...	Ninguno	4	Derecha	Nominal	Entrada
4	P02	Numérico	1	0	P02I01D1V1-¿Está satisfe...	{1, Totalmente en des...	Ninguno	4	Derecha	Nominal	Entrada
5	P03	Numérico	1	0	P03I02D1V1-¿La oficina de...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
6	P04	Numérico	1	0	P04I02D1V1-¿Considera q...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
7	P05	Numérico	1	0	P05I03D1V1-¿En qué medi...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
8	P06	Numérico	1	0	P06I03D1V1-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
9	P07	Numérico	1	0	P07I04D2V1-¿Cuán de acu...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
10	P08	Numérico	1	0	P08I04D2V1-¿Considera q...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
11	P09	Numérico	1	0	P09I05D2V1-¿Cree usted ...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
12	P10	Numérico	1	0	P10I05D2V1-¿Está de acu...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
13	P11	Numérico	1	0	P11I06D2V1-¿Cree usted ...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
14	P12	Numérico	1	0	P12I06D2V1-¿Está satisfe...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
15	P13	Numérico	1	0	P13I07D3V1-¿Cree usted ...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
16	P14	Numérico	1	0	P14I07D3V1-¿Considera q...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
17	P15	Numérico	1	0	P15I08D3V1-En su experie...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
18	P16	Numérico	1	0	P16I08D3V1-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
19	P17	Numérico	1	0	P17I09D3V1-¿Las incidenc...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
20	P18	Numérico	1	0	P18I09D3V1-¿En qué medi...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
21	P19	Numérico	1	0	P19I01D1V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
22	P20	Numérico	1	0	P20I01D1V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
23	P21	Numérico	1	0	P21I02D1V2-¿Puede afirm...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
24	P22	Numérico	1	0	P22I02D1V2-¿Qué tan con...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada



	Nombre	Tipo	Anchura	Decimales	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida	Rol
20	P18	Numérico	1	0	P18I09D3V1-¿En qué medi...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
21	P19	Numérico	1	0	P19I01D1V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
22	P20	Numérico	1	0	P20I01D1V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
23	P21	Numérico	1	0	P21I02D1V2-¿Puede afirm...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
24	P22	Numérico	1	0	P22I02D1V2-¿Qué tan con...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
25	P23	Numérico	1	0	P23I03D1V2-¿Coincide en ...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
26	P24	Numérico	1	0	P24I03D1V2-¿Está de acu...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
27	P25	Numérico	1	0	P25I04D2V2-¿Ha notado si...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
28	P26	Numérico	1	0	P26I04D2V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
29	P27	Numérico	1	0	P27I05D2V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
30	P28	Numérico	1	0	P28I05D2V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
31	P29	Numérico	1	0	P29I06D2V2-¿Cuándo se p...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
32	P30	Numérico	1	0	P30I06D2V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
33	P31	Numérico	1	0	P31I07D3V2-¿Considera u...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
34	P32	Numérico	1	0	P32I07D3V2-¿Puede usted...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
35	P33	Numérico	1	0	P33I08D3V2-¿Cree usted ...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
36	P34	Numérico	1	0	P34I08D3V2-¿Usted consi...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
37	P35	Numérico	1	0	P35I09D3V2-¿Está usted ...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
38	P36	Numérico	1	0	P36I09D3V2-¿Está confor...	{1, Totalmente en des...	Ninguno	3	Derecha	Nominal	Entrada
39	VI	Numérico	1	0	VI-Ciberseguridad	{1, Inseguro}...	Ninguno	11	Derecha	Nominal	Entrada
40	VD	Numérico	1	0	VD-Gestion de Seguridad ...	{1, Inadeacuado}...	Ninguno	10	Derecha	Nominal	Entrada
41	D1VI	Numérico	1	0	D1VI-Prevencion	{1, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
42	D2VI	Numérico	1	0	D2VI-Deteccion	{1, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
43	D3VI	Numérico	1	0	D3VI-Recuperacion	{1, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada

Anexo 8: Matriz de Consistencia

TÍTULO: Ciberseguridad y su incidencia en la Gestión de Seguridad de la Información en una entidad pública, Lima 2023

AUTOR: Wilfredo Elias Rivera Lazaro

PROBLEMA	OBJETIVOS	HIPÓTESIS
Problema principal: ¿De qué manera la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023? Problemas específicos: PE1: ¿De qué manera la prevención de la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023?	Objetivo principal: Determinar la incidencia de la ciberseguridad en la gestión de seguridad de la información en una entidad pública, Lima 2023 Objetivos específicos: OE1: Determinar la incidencia de la prevención de la ciberseguridad en la gestión de seguridad de la información en una entidad pública, Lima 2023	Hipótesis principal: La ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023 Hipótesis específicas: HE1: La prevención de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023

VARIABLES E INDICADORES

Variable Independiente: Ciberseguridad

Dimensiones	Indicadores	Ítems	Niveles
Prevención	Anticipación	1,2	Confiable Adecuado Inseguro
	Confiabilidad	3,4	
	Integridad	5,6	
Detección	Anticipación	7,8	
	Confiabilidad	9,10	
	Mejora	11,12	
Recuperación	Revisión	13,14	
	Disponibilidad	15,16	
	Mejora	17,18	

Variable Dependiente: Gestión de Seguridad de la Información

Dimensiones	Indicadores	Ítems	Niveles
Controles de seguridad	Revisión	19,20	
	Disponibilidad	21,22	

TÍTULO: Ciberseguridad y su incidencia en la Gestión de Seguridad de la Información en una entidad pública, Lima 2023

AUTOR: Wilfredo Elias Rivera Lazaro

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
PE2: ¿De qué manera la detección de la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023?	OE2: Determinar la incidencia de la detección de la ciberseguridad en la gestión de seguridad de la información en una entidad pública, Lima 2023	HE2: La detección de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023		Mejora	23,24	Optimo
			Evaluación de Riesgos	Revisión	25,26	Satisfactorio
				Confiabilidad	27,28	
				Verificación	29,30	Inadecuado
			Gestión de Incidentes de Seguridad	Revisión	31,32	
				Verificación	33,34	
				Mejora	35,36	
PE3: ¿De qué manera la recuperación de la ciberseguridad incide en la gestión de seguridad de la información en una entidad pública, Lima 2023?	OE3: Determinar la incidencia de la recuperación de la ciberseguridad en la gestión de seguridad de la información en una entidad pública, Lima 2023.	HE3: La recuperación de la ciberseguridad incide significativamente en la gestión de seguridad de la información en una entidad pública, Lima 2023				

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Básica **Diseño:** No experimental	**Población:** 75 trabajadores del Departamento de TI **Tamaño de muestra:** 75 encuestas realizadas a los trabajadores de una entidad publica **Muestreo:** Censal, en donde la muestra es toda la población	**Técnicas:** Encuesta **Instrumentos:** Cuestionario	**Descriptiva:** En el análisis descriptivo, se realizó la interpretación de los datos de información recolectada a través de histogramas y tablas de contingencia o tablas cruzadas **Inferencial:** En el análisis inferencial, se realizó el contraste de las hipótesis de las variables, utilizando métodos paramétricos y el coeficiente de análisis de regresión ordinal, que sirvió para determinar el grado correlación existente entre las dos variables de estudio