UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Chuqui Sulca, Josue David (orcid.org/0000-0002-4581-4978)

ASESORES:

Mtra. Alza Salvatierra, Silvia Del Pilar (orcid.org/0000-0002-7075-6167)

Dr. Vargas Huaman, Jhonatan Isaac (orcid.org/0000-0002-1433-7494)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2024

DEDICATORIA

A mi madre Agueda, por ser mi guía, motivación y fortaleza durante todos los años de crecimiento personal y profesional. A mis sobrinos, Amelia y Stephen por ser mi alegría y motivación. A mi enamorada Yasuri, por su comprensión, apoyo durante todos estos años de etapa universitaria y profesional. A mis queridos amigos del Gakko, Jose, Luis Fernando, Luis Carlos, Naomi, Kimberly, Marivict, Sumiko y Yolanda, por su sincera amistad.

AGRADECIMIENTO

Mi más profundo agradecimiento a mi madre por ser la mujer perfecta y luchadora que con coraje supo brindarme la educación necesaria para lograr grandes objetivos.

Al director Hénner Ortiz, subdirectora Maria del Pilar Sánchez, administradora Rosa Higa y todo el equipo institucional por confiar en mí y brindarme su apoyo incondicional durante la investigación y todo el tiempo de labores profesionales.

A los docentes de cada curso en esta maestría por sus conocimientos compartidos y a mi asesora Mtra. Silvia Alza por su apoyo riguroso y profesional en el desarrollo de mi tesis.

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, ALZA SALVATIERRA SILVIA DEL PILAR, 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 titulada: "Ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023", cuyo autor es CHUQUI SULCA JOSUE DAVID, constato que la investigación tiene un índice de similitud de 16.00%, 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 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, 06 de Enero del 2024

Apellidos y Nombres del Asesor:	**Firma**
ALZA SALVATIERRA SILVIA DEL PILAR **DNI:** 18110381 **ORCID:** 0000-0002-7075-6167	Firmado electrónicamente por: SALZAS el 14-01-2024 11:51:40

Código documento Trilce: TRI - 0722954

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, CHUQUI SULCA JOSUE DAVID 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 en la gestión de riesgos en una institución educativa, Callao 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
CHUQUI SULCA JOSUE DAVID **DNI:** 74720257 **ORCID:** 0000-0002-4581-4978	Firmado electrónicamente por: JCHUQUICH2698 el 09-01-2024 22:06:33

Código documento Trilce: INV - 1439166

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación titulada: Ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023. Tiene como objetivo determinar la influencia de la ciberseguridad en la gestión de riesgos, de esta manera se optó por un enfoque explicativo, utilizando un diseño de investigación no experimental correlacional causal. La población de estudio comprendió 30 trabajadores, y la técnica de recolección de datos utilizada fue la encuesta. Los resultados obtenidos a través de un análisis de regresión logística ordinal respaldan la hipótesis general, ya que el valor de significancia de 0.002 es inferior a 0.05, indicando una significativa adecuación de los resultados a las variables introducidas. Se concluye que la ciberseguridad ejerce una influencia significativa, atribuyendo el 37.7% de la variabilidad en la gestión de riesgos en la Institución Educativa en Callao en el año 2023.

Palabras clave: Ciberseguridad, conciencia digital, seguridad de la red escolar.

ABSTRACT

The present research titled: Cybersecurity in risk management in an educational institution, Callao 2023. Its objective is to determine the influence of cybersecurity in risk management, in this way an explanatory approach was chosen, using a research design not causal correlational experimental. The study population included 30 workers, and the data collection technique used was the survey. The results obtained through an ordinal logistic regression analysis support the general hypothesis, since the significance value of 0.002 is less than 0.05, indicating a significant adequacy of the results to the variables introduced. It is concluded that cybersecurity exerts a significant influence, attributing 37.7% of the variability in risk management in the Educational Institution in Callao in the year 2023.

Keywords: Cybersecurity, digital awareness, school network security.

I. INTRODUCCIÓN

En la última década, el entorno digital ha emergido como un terreno propicio para la participación en acciones ilegales por parte de personas con intenciones perjudiciales. Los estudios realizados por especialistas en criminología hasta el momento indican que, mientras que los delitos tradicionales están disminuyendo, el cibercrimen está en aumento. El ciberespacio ofrece ventajas como el anonimato, la rapidez y la falta de fronteras, que son aprovechadas tanto por criminales cibernéticos como por organizaciones delictivas, pero que al mismo tiempo representan un desafío para la seguridad cibernética. Además, la aparición de amenazas digitales ha cuestionado la efectividad de los métodos tradicionales del Estado Español para combatir el crimen y proteger la seguridad nacional, ya que estos métodos no están adaptados a las demandas del ciberespacio (Del-Real, 2022).

Según la Organización de los Estados Americanos (OEA, 2020), las estrategias de ciberseguridad juegan un papel fundamental en la salvaguarda de los derechos de los individuos hacia el entorno digital, incluyendo aspectos como la privacidad y la propiedad. Además, contribuyen significativamente a promover la confianza de la población en las. tecnologías digitales, posibilitando que las personas se sientan a gusto. al utilizar estas tecnologías. Es importante destacar que los delitos en línea representan alrededor de la mitad de todos los crímenes contra la propiedad a nivel mundial. A nivel global, los impactos económicos de los ciberataques podrían superar el 1% del Producto Interno Bruto (PIB) en algunas naciones. En el caso de ataques dirigidos a la infraestructura crítica, esta cifra podría elevarse incluso hasta el 6% del PIB.

La relevancia de implementar medidas para asegurar la seguridad cibernética en las empresas fue resaltada por los asistentes al Multi Cibersecurity Summit 2022 organizado por Movistar Empresas Hispam el 15 de junio pasado. Además, se prevé que, en 2023, un 55% de las empresas asignarán la mitad de sus recursos de seguridad a sistemas y plataformas tecnológicas especializadas en ciberseguridad, diseñadas para un despliegue ágil y capacidades de seguridad integradas.

La gestión de riesgos emerge como el guardián estratégico en el complejo escenario empresarial, donde la incertidumbre es moneda corriente. Este proceso

no solo implica el uso de tecnologías avanzadas y enfoques integrados, sino que se erige como el faro que guía a las empresas a través de la tormenta de desafíos económicos y geopolíticos. La gestión de riesgos no es solo una herramienta vital en el ámbito empresarial; su importancia se extiende también a las instituciones educativas, donde se erige como el guardián del bienestar académico y financiero. En un entorno educativo caracterizado por cambios rápidos y desafíos inesperados, la capacidad de anticipar y gestionar riesgos se vuelve esencial con el fin de preservar la estabilidad y fomentar el crecimiento. (Kulinich et al., 2023).

La incertidumbre incrementa los riesgos que una organización enfrenta, y es en este contexto que las empresas recurren al proceso de cobertura para reducir el impacto de situaciones inciertas. Este método resulta altamente beneficioso al asignar recursos de manera óptima. Las políticas empresariales son diseñadas con la intención de prever posibles riesgos futuros. La evaluación de riesgos está estrechamente vinculada a las posibilidades que surgen para la empresa, y la situación financiera juega un papel determinante en la evaluación cualitativa del riesgo. Una estructura eficaz de gestión de riesgos se convierte en un activo valioso para las empresas. Cabe destacar que la evaluación de riesgos no se limita únicamente al ámbito empresarial, sino que se extiende a todas las industrias (Shakatreh et al., 2023).

Según El Comercio (2023), el Perú experimentó alrededor de 5,2 mil millones de intentos de intrusiones, lo que implicó un incremento del 10% en relación con el mismo periodo de 2021, cuando se registraron alrededor de 4,7 mil millones de intentos. De acuerdo con Penna (2023), en México fue el país más afectado con un total de aproximadamente 85 mil millones de intentos de intrusión, seguido de cerca por Brasil con unos 31,5 mil millones y Colombia con unos 6,3 mil millones. Aparte de las cifras notablemente elevadas, la información indica un incremento en la aplicación de métodos más avanzados y especializados, como el ransomware. En los primeros seis meses de 2022, se identificaron aproximadamente 384 mil intentos de propagación de ransomware a nivel mundial.

En la actualidad, los incidentes y amenazas a la seguridad de la información son mayoritariamente desencadenados por la delincuencia organizada o individuos que obtienen ganancias ilegales al vender la información recopilada a estas redes organizadas. Los ciberdelincuentes aprovechan las vulnerabilidades o fallos

presentes en diversos programas informáticos o aplicaciones utilizados en entornos empresariales o privados. Estas vulnerabilidades son identificadas a través de un exhaustivo trabajo por parte de los ciberdelincuentes o adquiridas en el mercado negro. Es conocido que existe un mercado significativo de datos personales, identidades y vulnerabilidades de programas, al igual que existen profesionales y empresas de hackers "éticos" que se dedican a buscar posibles debilidades en programas que están a la venta o están por lanzarse al mercado. Su objetivo es corregir dichas vulnerabilidades una vez identificadas, un proceso conocido como "parchearlas" (Ballestero, 2022).

A nivel local, la ciberseguridad ha planteado desafíos significativos para las instituciones educativas en su esfuerzo por proteger la información sensible de posibles ataques cibernéticos. Este aspecto adquiere una relevancia aún mayor dentro del ámbito de la gestión de riesgos en una institución educativa, donde se busca salvaguardar de manera efectiva los activos de información que se gestionan a través de redes externas en el ciberespacio. Actualmente, la entidad opera con un nivel de seguridad básico debido, en gran medida, a la falta de familiaridad con diversas herramientas que podrían potenciar sus medidas de seguridad. Dentro del contexto de la gestión de riesgos, se observa un enfoque similar; siendo una institución educativa, no se le otorga la importancia debida en el entorno actual.

A pesar de esta realidad, no se ha evaluado cómo la mejora en ciberseguridad podría influir en la gestión de riesgos, y viceversa. Por lo tanto, resulta crucial identificar la interrelación entre ambos aspectos. Este conocimiento permitirá asignar, en un futuro cercano, una porción del presupuesto anual para fortalecer la ciberseguridad. Se comprende que esta inversión no solo mejorará la seguridad digital, sino que también impactará positivamente dentro de la gestión de riesgos de la entidad.

Ante lo mencionado se consideró propicio generar el siguiente problema general: ¿Cuál es la influencia de la ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023? De esta forma, se establecieron los problemas específicos: ¿Cuál es la influencia de la confidencialidad en la gestión de riesgos en una institución educativa, Callao 2023? ¿Cuál es la influencia de la integridad en la gestión de riesgos en una institución educativa, Callao 2023? ¿Cuál es la

influencia de la disponibilidad en la gestión de riesgos en una institución educativa, Callao 2023?

La justificación practica que respalda la presente investigación se centra en el ámbito educativo, ya que viene enfrentado un incremento significativo en las amenazas cibernéticas durante los últimos años. Se han registrado ataques digitales cada vez más avanzados dirigidos a las instituciones educativas, lo que ha resaltado la imperante necesidad de abordar de manera efectiva la seguridad cibernética en este sector. La salvaguardia de información confidencial perteneciente a estudiantes y personal, así como la protección de la infraestructura educativa, han adquirido una gran relevancia como blancos prioritarios para individuos malintencionados en el mundo digital. Adicionalmente, es importante destacar que las instituciones educativas gestionan una gran cantidad de datos personales y confidenciales, cuya pérdida o vulnerabilidad podría tener consecuencias graves tanto para las personas afectadas como para la reputación de la institución. En este entorno, la ciberseguridad emerge como un componente esencial con el propósito de garantizar la privacidad y la integridad de dicha información.

De la misma manera, la justificación teórica se fundamenta en los principios y marcos conceptuales de la ciberseguridad, abordando teorías relacionadas mediante la protección de sistemas, la gestión de riesgos y la prevención de ataques cibernéticos. La teoría de la ciberseguridad proporcionará una base sólida para comprender los conceptos clave, como la identificación de vulnerabilidades, la autenticación, la encriptación y la implementación de las prácticas más eficientes en la gestión de riesgos. Además, se explorarán los modelos de amenazas específicos que afectan a las instituciones educativas, considerando las características únicas de este entorno, como la diversidad de usuarios y la complejidad de la infraestructura tecnológica.

Asimismo, la justificación metodológica tiene su base en la necesidad de obtener una comprensión integral y rigurosa de la ciberseguridad en la gestión de riesgos de la institución educativa del Callao en el año 2023. Se utilizarán estadísticas descriptivas y herramientas visuales con el objetivo de exponer de forma clara y concisa la realidad actual de la ciberseguridad en la institución. Este enfoque proporcionará una base sólida para identificar áreas críticas, evaluar la

concienciación en ciberseguridad y comprender la implementación de medidas de protección. Por otro lado, el enfoque inferencial se aplicará para analizar las posibles influencias entre las variables identificadas en la fase descriptiva. Se utilizarán pruebas de hipótesis y análisis de regresión para examinar la influencia de las medidas de seguridad implementadas, la percepción de riesgos por parte de la comunidad educativa y cualquier otra relación significativa.

La presente investigación tiene como objetivo general: Determinar la influencia de la ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023. Además, se establecieron los siguientes objetivos específicos: Determinar la influencia de la confidencialidad en la gestión de riesgos en una institución educativa, Callao 2023. Determinar la influencia de la integridad en la gestión de riesgos en una institución educativa, Callao 2023. Determinar la influencia de la disponibilidad en la gestión de riesgos en una institución educativa, Callao 2023.

La presente investigación tiene como hipótesis general: La ciberseguridad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023. Además, se establecieron las siguientes hipótesis específicas: La confidencialidad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023 La integridad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023. La disponibilidad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023.

II. MARCO TEÓRICO

En los países en desarrollo, el fomento de la cohesión social y cultural desempeña un papel esencial en el fortalecimiento de la seguridad cibernética y la promoción de la concienciación sobre los riesgos cibernéticos. Esta estrategia podría resultar eficaz y económicamente viable para mejorar la resiliencia de la nación en el ámbito digital (Creese et al., 2021). No obstante, esta medida por sí sola no satisface las necesidades de desarrollo de capacidades cibernéticas a nivel nacional, las cuales demandan una visión estratégica cohesionada (Solar, 2020).

Se hace referencia aquí a la noción de seguridad cibernética que implica una visión integral y coherente garantizar la seguridad de las redes, sistemas, servicios e infraestructuras en la sociedad Esta concepción de gestión incluye las organizaciones, políticas, proyectos y otros métodos, tanto establecidos como no oficiales, que forman parte de un sistema de habilidades y deberes compartidos en el ámbito de la seguridad cibernética (Valverde Arcos & Hurel Franco, 2021). Sin embargo, es esencial destacar que la estrategia nacional de ciberseguridad juega un papel crucial en la consolidación de las capacidades cibernéticas de un país. Un componente integral de esta estrategia es la implementación de la gobernanza de ciberseguridad, que se introdujo por primera vez en la Estrategia E-Ciber de Brasil en el año 2020.

La ciberseguridad ha adquirido una posición fundamental en el desarrollo digital europeo. A medida que las tecnologías de la información y la comunicación se han extendido y la Unión Europea ha experimentado un crecimiento tanto en profundidad como en amplitud, las políticas de seguridad de datos inicialmente sectoriales y limitadas han evolucionado hacia un marco integral de seguridad cibernética. Este enfoque aborda no solo la resiliencia de la infraestructura y la soberanía tecnológica, sino también la lucha contra la ciberdelincuencia, el fortalecimiento de las capacidades de defensa cibernética y la promoción de un comportamiento estatal responsable en el ciberespacio (Kasper et al., 2021).

Las inquietudes relacionadas con las estrategias comerciales no se encuentran novedosas. No obstante, debido a la naturaleza electrónica de las operaciones comerciales, este tema ha tomado una relevancia nueva y apremiante. El entorno digital se configura como un entorno de flujos, una esfera virtual que experimenta un constante crecimiento debido a las interacciones propiciadas por

las tecnologías de la información y la comunicación. En respuesta a esta dinámica, numerosos gobiernos han iniciado el desarrollo de estrategias de ciberseguridad, al mismo tiempo que buscan fomentar los beneficios de un mundo hiperconectado y habilitado digitalmente (Becerril, 2019).

Un análisis de los datos disponibles muestra una imagen clara de la situación. El Instituto Nacional de Ciberseguridad (INCIBE, 2021) que su centro de respuesta atendió más de 109.216 incidentes, de los cuales 90.168 tuvieron un impacto en ciudadanos y empresas, y 18.287 afectaron a la red académica y de investigación española (RedIRIS). Es importante destacar que se registraron 44.777 casos en los que los ciudadanos tenían sus computadoras infectadas por redes zombi o botnets controladas de forma remota, aunque es probable que existan muchos más casos de los cuales los usuarios no están al tanto. Según los datos de la consultora Deloitte, el número promedio de incidentes cibernéticos aumentó significativamente entre 2020 y 2021, con un incremento del 26 %. De acuerdo con su encuesta, un 69 % de las empresas reportó haber experimentado entre uno y dos incidentes de ciberseguridad de gravedad durante el último año.

Según los datos obtenidos de la encuesta realizada entre directivos empresariales de veinte naciones, que se presenta en el informe Global Cibersecurity Outlook 2020 elaborado por el Foro Económico Mundial, un 87 % de los ejecutivos está enfocado en fortalecer su capacidad de ciberresiliencia, mejorando sus políticas, procedimientos y estándares en lo que respecta a colaboraciones con terceros. La ciberresiliencia se describe como la habilidad de una organización para prever, resistir, recuperarse y adaptarse a tensiones, fallos, incidentes y amenazas relacionadas con sus recursos cibernéticos dentro de su entorno, con el propósito de cumplir con su misión, preservar su cultura y mantener sus operaciones (World Economic Forum, 2022).

Al igual que en otras ramas de la industria financiera, los servicios de gestión de riesgos y seguros se ven fuertemente influenciados por los cambios en las regulaciones. Las limitaciones al acceso a las redes internacionales de intercambio de riesgos provocan modificaciones significativas tanto en el rendimiento actuarial y financiero de la industria de seguros como en las estrategias de gestión adoptadas por las empresas. La creación de estrategias de gestión de riesgos adaptadas al entorno educativo es imperativa. Así como las aseguradoras

españolas buscaron soluciones internas mediante la creación de reaseguradoras subsidiarias, las instituciones educativas deben explorar enfoques internos y flexibles para abordar las incertidumbres financieras. La colaboración dentro de grupos corporativos, análoga a las relaciones entre aseguradoras y reaseguradoras dependientes, podría ser una estrategia valiosa para compartir riesgos y mitigar pérdidas inesperadas (Gutiérrez González & Pons Pons, 2022).

Para abordar estas dificultades, ciertos especialistas proponen que una estrategia para contrarrestar estos efectos adversos involucra la educación y especialización de profesionales en este campo, los cuales podrían ser empleados tanto por compañías como por entidades gubernamentales para hacer frente a las amenazas resultantes de la actividad delictiva organizada en el ámbito de la seguridad cibernética. Además, diversas compañías elaboran informes anuales para identificar riesgos y, al mismo tiempo, contribuir a la mejora de las herramientas destinadas a mitigar las vulnerabilidades.

Vale la pena destacar la cuestión de los ataques cibernéticos, los cuales se caracterizan como un esfuerzo malintencionado y premeditado llevado a cabo por un individuo o una entidad con el propósito de penetrar en el sistema de información de otra persona u entidad. Generalmente, el agresor persigue algún tipo de ganancia al interferir con la red de la persona afectada (Cisco, 2022). Es importante resaltar que, según la empresa Cisco, los delitos cibernéticos aumentan de manera constante año tras año, a medida que individuos buscan sacar provecho de sistemas empresariales que presentan vulnerabilidades. En muchas ocasiones, los agresores buscan rescates económicos, y se ha observado que el 53 % de los ciberataques resulta en daños que ascienden a USD 500,000 o más (Cisco, 2022).

En los últimos meses, se ha observado un incremento en la frecuencia de los ataques cibernéticos en diversas partes del mundo, coincidiendo con el incremento en el uso de computadoras debido a los efectos de la pandemia de COVID-19. Según datos de la empresa Kaspersky, entre enero y agosto de 2020, se evidenció un incremento del 24% en la cantidad de incidentes de esta naturaleza en América Latina. Esto implica que en toda el área se están realizando numerosos ataques cada segundo, con cifras notables, como Brasil a la cabeza con más de 1,390 intentos de infección por minuto, seguido por México (299 por minuto), Perú

(96 por minuto), Ecuador (89 por minuto) y Colombia (87 por minuto) (Kaspersky, 2021).

De particular interés son las amenazas de ciberataques que, en ciertos casos, debido a la falta de medidas preventivas y de control, han llevado a empresas a involucrarse en prácticas fraudulentas, sobornos, corrupción y actividades delictivas para ingresar a nuevos mercados. Estas empresas cuentan con capacidades técnicas y recursos que les permiten obtener beneficios de índole política o económica en el contexto estatal. Esto ha dado lugar al surgimiento de la auditoría forense como una herramienta de prevención de los riesgos en ciberseguridad. Al combinar el talento humano con un alto nivel de habilidades, la auditoría forense ayuda a proteger a las organizaciones modernas contra ataques informáticos y comportamientos inapropiados que podrían tener graves consecuencias para la continuidad del negocio. Esto, a su vez, podría afectar la posición competitiva de la empresa en un entorno económico y tecnológico en constante evolución (Fernández, 2020).

Así mismo, a ciberseguridad en Europa se enfrenta a una amenaza de múltiples facetas que proviene de diversas fuentes. Esto incluye bandas criminales, grupos presuntamente vinculados a actores geopolíticos adversarios y también unidades de ciberseguridad regulares desplegadas como parte de las fuerzas militares que otros estados podrían utilizar en caso de conflicto, como se ha observado en el conflicto actual entre Rusia y Ucrania. Además, la naturaleza de estas amenazas cibernéticas es diversa, abarcando desde operaciones destinadas a debilitar o interrumpir infraestructuras hasta actividades de ciberespionaje o programas de extorsión que van desde la suplantación de identidad hasta la obtención de información comprometedora con fines de chantaje (Munkøe et al., 2019).

Esto abarca acciones como la apropiación no autorizada de propiedad intelectual, divulgación de información confidencial, estrategias de presión y amenazas dirigidas a clientes, así como la táctica de crear conflictos con la intención de dañar a competidores. Durante la administración de Trump en Estados Unidos, se emitió una orden ejecutiva que tenía como objetivo limitar las transacciones relacionadas con productos y servicios de tecnologías de la información y la comunicación (TIC) cuando estaban vinculados a un actor

extranjero adverso. Esta medida se fundamentaba en acusaciones de que empresas chinas, como Huawei, empleaban sus productos para llevar a cabo actividades de espionaje industrial.

Esta problemática también guarda relación con actividades ilegales que, en ciertos casos, pueden tener un respaldo por parte del gobierno. Un ejemplo de esto es que Corea del Norte obtiene una parte de sus ingresos a través de actividades de ciberdelincuencia (Reuters, 2019).

Según la norma ISO 31000, el riesgo se define como la consecuencia de la incertidumbre en relación con los objetivos. Un resultado se considera como una desviación de lo que se anticipaba, y los objetivos pueden abarcar una variedad de áreas, como las financieras, la salud y seguridad, el medio ambiente, entre otros, y aplicarse en diversos niveles. Esta norma proporciona orientación sobre cómo establecer e implementar el proceso de gestión de riesgos, lo cual implica definir el contexto, así como identificar, analizar, evaluar, tratar, comunicar y supervisar los riesgos (Pulido et al., 2020).

Según Dotres y Sanchez (2020), con el propósito de minimizar las ramificaciones en las etapas de planificación y ejecución, los hallazgos de esta interpretación pueden resultar en conclusiones y recomendaciones dirigidas a aquellos encargados de tomar decisiones. Para disminuir los impactos adversos, se requiere evaluar las habilidades de los líderes y personal involucrado, incluyendo su capacidad de liderazgo, su adaptabilidad al cambio y su experiencia comprobada en la toma de decisiones. En lo que respecta a la disminución de riesgos, se pueden contemplar las siguientes categorías: eliminarlos, disminuir tanto su frecuencia como sus consecuencias, transferir la responsabilidad del riesgo o aceptarlo.

Con frecuencia, los directivos seleccionan las estrategias apropiadas para reducir los riesgos, considerando diversos elementos, como la naturaleza y el origen de la potencial amenaza, así como los recursos disponibles. Se han llevado a cabo investigaciones y se han diseñado enfoques cualitativos para explorar las formas eficaces de reducir los riesgos (Díaz et al., 2018).

En el ámbito nacional, en el año 2017, Perú ostentó el primer puesto en América Latina en términos de vulnerabilidad a ataques cibernéticos, registrando un índice del 25.10%. Sin embargo, en 2018, descendió al segundo lugar con una vulnerabilidad del 14%. Mientras tanto, en el 2019, Perú se posicionó en el lugar 40

a nivel global como uno de los países que sufrieron ataques cibernéticos. Las principales causas de estos ataques fueron la distribución de malware por correo basura, que representó el 58.65% de los incidentes, seguido de amenazas web con un 43.60% y correos infectados con un 22.32%. Se observó que las empresas y entidades peruanas son generalmente blanco de infecciones por malware, como el Análisis de Atributos del Remitente, el Script Minergen de Troyano y el Fraude HTML genérico de Troyano (Poma & Vargas, 2019).

Además de Chile, Perú también ha sufrido numerosos ciberataques, lo que es motivo de preocupación tanto para los ciudadanos como para las empresas peruanas. Esta situación resalta la importancia de que los líderes peruanos prioricen la implementación de sistemas de seguridad sólidos y robustos para garantizar la protección de la información (Quiroga, 2021).

Es fundamental resaltar que a medida que el ámbito digital continúe expandiéndose en el ámbito comercial, los criminales cibernéticos mostrarán un mayor interés en desarrollar nuevas tácticas para perpetrar sus actividades fraudulentas. Estos criminales estarán vigilantes de situaciones que les brinden oportunidades para identificar posibles víctimas, tal como se observó al comienzo de la pandemia de COVID-19, momento en el que la mayoría de las denuncias presentadas por ciudadanos peruanos estaban relacionadas con delitos informáticos. En estas modalidades delictivas, los delincuentes se hacían pasar por instituciones financieras a través de diversos canales, como llamadas telefónicas, mensajes de WhatsApp y correos electrónicos.

La estrategia propuesta para fortalecer la ciberseguridad en el Estado peruano debe caracterizarse por basarse en un enfoque participativo y colaborativo. Esto implica fomentar y unir los esfuerzos de diversos actores, como la población, instituciones gubernamentales y privadas, así como fuerzas militares en servicio activo e incluso la comunidad internacional. El objetivo principal es desarrollar un programa efectivo para enfrentar cualquier tipo de amenaza y reducir la brecha en la capacidad de respuesta (Sheth et al., 2021). Para fortalecer la capacidad cibernética del país, es esencial establecer una clara separación entre las redes internas del Estado y la Internet pública. Además, se requiere la creación de una entidad dedicada a supervisar y administrar la ciberseguridad a nivel nacional, respaldada por un sistema tecnológico de alto rendimiento capaz de identificar y

contrarrestar ciberataques de manera inmediata y en tiempo real (Ormachea, 2020).

Perú ha enfrentado desafíos significativos en el ámbito de la ciberseguridad, y estos problemas se han agravado debido a la falta de atención y la inversión adecuada en este sector. A lo largo del año 2021, el país experimentó una oleada de ciberataques que no solo representaron una amenaza para la seguridad de las empresas y los ciudadanos, sino que también pusieron a Perú en la primera posición en América Latina en cuanto a ataques cibernéticos. Esta situación pone de manifiesto una debilidad preocupante en la infraestructura de seguridad cibernética del país. La falta de inversión en tecnologías y recursos de ciberseguridad, así como la subestimación de la importancia de este campo, ha dejado al país vulnerable a una serie de amenazas digitales. Estos ataques no solo tienen el potencial de causar daños financieros y pérdida de datos, sino que también pueden afectar la confianza en la tecnología digital y socavar la competencia de las empresas peruanas en el mercado global (Quevedo, 2023).

Tener Fuerzas Armadas con una capacidad sólida de defensa cibernética es esencial para enfrentar de manera efectiva las amenazas o ataques que se produzcan a través del ciberespacio y que representen un peligro para la soberanía, los intereses nacionales, los activos críticos del país y los recursos vitales para mantener las capacidades nacionales. Esto se hace aún más crítico al tener en cuenta las vulnerabilidades existentes en el Estado en el ámbito digital (Fuerman, 2023).

En lo que respecta a las teorías relacionadas sobre ciberseguridad, este estudio encuentra apoyo a través de las que se detallan posteriormente. En primer lugar, tenemos a la teoría de la seguridad de redes, donde Vega Briceño (2021) menciona que el correcto diseño de la red representa una de las herramientas fundamentales a nuestra disposición para defendernos contra la variedad de amenazas que podrían surgir en la red. Con una red debidamente estructurada, podemos prevenir por completo algunos ataques, mitigar otros y, en situaciones donde no podamos tomar otras medidas, gestionar las fallas de manera efectiva.

De igual manera, Pawar y Anuradha (2015) mencionan que la correcta subdivisión de redes puede mejorar el rendimiento al limitar la circulación de cierto tráfico únicamente a las áreas de la red que requieren visualizarlo, y puede

contribuir a la identificación de problemas técnicos en la red. Además, la segmentación de la red puede prevenir el acceso no autorizado o ataques a áreas de la red que preferiríamos mantener inaccesibles, además de simplificar significativamente la supervisión del flujo de datos en la red.

De la misma manera, se está considerando la teoría de la criptografía, en la cual Soto y Rodríguez (2019) plantean que la teoría de la criptografía se fundamenta en diversas formas de aritmética, que incluyen números enteros y racionales, números complejos. En el contexto de un texto, su aplicación implica la conversión de las letras que componen el mensaje en una secuencia de valores numéricos, seguida de operaciones matemáticas sobre estos números para alterar su significado y volverlos ininteligibles; al mismo tiempo, se garantiza que el destinatario tenga la capacidad de revertir dicha transformación. El procedimiento de transformar un mensaje para mantenerlo en secreto se denomina cifrado, mientras que la acción contraria, es decir, recuperar el mensaje original, se conoce como descifrado.

Adicional a ello, Córdoba (2023) explica que la teoría de la criptografía se basa en el conjunto de métodos empleados para salvaguardar datos confidenciales de accesos no autorizados constituye un área dentro de la criptología, que es la disciplina dedicada al análisis de técnicas de codificación y escritura secreta. Otra rama relevante es el criptoanálisis, cuya tarea consiste en identificar debilidades en los sistemas de cifrado con el objetivo de acceder a información confidencial sin disponer de las claves de encriptación correspondientes.

Luego tenemos a la teoría de la resiliencia cibernética, de igual manera para Massoni (2022) la teoría de la resiliencia cibernética se basa en la capacidad de una entidad u organización para mantener sus operaciones esenciales en medio de ciberataques. La planificación de la resiliencia cibernética, también conocida como ciber resiliencia, conlleva la formulación de una estrategia destinada a recuperarse de ataques cibernéticos y a salvaguardar a la organización de futuros asaltos de este tipo. Para crear un plan efectivo, el primer paso implica la identificación de las funciones críticas que dependen de tecnologías, seguido por la evaluación de los riesgos y vulnerabilidades asociados a estas funciones frente a posibles ciberataques, y finalmente, el desarrollo de un proceso que permita restaurar dichas funciones en caso de un ataque cibernético.

En el marco de esta investigación, abordaremos la ciberseguridad como variable de estudio. En consecuencia, presentaremos diversas definiciones de ciberseguridad proporcionadas por distintos autores, con el propósito de lograr una comprensión más sólida de este concepto. De acuerdo con Poma y Vargas (2019), la ciberseguridad representa un sistema que en diversas ocasiones ayuda a evitar que las personas sufran el robo de sus datos personales, incluyendo su identidad, y que estos datos no sean empleados de manera indebida. De igual manera, Dalal et al. (2021) nos indica que la ciberseguridad ofrece apoyo, al mismo tiempo que representa una estrategia de seguridad que contribuye a la igualdad en el ámbito internacional, buscando mejorar las prácticas utilizadas a nivel global.

Así mismo, para García y Pesántez (2023) la ciberseguridad se refiere a un proceso que implica la identificación de posibles amenazas y debilidades en una plataforma, la valoración de la eficacia de las medidas de seguridad actualmente en vigor y la recomendación de acciones medidas suplementarias para fortalecer la salvaguarda de la información y los datos confidenciales. Además, tiene como objetivo salvaguardar la información sensible, como los registros de estudiantes y profesores, asegurando la integridad de los cursos y materiales de enseñanza en línea, lo que garantiza un aprendizaje continuo y fiable sin interrupciones. Finalmente, Ignaczak et al. (2022) sostiene que la ciberseguridad como un método para supervisar tanto las amenazas convencionales como las nacientes que surgen en el ciberespacio. De esta forma, se obtiene información acerca de los potenciales peligros que podrían afectar la infraestructura de una entidad.

En base a las definiciones presentadas se consideró determinar como autores base a García y Pesántez (2023), por su relevancia y actualidad en el tema de ciberseguridad. La fuente proporciona una definición clara y precisa de la ciberseguridad, abordando la identificación de amenazas, la evaluación de medidas de seguridad y la importancia de proteger datos confidenciales en contextos educativos en línea. Además, enfatiza la necesidad de garantizar la integridad de la información y los registros de estudiantes y profesores para asegurar un aprendizaje continuo y fiable sin interrupciones. Estos conceptos establecen una base sólida para mi investigación y respaldarán mis argumentos a lo largo de la tesis.

En relación con las dimensiones que engloba la variable independiente de Ciberseguridad, se tomaron en cuenta las siguientes: confidencialidad, integridad y disponibilidad. Sobre la dimensión confidencialidad, Ogwara et al. (2019) señalan que es esencial debido a que los datos de los usuarios son transmitidos a través de la red pública y guardados en servidores de acceso público. Por lo tanto, es necesario tener un control riguroso sobre el acceso a la información, permitiendo únicamente que los usuarios autorizados puedan acceder a ella.

En relación a la dimensión integridad, Qayyum et al. (2020) indican que esencial asegurarse de que la información que un usuario se mantenga completa y sin cambios, evitando cualquier posible pérdida o alteración, ya sea accidental o intencionada. La integridad de estos datos es de suma importancia para su seguridad y confiabilidad. Finalmente, con respecto a la dimensión disponibilidad, Merdassi et al. (2020) precisan que el servicio debe estar accesible para los usuarios en todo momento, sin restricciones horarias, para satisfacer sus necesidades en cualquier momento. Los proveedores deben tomar medidas para prevenir ataques y garantizar que el servicio se mantenga operativo de manera continua y sin interrupciones.

En cuanto a las teorías vinculadas a la gestión de riesgos, este estudio recibe respaldo a través de las que se describen a continuación. Para comenzar tenemos la teoría de la prospectiva, donde Molins y Serrano (2019) quienes manifiestan que la teoría prospectiva se sustenta en dos principios esenciales. El inicial argumenta que, al tomar decisiones entre diferentes opciones, llamadas prospectos, nuestra elección depende más del marco de referencia que del valor absoluto de dichos prospectos, desafiando así la noción económica de racionalidad. El segundo pilar crucial en esta teoría es el fenómeno conocido como aversión a las pérdidas. La aversión a las pérdidas implica una mayor sensibilidad ante la posibilidad de sufrir pérdidas en comparación con la perspectiva de obtener ganancias de igual magnitud. En otras palabras, para aceptar un riesgo, generalmente se requiere la posibilidad de una ganancia potencial, mientras que las pérdidas potenciales tienden a generar un rechazo.

De la misma manera, Osorio-Barreto et al. (2022) precisan que, la teoría prospectiva examina la toma de decisiones en circunstancias de riesgo, dividida en dos fases: edición y evaluación. Destaca que las actitudes hacia el riesgo se forman

conjuntamente, considerando condiciones que influyen en la aversión o búsqueda del riesgo. Además, señala que las ganancias y pérdidas se comparan con expectativas, y las discrepancias pueden surgir debido a cambios recientes en la riqueza. También enfatiza el impacto del tiempo y las influencias sociales en la toma de decisiones.

A continuación, se ha considerado la teoría del aprendizaje organizacional, donde Xie (2019) precisa que este enfoque de aprendizaje tiene como objetivo que la empresa se convierta en un sistema cohesionado en el cual sus componentes adquieran conocimiento generado internamente por la organización. Esto implica la creación, retención y compartición de conocimiento entre los diferentes departamentos de la empresa, de manera que la organización se transforme en una entidad dinámica que adquiera saberes, se adapte y responda eficazmente a las demandas del entorno. La organización valora la capacidad de aprendizaje como un concepto de varias facetas, donde los niveles de conocimiento, la cultura empresarial y las condiciones de aprendizaje se consideran como dimensiones significativas en el ámbito empresarial.

Además, Martinez et al. (2020) indican que los miembros de la organización desempeñan un papel crucial como facilitadores del aprendizaje, identificando errores y corrigiéndolos para preservar las características esenciales y la memoria de la organización. Esto contribuye a mantener la estabilidad de la organización incluso en entornos cambiantes. Además, el proceso de aprendizaje organizacional, que implica la generación de diferentes comprensiones e interpretaciones, tiene el potencial de influir en el comportamiento de las personas en beneficio del desarrollo de la organización. La interpretación de la información se refleja claramente en los mapas conceptuales de la organización, la consistencia en la transmisión de información, la presencia de intermediarios para facilitar la transferencia de conocimiento, el manejo adecuado de la información y la eliminación de conocimientos obsoletos a través del proceso de desaprendizaje.

Para finalizar, se ha considerado la teoría de la agencia, donde Massa et al. (2020) indican que esta teoría se centra en analizar la relación existente entre los ejecutivos de una empresa, incluyendo a los directores ejecutivos y gerentes, y cómo estas relaciones influyen en la toma de decisiones dentro de la organización. Los mecanismos de gobierno y las formas de compensación desempeñan un papel

crucial como instrumentos de supervisión utilizados por los miembros internos, incluyendo la junta directiva, para evitar que los ejecutivos subvaloren los intereses de la empresa. Además, esta teoría sugiere que la compensación es uno de los principales incentivos empleados para motivar a los ejecutivos a tomar decisiones que promuevan el crecimiento y el rendimiento óptimo de la compañía.

Así mismo, Martínez-Rojas et al. (2021) sostienen que teoría de agencia se basa en una premisa fundamental que parte del supuesto de que los dueños de una organización, conocidos como el principal, confían a un tercero, denominado el agente, la responsabilidad de llevar a cabo los objetivos y metas del principal con el fin de maximizar sus propios beneficios. Bajo esta perspectiva, dado que ambas partes buscan maximizar sus ganancias y considerando que el agente generalmente posee más información que el principal (lo que se conoce como asimetría de información), surgen razones para sospechar que el agente no siempre actuará en beneficio exclusivo del principal. Por lo tanto, nos encontramos frente a lo que se conoce como un problema de agencia.

En el contexto de esta investigación, exploraremos la gestión de riesgos como variable estudio. Para lograr una comprensión más profunda de este concepto, presentaremos múltiples definiciones ofrecidas por diversos autores. Según Panduro y Sandoval (2022), el propósito es permitir que las organizaciones aborden los riesgos, tanto los que provienen de su entorno externo como los internos, con el objetivo de reducir la probabilidad de eventos adversos que puedan afectar negativamente el logro de sus metas. Al mismo tiempo, busca maximizar las oportunidades que puedan tener un impacto positivo en el logro de sus objetivos, abarcando áreas como las finanzas, la salud, la seguridad y la tecnología de la información.

De igual manera, Castro-Rivera et al. (2020) indican que la gestión de riesgos reside principalmente en la reducción de la incertidumbre que comúnmente se encuentra en cada proyecto. Esto se debe a que, en muchas ocasiones, los requisitos iniciales pueden ser ambiguos y sufrir modificaciones a medida que avanza el proyecto, además de que es común cometer errores al estimar los tiempos y recursos necesarios. La clave radica en tomar medidas proactivas y anticiparse a posibles riesgos que puedan amenazar el éxito del proyecto. En caso

de que se materialicen estos riesgos, es esencial desarrollar planes de contingencia para prevenirlos o minimizar su impacto en el desarrollo del proyecto.

Para culminar, Gutiérrez y Sánchez-Ortiz (2018) sostienen que la gestión de riesgos se fundamenta en la creación o adición de valor, en la contribución a la realización de los objetivos, en su integración dentro de los procedimientos de una entidad, en su inclusión como parte integral del sistema de gestión global de la organización, en su utilidad para respaldar la toma de decisiones, en su abordaje de la incertidumbre, en su fundamento en la información más sólida disponible, en su adaptación a las necesidades específicas, en su consideración de los aspectos humanos y culturales, y en su capacidad para fomentar la mejora constante en la entidad.

A partir de las definiciones expuestas, se optó por seleccionar a Panduro y Sandoval (2022) como autores base en esta investigación debido a la actualidad y relevancia global de su trabajo en gestión de riesgos. Sus investigaciones reflejan las tendencias más recientes en este campo en constante evolución y abordan la gestión de riesgos desde una perspectiva integral y estratégica. Destacan la importancia de gestionar tanto los riesgos negativos como las oportunidades y subrayan la necesidad de una estrategia efectiva. Además, su enfoque multidisciplinario, que abarca áreas como finanzas, salud, seguridad y tecnología de la información, proporciona una base sólida para comprender y aplicar principios de gestión de riesgos en diversos contextos.

Con respecto a las dimensiones que abarca la variable dependiente gestión de riesgos se consideró las siguientes: identificación de riesgos, evaluación de riesgos y mitigación del riesgo. Sobre la dimensión identificación de riesgos, Dotres y Sanchez (2020) mencionan que identificar los cambios que puedan surgir en las fases de planificación y ejecución es esencial en el proceso de identificación de riesgos. En este contexto, es crucial establecer una relación de causa y efecto sólida. La gestión de riesgos en estas etapas requiere una delimitación precisa de los límites y se apoya en el uso de técnicas y herramientas respaldadas por evidencias, así como en análisis cuantitativos y cualitativos que orientan la estrategia de gestión.

De la misma manera, Díaz Curbelo et al. (2018) precisan que la fase inicial en la gestión de riesgos involucra la identificación de riesgos como su paso inicial.

La mayoría de las investigaciones orientadas a esta etapa optan por la aplicación de enfoques cualitativos. Es importante señalar que en estas investigaciones no se otorga prioridad ni se realiza una cuantificación del impacto negativo asociado a los diversos tipos de riesgos ni a los factores de riesgo.

En consecuencia, en base a la dimensión evaluación de riesgos se consideró a Díaz Curbelo et al. (2018), quienes sostienen que la evaluación de riesgos está relacionada con la probabilidad de que se materialice un evento y la magnitud de sus repercusiones. Se utiliza un enfoque basado en el análisis de árbol para examinar y evaluar el riesgo operativo en diversos procesos. Aunque la literatura ha investigado en gran medida los riesgos financieros, estos siguen siendo el foco principal de estudio de manera generalizada. Así mismo, Dotres y Sanchez (2020) indican que examinar las implicaciones de las modificaciones que ocurren en las fases de planificación y ejecución en el contexto de la gestión de riesgos es el objetivo principal de esta revisión. Su finalidad radica en determinar la magnitud de los impactos derivados de los riesgos no anticipados durante la fase de planificación en la ejecución, y, además, cómo se incorpora al personal o a sus representantes en todo el proceso.

Para finalizar, en relación a la dimensión mitigación del riesgo, según lo indicado por Dotres y Sanchez (2020), la disminución de las repercusiones en las etapas de planificación y ejecución es fundamental ya que los resultados de este análisis pueden conducir a la formulación de conclusiones y sugerencias dirigidas a los responsables de la toma de decisiones. Para minimizar los impactos, es necesario evaluar las cualidades de los directivos y del personal involucrado, incluyendo sus aptitudes de liderazgo, capacidad de adaptación al cambio y competencia demostrada en la toma de decisiones.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

3.1.1 Tipo de investigación

En esta investigación se utilizó el enfoque de investigación aplicada, ya que se procuró abordar y resolver un problema específico. De acuerdo a Ñaupas et al. (2019), este enfoque de investigación es más complejo porque busca explicar las causas y factores de un problema, es decir, busca una o dos causas principales y dos o más causas secundarias, también conocidas como factores. Se usa para comparar la influencia de una variable independiente sobre la variable dependiente. Un ejemplo.

3.1.2 Diseño de investigación

En el presente trabajo de investigación, se utilizó el diseño no experimental, transversal de nivel correlacional causal ya que se evaluó la efectividad de las medidas de ciberseguridad en la gestión de riesgos en una institución educativa. La investigación se enmarca en un diseño no experimental, donde se examinan las variables sin realizar manipulaciones deliberadas. En otras palabras, no se altera intencionalmente la variable asociada; más bien, se observa el fenómeno en su contexto natural y se analiza posteriormente (Molina & Rojas, 2021).

3.2 Variables y operacionalización

3.2.1 Variable: Ciberseguridad

Según García y Pesántez (2023), la ciberseguridad se define como la identificación de amenazas, evaluación de medidas de seguridad y recomendación de acciones para proteger la información.

Escala de medición

En la presente investigación se utilizó la escala ordinal. Según Dagnino (2014), la comprensión de datos ordinales implica la clasificación en al menos tres categorías distintas, con un límite en el número total de categorías. De esta manera, que la información obtenida sobre la variable ciberseguridad será evaluada dentro de los siguientes niveles: nunca (1), casi nunca (2), a veces (3), casi siempre (4), siempre (5).

3.2.2 Variable: Gestión de riesgos

Según Panduro y Sandoval (2022), el propósito es que las organizaciones gestionen riesgos para disminuir eventos adversos y aprovechar oportunidades que impacten positivamente en sus objetivos en áreas como finanzas, salud, educación, seguridad y tecnología.

Definición Operacional de la variable gestión de riesgos

La definición operacional de gestión de riesgos, según Panduro y Sandoval (2022), consiste en un proceso mediante el cual las organizaciones identifican y enfrentan los riesgos tanto internos como externos. El objetivo es reducir la probabilidad de eventos negativos que puedan perjudicar el logro de sus metas, al mismo tiempo que buscan aprovechar las oportunidades que puedan tener un impacto positivo en áreas como finanzas, salud, seguridad y tecnología de la información. De esta manera, la variable se medirá en base a un cuestionario de 17 ítems que se centra en tres dimensiones con sus respectivos indicadores: identificación de riesgos, evaluación de riesgos y mitigación de riesgo (Ver anexo 2).

Escala de medición

En base al autor mencionado la información obtenida sobre la variable gestión de riesgos será evaluada dentro de los siguientes niveles: nunca (1), casi nunca (2), a veces (3), casi siempre (4), siempre (5).

3.3 Población, muestra y muestreo

3.3.1 Población

Ñaupas et al. (2019) señalan que, en el contexto de una investigación científica, es posible describir una población como un conjunto de personas o elementos bajo estudio que comparten atributos específicos necesarios para los objetivos de la investigación en curso.

De esta manera, en esta investigación se consideró el total de trabajadores de la institución educativa, conformada por docentes y administrativos, los cuales alcanzan la cantidad de 30 trabajadores. En vista que la población es pequeña se considerado como muestra el total de la población. De acuerdo con Valdivia et al. (2019) la muestra se refiere a una porción específica del universo o población, elegida mediante diversos métodos, siempre asegurándose de que sea

representativa del conjunto total. En otras palabras, una muestra se considera representativa cuando refleja las características de los individuos que componen el universo.

Criterios de inclusión: En el transcurso de esta investigación, se consideró como participantes fundamentales a instituciones educativas de carácter público o privado. Asimismo, se abrieron las puertas a las instituciones educativas que habían demostrado su compromiso con la ciberseguridad al adoptar políticas y estrategias formales en esta área.

Criterios de exclusión: Se excluyeron de esta investigación a todos aquellos trabajadores que no estaban directamente relacionadas con la temática de la ciberseguridad en el contexto educativo.

Unidad de análisis

Para esta investigación, se consideró 30 trabajadores de una institución educativa.

3.4 Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

Se establece que en este estudio se empleó la encuesta. De acuerdo con Hernández y Mendoza (2018), la encuesta se caracteriza por su enfoque en la formulación de preguntas como método de recopilación de datos.

Instrumento de recolección de datos

Se establece que en esta investigación se utilizó el cuestionario. Según Ñaupas et al. (2019), el cuestionario se clasifica como una forma de encuesta que se basa en la elaboración de preguntas escritas de manera sistemática para obtener respuestas relacionadas con las variables, objetivos e hipótesis del estudio.

En esta investigación se ha utilizado dos cuestionarios que se han diseñado considerando sus dimensiones con 34 ítems. Con respecto a la variable independiente ciberseguridad, el cuestionario tiene 18 ítems dividido en tres dimensiones, los cuales han sido mencionados anteriormente. De la misma manera, en base a la variable dependiente, se ha considerado16 dividido en tres dimensiones (ver Anexo 3).

Validez

Según Villasís-Keever et al. (2018), validez en investigación se refiere a la autenticidad o aproximación a la verdad de un concepto. En términos generales, se presume que los resultados de una investigación serán considerados válidos cuando el estudio carezca de errores. Para determinar la validez de un estudio en particular, es esencial examinar la presencia de sesgos, que son errores sistemáticos, en aspectos críticos como el diseño de la investigación, los criterios de selección y la ejecución de las mediciones, es decir, la manera en que se registran y evalúan las variables del estudio.

De la misma manera, se utilizó la validez de contenido para someterla al juicio de expertos. Una de las estrategias más utilizadas para evaluar la validez de contenido de un instrumento es someterlo al juicio de expertos. La tarea de los evaluadores consiste en analizar el contenido de los ítems. Para llevar a cabo la evaluación del instrumento, se empleó la plantilla de Juicio de Expertos, la cual incluye la valoración de cada ítem a través de tres indicadores: claridad, coherencia y relevancia. La calificación se realiza mediante seis opciones de respuesta, eliminando así la posición intermedia y buscando obtener respuestas más confiables (Torres-Malca et al., 2022) (ver Anexo 4).

Tabla 1

Consolidado de juicio de expertos

Nombres y apellidos del experto	Especialidad	Dictamen
Manuel Antonio Pereyra Acosta	Ciberseguridad	Aplicable
Jonathan Alexis Puente Zamora	Gestión	Aplicable
Roberto Juan Tejada Ruiz	Gestión	Aplicable

Confiabilidad

Los resultados de una investigación son considerados fiables cuando exhiben un nivel significativo de validez, lo que implica la ausencia de sesgos. Este término se aplica con mayor frecuencia durante la creación o escalas clínicas, como aquellas creadas para evaluar la depresión, la calidad de vida o la gravedad de enfermedades. En este contexto, una vez que se confirma la reproducibilidad y consistencia de una escala, se puede inferir que es confiable. (Villasís-Keever et al., 2018).

Asimismo, en este estudio se utilizó la prueba de confiabilidad alfa de cronbach, ya que se utiliza para evaluar la consistencia interna de un conjunto de elementos, es decir, la estrecha relación entre ellos como grupo. Esta medida se emplea como indicador de la confiabilidad de la escala. Las pruebas α-Cronbach son útiles para determinar la confiabilidad de encuestas que utilizan escalas de Likert con preguntas múltiples en un cuestionario. Estas preguntas evalúan variables latentes o no observables (Pérez-León, 2023) (ver Anexo 5).

3.5 Procedimientos

En lo que respecta a la recopilación de datos en este estudio, se llevó a cabo un proceso que involucró la obtención de la autorización de las autoridades de la institución. Dicha autorización fue fundamental para poder recopilar información de acuerdo con los objetivos de la investigación, y se formalizó a través de un documento firmado por las autoridades, cuyo contenido se encuentra detallado (ver Anexo 6).

Posteriormente, se procedió a la ejecución de las encuestas. Para ello, se organizó una reunión virtual con la participación de todos los trabajadores involucrados en el estudio. Esta reunión virtual no solo facilitó la difusión de la investigación, sino que también se utilizaron dinámicas interactivas para motivar a los participantes y fomentar su compromiso con la encuesta en cuestión.

Una vez que se verificó que todos los participantes se encuentren en la reunión, se les proporcionó un enlace para acceder al cuestionario. Al momento de realizar la encuesta, se estableció un período definido y se enfatizó la importancia de que los participantes respondieran a cada pregunta con objetividad e imparcialidad. Esto se hizo con el propósito de obtener datos precisos y fiables que sean fundamentales para el análisis posterior. Finalizada la etapa de recopilación de datos, se procedió a ingresarlos en una base de datos para un posterior procesamiento de información.

3.6 Método de análisis de datos

En el marco de la presente investigación, se llevó a cabo un exhaustivo análisis de datos que abarcó tanto enfoques descriptivos como inferenciales. En lo que respecta al análisis descriptivo, se optó por emplear la distribución por frecuencias, aprovechando nuestra escala de medición ordinal. Esta elección permitió la

categorización y recuento de datos en intervalos o categorías, facilitando así la identificación de patrones, tendencias y la dispersión dentro del conjunto de datos.

Adicionalmente, se llevaron a cabo procedimientos específicos para enriquecer el análisis. Se efectuó la baremación de los datos, separándolos por dimensiones, y se procedió a su clasificación en niveles (escasa, regular, adecuada) a partir de los resultados obtenidos mediante la encuesta. Estos datos fueron luego trasladados a una base de datos, donde se utilizaron herramientas como SPSS 25 para agrupar la información por dimensiones y variables, permitiendo así obtener estadísticas descriptivas mediante el análisis de frecuencias.

En el siguiente paso, se aplicó la regresión ordinal como método inferencial para determinar la influencia de la variable independiente sobre la dependiente. Este enfoque, caracterizado por su capacidad para manejar datos ordinales, brindó una perspectiva más profunda sobre la influencia entre las variables en estudio. Este riguroso proceso metodológico garantiza la coherencia y consistencia en la interpretación de los resultados, contribuyendo a una comprensión integral de los aspectos analizados en la investigación.

3.7 Aspectos éticos

En la presente investigación, se consideró los principios éticos de investigación enfatizando la participación voluntaria de los sujetos de estudio, asegurando que se unieran al estudio de forma libre y sin presiones. Se proporcionó información clara sobre sus derechos y la posibilidad de retirarse en cualquier momento sin consecuencias negativas. En relación al riesgo, se ha comunicado de manera explícita a los participantes que no existe ningún peligro ni daño asociado con su involucramiento en la investigación.

En lo que respecta a los beneficios, se ha informado a los participantes que los resultados obtenidos serán compartidos con la institución al concluir la investigación. Es importante destacar que no se ofrecerán beneficios económicos ni de ninguna otra índole a los participantes. En relación con la confidencialidad, se ha establecido con firmeza que los datos recopilados serán tratados de forma anónima, sin ninguna posibilidad de identificar a los participantes.

Alineado a los principios reglamentados por el código de ética de la Universidad César Vallejo dispuesto por la Resolución de Consejo Universitario

Nº0340-2021-UCV. Se consideraron los diferentes artículos tales como el Artículo 7°. Del consentimiento y asentimiento informado del código de ética ya que se ha proporcionado a los participantes información completa y comprensible acerca del propósito y la duración de la investigación. Asimismo, se utilizó el Artículo 8º. De la publicación de las investigaciones permitiendo que el investigador mantenga una participación activa durante todo el proceso y manteniendo bajo anonimato el nombre de la institución, donde se viene desarrollando la investigación.

Se tuvo en cuenta el Artículo 10º. De la Originalidad de la investigación ya que, se fomenta y requiere la autenticidad en los resultados finales de la investigación. Artículo 11º. De los Derechos del autor, de esta manera la universidad, en congruencia con estos marcos legales, observa y protege los derechos de autor, aplicando sanciones a aquellos que incurran en plagio o violen los principios éticos de la investigación. La investigación actual se ajusta rigurosamente a todos los parámetros establecidos, incluyendo las citas y el formato APA en su séptima edición.

IV. RESULTADOS

Resultados descriptivos

Tabla 2

Distribución de frecuencias de ciberseguridad

Nivel	Rango	Frecuencia	Porcentaje
Escasa	18 - 41	11	36,7
Regular	42 - 65	10	33,3
Adecuada	66 - 90	9	30,0
Total		30	100,0

Los resultados indican que la ciberseguridad en la institución se encuentra dentro de un rango escaso, situándose en un 36,7%, lo que muestra que los trabajadores consideran que la ciberseguridad es escasa. Esto se debe a que perciben la presencia de accesos no autorizados, pérdidas de datos, problemas de confidencialidad y momentos de inactividad en el sistema. Además, observan casos de corrupción de datos almacenados en dispositivos en red. Estos hallazgos resaltan preocupaciones significativas sobre la protección y seguridad de la información en la institución, sugiriendo la necesidad de mejorar las prácticas de la ciberseguridad.

Tabla 3

Distribución de frecuencias de confidencialidad

Nivel	Rango	Frecuencia	Porcentaje
Escasa	6 - 13	11	46,7
Regular	14 - 21	10	33,3
Adecuada	22 - 30	9	20,0
Total		30	100,0

Los resultados indican que la percepción de la confidencialidad en la institución ha obtenido un rango escaso, situándose en un 46,7%. La confidencialidad, se refiere a la capacidad de proteger la información sensible y restringir el acceso no autorizado a la misma. La presencia de accesos no autorizados en los sistemas genera inquietudes sobre la seguridad de la información sensible, indicando posibles debilidades en la protección de datos confidenciales. Aunque la institución implementa medidas para prevenir y detectar estos accesos, la baja calificación

sugiere que estas medidas pueden no ser completamente efectivas, subrayando la necesidad de fortalecer los controles de seguridad.

Tabla 4

Distribución de frecuencias de disponibilidad

Nivel	Rango	Frecuencia	Porcentaje
Escasa	6 - 13	10	33,3
Regular	14 - 21	16	53,3
Adecuada	22 - 30	4	13,3
Total		30	100,0

La disponibilidad en la institución, es percibida de manera regular con un 53,3%, lo cual plantea inquietudes sobre cómo asegurar que los servicios y datos estén siempre accesibles cuando se necesiten. La disponibilidad se refiere a la capacidad de garantizar que los servicios y datos estén disponibles cuando se necesiten. La institución evalúa el tiempo de recuperación de datos ante un desastre, indicando un enfoque proactivo para garantizar la continuidad de las operaciones en situaciones adversas. A pesar de la percepción regular, la experiencia de tiempo de inactividad no planificado en el sistema sugiere áreas donde la disponibilidad podría fortalecerse, destacando la importancia de abordar y reducir estas interrupciones imprevistas.

La evaluación de la capacidad de escalabilidad y la medición de la eficacia del sistema de recuperación de datos son aspectos positivos, mostrando un esfuerzo consciente para adaptarse a las demandas cambiantes y asegurar una recuperación exitosa en situaciones de desastre. Aunque la disponibilidad es percibida de manera regular, existe una oportunidad para mejorar la gestión del tiempo de inactividad no planificado

Tabla 5

Distribución de frecuencias de integridad

Nivel	Rango	Frecuencia	Porcentaje
Escasa	6 - 13	11	36,7
Regular	14 - 21	12	40,0
Adecuada	22 - 30	7	23,3
Total		30	100,0

La integridad en la institución, es percibida de manera regular con un 40,0%, la misma que se refiere a mantener la precisión y coherencia de los datos, asegurando que la información no se vea comprometida ni alterada de manera no autorizada. De esta manera, se observa que la institución ha establecido como objetivo la restauración de la integridad de los datos en un plazo no mayor a dos horas después de una incidencia. Este enfoque indica una preocupación por actuar rápidamente para mantener la precisión de la información. Sin embargo, las preocupaciones surgen al identificar que la institución experimenta casos de corrupción de datos en sus sistemas y ha registrado incidencias de este tipo. Estos hallazgos indican desafíos reales en la preservación de la integridad de los datos, destacando la necesidad de abordar las fuentes y las causas de la corrupción de datos.

Tabla 6

Distribución de frecuencias de gestión de riesgos

Nivel	Rango	Frecuencia	Porcentaje
Escasa	16 - 36	10	33,3
Regular	37- 58	12	40,0
Adecuada	59 - 80	8	26,7
Total		30	100,0

La gestión de riesgos en la institución es percibida de manera regular, obteniendo un 40,0%. Se destaca positivamente que la institución realiza evaluaciones semanales para identificar riesgos en sus sistemas de información, indicando una atención continua a posibles amenazas. Además, la medición frecuente de la incidencia de ataques cibernéticos, el registro de riesgos potenciales y el análisis de sensibilidad de los riesgos identificados reflejan una conciencia activa y proactiva de las amenazas cibernéticas. El uso de herramientas como la matriz de

riesgos para comunicar los ataques cibernéticos y la eficiencia en las estrategias de mitigación de riesgos son aspectos positivos. Sin embargo, la percepción regular sugiere oportunidades para fortalecer aún más estas estrategias y mejorar la eficacia general de la gestión de riesgos en el entorno de los sistemas de información.

Tabla 7

Distribución de frecuencias de identificación de riesgos

Nivel	Rango	Frecuencia	Porcentaje
Escasa	5 - 11	9	30,0
Regular	12 - 18	13	45,0
Adecuada	19-25	8	25,0
Total		30	100,0

La identificación de riesgos, es percibida en un regular con un 45,0%, el cual es un proceso fundamental para evaluar y comprender las posibles amenazas que pueden afectar los sistemas de información de la institución. Se destaca positivamente que la institución lleva a cabo el proceso de identificación de riesgos ante posibles ataques cibernéticos, indicando un enfoque proactivo para reconocer amenazas potenciales. La evaluación semanal de la identificación de riesgos en los sistemas de información y la medición frecuente de la frecuencia de ataques cibernéticos demuestran una atención continua y consciente a las amenazas en el entorno digital. Sin embargo, la oportunidad de mejorar podría centrarse en la implementación de enfoques más específicos y detallados para abordar las amenazas cibernéticas.

Tabla 8

Distribución de frecuencias de evaluación de riesgos

Nivel	Rango	Frecuencia	Porcentaje
Escasa	6 - 13	14	48,0
Regular	14 - 21	10	33,0
Adecuada	22-30	6	19,0
Total		30	100,0

La evaluación de riesgos, es percibida por los trabajadores de manera escasa con un 48,0%, la misma que implica analizar la probabilidad de que ocurran eventos no deseados y el impacto que podrían tener en el funcionamiento normal de la

institución. De esta manera, se evidencia que se utiliza la matriz de riesgos para comunicar los posibles ataques cibernéticos a sus sistemas de información, indicando un enfoque estructurado para entender y visualizar las amenazas. Sin embargo, la baja percepción sugiere la necesidad de mejorar la eficacia de la evaluación de riesgos. Esto podría implicar revisar y ajustar la metodología utilizada, así como aumentar la frecuencia y la profundidad de la evaluación para garantizar una comprensión más completa y precisa de los riesgos asociados a los sistemas de información.

Tabla 9

Distribución de frecuencias de mitigación de riesgos

Nivel	Rango	Frecuencia	Porcentaje
Escasa	5 - 11	12	40,0
Regular	12 - 18	8	26,7
Adecuada	19 - 25	10	33,3
Total		30	100,0

La mitigación de riesgos, es percibida de manera escasa con un 40%, la cual se basa en tomar medidas preventivas y correctivas para proteger los activos de la organización y mantener la continuidad de las operaciones. Las estrategias de mitigación han logrado reducir eficazmente el riesgo de ataques cibernéticos, lo que refleja esfuerzos exitosos para minimizar la vulnerabilidad ante posibles amenazas.

Resultados inferenciales

Prueba de hipótesis general

Formulación de hipótesis estadística:

Ha: La ciberseguridad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023

Ho: La Ciberseguridad no influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023.

Tabla 10

Prueba de ajuste de modelo

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	27,730			
Final	15,552	12,178	2	,002

El modelo de regresión logística ordinal elegido demostró un sig. de 0,002, cuyo resultado es inferior a 0,05, de esta manera observamos que los resultados se ajustas de forma significativa a las variables introducidas.

Tabla 11

Pseudo R cuadrado

Pseudo R cuadrado	
Cox y Snell	,334
Nagelkerke	,377
McFadden	,187

La variabilidad de la variable dependiente gestión de riesgos es de 37.7% como resultado de la influencia de la variable independiente. Por tanto, se considera la hipótesis alterna (Ha).

Prueba de hipótesis específica 1

Formulación de hipótesis estadística:

Ha: La confidencialidad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023.

Ho: La confidencialidad no influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023.

Tabla 12

Prueba de ajuste de modelo

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	19,233			
Final	14,545	4,688	2	,036

El modelo de regresión logística ordinal elegido demostró un sig. de 0,036, cuyo resultado es inferior a 0,05, La misma que establece influencia de la dimensión confidencialidad sobre la gestión de riesgos, mediante la aplicación de un enfoque de análisis de regresión ordinal.

Tabla 13

Pseudo R cuadrado

Pseudo R cuadrado	
Cox y Snell	,145
Nagelkerke	,163
McFadden	,072

La variabilidad de la variable dependiente gestión de riesgos es de 16.3% como resultado de la influencia de la dimensión confidencialidad. Por tanto, se considera la hipótesis alterna (Ha).

Prueba de hipótesis específica 2

Formulación de hipótesis estadística:

Ha: La integridad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023.

Ho: La integridad no influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023.

Tabla 14

Prueba de ajuste de modelo

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	24,029			
Final	17,775	6,254	2	,044

El modelo de regresión logística ordinal elegido demostró un sig. de 0,044, cuyo resultado es inferior a 0,05, La misma que establece influencia de la dimensión integridad sobre la gestión de riesgos, mediante la aplicación de un enfoque de análisis de regresión ordinal.

Tabla 15

Pseudo R cuadrado

Pseudo R cuadrado	
Cox y Snell	,178
Nagelkerke	,201
McFadden	,090

La variabilidad de la variable dependiente gestión de riesgos es de 20.1% como resultado de la influencia de la dimensión integridad. Por tanto, se considera la hipótesis alterna (Ha).

Prueba de hipótesis específica 3

Formulación de hipótesis estadística:

Ha: La disponibilidad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023.

Ho: La disponibilidad no influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023.

Tabla 16

Prueba de ajuste de modelo

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	30,621			
Final	13,462	17,158	2	,000

El modelo de regresión logística ordinal elegido demostró un sig. de 0,000, cuyo resultado es inferior a 0,05, La misma que establece influencia de la dimensión disponibilidad sobre la gestión de riesgos, mediante la aplicación de un enfoque de análisis de regresión ordinal.

Tabla 17

Pseudo R cuadrado

Pseudo R cuadrado	
Cox y Snell	,436
Nagelkerke	,492
McFadden	,264

La variabilidad de la variable dependiente gestión de riesgos es de 49.2% como resultado de la influencia de la dimensión disponibilidad. Por tanto, se considera la hipótesis alterna (Ha).

V. DISCUSIÓN

Con base en los resultados detallados en el capítulo anterior, se desarrolló la discusión acerca de la influencia de la ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023.

Respecto a la dimensión 1, los resultados obtenidos afirman la influencia significativa de la dimensión de confidencialidad en la gestión de riesgos. El modelo de regresión logística ordinal utilizado reveló un nivel de significancia de 0,036, inferior al umbral establecido de 0,05. Este resultado conduce a la aceptación de la hipótesis alterna (Ha), indicando que la dimensión de confidencialidad tiene un impacto estadísticamente significativo en la gestión de riesgos, contribuyendo con un 16.3% a la variabilidad de la variable dependiente.

Del mismo modo, al analizar una tabla cruzada acerca de la confidencialidad, se pudo constatar que los trabajadores perciben de manera habitual la confidencialidad en la gestión de riesgos en un 40,0%. Además, se identificó una percepción escasa del 54,5%, originada por una gestión de riesgos deficiente cuando la confidencialidad es escasa. Posteriormente, se observó que la percepción de un nivel regular era del 40,0%, indicando que la confidencialidad en este caso también está relacionada con una gestión de riesgos inadecuada. De igual manera, el nivel considerado adecuado mostró una percepción del 44,4%, señalando que cuando la confidencialidad alcanza este nivel, la gestión de riesgos es adecuada. Estas variaciones en los resultados nos alertan sobre la presencia de una influencia significativa de la confidencialidad sobre la gestión de riesgos.

La variabilidad del 16.3% en la variable dependiente, la gestión de riesgos, puede atribuirse a la influencia de la dimensión de confidencialidad. Este hallazgo sugiere que la confidencialidad desempeña un papel significativo en la explicación de las variaciones en la gestión de riesgos cibernéticos en la muestra analizada. Estos resultados encuentran respaldo en el marco teórico, donde se destaca la importancia estratégica de la seguridad cibernética en países en desarrollo para fortalecer la resiliencia nacional en el ámbito digital (Creese et al., 2021). La estrategia nacional de ciberseguridad, como ejemplificado por la Estrategia E-Ciber de Brasil, emerge como un componente esencial para consolidar las capacidades cibernéticas de un país (Solar, 2020).

Este hallazgo encuentra respaldo en el marco teórico, donde se subraya la importancia de la seguridad cibernética, entendida como una visión integral y coherente que abarca redes, sistemas, servicios e infraestructuras. La dimensión de confidencialidad, según Valverde Arcos & Hurel Franco (2021), desempeña un papel crucial en esta concepción de seguridad cibernética. La estrategia nacional de ciberseguridad, como se describe en el marco teórico, se identifica como un componente esencial para consolidar las capacidades cibernéticas de un país, y la implementación de la gobernanza de ciberseguridad se considera crucial, como se evidencia en la Estrategia E-Ciber de Brasil.

Al conectar los resultados con el marco teórico, se destaca la relevancia práctica de la influencia de la confidencialidad en la gestión de riesgos. Los datos del Instituto Nacional de Ciberseguridad (INCIBE, 2021) y la consultora Deloitte refuerzan esta conexión al revelar un aumento significativo en los incidentes cibernéticos y la frecuencia de los informes de empresas que experimentaron incidentes de ciberseguridad. Estos hallazgos indican la urgencia de abordar la confidencialidad como parte integral de las estrategias de gestión de riesgos en un entorno cibernético en constante evolución.

Al explorar datos concretos, el informe del Instituto Nacional de Ciberseguridad (INCIBE, 2021) resalta que su centro de respuesta atendió más de 109,000 incidentes, con un impacto significativo en ciudadanos, empresas y la red académica. Esta evidencia empírica subraya la magnitud de los desafíos actuales en ciberseguridad. Adicionalmente, la encuesta del Foro Económico Mundial revela que un 87% de los ejecutivos están dedicados a fortalecer la ciberresiliencia, indicando una creciente conciencia y acción en el ámbito empresarial para hacer frente a los riesgos cibernéticos (World Economic Forum, 2022).

La conexión entre nuestra investigación y la encuesta global sugiere que la atención a la confidencialidad no solo es un requisito local, sino una necesidad global. La mejora de políticas, procedimientos y estándares en colaboraciones con terceros, como destacado en la encuesta, puede estar vinculada directamente a la gestión de riesgos que nuestra investigación asocia con la dimensión de confidencialidad.

Respecto a la dimensión 2, los resultados obtenidos afirman la influencia significativa de la dimensión de integridad en la gestión de riesgos. El modelo de

regresión logística ordinal utilizado reveló un nivel de significancia de 0,044, inferior al umbral establecido de 0,05. Este resultado conduce a la aceptación de la hipótesis alterna (Ha), indicando que la dimensión de confidencialidad tiene un impacto estadísticamente significativo en la gestión de riesgos, contribuyendo con un 20,1% a la variabilidad de la variable dependiente.

De igual manera, al examinar una tabla cruzada acerca de la integridad, se pudo constatar que los trabajadores perciben de manera regular la integridad en la gestión de riesgos en un 40,0%. Asimismo, se identificó una percepción escasa del 72,7%, derivada de una gestión de riesgos deficiente cuando la integridad es escasa. Posteriormente, se observó que la percepción de un nivel regular era del 66,7%, indicando que la integridad en este caso también está relacionada con una gestión de riesgos regular. De manera similar, el nivel considerado adecuado mostró una percepción del 71,4%, señalando que cuando la integridad alcanza este nivel, la gestión de riesgos es adecuada. Estas variaciones en los resultados nos alertan sobre la presencia de una influencia significativa de la integridad en la gestión de riesgos.

Estos hallazgos respaldan la idea de que contar con profesionales capacitados en ciberseguridad es esencial tanto para empresas como para entidades gubernamentales. La capacitación de profesionales en este campo podría ser clave para abordar las amenazas asociadas a la delincuencia organizada en el ámbito de la seguridad cibernética. El aumento constante de los delitos cibernéticos es motivo de preocupación, con el 53% de los ciberataques resultando en daños significativos, según Cisco (2022). Además, América Latina experimentó un aumento del 24% en la cantidad de incidentes de este tipo entre enero y agosto de 2020, según Kaspersky (2021), resaltando la necesidad urgente de abordar estos desafíos en la región.

La relación entre ataques cibernéticos y prácticas fraudulentas, sobornos y corrupción destaca la complejidad de los riesgos en ciberseguridad. La auditoría forense, que combina talento humano con habilidades técnicas, emerge como una herramienta crucial para prevenir y abordar estas amenazas (Fernández, 2020).

A nivel internacional, la diversidad de amenazas cibernéticas desde bandas criminales hasta grupos geopolíticos adversarios (Munkøe et al., 2019) resalta la necesidad de medidas internacionales. La conexión entre actividades ilegales

respaldadas por gobiernos, como en el caso de Corea del Norte, y la ciberdelincuencia, revela la complejidad geopolítica de los riesgos cibernéticos (Reuters, 2019).

Respecto a la dimensión 3, los resultados obtenidos afirman la influencia significativa de la dimensión de disponibilidad en la gestión de riesgos. El modelo de regresión logística ordinal utilizado reveló un nivel de significancia de 0,000, inferior al umbral establecido de 0,05. Este resultado conduce a la aceptación de la hipótesis alterna (Ha), indicando que la dimensión de confidencialidad tiene un impacto estadísticamente significativo en la gestión de riesgos, contribuyendo con un 49,2% a la variabilidad de la variable dependiente.

De igual modo, al analizar una tabla cruzada referente a la disponibilidad, se pudo observar que los trabajadores perciben de manera regular la disponibilidad en la gestión de riesgos en un 40,0%. Asimismo, se identificó la percepción escasa de un 60,0%, debido a que cuando la disponibilidad es escasa, se refleja una gestión de riesgos deficiente. Posteriormente, se notó que la percepción de un nivel regular era del 50,0%, indicando que la disponibilidad en este caso también se vincula con una gestión de riesgos regular. De manera similar, el nivel considerado adecuado mostró una percepción del 65,0%, indicando que cuando la disponibilidad alcanza este nivel, la gestión de riesgos es adecuada. Estas variaciones en los resultados nos alertan sobre la presencia de una influencia significativa de la disponibilidad en la gestión de riesgos.

La problemática de la disponibilidad, como se evidencia en la relación entre empresas y tecnologías de la información y la comunicación (TIC), se asocia con acciones como la apropiación no autorizada de propiedad intelectual y la creación de conflictos para dañar a competidores. La orden ejecutiva durante la administración de Trump para limitar transacciones relacionadas con TIC vinculadas a actores extranjeros adversos resalta la preocupación por la seguridad en este ámbito. Además, las actividades ilegales respaldadas por gobiernos, como en el caso de Corea del Norte, subrayan la necesidad crítica de gestionar los riesgos asociados con la disponibilidad.

La norma ISO 31000 proporciona una definición integral de riesgo y orientación sobre el proceso de gestión de riesgos (Pulido et al., 2020). Esta perspectiva se alinea con la necesidad de evaluar y abordar los riesgos asociados

con la disponibilidad. La gestión de riesgos, según Dotres y Sanchez (2020), no solo implica identificar y analizar riesgos, sino también formular conclusiones y recomendaciones dirigidas a los encargados de tomar decisiones. La evaluación de competencias de líderes y personal, junto con estrategias para reducir riesgos, es crucial en el contexto de la disponibilidad.

Las estadísticas sobre la vulnerabilidad a ataques cibernéticos en Perú, como se presenta en el marco teórico, añaden una dimensión práctica a la discusión. La variabilidad en la posición de Perú en términos de vulnerabilidad a ataques cibernéticos resalta la dinámica y la evolución de las amenazas. Los tipos específicos de ataques, como la distribución de malware por correo basura, subrayan la importancia de abordar la disponibilidad para mitigar estos riesgos.

La perspectiva presentada en el marco teórico destaca la evolución constante de las tácticas de los criminales cibernéticos, especialmente en un entorno digital en expansión. La observación de que la mayoría de las denuncias durante el inicio de la pandemia de COVID-19 en Perú estaban relacionadas con delitos informáticos subraya la agilidad de estos criminales para identificar oportunidades, utilizando canales variados como llamadas telefónicas, mensajes de WhatsApp y correos electrónicos (Quiroga, 2021). Este contexto refuerza la importancia crítica de abordar la dimensión de disponibilidad, ya que los criminales buscan aprovechar vulnerabilidades para llevar a cabo sus actividades fraudulentas.

La estrategia propuesta para fortalecer la ciberseguridad en el Estado peruano, según el marco teórico, destaca la necesidad de un enfoque participativo y colaborativo que involucre a diversos actores, desde la población hasta instituciones gubernamentales y fuerzas militares (Sheth et al., 2021). Esta estrategia refuerza la importancia de abordar la disponibilidad no solo desde una perspectiva tecnológica, sino también desde un enfoque holístico que incluya la participación y la colaboración de múltiples partes interesadas.

De acuerdo a la hipótesis general, los resultados obtenidos afirman la influencia significativa de la dimensión de disponibilidad en la gestión de riesgos. El modelo de regresión logística ordinal utilizado reveló un nivel de significancia de 0,002, inferior al umbral establecido de 0,05. Este resultado conduce a la aceptación de la hipótesis alterna (Ha), indicando que la dimensión de

confidencialidad tiene un impacto estadísticamente significativo en la gestión de riesgos, contribuyendo con un 37,7% a la variabilidad de la variable dependiente.

De manera similar, al examinar una tabla cruzada en relación con la ciberseguridad, se pudo constatar que los trabajadores perciben de manera regular la ciberseguridad en la gestión de riesgos en un 40,0%. También se identificó una percepción elevada del 72,7%, indicando que cuando la ciberseguridad es escasa, refleja una gestión de riesgos deficiente. Posteriormente, se observó que la percepción de un nivel regular era del 60,0%, señalando que la ciberseguridad en este caso está vinculada con una gestión de riesgos regular. De igual manera, el nivel considerado adecuado mostró una percepción del 44,4%, indicando que cuando la ciberseguridad alcanza este nivel, la gestión de riesgos es adecuada. Estas variaciones en los resultados nos alertan sobre la presencia de una influencia significativa de la ciberseguridad en la gestión de riesgos.

El marco teórico aporta una perspectiva valiosa para comprender el entorno cibernético peruano y la necesidad imperante de una gestión efectiva de riesgos. La expansión del ámbito digital ha aumentado la sofisticación de los criminales cibernéticos, quienes buscan oportunidades, como se evidenció durante la pandemia de COVID-19 con delitos informáticos relacionados con suplantación de identidad (Quiroga, 2021). Esta realidad destaca la importancia crítica de abordar la dimensión de disponibilidad, ya que los delincuentes buscan explotar vulnerabilidades en el entorno digital.

La estrategia propuesta para fortalecer la ciberseguridad en el Estado peruano, basada en un enfoque participativo y colaborativo, resuena con la necesidad de involucrar a diversos actores para desarrollar un programa efectivo y cerrar la brecha en la capacidad de respuesta (Sheth et al., 2021). Además, la llamada a establecer una clara separación entre las redes internas del Estado y la Internet pública, respaldada por una entidad dedicada y un sistema tecnológico avanzado, destaca la necesidad de medidas estructurales y tecnológicas para gestionar la disponibilidad (Ormachea, 2020).

Los desafíos específicos enfrentados por Perú en términos de ciberseguridad, como la falta de inversión y la oleada de ciberataques en 2021, subrayan la vulnerabilidad del país y la necesidad urgente de una gestión de riesgos efectiva (Quevedo, 2023). La mención de tener Fuerzas Armadas con sólida

capacidad de defensa cibernética refuerza la importancia de abordar la disponibilidad desde una perspectiva nacional de seguridad (Fuerman, 2023).

La mención de teorías relacionadas con la seguridad de redes enfatiza la importancia del diseño adecuado de la red para prevenir, mitigar y gestionar efectivamente los riesgos cibernéticos (Vega, 2021).

La discusión general entre la variable de ciberseguridad y la variable de gestión de riesgos revela una relación intrínseca que impacta significativamente en la protección de la información y la toma de decisiones estratégicas. A través de la evaluación de hipótesis general y especifica, junto con el marco teórico, se desglosa la conexión entre estas variables.

Las dimensiones de ciberseguridad, representadas por la confidencialidad, integridad y disponibilidad, desempeñan un papel crucial en la gestión de riesgos. La confidencialidad, al salvaguardar la información sensible, directamente influye en la capacidad de una organización para protegerse contra amenazas y pérdidas de datos no autorizadas. La integridad, al mantener la coherencia y exactitud de los datos, contribuye a la toma de decisiones informadas y a la prevención de manipulaciones maliciosas. La disponibilidad, al asegurar el acceso y la operatividad de los sistemas, minimiza la interrupción y garantiza la continuidad de las operaciones, reduciendo así los riesgos asociados.

En el marco teórico, se destaca la importancia de estrategias internacionales de ciberseguridad, como en el caso de Brasil, que refuerzan la idea de que la gestión efectiva de riesgos cibernéticos es esencial para la seguridad a nivel nacional. Asimismo, el aumento de ataques cibernéticos durante la pandemia de COVID-19 subraya la relevancia continua de la ciberseguridad en la gestión de riesgos, incluso en situaciones de crisis global.

La gestión de riesgos cibernéticos, representada por la variable dependiente "gestión de riesgos", refleja la interacción directa con las dimensiones de ciberseguridad. La variabilidad significativa en la gestión de riesgos, influenciada por la confidencialidad, integridad y disponibilidad, indica que una estrategia integral de ciberseguridad es esencial para gestionar eficazmente los riesgos en el entorno digital.

VI. CONCLUSIONES

Primero. El análisis de regresión logística ordinal realizado respalda la hipótesis general, ya que el valor de significancia obtenido 0.002 es inferior a 0.05. Esto indica que los resultados se ajustan de manera significativa a las variables introducidas. La variabilidad del 37.7% en la gestión de riesgos se atribuye a la influencia de la variable independiente de ciberseguridad. En consecuencia, se concluye que la ciberseguridad influye de manera significativa en la gestión de riesgos en una institución educativa en Callao en 2023.

Segundo. El análisis de regresión logística ordinal muestra una significancia de 0.036, validando así la influencia de la dimensión de confidencialidad en la gestión de riesgos. La variabilidad del 16.3% en la gestión de riesgos se atribuye a la dimensión de confidencialidad. Por lo tanto, se concluye que la confidencialidad tiene una influencia significativa en la gestión de riesgos en una institución educativa en Callao en 2023.

Tercero. El análisis de regresión logística ordinal respalda la Hipótesis Específica 2, con un valor de significancia de 0.044. Esto confirma la influencia significativa de la dimensión de integridad en la gestión de riesgos. La variabilidad del 20.1% en la gestión de riesgos se atribuye a la dimensión de integridad. Por lo tanto, se concluye que la integridad influye significativamente en la gestión de riesgos en una institución educativa en Callao en 2023.

Cuarto. El análisis de regresión logística ordinal muestra una significancia de 0.000, respaldando así la influencia significativa de la dimensión de disponibilidad en la gestión de riesgos. La variabilidad del 49.2% en la gestión de riesgos se atribuye a la dimensión de disponibilidad. En consecuencia, se concluye que la disponibilidad tiene una influencia significativa en la gestión de riesgos en una institución educativa en Callao en 2023.

VII. RECOMENDACIONES

Primero. Para los administrativos y docentes, se recomienda participar en programas de formación continuada en ciberseguridad. Esto garantizará un mayor conocimiento de las amenazas cibernéticas actuales y las mejores prácticas para la prevención, lo que contribuirá significativamente a la seguridad de los datos institucionales.

Segundo. Dada la influencia positiva de la dimensión de confidencialidad en la gestión de Riesgos, se sugiere establecer políticas específicas de confidencialidad. Los administrativos y docentes deben ser conscientes de la importancia de salvaguardar la información sensible y seguir prácticas seguras en el manejo de datos confidenciales.

Tercero. Para asegurar la integridad de los datos, se recomienda que los administrativos y docentes participen en la implementación de procesos de gestión de datos robustos. Esto implica la validación regular de la integridad de la información y la adhesión a procedimientos específicos para garantizar la exactitud de los datos utilizados en la gestión educativa.

Cuarto. Los administrativos y docentes desempeñan un papel clave en el monitoreo constante de los recursos de TI. Se sugiere la colaboración activa en la identificación de posibles amenazas y la notificación rápida a los responsables de ciberseguridad ante cualquier irregularidad. Esto garantizará una respuesta rápida y eficiente a posibles incidentes.

Quinto. Para los administrativos, se les insta a priorizar la seguridad cibernética en el entorno educativo. Esto implica fomentar prácticas seguras entre los estudiantes y agregar contenido específico de ciberseguridad en los planes de estudio. Esto no solo protegerá la infraestructura del colegio, sino que también formará a los estudiantes como usuarios conscientes de la seguridad informática.

Sexto. Al director, se recomienda enfocarse en medidas clave de ciberseguridad, establecer políticas de confidencialidad, supervisar la gestión de datos y dar prioridad a la seguridad cibernética en los planes de estudio para formar estudiantes conscientes y seguros en el uso de la tecnología.

REFERENCIAS

Ballestero, F. (2022). Cómo mejorar la ciberseguridad en España. *Boletín Económico De ICE*, *3148*. https://doi.org/10.32796/bice.2022.3148.7457

Becerril, A. (2019). La ciberseguridad en los Tratados de Libre Comercio. Revista Chilena De Derecho Y Tecnología, 8(2), 111. https://doi.org/10.5354/0719-2584.2019.53447

Castro, V., Herrera, R., & Villalobos, M. (2020). Desarrollo de un software web para la generación de planes de gestión de riesgos de software. *Información Tecnológica*, *31*(3), 135–148. https://doi.org/10.4067/s0718-07642020000300135

Córdoba, D. (2023) *Criptografía y seguridad*. Junco TIC. https://juncotic.com/criptografia-y-seguridad/

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and Ubiquitous Computing, 25*. https://doi.org/10.1007/s00779-021-01569-6

Curbelo, A. D., Municio, N. M. G., & Delgado, F. M. (2018). Herramientas para la gestión de riesgos en cadenas de suministro: una revisión de la literatura. *Dirección y Organización*, *64,* 5-35. https://doi.org/10.37610/dyo.v0i64.519

Dagnino S., J. (2014). Tipos de datos y escalas de medida. *Revista Chilena De Anestesia*, *43*(2). https://doi.org/10.25237/revchilanestv43n02.06

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of Business and Psychology*, *37*(1), 1–29. https://doi.org/10.1007/s10869-021-09732-9

Del-Real, C. (2022). Panorama institucional de la gobernanza de la ciberseguridad en España. *Revistas de Estudios Jurídicos y Criminológicos,* (6), 15-51. https://doi.org/10.25267/rejucrim.2022.i6.03.

Díaz, A., Manuel, Á., & Marrero, F. (2018). Herramientas Para La Gestion De Riesgos En Cadenas De Su-Ministro: Una Revisión De La Literatura Tools

for Risk Management in Supply Chains: a Review of Literature. *Dirección y Organización*, *64*, 5–35.

Dotres Zuniga, S., & Sanchez Paz, N. (2020). Integration of corporate social responsibility in the risk management in constructive investments. *Avances*, 22(2), 170–182.

Fernández, E., & Gil, R. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. *Novum, 1*(20), 61-80. *Redalyc*.org. https://www.redalyc.org/articulo.oa?id=571361695004

Fitni, Q., & Ramli, K. (2020). *Implementation of Ensemble Learning and Feature Selection for Performance Improvements in Anomaly-Based Intrusion Detection Systems*. IEEE Conference Publication | IEEE Xplore. https://doi.org/10.1109/IAICT50021.2020.9172014

Fuerman. (2023). *Política Sectorial de Ciberdefensa: una necesidad impostergable Centro de Estudios Estratégicos del Ejército del Perú*. Centro De Estudios Estratégicos Del Ejército Del Perú | Think Tank Del Ejército Del Perú. https://ceeep.mil.pe/2021/11/18/politica-sectorial-de-ciberdefensa-una-necesidad-impostergable/

García, P., & Pesantez, D. (2023). Analysis of cybersecurity in e-learning platforms: systematic review of the literature. *Perspectives Magazine, 5*(1), 19–29. https://doi.org/10.47187/perspectivas.5.1.179

Gutiérrez, Y., & Sánchez, A. (2018). Diseño de un Modelo de Gestión de Riesgos basado en ISO 31.000:2012 para los Procesos de Docencia de Pregrado en una Universidad Chilena. *Formación Universitaria*, *11*(4), 15–32. https://doi.org/10.4067/s0718-50062018000400015

Gutiérrez González, P., & Pons Pons, J. (2022, March 15). Risk management regulation and corporate demand for reinsurance in the Spanish Autarky (1940-1952). Revista De Historia Industrial Economía Y Empresa, 31(84), 175–203. https://doi.org/10.1344/rhiihr.v31i84.31954

Ignaczak, L., Goldschmidt, G., Costa, C., & Righi, R. (2021). Text Mining in Cybersecurity. *ACM Computing Surveys*, *54*(7), 1–36. https://doi.org/10.1145/3462477

Instituto Nacional de Ciberseguridad. (2021). Balance de ciberseguridad 2021. https://www.incibe.es/sites/default/files/paginas/quehacemos/balance_ciberseguridad_2021_incibe.pdf

Kaspersky. (2021). *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021*. Blog Oficial De Kaspersky. https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Kasper, A., Osula, A. M., & Molnár, A. (2021). EU cybersecurity and cyber diplomacy. IDP Revista De Internet Derecho Y Política, 34, 1–15. https://doi.org/10.7238/idp.v0i34.387469

Kulinich, T., Andrushko, R., Prosovych, O., Sternyuk, O., & Tymchyna, Y. (2023) Enterprise Risk Management in an Uncertain Environment. International Journal of Professional Business Review, 8(4), e01700. https://doi.org/10.26668/businessreview/2023.v8i4.1700

Martinez, M., Ariza, G., & Rey, A. (2020). *El rol de los modelos en el aprendizaje organizacional y el diseño de políticas*. ResearchGate. https://www.researchgate.net/publication/339627880

Massa, R. M., Partyka, R., & Lana, J. (2020). *Behavioral agency research and theory: a review and research agenda*. *Cadernos Ebape.BR*, *18*(2). https://doi.org/10.1590/1679-395177017x

Massoni, A. (2022). *Resiliencia cibernética: la clave para mantener protegida tu organización*. Hacknoid. https://www.hacknoid.com/hacknoid/resiliencia-cibernetica-la-clave-para-mantener-protegida-tu-organizacion/

Merdassi, I., Ghazel, C., & Saidane, L. (2020). Surveying and Analyzing Security Issues in Mobile Cloud Computing. *2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks (PEMWN)*. https://doi.org/10.23919/pemwn50727.2020.9293077

Molina, C., & Rojas, I. (2021). Uso de herramientas TIC en investigación científica de los estudiantes de administración en la UNAS - Tingo María. *RevIA, 8*(5), 40–47. https://revistas.unas.edu.pe/index.php/revia/article/view/204/187

Molins, F., & Serrano, M. A. (2019). *Bases neurales de la aversión a las pérdidas en contextos económicos: revisión sistemática según las directrices PRISMA*. [Sncpharma.com]. https://sncpharma.com/wp-content/uploads/2019/02/Bases-neurales-de-la-aversión-a-las-pérdidas-en-contextos-económicos-revisión-sistemática-según-las-directrices-PRISMA.pdf

Munkøe, M., & Mölder, H. (2022). La ciberseguridad en la era de hipercompetitividad: ¿Puede la Unión europea afrontar los nuevos retos? *Revista CIDOB D'Afers Internacionals*, *131*, 69–94. https://doi.org/10.24241/rcai.2022.131.2.69

Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2019). M*etodología de la investigación cuantitativa-cualitativa y redacción de la tesis*. Ed. Ediciones de la U. ISBN 978-958-762-876-0.

Ogwara, N. O., Petrova, K., & Yang, M. (2019). Data Security Frameworks for Mobile Cloud Computing: A Comprehensive Review of the Literature. *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*. https://doi.org/10.1109/itnac46935.2019.9078007

Ormachea, J. (2020). *Estrategias Integradas de Ciberseguridad para el fortalecimiento de la Seguridad Nacional*. https://hdl.handle.net/20.500.13097/156

Osorio, D., Landínez, D., & Chica, J. (2022). Neuroeconomía y toma de decisiones financieras: aproximación desde una revisión sistemática de literatura. *Revista CEA*, *8*(16), e1911. https://doi.org/10.22430/24223182.1911

Panduro, E., & Sandoval, J. (2022). Gestión de riesgos para la seguridad de edificaciones públicas. *Revista Minerva*, *4*(3), 71–77. https://doi.org/10.5377/revminerva.v4i3.12950

Pawar, M., & Anuradha, J. (2015). Network Security and Types of Attacks in Network. *Procedia Computer Science*, *48*, 503–506. https://doi.org/10.1016/j.procs.2015.04.126

Penna, A. F., Gómez, R., & De Dios, J. (2023). La Ciberseguridad en México y los derechos humanos en la era digital. *Espacios Públicos, 23*(61). https://doi.org/10.36677/espaciospublicos.v23i61.21083

Pérez, G. (2023, March 6). *Coeficiente Alfa de Cronbach: ¿Qué es y para qué sirve el Alfa de Cronbach?* GPL Research. https://gplresearch.com/coeficiente-alfa-de-cronbach/

Poma, A., & Vargas, R. (2019). Problematic in cybersecurity as protection of computer system and social networks in Peru and the World. *SCIÉNDO*, *22*(4), 275–282. https://doi.org/10.17268/sciendo.2019.034

Pulido, A., Ruiz, A., & Ortiz, L. (2020). Mejora de procesos de producción a través de la gestión de riesgos y herramientas estadísticas. *Ingeniare. Revista Chilena De Ingeniería*, *28*(1), 56–67. https://doi.org/10.4067/s0718-33052020000100056

Qayyum, R., & Ejaz, H. (2020, April 8). Data Security in Mobile Cloud Computing: A State of the Art Review. *International Journal of Modern Education and Computer Science*, *12*(2), 30–35. https://doi.org/10.5815/ijmecs.2020.02.04

Quevedo, C. (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

Quiroga, J. (2021). Ciberseguridad y protección de datos personales en el Perú. *Advocatus*, *039*, 15–21. https://doi.org/10.26439/advocatus2021.n39.5114

Reuters. (2019). *North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report*. U.S. https://www.reuters.com/article/us-northkorea-cyber-unidUSKCN1UV1ZX

Ríos, J., Vásquez, R., & Mendoza, A. (2023). Métodos emergentes de auditoría en integridad de datos en la nube: una revisión sistemática de las últimas

tendencias. *Investigación & Desarrollo*, *23*(1). https://doi.org/10.23881/idupbo.023.1-8i

Shakatreh, M., Rumman, M. A. A., & Mugableh, M. I. (2023, January 31). Reviewing the Framework of Risk Management: Policy and Hedging. International Journal of Professional Business Review, 8(1), e0928. https://doi.org/10.26668/businessreview/2023.v8i1.928

Sheth, A., Bhosale, S., Kurupkar, F., & Prof, A. (2021). *Research Paper on Cyber Security*. *Contemporary research in India, 1*(1), 246 251 https://www.researchgate.net/publication/352477690

Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, *5*(3), 392–412. https://doi.org/10.1080/23738871.2020.1820546

Soto, J., & Rodríguez, D. (2019). A new approach to mathematical cryptography using the discrete ambiguity function. *Mathematics Magazine: Theory and Applications, 26*(2), 281–297. https://doi.org/10.15517/rmta.v26i2.38319

Torres, J., Vera, V., Zuzunaga, F., Talavera, J., & De La Cruz, J. (2022). Content validity by expert judgment of an instrument to measure knowledge, attitudes and practices about salt consumption in the peruvian population. *Revista De La Facultad De Medicina Humana*, *22*(2), 273–279. https://doi.org/10.25176/rfmh.v22i2.4768

Valverde Arcos, D. A., & Hurel Franco, G. P. (2021, October 24). Seguridad de la información de los reclamos en modalidad teletrabajo. RECIMUNDO, 5(4), 344–355. https://doi.org/10.26820/recimundo/5.(4).dic.2021.344-355

Vega, E. (2021). *Seguridad de la información*. Editorial Área de Innovación y Desarrollo S.L. https://doi.org/10.17993/tics.2021.4

Villasís, M., Márquez, H., Zurita, J., Miranda, M., & Escamilla, A. (2018). El protocolo de investigación VII. Validez y confiabilidad de las mediciones. *Revista Alergia México*, *65*(4), 414–421. https://doi.org/10.29262/ram.v65i4.560

Xie, L. (2019). Leadership and organizational learning culture: a systematic literature review. *European Journal of Training and Development*, *43*(1/2), 76–104. https://doi.org/10.1108/ejtd-06-2018-0056

ANEXOS

Anexo 1: Matriz de Consistencia

MATRIZ DE CONSISTENCIA

TITULO: Ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023.
AUTOR: Chuqui Sulca, Josue David

PROBLEMA	OBJETIVOS	HIPÓTESIS
Problema general ¿Cuál es la influencia de la Ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023? **Problemas específicos** P1. ¿Cuál es la influencia de la confidencialidad en la gestión de riesgos en una institución educativa, Callao 2023? P2. ¿Cuál es la influencia de la integridad en la gestión de riesgos en una institución educativa, Callao 2023? P3. ¿Cuál es la influencia de la disponibilidad en la gestión de riesgos en una institución educativa, Callao 2023?	**Objetivo general** Determinar la influencia de la Ciberseguridad en la gestión de riesgos en una institución educativa, Callao 2023. **Objetivos específicos** O1. Determinar la influencia de la confidencialidad en la gestión de riesgos en una institución educativa, Callao 2023. O2. Determinar la influencia de la integridad en la gestión de riesgos en una institución educativa, Callao 2023. O3. Determinar la influencia de la disponibilidad en la gestión de riesgos en una institución educativa, Callao 2023.	**Hipótesis general** La Ciberseguridad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023. **Hipótesis específicas** HE 1. La confidencialidad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023 HE2. La integridad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023 HE3. La disponibilidad influye significativamente en la gestión de riesgos en una institución educativa, Callao 2023

VARIABLES E INDICADORES

Variable independiente: Ciberseguridad

Dimensiones	Indicadores	Ítem	Escala	Nivel y rango
Confidencialidad	▪ Accesos no Autorizados ▪ Encriptación ▪ Incidentes de Pérdida de Datos	1 - 6	Escala ordinal. Opciones de respuesta: Nunca (1) Casi nunca (2) A veces (3) Casi siempre (4) Siempre (5)	Escasa [18-41] Regular [42-65] Adecuada [66-90]
Integridad	▪ Datos corruptos ▪ Tiempo promedio de restauración ▪ Registros de cambios registrados	7 - 12		
Disponibilidad	▪ Recuperación de desastres. ▪ Tiempo de inactividad no planificado. ▪ Capacidad de escalabilidad	13-18		

Variable dependiente: Gestión de riesgos

Dimensiones	**Indicadores**	**Ítems**	**Escalas**	**Nivel y rango**
Identificación de riesgos	▪ Riesgos identificados ▪ Categorización de riesgos ▪ Origen de riesgos	19-23	Escala: Ordinal Opciones de respuesta: Nunca (1) Casi nunca (2) A veces (3) Casi siempre (4) Siempre (5)	Escasa [16-36] Regular [37-58] Adecuada [59-80]
Evaluación de riesgos	▪ Índice de riesgo ▪ Análisis de sensibilidad ▪ Matriz de riesgos	24-29		
Mitigación del riesgo	▪ Eficiencia de las estrategias ▪ Reducción del riesgo ▪ Riesgos no identificados	30-34		

TIPO Y DISEÑO DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA	INSTRUMENTOS	ESTADÍSTICA
Enfoque: Cuantitativo Tipo: Aplicada Diseño: No experimental Nivel: Correlacional causal Método: Descriptiva e inferencial	**Población:** 30 trabajadores de una institución educativa.	**Variable 1:** Técnica: Cuestionario Instrumento: Cuestionario de Ciberseguridad Autor: Chuqui Sulca, Josue David (2023) **Variable 2**: Técnica: Cuestionario gestión de riesgos Autor: Chuqui Sulca, Josue David (2023)	**Estadística descriptiva:** Se consideró utilizar la distribución por frecuencias ya que nos permite la clasificación y conteo de los datos en categorías o intervalos, lo que facilita la identificación de patrones, tendencias y la dispersión en el conjunto de datos. **Estadística inferencial:** La determinación a la prueba a elegir, será paramétrica cuando tenga una distribución normal y será no paramétrica cuando los datos no se ajusten a una distribución normal.

Anexo 2: Operacionalización de variables

Tabla 17

Operacionalización de variables

Variable 1	Definición Conceptual	Definición Operacional	Dimensión	Indicadores	Escala de medición
Ciberseguridad	García y Pesántez (2023) describen la ciberseguridad como la identificación de amenazas, evaluación de medidas de seguridad y recomendación de acciones para proteger la información.	García y Pesántez (2023), se materializa como un proceso integral que involucra la meticulosa identificación de amenazas cibernéticas potenciales, seguida de una evaluación exhaustiva de las medidas de seguridad existentes.	Confidencialidad	▪ Accesos no Autorizados ▪ Encriptación ▪ Incidentes de Pérdida de Datos	Escala ordinal. Opciones de respuesta: Nunca (1) Casi nunca (2) A veces (3) Casi siempre (4) Siempre (5)
			Integridad	▪ Datos corruptos ▪ Tiempo promedio de restauración ▪ Registros de cambios registrados	
			Disponibilidad	▪ Recuperación de desastres. ▪ Tiempo de inactividad no planificado. ▪ Capacidad de escalabilidad	

Variable 2	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Niveles
Gestión de riesgos	Panduro y Sandoval (2022), el propósito es que las organizaciones gestionen riesgos para disminuir eventos adversos y aprovechar oportunidades que impacten positivamente en sus objetivos en áreas como finanzas, salud, educación, seguridad y tecnología.	Panduro y Sandoval (2022), consiste en un proceso mediante el cual las organizaciones identifican y enfrentan los riesgos tanto internos como externos. El objetivo es reducir la probabilidad de eventos negativos que puedan perjudicar el logro de sus metas, al mismo tiempo que buscan aprovechar las oportunidades que puedan tener un impacto positivo en áreas como finanzas, salud, seguridad y tecnología de la información	Identificación de riesgos	▪ Riesgos identificados ▪ Categorización de riesgos ▪ Origen de riesgos	Escala ordinal. Opciones de respuesta: Nunca (1) Casi nunca (2) A veces (3) Casi siempre (4) Siempre (5)
			Evaluación de riesgos	▪ Índice de riesgo ▪ Análisis de sensibilidad ▪ Matriz de riesgos	
			Mitigación del riesgo	▪ Eficiencia de las estrategias ▪ Reducción del riesgo ▪ Riesgos no identificados	

Anexo 3: Cuestionario de variable dependiente e independiente

Cuestionario de Ciberseguridad

El presente instrumento está elaborado por Josue David Chuqui Sulca, estudiante de la Maestría en Ingeniería de Sistemas, el instrumento se centra en dos variables cruciales: "Ciberseguridad" y "Gestión de Riesgos". Le pedimos que proporcione respuestas sinceras y basadas en sus experiencias laborales del último año. Sus aportes son fundamentales para nuestra investigación en el ámbito de la ciberseguridad y la gestión de riesgos. Sus datos contribuirán al avance en la comprensión de estos aspectos críticos. Agradecemos sinceramente su participación. Opciones de respuesta: nunca (1), casi nunca (2), a veces, (3) casi siempre (4), siempre (5).

Nº	Dimensiones / Ítems	Calificación				
		1	2	3	4	5
Confidencialidad						
1	La institución experimenta accesos no autorizados a sus sistemas informáticos					
2	La institución toma medidas para prevenir y detectar accesos no autorizados en su red					
3	La institución evalúa la efectividad de las políticas y procedimientos de seguridad de la información					
4	La institución realiza una encriptación adecuada para proteger los datos confidenciales en su infraestructura de TI					
5	Durante el año 2022, la institución ha experimentado incidentes de pérdida de datos					
6	Las prácticas actuales de su institución, garantizan la confidencialidad de la información					
Integridad						
7	La institución experimenta casos de corrupción de datos en sus sistemas					
8	Durante el año 2022, la institución ha registrado incidencias de corrupción de datos en sus sistemas					

9	La institución ha logrado restaurar los datos después de una incidencia de corrupción					
10	La institución ha logrado la restauración de la integridad de los datos en un tiempo no mayor a dos horas después de una incidencia					
11	La institución registra cambios o modificaciones en los registros de datos en sus sistemas					
12	La institución ha registrado modificaciones en los registros de datos en sus sistemas					
Disponibilidad						
13	La institución evalúa el tiempo de recuperación de datos ante un desastre					
14	La institución mide la eficacia de su sistema de recuperación de datos, contribuye a lograr una recuperación exitosa en situaciones de desastre.					
15	La institución ha experimentado tiempo de inactividad no planificado en su sistema.					
16	La institución mide el tiempo de inactividad no planificado en su sistema de ciberseguridad					
17	La institución realiza una evaluación de la capacidad de escalabilidad					
18	El sistema de ciberseguridad de su institución está preparado para adaptarse a las amenazas cibernéticas					

Cuestionario de Gestión de Riesgo

Nº	Dimensiones / Ítems	Calificación				
		1	2	3	4	5
Identificación de riesgos						
1	La institución lleva a cabo el proceso de identificación de riesgos ante posibles ataques cibernéticos					
2	La institución evalúa semanalmente la identificación de riesgos en sus sistemas de información					
3	La institución mide la frecuencia de ataques cibernéticos a sus sistemas de información					
4	La institución establece una gestión de riesgos en función al impacto en sus sistemas de información					
5	La institución registra los riesgos de posibles ataques cibernéticos					
Evaluación de riesgos						
6	La institución calcula el índice de riesgo en sus sistemas de información					
7	La institución evalúa el nivel de riesgo considerado bajo con una cierta frecuencia.					
8	La institución lleva un análisis de sensibilidad de los riesgos identificados					
9	La institución utiliza un análisis de sensibilidad para tomar decisiones estratégicas					
10	La institución actualiza la matriz de riesgos de manera regular					
11	La institución utiliza la matriz de riesgos, para comunicar los ataques cibernéticos a sus sistemas de información					
Mitigación del riesgo						
12	La institución experimenta eficiencia en las estrategias de mitigación de riesgos.					
13	Las estrategias de mitigación han logrado reducir eficazmente el riesgo de ataques cibernéticos					
14	La institución ha implementado estrategias de mitigación para reducir los riesgos de ataques cibernéticos					
15	La institución ha implementado estrategias de mitigación para reducir los riesgos de ataques cibernéticos					
16	La institución ha logrado reducir con éxito los riegos previamente identificados					

Anexo 4: Evaluación por juicio de expertos

Certificado de validación – Experto 1

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de Ciberseguridad". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	ROBERTO JUAN TEJADA RUIZ
Grado profesional:	Maestría (X) Doctorado ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	GESTION / SISTEMAS DE GESTION DE CALIDAD / LOGISTICA / MARKETING
Institución donde labora:	UTP
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	-

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de Ciberseguridad
Autor (a):	Chuqui Sulca, Josue David
Procedencia:	Perú
Administración:	Auto complementado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una institución educativa - Callao
Significación:	Nivel de significancia: 0.05

4. Soporte teórico

Variable	Dimensiones	Definición
Ciberseguridad	Confidencialidad	García y Pesántez (2023) describen la ciberseguridad como la identificación de amenazas, evaluación de medidas de seguridad y recomendación de acciones para proteger la información.
	Integridad	
	Disponibilidad	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de ciberseguridad elaborado por Josue David Chuqui Sulca en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

1. *No cumple con el criterio*
2. *Bajo Nivel*
3. *Moderado nivel*
4. *Alto nivel*

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE CIBERSEGURIDAD

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: Cuestionario de Ciberseguridad

- **Primera dimensión: Confidencialidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es salvaguardar la información sensible y crítica, garantizando que se mantenga protegida de accesos no autorizados.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Porcentaje de Accesos no Autorizados	1. La institución experimenta accesos no autorizados a sus sistemas informáticos				X				X				X	
	2. La institución toma medidas para prevenir y detectar accesos no autorizados en su red				X				X				X	
	3. La institución evalúa la efectividad de las políticas y procedimientos de seguridad de la información				X				X				X	
Nivel de Encriptación	4. La institución realiza una encriptación adecuada para proteger los datos confidenciales en su infraestructura de TI				X				X				X	
Número de Incidentes de Pérdida de Datos	5. En el último año, la institución ha experimentado incidentes de pérdida de datos				X				X				X	
	6. Las prácticas actuales de su institución, garantizan la confidencialidad de la información				X				X				X	

- **Segunda dimensión: Integridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es asegurar que los datos y la información se mantengan completos, precisos y no sean alterados de manera no autorizada o inapropiada.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Porcentaje de datos corruptos	7. La institución experimenta casos de corrupción de datos en sus sistemas				X				X				X	
	8. En el último año, la institución ha registrado incidencias de corrupción de datos en sus sistemas				X				X				X	
Tiempo promedio de restauración	9. La institución ha logrado restaurar los datos después de una incidencia de corrupción				X				X				X	
	10. La institución ha logrado la restauración de la integridad de los datos en un tiempo razonable después de una incidencia				X				X				X	
Porcentaje de registros de cambios registrados	11. La institución registra cambios o modificaciones en los registros de datos en sus sistemas				X				X				X	
	12. La institución ha registrado modificaciones en los registros de datos en sus sistemas				X				X				X	

- **Tercera dimensión: Disponibilidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es garantizar que los sistemas, servicios y datos críticos estén disponibles y accesibles cuando se necesiten.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Tiempo de recuperación de desastres.	13. La institución evalúa el tiempo de recuperación de datos ante un desastre				X				X				X	
	14. La institución mide la eficacia de su sistema de recuperación de datos, contribuye a lograr una recuperación exitosa en situaciones de desastre.				X				X				X	
Porcentaje de tiempo de inactividad no planificado	15. La institución ha experimentado tiempo de inactividad no planificado en su sistema.				X				X				X	
	16. La institución mide el tiempo de inactividad no planificado en su sistema de ciberseguridad				X				X				X	

Capacidad de escalabilidad	17. La institución realiza una evaluación de la capacidad de escalabilidad				X				X				X		
	18. El sistema de ciberseguridad de su institución está preparado para adaptarse a las amenazas cibernéticas				X				X				X		

Roberto Juan Tejada Ruiz

Firma del evaluador

DNI: 17930425

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de Gestión de Riesgos". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	ROBERTO JUAN TEJADA RUIZ
Grado profesional:	Maestría (X) Doctorado ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	GESTION / SISTEMAS DE GESTION DE CALIDAD / LOGISTICA / MARKETING
Institución donde labora:	UTP
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	-

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de Gestión de Riesgos
Autor (a):	Chuqui Sulca, Josue David
Procedencia:	Perú
Administración:	Auto complementado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una institución educativa - Callao
Significación:	Nivel de significancia: 0.05

4. Soporte teórico

Variable	Dimensiones	Definición
Gestión de Riesgos	Identificación de riesgos	Panduro-Alvarado y Sandoval-Ríos (2022), el propósito es que las organizaciones gestionen riesgos para disminuir eventos adversos y aprovechar oportunidades que impacten positivamente en sus objetivos en áreas como finanzas, salud, educación, seguridad y tecnología.
	Evaluación de riesgos	
	Mitigación del riesgo	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de gestión de riesgos elaborado por Josue David, Chuqui Sulca en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. *No cumple con el criterio*
2. *Bajo Nivel*
3. *Moderado nivel*
4. *Alto nivel*

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE GESTIÓN DE RIESGOS

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: Cuestionario de Gestión de Riesgos

- **Primera dimensión: Identificación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es conocer y evaluar los posibles riesgos a los que una institución o sistema puede estar expuesta.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Número de riesgos identificados	1. La institución lleva a cabo el proceso de identificación de riesgos ante posibles ataques cibernéticos				X				X				X	
	2. La institución evalúa constantemente la identificación de riesgos en sus sistemas de información				X				X				X	
Categorización de riesgos	3. La institución mide la frecuencia de ataques cibernéticos a sus sistemas de información				X				X				X	
	4. La institución establece una clara gestión de riesgos en función al impacto en sus sistemas de información				X				X				X	
Origen de riesgos	5. La institución registra los riesgos de posibles ataques cibernéticos				X				X				X	

- **Segunda dimensión: Evaluación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es analizar y comprender de manera más profunda los riesgos previamente identificados en una institución educativa.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Índice de riesgo	6. La institución calcula el índice de riesgo en sus sistemas de información				X				X				X	
	7. La institución evalúa el nivel de riesgo considerado bajo con una cierta frecuencia.				X				X				X	
Análisis de sensibilidad	8. La institución lleva un análisis de sensibilidad de los riesgos identificados				X				X				X	
	9. La institución utiliza un análisis de sensibilidad para tomar decisiones estratégicas				X				X				X	
Matriz de riesgos	10. La institución actualiza la matriz de riesgos de manera regular				X				X				X	
	11. La institución utiliza la matriz de riesgos, para comunicar los ataques cibernéticos a sus sistemas de información				X				X				X	

- **Tercera dimensión: Mitigación del riesgo**
- Objetivos de la Dimensión: El objetivo de esta dimensión es la implementación de acciones y estrategias destinadas a reducir o controlar los riesgos previamente identificados y evaluados en una institución.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Eficiencia de las estrategias	12. La institución experimenta eficiencia en las estrategias de mitigación de riesgos.				X				X				X	
	13. Las estrategias de mitigación han logrado reducir eficazmente el riesgo de ataques cibernéticos				X				X				X	
Reducción del riesgo	14. La institución ha implementado estrategias de mitigación para reducir los riesgos de ataques cibernéticos				X				X				X	
	15. La institución ha implementado estrategias de mitigación para reducir los riesgos de ataques cibernéticos				X				X				X	
Riesgos no identificados	16. La institución registra riesgos de ataques cibernéticos que no habían sido previamente identificados				X				X				X	

Roberto Juan Tejada Ruiz

Firma del evaluador

DNI: 17930425

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
TEJADA RUIZ, ROBERTO JUAN **DNI 17930425**	**INGENIERO INDUSTRIAL** **Fecha de diploma:** Modalidad de estudios: -	UNIVERSIDAD NACIONAL DE TRUJILLO ***PERU***
TEJADA RUIZ, ROBERTO JUAN **DNI 17930425**	**BACHILLER EN INGENIERIA INDUSTRIAL** **Fecha de diploma:** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL DE TRUJILLO ***PERU***
TEJADA RUIZ, ROBERTO JUAN **DNI 17930425**	**MAESTRO EN CIENCIAS DE LA EDUCACION CON MENCION EN GERENCIA EDUCATIVA ESTRATEGICA** **Fecha de diploma: 02/06/20** Modalidad de estudios: PRESENCIAL Fecha matrícula: 26/01/2004 Fecha egreso: 05/05/2006	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO ***PERU***

Certificado de validación – Experto 2

ESCUELA DE POSTGRADO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de Ciberseguridad". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Jonathan Alexis Puente Zamora
Grado profesional:	Maestría (x) Doctorado ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional ( )
Áreas de experiencia profesional:	Docente de Posgrado
Institución donde labora:	Universidad Cesar Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación Psicométrica: (si corresponde)	-

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de Ciberseguridad
Autor (a):	Chuqui Sulca, Josue David
Procedencia:	Perú
Administración:	Auto complementado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una institución educativa - Callao
Significación:	Nivel de significancia: 0.05

4. Soporte teórico

Variable	Dimensiones	Definición
Ciberseguridad	Confidencialidad	García y Pesántez (2023) describen la ciberseguridad como la identificación de amenazas, evaluación de medidas de seguridad y recomendación de acciones para proteger la información.
	Integridad	
	Disponibilidad	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de ciberseguridad elaborado por Josue David Chuqui Sulca en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

1. *No cumple con el criterio*
2. *Bajo Nivel*
3. *Moderado nivel*
4. *Alto nivel*

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE CIBERSEGURIDAD

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: Cuestionario de Ciberseguridad

- **Primera dimensión: Confidencialidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es salvaguardar la información sensible y crítica, garantizando que se mantenga protegida de accesos no autorizados.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Porcentaje de Accesos no Autorizados	1. La institución experimenta accesos no autorizados a sus sistemas informáticos				x				x				x	
	2. La institución toma medidas para prevenir y detectar accesos no autorizados en su red				x				x				x	
	3. La institución evalúa la efectividad de las políticas y procedimientos de seguridad de la información				x				x				x	
Nivel de Encriptación	4. La institución realiza una encriptación adecuada para proteger los datos confidenciales en su infraestructura de TI				x				x				x	
Número de Incidentes de Pérdida de Datos	5. Durante el año 2022, la institución ha experimentado incidentes de pérdida de datos				x				x				x	
	6. Las prácticas actuales de su institución, garantizan la confidencialidad de la información				x				x				x	

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

- **Segunda dimensión: Integridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es asegurar que los datos y la información se mantengan completos, precisos y no sean alterados de manera no autorizada o inapropiada.

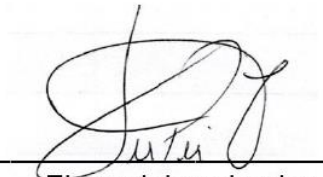
Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Porcentaje de datos corruptos	7. La institución experimenta casos de corrupción de datos en sus sistemas				X				X				X	
	8. Durante el año 2022, la institución ha registrado incidencias de corrupción de datos en sus sistemas				X				X				X	
Tiempo promedio de restauración	9. La institución ha logrado restaurar los datos después de una incidencia de corrupción				X				X				X	
	10. La institución ha logrado la restauración de la integridad de los datos en un tiempo no mayor a dos horas después de una incidencia				X				X				X	
Porcentaje de registros de cambios registrados	11. La institución registra cambios o modificaciones en los registros de datos en sus sistemas				X				X				X	
	12. La institución ha registrado modificaciones en los registros de datos en sus sistemas				X				X				X	

- **Tercera dimensión: Disponibilidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es garantizar que los sistemas, servicios y datos críticos estén disponibles y accesibles cuando se necesiten.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Tiempo de recuperación de desastres.	13. La institución evalúa el tiempo de recuperación de datos ante un desastre				X				X				X	
	14. La institución mide la eficacia de su sistema de recuperación de datos, contribuye a lograr una recuperación exitosa en situaciones de desastre.				X				X				X	
Porcentaje de tiempo de inactividad no planificado	15. La institución ha experimentado tiempo de inactividad no planificado en su sistema.				X				X				X	
	16. La institución mide el tiempo de inactividad no planificado en su sistema de ciberseguridad				X				X				X	

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

Capacidad de escalabilidad	17. La institución realiza una evaluación de la capacidad de escalabilidad				X				X				X		
	18. El sistema de ciberseguridad de su institución está preparado para adaptarse a las amenazas cibernéticas				X				X				X		



Firma del evaluador
DNI:

ESCUELA DE POSTGRADO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de Gestión de Riesgos". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Jonathan Alexis Puente Zamora
Grado profesional:	Maestría (X) Doctorado ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional ( )
Áreas de experiencia profesional:	Docencia
Institución donde labora:	Universidad Cesar Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación Psicométrica: (si corresponde)	-

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de Gestión de Riesgos
Autor (a):	Chuqui Sulca, Josue David
Procedencia:	Perú
Administración:	Auto complementado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una institución educativa - Callao
Significación:	Nivel de significancia: 0.05

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

4. Soporte teórico

Variable	Dimensiones	Definición
Gestión de Riesgos	Identificación de riesgos	Panduro-Alvarado y Sandoval-Ríos (2022), el propósito es que las organizaciones gestionen riesgos para disminuir eventos adversos y aprovechar oportunidades que impacten positivamente en sus objetivos en áreas como finanzas, salud, educación, seguridad y tecnología.
	Evaluación de riesgos	
	Mitigación del riesgo	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de gestión de riesgos elaborado por Josue David, Chuqui Sulca en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. *No cumple con el criterio*
2. *Bajo Nivel*
3. *Moderado nivel*
4. *Alto nivel*

ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE GESTIÓN DE RIESGOS

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: Cuestionario de Gestión de Riesgos

- **Primera dimensión: Identificación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es conocer y evaluar los posibles riesgos a los que una institución o sistema puede estar expuesta.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Número de riesgos identificados	1. La institución lleva a cabo el proceso de identificación de riesgos ante posibles ataques cibernéticos				X				X				X	
	2. La institución evalúa semanalmente la identificación de riesgos en sus sistemas de información				X				X				X	
Categorización de riesgos	3. La institución mide la frecuencia de ataques cibernéticos a sus sistemas de información				X				X				X	
	4. La institución establece una gestión de riesgos en función al impacto en sus sistemas de información				X				X				X	
Origen de riesgos	5. La institución registra los riesgos de posibles ataques cibernéticos				X				X				X	

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

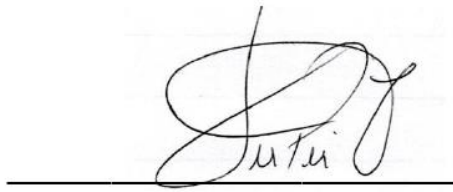
- **Segunda dimensión: Evaluación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es analizar y comprender de manera más profunda los riesgos previamente identificados en una institución educativa.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Índice de riesgo	6. La institución calcula el índice de riesgo en sus sistemas de información				X				X				X	
	7. La institución evalúa el nivel de riesgo considerado bajo con una cierta frecuencia.				X				X				X	
Análisis de sensibilidad	8. La institución lleva un análisis de sensibilidad de los riesgos identificados				X				X				X	
	9. La institución utiliza un análisis de sensibilidad para tomar decisiones estratégicas				X				X				X	
Matriz de riesgos	10. La institución actualiza la matriz de riesgos de manera regular				X				X				X	
	11. La institución utiliza la matriz de riesgos, para comunicar los ataques cibernéticos a sus sistemas de información				X				X				X	

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

- **Tercera dimensión: Mitigación del riesgo**
- Objetivos de la Dimensión: El objetivo de esta dimensión es la implementación de acciones y estrategias destinadas a reducir o controlar los riesgos previamente identificados y evaluados en una institución.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Eficiencia de las estrategias	12. La institución experimenta eficiencia en las estrategias de mitigación de riesgos.				X				X				X	
	13. Las estrategias de mitigación han logrado reducir eficazmente el riesgo de ataques cibernéticos				X				X				X	
Reducción del riesgo	14. La institución ha implementado estrategias de mitigación para reducir los riesgos de ataques cibernéticos				X				X				X	
	15. La institución ha logrado reducir con éxito los riegos previamente identificados				X				X				X	
Riesgos no identificados	16. La institución registra riesgos de ataques cibernéticos que no habían sido previamente identificados				X				X				X	



Firma del evaluador
DNI:

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
PUENTE ZAMORA, JONATHAN ALEXIS **DNI 44268195**	**INGENIERO DE SISTEMAS** **Fecha de diploma: 06/05/2014** Modalidad de estudios: -	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***
PUENTE ZAMORA, JONATHAN ALEXIS **DNI 44268195**	**BACHILLER EN INGENIERIA DE SISTEMAS** **Fecha de diploma: 03/12/2013** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***
PUENTE ZAMORA, JONATHAN ALEXIS **DNI 44268195**	**MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN** **Fecha de diploma: 17/06/19** Modalidad de estudios: PRESENCIAL Fecha matrícula: 14/10/2016 Fecha egreso: 20/01/2019	UNIVERSIDAD CÉSAR VALLEJO S.A.C. ***PERU***

Certificado de validación – Experto 3

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de Ciberseguridad". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer de la ciberseguridad. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Manuel Antonio Pereyra Acosta
Grado profesional:	Maestría ( ) Doctorado (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Campo de la ciberseguridad en una institución publica
Institución donde labora:	Universidad Cesar Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de Ciberseguridad
Autor (a):	Chuqui Sulca, Josue David
Procedencia:	Perú
Administración:	Auto complementado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una institución educativa - Callao
Significación:	Nivel de significancia: 0.05

4. Soporte teórico

Variable	Dimensiones	Definición
Ciberseguridad	Confidencialidad	García y Pesántez (2023) describen la ciberseguridad como la identificación de amenazas, evaluación de medidas de seguridad y recomendación de acciones para proteger la información.
	Integridad	
	Disponibilidad	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de ciberseguridad elaborado por Josue David Chuqui Sulca en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

1. *No cumple con el criterio*
2. *Bajo Nivel*
3. *Moderado nivel*
4. *Alto nivel*

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE CIBERSEGURIDAD

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: Cuestionario de Ciberseguridad

- **Primera dimensión: Confidencialidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es salvaguardar la información sensible y crítica, garantizando que se mantenga protegida de accesos no autorizados.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Porcentaje de Accesos no Autorizados	1. La institución experimenta accesos no autorizados a sus sistemas informáticos				x				x				x	
	2. La institución toma medidas para prevenir y detectar accesos no autorizados en su red				x				x				x	
	3. La institución evalúa la efectividad de las políticas y procedimientos de seguridad de la información				x				x				x	
Nivel de Encriptación	4. La institución realiza una encriptación adecuada para proteger los datos confidenciales en su infraestructura de TI				x				x				x	
Número de Incidentes de Pérdida de Datos	5. En el último año, la institución ha experimentado incidentes de pérdida de datos				x				x				x	
	6. Las prácticas actuales de su institución, garantizan la confidencialidad de la información				x				x				x	

- **Segunda dimensión: Integridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es asegurar que los datos y la información se mantengan completos, precisos y no sean alterados de manera no autorizada o inapropiada.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Porcentaje de datos corruptos	7. La institución experimenta casos de corrupción de datos en sus sistemas				x				x				x	
	8. En el último año, la institución ha registrado incidencias de corrupción de datos en sus sistemas				x				x				x	
Tiempo promedio de restauración	9. La institución ha logrado restaurar los datos después de una incidencia de corrupción				x				x				x	
	10. La institución ha logrado la restauración de la integridad de los datos en un tiempo razonable después de una incidencia				x				x				x	
Porcentaje de registros de cambios registrados	11. La institución registra cambios o modificaciones en los registros de datos en sus sistemas				x				x				x	
	12. La institución ha registrado modificaciones en los registros de datos en sus sistemas				x				x				x	

- **Tercera dimensión: Disponibilidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es garantizar que los sistemas, servicios y datos críticos estén disponibles y accesibles cuando se necesiten.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Tiempo de recuperación de desastres.	13. La institución evalúa el tiempo de recuperación de datos ante un desastre				x				x				x	
	14. La institución mide la eficacia de su sistema de recuperación de datos, contribuye a lograr una recuperación exitosa en situaciones de desastre.				x				x				x	
Porcentaje de tiempo de inactividad no planificado	15. La institución ha experimentado tiempo de inactividad no planificado en su sistema.				x				x				x	
	16. La institución mide el tiempo de inactividad no planificado en su sistema de ciberseguridad				x				x				x	

Capacidad de escalabilidad	17. La institución realiza una evaluación de la capacidad de escalabilidad				x				x				x	
	18. El sistema de ciberseguridad de su institución está preparado para adaptarse a las amenazas cibernéticas				x				x				x	

Firma del evaluador
DNI: 07268839

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de Gestión de Riesgos". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer de la ciberseguridad. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Manuel Antonio Pereyra Acosta
Grado profesional:	Maestría ( ) Doctorado (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Campo de la ciberseguridad en una institución publica
Institución donde labora:	Universidad Cesar Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de Gestión de Riesgos
Autor (a):	Chuqui Sulca, Josue David
Procedencia:	Perú
Administración:	Auto complementado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una institución educativa - Callao
Significación:	Nivel de significancia: 0.05

4. Soporte teórico

Variable	Dimensiones	Definición
Gestión de Riesgos	Identificación de riesgos	Panduro-Alvarado y Sandoval-Ríos (2022), el propósito es que las organizaciones gestionen riesgos para disminuir eventos adversos y aprovechar oportunidades que impacten positivamente en sus objetivos en áreas como finanzas, salud, educación, seguridad y tecnología.
	Evaluación de riesgos	
	Mitigación del riesgo	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de gestión de riesgos elaborado por Josue David, Chuqui Sulca en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. *No cumple con el criterio*
2. *Bajo Nivel*
3. *Moderado nivel*
4. *Alto nivel*

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE GESTIÓN DE RIESGOS

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: Cuestionario de Gestión de Riesgos

- **Primera dimensión: Identificación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es conocer y evaluar los posibles riesgos a los que una institución o sistema puede estar expuesta.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Número de riesgos identificados	1. La institución lleva a cabo el proceso de identificación de riesgos ante posibles ataques cibernéticos				x				x				x	
	2. La institución evalúa constantemente la identificación de riesgos en sus sistemas de información				x				x				x	
Categorización de riesgos	3. La institución mide la frecuencia de ataques cibernéticos a sus sistemas de información				x				x				x	
	4. La institución establece una clara gestión de riesgos en función al impacto en sus sistemas de información				x				x				x	
Origen de riesgos	5. La institución registra los riesgos de posibles ataques cibernéticos				x				x				x	

- **Segunda dimensión: Evaluación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es analizar y comprender de manera más profunda los riesgos previamente identificados en una institución educativa.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Índice de riesgo	6. La institución calcula el índice de riesgo en sus sistemas de información				x				x				x	
	7. La institución evalúa el nivel de riesgo considerado bajo con una cierta frecuencia.				x				x				x	
Análisis de sensibilidad	8. La institución lleva un análisis de sensibilidad de los riesgos identificados				x				x				x	
	9. La institución utiliza un análisis de sensibilidad para tomar decisiones estratégicas				x				x				x	
Matriz de riesgos	10. La institución actualiza la matriz de riesgos de manera regular				x				x				x	
	11. La institución utiliza la matriz de riesgos, para comunicar los ataques cibernéticos a sus sistemas de información				x				x				x	

- **Tercera dimensión: Mitigación del riesgo**
- Objetivos de la Dimensión: El objetivo de esta dimensión es la implementación de acciones y estrategias destinadas a reducir o controlar los riesgos previamente identificados y evaluados en una institución.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Eficiencia de las estrategias	12. La institución experimenta eficiencia en las estrategias de mitigación de riesgos.				x				x				x	
	13. Las estrategias de mitigación han logrado reducir eficazmente el riesgo de ataques cibernéticos				x				x				x	
Reducción del riesgo	14. La institución ha implementado estrategias de mitigación para reducir los riesgos de ataques cibernéticos				x				x				x	
	15. La institución ha implementado estrategias de mitigación para reducir los riesgos de ataques cibernéticos				x				x				x	
Riesgos no identificados	16. La institución registra riesgos de ataques cibernéticos que no habían sido previamente identificados				x				x				x	

Firma del evaluador
DNI: 07268839

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
PEREYRA ACOSTA, MANUEL ANTONIO **DNI 07268839**	**MAESTRO EN INGENIERIA DE SISTEMAS** **Fecha de diploma: 23/07/2013** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***
PEREYRA ACOSTA, MANUEL ANTONIO **DNI 07268839**	**LICENCIADO EN CIENCIAS DE LA ADMINISTRACION AEROESPACIAL** **Fecha de diploma: 09/08/2011** Modalidad de estudios: -	ESCUELA DE OFICIALES DE LA FUERZA AÉREA DEL PERÚ ***PERU***
PEREYRA ACOSTA, MANUEL ANTONIO **DNI 07268839**	**INGENIERO DE COMPUTACION Y SISTEMAS** **Fecha de diploma: 04/11/2005** Modalidad de estudios: -	UNIVERSIDAD DE SAN MARTÍN DE PORRES ***PERU***
PEREYRA ACOSTA, MANUEL ANTONIO **DNI 07268839**	**BACHILLER EN CIENCIAS DE LA ADMINISTRACION AEROESPACIAL** **Fecha de diploma: 09/12/2010** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	ESCUELA DE OFICIALES DE LA FUERZA AÉREA DEL PERÚ ***PERU***
PEREYRA ACOSTA, MANUEL ANTONIO **DNI 07268839**	**MAGÍSTER EN GOBIERNO Y POLÍTICAS PÚBLICAS** **Fecha de diploma: 11/03/20** Modalidad de estudios: PRESENCIAL Fecha matrícula: 18/03/2019 Fecha egreso: 19/02/2020	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ ***PERU***
PEREYRA ACOSTA, MANUEL ANTONIO **DNI 07268839**	**DOCTOR EN GESTIÓN PÚBLICA Y GOBERNABILIDAD** **Fecha de diploma: 10/11/21** Modalidad de estudios: PRESENCIAL Fecha matrícula: 03/08/2018 Fecha egreso: 08/08/2021	UNIVERSIDAD CÉSAR VALLEJO S.A.C. ***PERU***

Anexo 5: Confiabilidad

Tabla 19

Análisis de confiabilidad

Instrumento	Alfa de cronbach	Nº elementos
Cuestionario de ciberseguridad	0,831	18
Cuestionario de gestión de riesgos	0,960	16

Figura 1

Grados de confiabilidad del coeficiente Alfa de cronbach

Alfa de Cronbach	Consistencia Interna
$\alpha \geq 0,9$	Excelente
$0,8 \leq \alpha < 0,9$	Buena
$0,7 \leq \alpha < 0,8$	Aceptable
$0,6 \leq \alpha < 0,7$	Cuestionable
$0,5 \leq \alpha < 0,6$	Pobre
$\alpha < 0,5$	Inaceptable

Nota. Análisis de confiabilidad (Pérez-León, 2023).

Según la tabla 19 de análisis de confiabilidad, podemos concluir que ambos instrumentos cumplen con el nivel de confiabilidad esperado. En particular, al examinar el cuestionario de ciberseguridad, notamos que el coeficiente alfa de Cronbach es 0,831, indicando un nivel de confiabilidad considerado como "bueno". Del mismo modo, al analizar el cuestionario de gestión de riesgos, se destaca que el coeficiente alfa de Cronbach es 0,960, lo cual refleja un nivel de confiabilidad clasificado como "excelente".

Figura 2

Análisis de confiabilidad del cuestionario de ciberseguridad

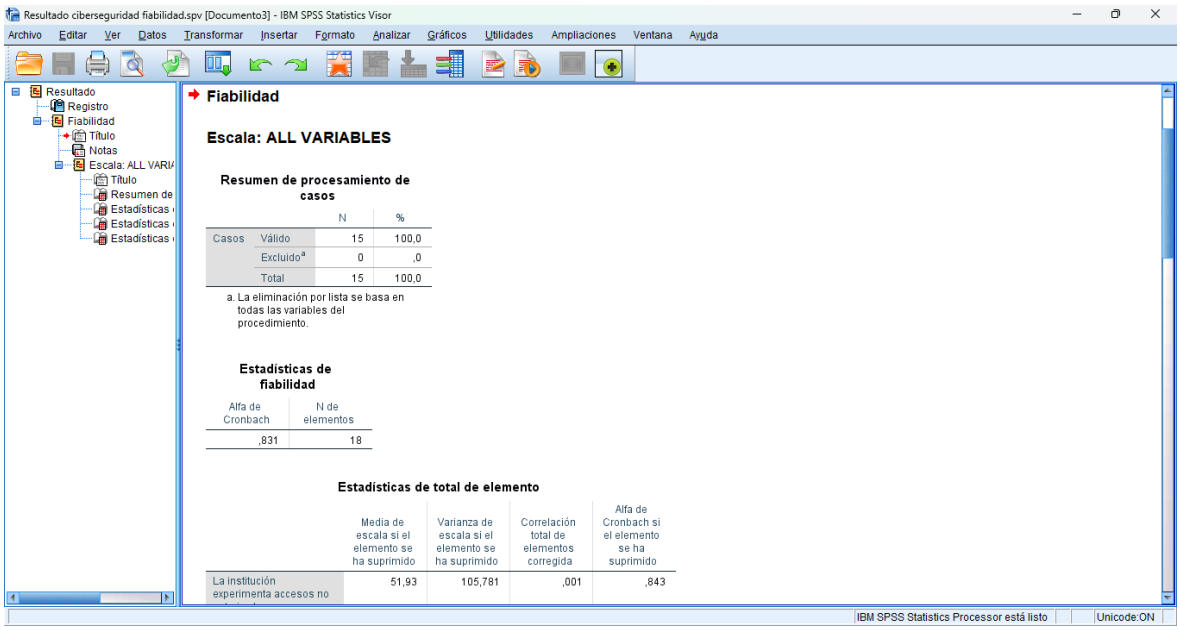


Figura 3

Análisis de confiabilidad del cuestionario de gestión de riesgos

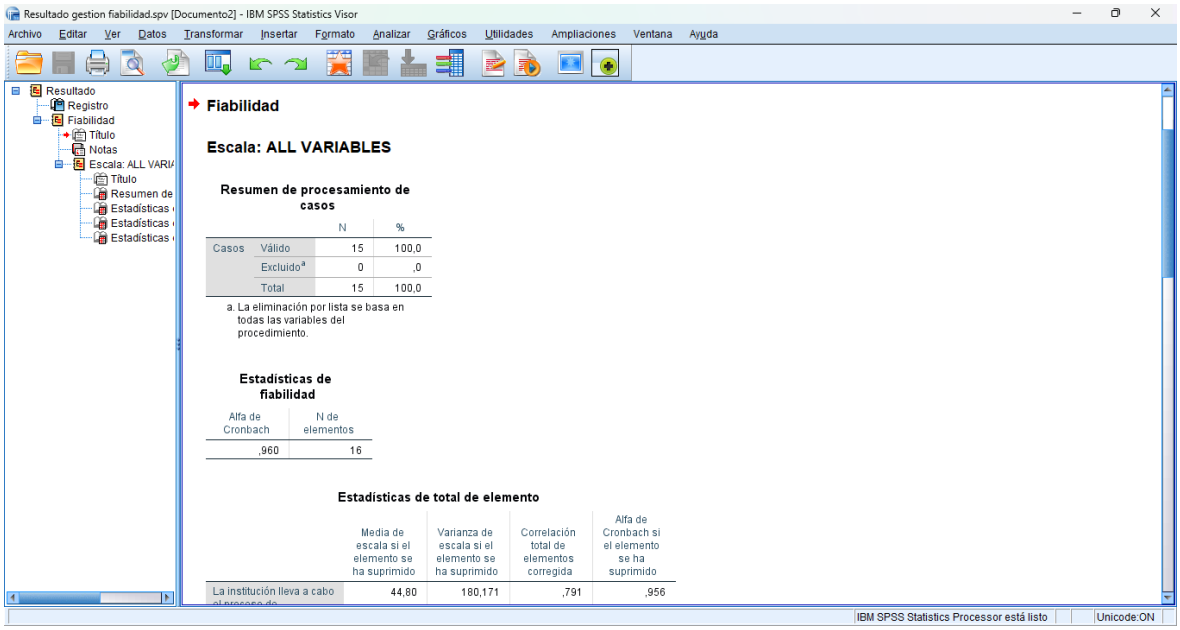
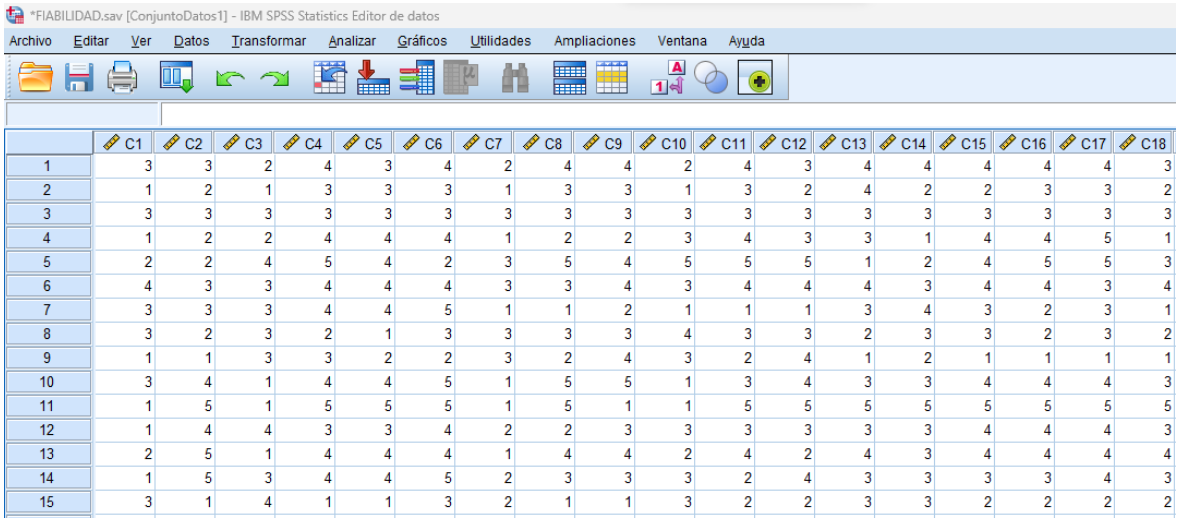


Figura 4

Base de datos prueba piloto del cuestionario de ciberseguridad

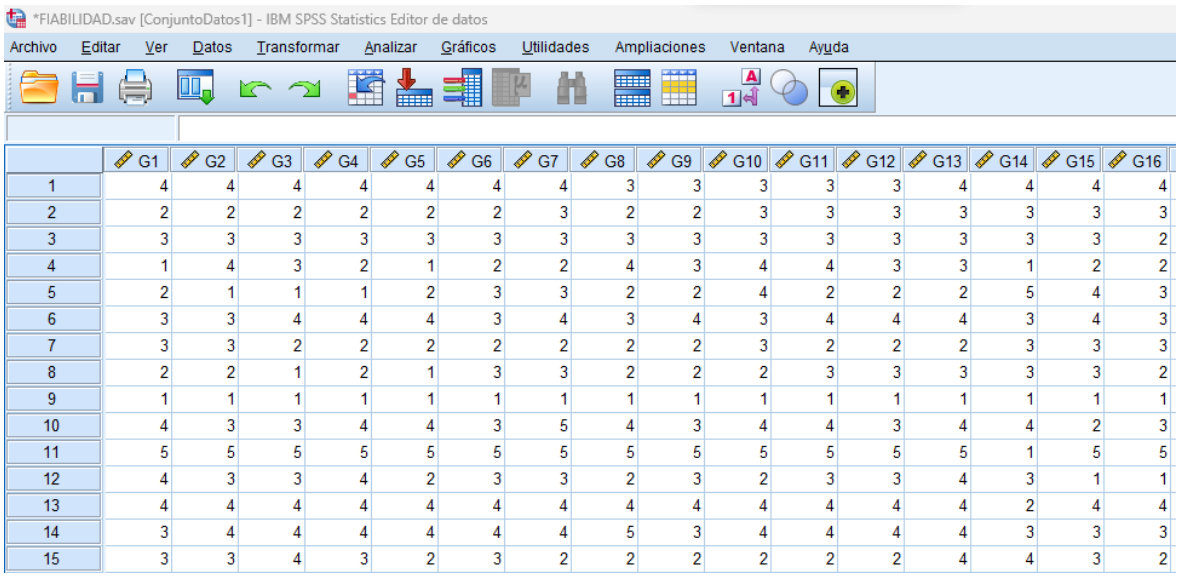

*FIABILIDAD.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18
1	3	3	2	4	3	4	2	4	4	2	4	3	4	4	4	4	4	3
2	1	2	1	3	3	3	1	3	3	1	3	2	4	2	2	3	3	2
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
4	1	2	2	4	4	4	1	2	2	3	4	3	3	1	4	4	5	1
5	2	2	4	5	4	2	3	5	4	5	5	5	1	2	4	5	5	3
6	4	3	3	4	4	4	3	3	4	3	4	4	4	3	4	4	3	4
7	3	3	3	4	4	5	1	1	2	1	1	1	3	4	3	2	3	1
8	3	2	3	2	1	3	3	3	3	4	3	3	2	3	3	2	3	2
9	1	1	3	3	2	2	3	2	4	3	2	4	1	2	1	1	1	1
10	3	4	1	4	4	5	1	5	5	1	3	4	3	3	4	4	4	3
11	1	5	1	5	5	5	1	5	1	1	5	5	5	5	5	5	5	5
12	1	4	4	3	3	4	2	2	3	3	3	3	3	3	4	4	4	3
13	2	5	1	4	4	4	1	4	4	2	4	2	4	3	4	4	4	4
14	1	5	3	4	4	5	2	3	3	3	2	4	3	3	3	3	4	3
15	3	1	4	1	1	3	2	1	1	3	2	2	3	3	2	2	2	2

Figura 5

Base de datos prueba piloto del cuestionario de gestión de riesgos


*FIABILIDAD.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16
1	4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	4
2	2	2	2	2	2	2	3	2	2	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2
4	1	4	3	2	1	2	2	4	3	4	4	3	3	1	2	2
5	2	1	1	1	2	3	3	2	2	4	2	2	2	5	4	3
6	3	3	4	4	4	3	4	3	4	3	4	4	4	3	4	3
7	3	3	2	2	2	2	2	2	2	3	2	2	2	3	3	3
8	2	2	1	2	1	3	3	2	2	2	3	3	3	3	3	2
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	4	3	3	4	4	3	5	4	3	4	4	3	4	4	2	3
11	5	5	5	5	5	5	5	5	5	5	5	5	5	1	5	5
12	4	3	3	4	2	3	3	2	3	2	3	3	4	3	1	1
13	4	4	4	4	4	4	4	4	4	4	4	4	4	2	4	4
14	3	4	4	4	4	4	4	5	3	4	4	4	4	3	3	3
15	3	3	4	3	2	3	2	2	2	2	2	2	4	4	3	2

Figura 6

Base de datos ciberseguridad

DISPONIBILIDAD						CONFIDENCIALIDAD						INTEGRIDAD									
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	d1v1	d2v1	d3v1	v1
3	3	2	4	3	4	2	4	4	2	4	3	4	4	4	4	4	3	19	19	23	61
1	2	1	3	3	3	1	3	3	1	3	2	4	2	2	3	3	2	13	13	16	42
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	18	18	18	54
1	2	2	4	4	4	1	2	2	3	4	3	3	1	4	4	5	1	17	15	18	50
2	2	4	5	4	2	3	5	4	5	5	5	1	2	4	5	5	3	19	27	20	66
4	3	3	4	4	4	3	3	4	3	4	4	4	3	4	4	3	4	22	21	22	65
3	3	3	4	4	5	1	1	2	1	1	1	3	4	3	2	3	1	22	7	16	45
3	2	3	2	1	3	3	3	3	4	3	3	2	3	3	2	3	2	14	19	15	48
1	1	3	3	2	2	3	2	4	3	2	4	1	2	1	1	1	1	12	18	7	37
3	4	1	4	4	5	1	5	5	1	3	4	3	3	4	4	4	3	21	19	21	61
1	5	1	5	5	5	1	5	1	1	5	5	5	5	5	5	5	5	22	18	30	70
1	4	4	3	3	4	2	2	3	3	3	3	3	3	4	4	4	3	19	16	21	56
2	5	1	4	4	4	1	4	4	2	4	2	4	3	4	4	4	4	20	17	23	60
1	5	3	4	4	5	2	3	3	3	2	4	3	3	3	3	4	3	22	17	19	58
3	1	4	1	1	3	2	1	1	3	2	2	3	3	2	2	2	2	13	11	14	38
3	3	2	4	3	4	2	4	4	2	4	3	4	4	4	4	4	3	19	19	23	61
1	2	1	3	3	3	1	3	3	1	3	2	4	2	2	3	3	2	13	13	16	42
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	18	18	18	54
1	2	2	4	4	4	1	2	2	3	4	3	3	1	4	4	5	1	17	15	18	50
2	2	4	5	4	2	3	5	4	5	5	5	1	2	4	5	5	3	19	27	20	66
4	3	3	4	4	4	3	3	4	3	4	4	4	3	4	4	3	4	22	21	22	65
3	3	3	4	4	5	1	1	2	1	1	1	3	4	3	2	3	1	22	7	16	45
3	2	3	2	1	3	3	3	3	4	3	3	2	3	3	2	3	2	14	19	15	48
1	1	3	3	2	2	3	2	4	3	2	4	1	2	1	1	1	1	12	18	7	37
3	4	1	4	4	5	1	5	5	1	3	4	3	3	4	4	4	3	21	19	21	61
1	5	1	5	5	5	1	5	1	1	5	5	5	5	5	5	5	5	22	18	30	70
1	4	4	3	3	4	2	2	3	3	3	3	3	3	4	4	4	3	19	16	21	56
2	5	1	4	4	4	1	4	4	2	4	2	4	3	4	4	4	4	20	17	23	60
1	5	3	4	4	5	2	3	3	3	2	4	3	3	3	3	4	3	22	17	19	58
3	1	4	1	1	3	2	1	1	3	2	2	3	3	2	2	2	2	13	11	14	38

Figura 7

Base de datos gestión de riesgos

Identificación de riesgos					Evaluación de riesgos						Mitigación del riesgo								
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	d1v2	d2v2	d3v2	v2
4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	4	20	20	19	59
2	2	2	2	2	2	3	2	2	3	3	3	3	3	3	3	10	15	15	40
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	15	18	14	47
1	4	3	2	1	2	2	4	3	4	4	3	3	1	2	2	11	19	11	41
2	1	1	1	2	3	3	2	2	4	2	2	2	5	4	3	7	16	16	39
3	3	4	4	4	3	4	3	4	3	4	4	4	3	4	3	18	21	18	57
3	3	2	2	2	2	2	2	2	3	2	2	2	3	3	3	12	13	13	38
2	2	1	2	1	3	3	2	2	2	3	3	3	3	3	2	8	15	14	37
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	6	5	16
4	3	3	4	4	3	5	4	3	4	4	3	4	4	2	3	18	23	16	57
5	5	5	5	5	5	5	5	5	5	5	5	5	1	5	5	25	30	21	76
4	3	3	4	2	3	3	2	3	2	3	3	4	3	1	1	16	16	12	44
4	4	4	4	4	4	4	4	4	4	4	4	4	2	4	4	20	24	18	62
3	4	4	4	4	4	4	5	3	4	4	4	4	3	3	3	19	24	17	60
3	3	4	3	2	3	2	2	2	2	2	2	4	4	3	2	15	13	15	43
4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	4	20	20	19	59
2	2	2	2	2	2	3	2	2	3	3	3	3	3	3	3	10	15	15	40
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	15	18	14	47
1	4	3	2	1	2	2	4	3	4	4	3	3	1	2	2	11	19	11	41
2	1	1	1	2	3	3	2	2	4	2	2	2	5	4	3	7	16	16	39
3	3	4	4	4	3	4	3	4	3	4	4	4	3	4	3	18	21	18	57
3	3	2	2	2	2	2	2	2	3	2	2	2	3	3	3	12	13	13	38
2	2	1	2	1	3	3	2	2	2	3	3	3	3	3	2	8	15	14	37
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	6	5	16
4	3	3	4	4	3	5	4	3	4	4	3	4	4	2	3	18	23	16	57
5	5	5	5	5	5	5	5	5	5	5	5	5	1	5	5	25	30	21	76
4	3	3	4	2	3	3	2	3	2	3	3	4	3	1	1	16	16	12	44
4	4	4	4	4	4	4	4	4	4	4	4	4	2	4	4	20	24	18	62
3	4	4	4	4	4	4	5	3	4	4	4	4	3	3	3	19	24	17	60
3	3	4	3	2	3	2	2	2	2	2	2	4	4	3	2	15	13	15	43