Risk Management and Information Security in an Educational Community in the Andean Region of Peru

Miguel Angel De La Cruz Contreras[1], Joe Erick Flores Soriano[1], Paolo Andre Amaya Alvarado[2], Ghandy Allizon Rengifo-Calvanapón[3], Carlos Jesus Alza Collantes[3], Fabrizio Alonso Morales Novoa[3], Tula Luz Benites Vásquez[4]

[1] Universidad Católica de Trujillo - (PE); [2]Universidad César Vallejo, Perú; [3]Universidad Privada de Trujillo - (PE); [4]Universidad Privada Antenor Orrego - (PE)

Abstract– ***The purpose of the study was to identify the relationship between Risk Management and Information Security in an Educational Community in the Andean Zone of Peru. In the methodological aspect, we have an applied study, non-experimental design, descriptive correlational, with the survey and validated and reliable questionnaires as tools to obtain data, applied to a sample of 69 collaborators and a census type sampling. The main findings were the level of Risk Management with 67.2% approval and the level of Information Security with 64.7% approval, according to the perception of the members of the educational community of interest. The data did not adjust to a normal distribution, in such sense the correlation statistic of Spearman's Rho was applied, concluding the existence of a low positive significant correlation (Rho=0, 315) between Risk Management and Computer Security in an Educational Community of the Andean Zone of Peru.***

Keywords-- Risk management, information security, educational community, relationship.

Gestión del Riesgo y Seguridad Informática en una Comunidad Educativa de la Zona Andina del Perú

Miguel Angel De La Cruz Contreras[1], Joe Erick Flores Soriano[1], Paolo Andre Amaya Alvarado[2], Ghandy Allizon Rengifo-Calvanapón[3], Carlos Jesus Alza Collantes[3], Fabrizio Alonso Morales Novoa[3], Tula Luz Benites Vásquez[4]

[1] Universidad Católica de Trujillo - (PE); [2]Universidad César Vallejo, Perú; [3]Universidad Privada de Trujillo - (PE); [4]Universidad Privada Antenor Orrego - (PE)

***Resumen*– La finalidad del estudio fue identificar la relación entre la Gestión del Riesgo y la Seguridad Informática en una Comunidad Educativa de la Zona Andina del Perú. En el aspecto metodológico se tiene un estudio aplicado, diseño no experimental, descriptivo correlacional, se tuvieron como herramientas para obtener datos la encuesta y cuestionarios validados y confiables, aplicados a una muestra de 69 colaboradores y un muestreo de tipo censal. Siendo los principales hallazgos el nivel de la Gestión de Riesgo presento un 67.2% de aprobación y el nivel de la Seguridad Informática fue un 64.7% de aprobación, según la percepción de los integrantes de la comunidad educativa de interés. Los datos no se ajustaron a una distribución normal, en tal sentido se aplicó el estadígrafo de correlación de Rho de Spearman, concluyendo la existencia de una correlación significativa positiva baja (Rho=0, 315) entre Gestión del Riesgo y la Seguridad Informática en una Comunidad Educativa de la Zona Andina del Perú.**

***Palabras clave*-- Gestión del riesgo, seguridad informática comunidad educativa, relación.**

I. Introducción

Existen masivamente vulneraciones sobre seguridad informática, las cuales crecen sorprendentemente, como es el caso de 350 mil vulneraciones informáticas, incrementando la ciber criminalidad registrados en uno de los países más importantes de Europa, dichas cifras suelen ser muy preocupantes [1]. Los incidentes de seguridad en una organización se consideran como la fuente principal para evaluar la correcta aplicación de los controles de seguridad en organizaciones públicas o privadas [2].

En México, diversas organizaciones han sido víctimas de agresiones contra la seguridad informática de sus sistemas, empresas e instituciones como Petróleos Mexicanos, La Lotería Nacional, Secretaría de la Función Pública, entre otras, sufrieron intentos de hackeo [3]. En Colombia, la empresa especializada en seguridad informática "Trend Micro" indicó que "las redes domésticas, el software de trabajo remoto y los sistemas en la nube, estuvieron en el centro de una nueva ola de ataques" en el 2021. Otro dato importante es que el 2020 la sustitución en sitios web para recabar datos personales (phishing) se incrementó al 372% con respecto al año 2019 [4].

Los problemas de seguridad informática frente a las diversas amenazas modernas que asechan los datos de las organizaciones, se analiza la gestión de riesgo, estándares de calidad, sistemas de gestión entre otros, se conocen las debilidades y oportunidades para fortalecerlas y de esta manera contribuir a la mejora de la seguridad en una organización cuyos procesos se encuentran siempre en la red del mundo como es el internet, en conclusión el estudio enseña que los procesos de seguridad deben contener políticas y estándares de calidad [5].

En territorio peruano, la empresa Card Perú SA, quien opera como emisor de la tarjeta de crédito, señala que existe la posibilidad, que delincuentes roben, sustraigan y modifiquen datos y accedan a esos datos sin permiso, como fue el caso del Banco BCP, donde los dispositivos USB se encuentran en las instalaciones de la empresa, su Sistema de seguridad informática una vez que haya sido violentado, esto hace posible retirar fondos de la cuenta del cliente y de esta amanera se concretice el daño [6].

Algunas investigaciones, detallan que existen riesgos, en tal sentido se requiere trabajar la seguridad, haciendo un uso adecuado de las redes sociales e Internet para vincularse con los compañeros de clase con mínimo riesgo de hakeo [7]. De esta manera resulta necesario indicar que se percibe deficiente la guía de gestión de riesgo, además hay vulnerabilidad de recursos, sistemas y procesos, también menos de la mitad del personal demuestra habilidades en primeros auxilios ante riesgos escolares en escenarios educativos [8].

Por lo antes expuesto, se formuló la interrogante ¿Cuál es la relación entre la Gestión del Riesgo y la Seguridad Informática en una Comunidad Educativa de la Zona Andina del Perú?

Al abordar la temática de interés, se estaría contribuyendo al conocimiento sobre la seguridad informática en instituciones educativas peruanas, analizando los riesgos actuales y proponiendo estrategias basadas en estándares internacionales como ISO 27001 o metodologías como las descritas en la ISO 31001. Esto permitirá desarrollar modelos de gestión de seguridad adaptados al contexto educativo nacional.

Para ello, se consideró como objetivo general de estudio Determinar la relación entre la Gestión del Riesgo y la Seguridad Informática en una Comunidad Educativa de la Zona Andina del Perú. Asimismo, se platearon los siguientes

objetivos específicos: OE1: Establecer la relación entre la dimensión alcance, contexto y criterio de la variable gestión de riesgo con la variable Seguridad Informática. OE2: Establecer la relación entre la dimensión evaluación del riesgo y la variable seguridad Informática. OE3: Establecer la relación entre la dimensión tratamiento del riesgo y la variable seguridad informática. OE4: Establecer la relación entre la dimensión seguimiento y revisión de la variable Gestión del riesgo con la variable Seguridad informática y como ultimo objetivo específico se planteó OE5: Establecer la relación entre la dimensión Registro e informe de la variable Gestión del riesgo con la Variable Seguridad Informática

Estudio que respaldan la investigación fueron, como lo realizado en territorio ecuatoriano por la Ref. [9] quienes exponen que la finalidad fue realizar un análisis de factores de seguridad informática mediante la metodología OWASP v4. Enfoque metodológico fue cuantitativo usando una encuesta a una muestra de La Seguridad Web aplicado a 45 operadores, los resultados enseñan que sus principales pilares en preservar la integridad, confidencialidad y disponibilidad de los datos se realiza en un 78%, Concluyendo que las pruebas de aplicaciones, los ataques simples, el escaneo de puertos, los servicios y la transmisión de datos a las aplicaciones y servidores de Moodle también se pueden aplicar al servidor web Apache utilizando herramientas automatizadas o Servidor web Apache.

En territorio colombiano, según Ref. [10] sostienen que lo realizado aporta con un diseñó de una herramienta para evaluar el estado actual de las vulnerabilidades informáticas en las pequeñas y medianas empresas (PYMES) midiendo la seguridad de su software. Fue un estudio descriptivo cuantitativo no experimental, teniendo una muestra de 80 operadores, asimismo se aplicó elementos de la herramienta se identifican y describen, con el apoyo de la base de datos de exposición y vulnerabilidad comunes (CVE), y proporcionan mecanismos y enfoques recomendados para la evaluación del riesgo. Resulto, al examinar a las pequeñas y medianas empresas del ámbito colombiano de la innovación y la tecnología, se demostró el desempeño de cada componente de la herramienta se encuentra en un 70%. Cada software comercial se evalúa frente a diferentes versiones y el curso de acción recomendado se basa en niveles de riesgo calculado. Concluyendo que la herramienta propuesta permite culminar la primera fase de detección, reporte y asesoramiento ante una ciber vulnerabilidad, a partir de un trabajo sistemático, continuo e integral, preventivo más que reparador.

Investigaciones desarrolladas en territorio peruano, tales como lo realizado según Ref. [11] quienes tuvieron la intención de analizar la influencia de la aplicación del ISO 27001 en la seguridad de la información de una empresa privada de Lima (Perú). A partir de la aplicación de una metodología cuantitativa, se empleó un estudio preexperimental en el que se determinó la influencia de la aplicación del ISO 27001.Para ello se consideró a una muestra de 30 colaboradores de la empresa. La conclusión cuantitativa muestra que si existe una influencia de la aplicación del ISO en la seguridad de la información y en las dimensiones confidencialidad, integridad y disponibilidad.

Investigación que otorga detalles según Ref. [12] sostiene que el propósito investigativo fue determinar la relación entre la seguridad de los datos y la gestión de riesgos. Teniendo como 106 y 83 empleados en población y muestra respectivamente y un muestreo aleatorio simple, diseño descriptivo, corte transversal. Los resultados indican que se encuentra una relación directa entre la seguridad de los datos y la gestión de riesgos en los trabajadores del MINEDU DIGER, ya que se posee un valor de significación cero para Rho Spearman (0.886**). Se concluye: valor de la sigma bilateral inferior a 0,05, se ha probado la conjetura del investigador, en este caso: Existe relación significativa y directa entre la Seguridad de los datos y la Gestión del Riesgo para una institución pública del Perú.

También se tiene un estudio, desarrollado según Ref. [13] quienes pretendieron busca establecer la relación entre riesgo y seguridad que ofrecen dispositivos móviles en centros de educación superior de Perú, desde el punto de vista de los alumnos. La metodología incluye el uso de un cuestionario con escala de Likert. Los resultados dan cuenta que, existe relación inversa estadísticamente significativa (Rho=0,736) entre las variables citadas. Se recomienda a los alumnos concientizarlos sobre la existencia de ciberdelincuentes, mediante charlas de capacitación respecto a modalidades de hackeo y crakeo. Así, es de esperar que se realicen nuevas investigaciones equivalentes, para sensibilizar tanto a alumnos como a los que dirigen organizaciones educativas de nivel superior y que sus decisiones consideren lo apreciable que son las capacitaciones para generar impacto positivo.

El respaldo teórico considerado para la investigación se concentró en: Gestión de riesgo, es un proceso que permite analizar, identificar, cuantificar y prever posibilidades de pérdidas y efectos secundarios que son ocasionados por desastres, siniestros, imprevistos, accidentes [14]. Complementándose que la gestión de riesgos, según la ISO 31001, Tomando como referencia un enfoque basado en una norma de estandarización mundial la cual muestra principios sobre cómo abordar el riesgo como un componente de la creación de valor. Añade valor al permitir alcanzar sus objetivos considerando el riesgo como un factor que añade valor. La creación de valor es crucial porque le permite tomar decisiones basadas en el riesgo los cuales, al ser tratados oportunamente, ayudarán a alcanzar objetivos y metas. Por lo tanto, todo profesional que desee dedicarse a la gestión de riesgos debe ser consciente de la finalidad de esta norma [15].

Al revisar a profundidad la variable de interés se precisan que las dimensiones según Ref. [16], son: (D1) Alcance,

contexto y criterios, determinando qué procesos, actividades o áreas de la organización estarán cubiertas por la gestión de riesgos y considerando factores internos y externos que pueden influir en los riesgos. Asimismo, establecen parámetros para evaluar y comparar los riesgos, incluyendo niveles de aceptabilidad. (D2) Evaluación del riesgo, es el proceso de identificar, analizar y evaluar los riesgos (D3) Tratamiento del riesgo, consiste en seleccionar e implementar medidas para abordar los riesgos de acuerdo con la evaluación realizada. (D4) Seguimiento y revisión, la organización debe supervisar y revisar los riesgos de manera continua para asegurarse de que los controles siguen siendo efectivos y ajustar estrategias si es necesario. (D5) Registro e informe, La documentación de los riesgos y las decisiones tomadas es clave para la transparencia y la mejora continua. Se deben registrar los riesgos identificados, su evaluación, las acciones tomadas y los resultados de la supervisión.

Con respecto a Seguridad informática, [17] la consideran como cualquier medida para evitar la actividad no autorizada en un sistema informático o red que podría dañar los datos, el hardware o el software. Asimismo [18] la define como aquella medida para proteger los datos y los sistemas de TI contra el acceso no autorizado. Las principales dimensiones consideradas según Ref. [19] son (D1) Confidencialidad, se refiere a la protección de la información para asegurar que solo las personas autorizadas puedan acceder a ella. Este principio es esencial para salvaguardar datos sensibles y prevenir accesos no autorizados. (D2) Integridad, implica que los datos están protegidos de cambios no autorizados para garantizar que son fiables y correctos. Esto asegura que la información se mantenga completa y sin alteraciones indebidas. (D3) Disponibilidad, significa que los usuarios autorizados tienen acceso a los sistemas y recursos que necesitan. Es decir, la información y los sistemas deben estar accesibles cuando se requieran y (D4) Autenticación, es el proceso de verificar la identidad de un usuario o sistema antes de otorgar acceso a la información. Este proceso es fundamental para garantizar que solo las entidades legítimas accedan a los recursos. Estos principios son esenciales para establecer un marco robusto de seguridad de la información en cualquier organización.

El estudio se basa en Triángulo de la Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad - CIA), el modelo CIA es una base fundamental en la seguridad de la información. Se centra en tres principios clave: Confidencialidad: Garantiza que solo las personas autorizadas puedan acceder a la información, Integridad: Asegura que la información no sea alterada sin autorización y Disponibilidad: Garantiza que la información esté accesible cuando sea necesaria [20].

Además del Modelo de Gestión de Riesgos ISO 31000, este modelo proporciona un enfoque sistemático para la gestión de riesgos en cualquier tipo de organización. Se basa en la identificación, evaluación, tratamiento, monitoreo y revisión de riesgos [16], con ello el Modelo de Defensa en Profundidad (Defense in Depth), este modelo propone múltiples capas de seguridad para proteger los sistemas de información. Se basa en la idea de que ninguna medida de seguridad individual es completamente efectiva por sí sola [22].

También se respalda con el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology), el marco NIST propone cinco funciones esenciales para gestionar el riesgo en ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar [21].

II. METODOLOGÍA

La metodología adoptada para esta investigación aplicada de tipo cuantitativo se basa en un diseño no experimental descriptivo correlacional. La población y muestra consistieron en 69 colaboradores, abarcando a toda la población objetivo a través de un muestreo censal, lo que permitió la inclusión de cada miembro relevante para el estudio. Esta estrategia de muestreo asegura una representatividad total y elimina el sesgo de selección, proporcionando una base sólida para la generalización de los resultados dentro del contexto estudiado [23].

Para la recolección de datos, se emplearon dos cuestionarios que fueron previamente validados para asegurar su confiabilidad y validez, elementos esenciales para la obtención de datos precisos y relevantes. La confiabilidad se refiere a la consistencia de los resultados que el instrumento produce en diferentes aplicaciones, mientras que la validez indica qué tan bien el instrumento mide la variable que pretende medir [23].

En el análisis de datos, se calculó descriptivamente las frecuencias para cada nivel de las dimensiones estudiadas, proporcionando una visión detallada de la distribución de las respuestas. Al enfrentarse al incumplimiento del supuesto de normalidad de los datos, crucial para aplicar pruebas paramétricas, se optó por emplear el coeficiente Rho de Spearman para las correlaciones. Este enfoque no paramétrico es adecuado para datos que no se distribuyen normalmente, ofreciendo una alternativa robusta para examinar la fuerza y la dirección de las asociaciones entre variables [23].

Finalmente, se utilizó software estadístico apropiado para manejar las particularidades de los datos y los métodos de análisis seleccionados, garantizando la precisión técnica y la relevancia de los procedimientos estadísticos. Este enfoque metodológico asegura que los hallazgos sean tanto confiables como aplicables, contribuyendo significativamente al cuerpo de conocimiento en el campo de estudio [23].

III. Resultados

A. Gestión de riesgo

TABLA I
NIVEL DE LA PRECEPCIÓN POR CADA DIMENSIÓN DE LA VARIABLE GESTIÓN DE RIESGO

Nivel	Alcance, contexto y criterios		Evaluación del riesgo		Tratamiento del riesgo		Seguimiento y revisión		Registro e informe	
	F	%	F	%	F	%	F	%	F	%
Buena	13	19	17	25	18	26	6	9	6	9
Regular	45	65	39	57	39	57	52	75	50	72
Mala	11	16	13	19	12	18	11	16	13	19

La Tabla I detalla la percepción de la gestión de riesgo en cinco dimensiones clave dentro de una comunidad educativa andina, mostrando que la mayoría de las percepciones son regulares en todas las dimensiones, especialmente destacadas en el seguimiento y revisión, y en el registro e informe donde el 75% y 72% de los encuestados las califican como regulares. Esto sugiere una necesidad de mejorar prácticas en estas áreas para elevar la percepción de eficacia en la gestión de riesgos.

B. Seguridad Informática

TABLA II
NIVEL DE LA PRECEPCIÓN POR CADA DIMENSIÓN DE LA VARIABLE SEGURIDAD INFORMÁTICA

Nivel	Confidencialidad		Integridad		Disponibilidad		Autenticación	
	F	%	F	%	F	%	F	%
Alta	13	19	17	25	19	27.6	6	9
Media	46	66.7	41	59.1	39	56.5	53	76.8
Baja	10	14.3	11	15.9	11	15.9	10	14.2

La Tabla II revela que las percepciones sobre la seguridad informática, particularmente en términos de confidencialidad, integridad, disponibilidad y autenticación, tienden a ser moderadas, con una mayoría que considera que el desempeño es medio en todas las dimensiones. Sin embargo, la disponibilidad se percibe levemente mejor que las otras dimensiones, lo que podría indicar un enfoque específico o recientes mejoras en esta área.

C. Relación entre Gestión de Riesgo y Seguridad Informática

TABLA III
CORRELACIÓN DE RHO SPEARMAN GESTIÓN DE RIESGO Y SEGURIDAD INFORMÁTICA EN UNA COMUNIDAD EDUCATIVA DE LA ZONA ANDINA DEL PERÚ

	Seguridad informática		
	Rho Spearman	p-valor	N
Gestión de Riesgo	,315	,000	69

*Significativa en el nivel 0,01 (bilateral).

Esta tabla presenta una correlación positiva moderada entre la gestión de riesgo y la seguridad informática, con un coeficiente de Spearman de 0.315, indicativo de una asociación estadísticamente significativa. Este resultado subraya la interdependencia entre gestionar riesgos efectivamente y mejorar la seguridad informática en el contexto educativo evaluado.

TABLA IV
CORRELACIÓN DE RHO SPEARMAN DE LA DIMENSIÓN ALCANCE, CONTEXTO Y CRITERIO Y SEGURIDAD INFORMÁTICA EN UNA COMUNIDAD EDUCATIVA DE LA ZONA ANDINA DEL PERÚ

	Seguridad informática		
Dimensión Alcance, contexto y criterio	Rho Spearman	p-valor	**N**
	,378	,000	69

*Significativa en el nivel 0,01 (bilateral).

La Tabla IV muestra una correlación de Rho Spearman de 0.378 entre la dimensión de gestión de riesgo "Alcance, contexto y criterio" y la seguridad informática, lo que indica una relación positiva y moderadamente fuerte. Esto sugiere que una adecuada definición del alcance, comprensión del contexto y establecimiento de criterios en la gestión de riesgo están significativamente relacionados con la percepción de efectividad en la seguridad informática dentro de la comunidad educativa.

TABLA V
CORRELACIÓN DE RHO SPEARMAN DE LA DIMENSIÓN EVALUACIÓN DE RIESGO Y SEGURIDAD INFORMÁTICA EN UNA COMUNIDAD EDUCATIVA DE LA ZONA ANDINA DEL PERÚ

	Seguridad informática		
Dimensión Evaluación de riesgo	Rho Spearman	p-valor	**N**
	,344	,000	69

*. Significativa en el nivel 0,01 (bilateral).

En la Tabla V, la correlación entre la evaluación del riesgo y la seguridad informática muestra un coeficiente de Spearman de 0.344. Esto refleja una asociación estadísticamente significativa, indicando que una evaluación efectiva de riesgos puede influir positivamente en la seguridad informática. Este vínculo resalta la importancia de evaluar sistemáticamente los riesgos como una parte integral de la gestión de la seguridad informática.

TABLA VI
CORRELACIÓN DE RHO SPEARMAN DE LA DIMENSIÓN TRATAMIENTO DEL RIESGO Y SEGURIDAD INFORMÁTICA EN UNA COMUNIDAD EDUCATIVA DE LA ZONA ANDINA DEL PERÚ

	Aprendizaje en Ciencia y Tecnología		
Dimensión Tratamiento del riesgo	Rho Spearman	p-valor	**N**
	,434	,000	69

*. Significativa en el nivel 0,01 (bilateral).

La Tabla VI ilustra que la dimensión "Tratamiento del riesgo" tiene una correlación de 0.434 con la seguridad informática, la más alta entre las presentadas. Este resultado subraya la significativa influencia que tiene el tratamiento efectivo de los

riesgos en la mejora de la seguridad informática, evidenciando que intervenciones adecuadas en el manejo de riesgos pueden reforzar directamente la protección de los sistemas informáticos.

TABLA VII
CORRELACIÓN DE RHO SPEARMAN DE LA DIMENSIÓN SEGUIMIENTO Y REVISIÓN Y SEGURIDAD INFORMÁTICA EN UNA COMUNIDAD EDUCATIVA DE LA ZONA ANDINA DEL PERÚ

	Aprendizaje en Ciencia y Tecnología		
Dimensión Seguimiento y Revisión	Rho Spearman	p-valor	**N**
	,404	,000	69

*. Significativa en el nivel 0,01 (bilateral).

Según la Tabla VII, la correlación entre el seguimiento y revisión de la gestión de riesgo y la seguridad informática es también fuerte y significativa, con un coeficiente de Spearman de 0.404. Este resultado confirma la importancia del monitoreo continuo y la revisión de las políticas de riesgo para asegurar y mantener una infraestructura informática segura en el ambiente educativo.

TABLA VIII
CORRELACIÓN DE RHO SPEARMAN DE LA DIMENSIÓN REGISTRO E INFORME Y SEGURIDAD INFORMÁTICA EN UNA COMUNIDAD EDUCATIVA DE LA ZONA ANDINA DEL PERÚ

	Aprendizaje en Ciencia y Tecnología		
Dimensión Registro e Informe	Rho Spearman	p-valor	**N**
	,454	,000	69

*. Significativa en el nivel 0,01 (bilateral).

La Tabla VIII muestra la correlación entre el registro e informe en la gestión de riesgo y la seguridad informática con un coeficiente de Spearman de 0.454, lo cual es estadísticamente significativo y la correlación más fuerte reportada en estas tablas. Este hallazgo destaca que la documentación precisa y la comunicación efectiva de los incidentes y acciones de riesgo son críticos para el manejo eficaz de la seguridad informática.

IV. DISCUSIÓN

Después de confirmar la existencia de una asociación entre las variables de estudio en este trabajo de investigación, se decidió contrastar hallazgos y comprender sucesos encontrados, en respuesta a la intención principal del estudio, se evidencio una relación existente y significativa, además de ser positiva y baja entre Gestión del Riesgo y la Seguridad Informática en una comunidad educativa de la zona andina del Perú, el cual posee una similitud con lo reportado en la Ref. [12] donde existe una relación significativa entre Seguridad de los datos y la Gestión del Riesgo, esquema que responde al Modelo de Gestión de Riesgos ISO 31000, este modelo proporciona un enfoque sistemático para la gestión de riesgos en cualquier tipo de organización. Se basa en la identificación, evaluación, tratamiento, monitoreo y revisión de riesgos [16] y apoyado por el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology), el marco NIST propone cinco funciones esenciales para gestionar el riesgo en ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar [20].

Considerando lo encontrado en respuesta al primer objetivo específico, en donde se evidencia que existe una relación significativa, siendo esta positiva y baja entre la dimensión alcance, contexto y criterio y la Seguridad Informática, este hallazgo guarda similitud con lo reportado por la Ref. [13] quienes señalan que encontraron una relación entre riesgo y seguridad que ofrecen dispositivos móviles. Siendo comprendido con el Triángulo de la Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad - CIA), el modelo CIA es una base fundamental en la seguridad de la información [19].

De esta manera se da respuesta al segundo objetivo específico, en donde se evidencia que existe una relación significativa, siendo esta positiva y baja entre la dimensión evaluación del riesgo y la Seguridad Informática, este hallazgo guarda un gran parecido con lo reportado por la Ref. [12] quienes señalan la existencia de una relación significativa, es por ello que se apoya con lo explicado en el Modelo de Gestión de Riesgos ISO 31000, este modelo proporciona un enfoque sistemático para la gestión de riesgos en cualquier tipo de organización. Se basa en la identificación, evaluación, tratamiento, monitoreo y revisión de riesgos [16].

Respecto al tercer objetivo específico de la investigación, |, siendo explicada por la Ref. [18] enfatizando que la seguridad de la información es aquella medida para proteger los datos y los sistemas de TI contra el acceso no autorizado.

Al responde el cuarto objetivo específico, donde se tuvo la existencia de relación significativa, siendo esta positiva y moderada entre la dimensión seguimiento y revisión y la Seguridad Informática, el cual posee un similar hallazgo en un escenario del sector educación, tal como lo muestra la la Ref. [12]. Lo encontrado evidencia que con seguimiento y control se logra el propósito de tener seguridad en la información, tal como lo recomienda el Modelo de Gestión de Riesgos ISO 31000, este modelo proporciona un enfoque sistemático para la gestión de riesgos en cualquier tipo de organización. Se basa en la identificación, evaluación, tratamiento, monitoreo y revisión de riesgos [16].

Finalmente, en el último objetivo específico se encontró una relación significativa, siendo esta positiva y moderada entre la dimensión registro e informe y la Seguridad Informática, hecho que guarda similitud con el estudio que se expone en la Ref. [13] y cuya explicación se apoya con el el Marco de Ciberseguridad del NIST (National Institute of

Standards and Technology), el marco NIST propone cinco funciones esenciales para gestionar el riesgo en ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar [21].

V. Conclusiones

Se identificó una relación estadísticamente significativa ($p < 0.05$) entre la Gestión del Riesgo y la Seguridad Informática, caracterizada por ser positiva, aunque de magnitud baja, con un coeficiente Rho de Spearman de 0.315. Este resultado subraya la interconexión entre la gestión efectiva de riesgos y el fortalecimiento de la seguridad informática, aunque sugiere que otros factores podrían estar influyendo en esta relación.

Respecto a la dimensión de "alcance, contexto y criterio" de la gestión del riesgo, se encontró una correlación positiva y baja con la Seguridad Informática, presentando un coeficiente Rho de 0.378. Esta correlación indica que un adecuado entendimiento del alcance y contexto en el que operan las políticas de gestión de riesgo tiene un impacto directo, aunque limitado, en la eficacia de las medidas de seguridad informática implementadas.

Por otro lado, la dimensión "evaluación del riesgo" mostró una relación similarmente positiva y baja con la Seguridad Informática, con un Rho de 0.344. Este hallazgo refuerza la importancia de las evaluaciones de riesgo regulares y meticulosas para anticipar y mitigar amenazas de seguridad, aunque también destaca que la evaluación por sí sola es solo una parte de una estrategia de seguridad más integral.

La dimensión "tratamiento del riesgo" reflejó una relación positiva y de magnitud moderada con la Seguridad Informática, evidenciada por un Rho de 0.434. Esto implica que las acciones tomadas para gestionar y mitigar los riesgos identificados juegan un papel crucial y más significativo en la protección de los recursos informáticos frente a potenciales amenazas.

Similarmente, la dimensión "seguimiento y revisión" de la gestión del riesgo se asoció positiva y moderadamente con la Seguridad Informática, con un coeficiente Rho de 0.404. Este resultado sugiere que el monitoreo continuo y la revisión de las estrategias de riesgo son fundamentales para mantener y mejorar la seguridad de los sistemas informáticos.

Finalmente, la dimensión "registro e informe" mostró la correlación más fuerte entre las medidas evaluadas, con un Rho de 0.454, indicando una relación positiva y moderada. Este vínculo resalta la importancia de una documentación detallada y precisa de los incidentes de seguridad y las respuestas a estos, como un componente esencial para una gestión de seguridad informática eficaz.

Referencias

[1] B. Quintero, *Panorama actual de la seguridad informática en España*, 2020. [En línea]. Disponible: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

[2] M. E. Tasa-Catanzaro, H. G. Maquera-Quispe, J. F. Rojas-Bujaico, y M. G. Delgado-Rospigliosi, "Análisis de información de la gestión de incidentes de seguridad en organizaciones," *Puriq*, vol. 4, p. e196, 2022. doi: 10.37073/puriq.4.1.196.

[3] Ethics Global, "México y su posición en ciberseguridad," 2022. [En línea]. Disponible: https://blog.ethicsglobal.com/mexico-y-su-posicion-en-ciberseguridad/

[4] Trend Micro, "Ciberseguridad en Colombia y el mundo: 10 cifras para tener en el radar," 2022. [En línea]. Disponible: https://resetmarketingdigital.com/ciberseguridad-en-colombia-y-mundo-cifras

[5] J. Ospina, "Modelo de seguridad basado en políticas de protección, para el procesamiento y manejo de datos asociados a sistemas BCI, mediante una gestión del riesgo con base en la ISO 27005 y su plan de tratamiento con el fin de reducir los niveles de exposición," Tesis de maestría, ITM, 2022. [En línea]. Disponible: http://hdl.handle.net/20.500.12622/5744

[6] Autoridad Nacional de Protección de Datos Personales, "ANPD sanciona a entidad bancaria con S/ 166 mil (40 UITs) por no resguardar la confidencialidad de los datos personales de sus clientes," 2020. [En línea]. Disponible: https://www.gob.pe/institucion/anpd/noticias/305427-anpd-sanciona-a-entidad-bancaria-con-s-166-mil-40-uits-por-no-resguardar-la-confidencialidad-de-los-datos-personales-de-sus-clientes

[7] L. D. Leal Acanda, C. Martínez Gandol, y Y. Martínez Gandol, "La gestión integral de la seguridad en la educación primaria," *Revista De Investigación Del Departamento De Humanidades Y Ciencias Sociales*, no. 22, pp. 101–117, 2022. doi: 10.54789/rihumso.22.11.22.6.

[8] E. G. Tapia Pambabay, "Evaluación del plan de reducción de riesgos y seguridad integral para instituciones educativas de la Escuela de Educación Básica Marquesa de Solanda del Distrito Metropolitano de Quito en el período de enero-junio 2018," Tesis, Universidad Central del Ecuador, 2019. [En línea]. Disponible: http://www.dspace.uce.edu.ec/handle/25000/20514

[9] C. Vega, E. Tapia, y F. Gallardo, "Análisis de factores de seguridad informática mediante la metodología OWASP v4.2: Caso de estudio ISTJO," 2022. [En línea]. Disponible: https://www.espirituemprendedortes.com/index.php/revista/article/view/293

[10] P. A. Sánchez-Sánchez, J. R. García-González, A. Triana, y L. Perez-Coronell, "Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia," *Información tecnológica*, vol. 32, no. 5, pp. 121–128, 2021. doi: 10.4067/S0718-07642021000500121.

[11] L. S. Rodriguez Baca, C. F. Cruzado Puente de la Vega, C. Mejía Corredor, y M. A. A. Diaz, "Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana," *Propósitos y Representaciones*, vol. 8, no. 3, 2020. doi: 10.20511/pyr2020.v8n3.786.

[12] J. Calderón, "Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018," Tesis de maestría, Universidad Cesar Vallejo, 2019. [En línea]. Disponible: https://hdl.handle.net/20.500.12692/30014

[13] J. A. Tiznado Ubillús, C. A. Atoche Pacherres, y A. Valdiviezo Valdiviezo, "Riesgo y seguridad en dispositivos móviles de centros de educación superior Perú," *Ciencia Latina Revista Científica Multidisciplinar*, vol. 7, no. 3, pp. 1953–1960, 2023. doi: 10.37811/cl_rcm.v7i3.6320.

[14] ESAM, "Gestión de riesgos: mejores prácticas," 2024. [En línea]. Disponible: https://www.ue.edu.pe/pregrado/blog/noticias/gestion-de-riesgos-mejores-practicas

[15] Bonaterra Calidad y Seguridad, "Sistema de Gestión de Riesgo ISO 31001," 2022. [En línea]. Disponible: https://bonaterraconsultores.com/gestion-del-riesgo.php

[16]International Organization for Standardization, *ISO 31000:2018 - Risk management – Guidelines*, 2018. [En línea]. Disponible: https://www.iso.org/standard/65694.html
[17]A. Gómez, *Enciclopedia de la seguridad informática*. RA-MA, España, 2006. [En línea]. Disponible: http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/seguridadinformatica.aspx
[18]IBM, "¿Qué es la seguridad de TI?," 2022. [En línea]. Disponible: https://www.ibm.com/es-es/topics/it-security
[19]International Organization for Standardization, *ISO/IEC 27001:2013 - Information security management systems - Requirements*, 2013. [En línea]. Disponible: https://www.iso.org/isoiec-27001-information-security.html
[20]W. Stallings y L. Brown, *Computer security: Principles and practice*, 4ª ed. Pearson, 2018.
[21]National Institute of Standards and Technology, *Framework for improving critical infrastructure cybersecurity (Version 1.1)*, 2018. [En línea]. Disponible: https://www.nist.gov/cyberframework
[22]SANS Institute, *Defense in depth: A practical strategy for cybersecurity*, 2020. [En línea]. Disponible: https://www.sans.org/white-papers/defense-in-depth/
[23]R. Hernández, C. Fernández, y P. Baptista, "Metodología de la investigación," 6ª ed., McGraw-Hill Interamericana, 2014.