Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

RELACIÓN ENTRE LA SEGURIDAD DE DATOS Y LA IMPLEMENTACIÓN EXITOSA DE APLICACIONES DE REALIDAD AUMENTADA EN EVENTOS DEPORTIVOS, 2023

Línea de investigación:
Ingeniería de software, simulación y desarrollo de TICs

Tesis para optar el Grado Académico de Maestro en Ingeniería de Sistemas con mención en Gestión de Tecnologías de la Información

Autor

Minaya Isique, Jesus Francisco

Asesor

Soto Soto, Luis

ORCID: 0000-0002-3799-645X

Jurado

Paredes Paredes, Pervis

Carrillo Balceda, Jesus Elias

Lezama Gonzales, Pedro Martin

Lima - Perú

2025

RELACIÓN ENTRE LA SEGURIDAD DE DATOS Y LA IMPLEMENTACIÓN EXITOSA DE APLICACIONES DE REALIDAD AUMENTADA EN EVENTOS DEPORTIVOS, 2023

INFORME DE ORIGINALIDAD

27%	18%	4%	19%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	16%
2	www.coursehero.com Fuente de Internet	1%
3	Submitted to Submitted on 1693244762802 Trabajo del estudiante	1%
4	repositorio.upla.edu.pe Fuente de Internet	<1%
5	hdl.handle.net Fuente de Internet	<1%
6	repositorio.ulasamericas.edu.pe Fuente de Internet	<1%
7	repositorio.unfv.edu.pe Fuente de Internet	<1%
8	ifai.org.mx Fuente de Internet	<1%

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

RELACIÓN ENTRE LA SEGURIDAD DE DATOS Y LA IMPLEMENTACIÓN EXITOSA DE APLICACIONES DE REALIDAD AUMENTADA EN EVENTOS DEPORTIVOS, 2023

Línea de investigación:

Ingeniería de Software, Simulación y Desarrollo de TICs

Tesis para optar el Grado Académico de

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

Autor:

Minaya Isique, Jesus Francisco

Asesor:

Soto Soto, Luis

ORCID: 0000-0002-3799-645X

Jurado:

Paredes Paredes, Pervis

Carrillo Balceda, Jesus Elias

Lezama Gonzales, Pedro Martin

Lima – Perú

2025

DEDICATORIA

Deseo agradecer, en primer lugar, a Dios por brindarme la oportunidad de llegar a este punto en mi vida. También quiero expresar mi aprecio a mi familia, en particular a mis padres, por su guía, y a mis profesores, por ofrecerme las herramientas académicas fundamentales que han hecho viable la culminación de la presente investigación.

RECONOCIMIENTO

Mi especial reconocimiento para los distinguidos Miembros del Jurado:

Dr. Paredes Paredes, Pervis

Dr. Carrillo Balceda, Jesus Elias

Mg. Lezama Gonzales, Pedro Martin

Por su criterio objetivo en la evaluación de este trabajo de investigación.

Asimismo, mi reconocimiento para mi asesor

Por las sugerencias recibidas para el mejoramiento de este trabajo.

Muchas gracias a todos.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El estudio tuvo como propósito general analizar la conexión entre la protección de la información y la implementación exitosa de aplicaciones de realidad aumentada en el contexto de eventos deportivos, durante el año 2023. La investigación se caracterizó por ser de nivel fundamental, de naturaleza descriptiva correlacional y con un diseño no experimental. La muestra seleccionada de forma probabilística incluyó a 50 individuos que laboran en el ámbito de eventos deportivos. Para la obtención de datos, se utilizó la técnica de encuestas, aplicando un cuestionario enfocado en la protección de la información con 20 preguntas y otro centrado en la implementación exitosa de aplicaciones de realidad aumentada, compuesto por 16 preguntas. Los hallazgos revelaron que la protección de la información desempeña un rol esencial en la exitosa integración de aplicaciones de realidad aumentada en eventos deportivos durante 2023 (Rho de Spearman: 0.402 y sig.0.004). Asimismo, se determinó que el desarrollo de dichas aplicaciones en eventos deportivos de 2023 mantiene una relación significativa con la seguridad de datos (Rho de Spearman: 0.499 y sig.0.000). Adicionalmente, se identificó que la adecuada implementación de la gestión de planes en este contexto (Rho de Spearman: 0.409 y sig.0.002) influye en la satisfacción de los usuarios en eventos deportivos, la cual se relaciona de manera directa con la protección de la información (Rho de Spearman: 0.389 y sig.0.002).

Palabras clave: Seguridad, datos, realidad aumentada, eventos deportivos.

ABSTRACT

The study aimed to analyze the connection between data security and the successful implementation of augmented reality applications in the context of sports events during 2023. The research was characterized as fundamental, of a descriptive correlational nature, and with a non-experimental design. The probabilistic sample included 50 individuals working in the field of sports events. For data collection, the survey technique was used, applying a questionnaire focused on data security with 20 items and another centered on the successful implementation of augmented reality applications, consisting of 16 items. The findings revealed that data security plays a crucial role in the successful integration of augmented reality applications in sports events during 2023 (Spearman's Rho: 0.402, p-value 0.004). Likewise, it was determined that the development of such applications in sports events of 2023 is significantly related to data security (Spearman's Rho: 0.499, p-value 0.000). Additionally, it was identified that the proper implementation of plan management in this context (Spearman's Rho: 0.409, p-value 0.002) influences user satisfaction in sports events, which is directly related to data security (Spearman's Rho: 0.389, p-value 0.002).

Keywords: Security, data, augmented reality, sporting events.

I. INTRODUCCIÓN

El cruce entre la protección de información y la ejecución efectiva de programas de realidad aumentada en eventos deportivos se erige como un terreno de estudio vital en el contexto tecnológico actual. El presente estudio se enfoca en explorar y desentrañar la conexión existente entre dos componentes esenciales: la salvaguarda de datos y la implementación eficiente de aplicaciones basadas en realidad aumentada. Se busca examinar de qué manera la robustez en la seguridad de los datos incide directamente en la implantación eficaz de aplicaciones de realidad aumentada en el ámbito de eventos deportivos.

La relevancia de la protección de datos se fundamenta en la obligación de garantizar la integridad y la confidencialidad de la información, asegurando que los datos se mantengan completos y protegidos contra accesos no autorizados, ya que su exposición a individuos no autorizados puede conllevar a consecuencias perjudiciales, tales como pérdidas financieras, suplantación de identidad o la perpetración de estafas. En otras palabras, descuidar la protección de datos puede dar lugar a la comisión de delitos relacionados con la ciberdelincuencia (Ministerio Público Fiscalía de la Nación [MPFN], 2023). La correcta ejecución de herramientas de realidad aumentada aborda tanto las tecnologías de realidad virtual como las de realidad aumentada. Estas herramientas, dada su flexibilidad y amplio espectro de aplicaciones, han generado interés en diversas esferas del saber (Rodríguez et al., 2020). Los dos factores se integran dentro de un escenario en el cual la protección de la información asume una función esencial para garantizar la ejecución óptima de la realidad aumentada en eventos deportivos.

Por ello, en la era digital actual, donde los eventos deportivos incorporan cada vez más tecnologías emergentes, la seguridad de datos se erige como el pilar que sustenta la confiabilidad y efectividad de estas iniciativas. La exitosa ejecución de aplicaciones de realidad aumentada en eventos deportivos no solo enriquece la vivencia del usuario, sino que también

transforma la forma en que nos relacionamos con el deporte. La relevancia de esta investigación reside en entender cómo la protección de datos puede impulsar o limitar este procedimiento, y cómo estas consideraciones impactan en el éxito global de los eventos deportivos.

La motivación detrás de este estudio se origina en la necesidad de satisfacer una carencia presente en la literatura que trata sobre la relación específica entre la protección de datos y la ejecución de aplicaciones de realidad aumentada en eventos deportivos. La ausencia de un análisis detallado de esta conexión ha generado la oportunidad de contribuir con conocimientos significativos que beneficiarán a profesionales, investigadores y entusiastas del ámbito deportivo y tecnológico.

Una vez concluida la revisión de este documento, el lector habrá adquirido un entendimiento exhaustivo sobre la intrincada relación entre la salvaguarda de datos y la implementación eficaz de aplicaciones de realidad aumentada en eventos deportivos. Además, estará provisto de conocimientos tanto prácticos como teóricos que podrán ser aplicados en la formulación de decisiones y la concepción de estrategias para garantizar la viabilidad y el éxito de eventos deportivos que integran tecnologías de realidad aumentada.

La investigación se basará en un análisis detallado de eventos deportivos específicos, sirviéndose de una muestra representativa que abarcará diversas disciplinas y enfoques tecnológicos. Esto permitirá extraer conclusiones significativas aplicables a contextos deportivos variados, contribuyendo así a la generalización y aplicabilidad de los resultados obtenidos.

1.1. Planteamiento del problema

A nivel internacional, según el informe de EasyDMARC (2022), se ha logrado registrar más de 90 millones de intentos de ataques de phishing, marcando un incremento significativo del 62,9% en comparación con el año anterior; en dicha situación, los resultados revelan que un abrumador 89% de los clientes han enfrentado ataques de esta índole, siendo la industria

financiera la más afectada, con un aumento trimestral del 5,8%; en cuanto a la distribución geográfica de estos ataques, Holanda encabeza la lista de los países más afectados, seguido por Rusia, Moldavia, Estados Unidos y Tailandia; además, se implementaron medidas de cuarentena para más de 20 millones de correos electrónicos, subrayando la importancia del desafío y la urgencia de encontrar soluciones eficaces para hacer frente a la creciente amenaza cibernética.

Un informe de BlackCloak y el Instituto Ponemon, corporaciones dedicadas a la seguridad digital, revela que un considerable 42% de altos ejecutivos han sido víctimas de ciberataques, donde estas amenazas abarcan diversas formas, siendo las más comunes el malware detectado en dispositivos personales, con un preocupante 56%; además, la suplantación de identidad afecta al 34% de estos ejecutivos, mientras que el ransomware y el swatting afectan al 31% y al 25%, respectivamente, por lo que este estudio subraya la creciente vulnerabilidad de los líderes empresariales frente a diversas formas de ataques cibernéticos (Seminario Interdiocesano de Caracas [SIC], 2023).

En ese contexto, según el informe del FBI sobre Crímenes en Internet del año 2022, se reveló que los ataques de phishing alcanzaron la cifra de 3.400 millones de correos no solicitados diariamente, prevalecen como el ciberataque más común, representando el 90% de las violaciones de datos, utilizando estrategias fraudulentas mediante el uso de correos electrónicos o páginas web engañosas, los phishers se hacen pasar por entidades confiables, comprometiendo la seguridad al inducir a revelar información sensible (Kolesnikov, 2023).

A nivel europeo, durante el año 2022, la seguridad de datos se ha visto vulnerada, tal como menciona el Instituto Nacional de Ciberseguridad de España que tuvo la responsabilidad de gestionar un total de 118,820 incidentes, lo que representó un incremento del 9%, de este conjunto, más de 110,100 afectaron directamente a ciudadanos y empresas, destacándose que

aproximadamente 1 de cada 3 incidentes estuvo relacionado con filtraciones de datos; en donde, los problemas más prominentes abordados abarcaron áreas como phishing, con 17,000 casos, malware, con 14,000 casos, y ransomware, con 450 casos (Instituto Nacional de Ciberseguridad [INCIBE], 2023).

A nivel latinoamericano, las estadísticas adquieren una importancia destacada, según el diario la Expansión, revela que el 76% de las organizaciones en la región enfrentan al menos un ataque cibernético al año, de ese porcentaje, el 24% se vio imposibilitado de recuperar los datos cifrados incluso después de realizar pagos de rescate, lo que indica que las repercusiones no se limitan únicamente al ámbito económico, sino que impactan en todas las operaciones de la entidad. (Guarneros, 2022).

Por otro lado, los intentos de ingeniería social, como el phishing, se duplicaron, con Perú liderando con el 31% de las detecciones, seguido por Brasil (18%) y México (17%), la persistencia de estos ataques revela la falta de concientización de los usuarios, permitiendo a los cibercriminales robar información personal y financiera, así como llevar a cabo ataques más sofisticados, la mejora constante de los atacantes contribuye a la amenaza continua (Lubeck, 2021).

Ambas variables convergen en un contexto donde la protección de datos cumple una función determinante para garantizar la adecuada incorporación de la realidad aumentada en competiciones deportivas, dado que los dispositivos tienen la capacidad de recolectar información delicada; por ejemplo, auriculares VR con micrófonos pueden grabar conversaciones, y sistemas de seguimiento con cámaras pueden obtener videos de espacios privados, creando un riesgo para la seguridad con información biométrica valiosa (Micucci, 2023).

1.2. Descripción del problema

Cada mes, se reportan aproximadamente 300 denuncias de delitos informáticos, incluyendo phishing en páginas falsas de bancos y ofertas fraudulentas en redes sociales. Los ciberdelincuentes realizan depósitos no autorizados tras engañar a usuarios con sus datos personales y desactivan perfiles tras estafar con productos a bajos precios en plataformas como Facebook y WhatsApp. La suplantación de perfiles en redes sociales se utiliza para persuadir a amigos y familiares a realizar transferencias por compras ficticias, préstamos falsos o pagos de impuestos (El Peruano, 2021).

En el año 2021, de acuerdo con el reporte de la Defensoría del Pueblo, se observó la mayor frecuencia de denuncias por ciberdelitos en Perú se focalizó principalmente en Lima Metropolitana y Lima Provincias, representando conjuntamente el 53% del total, y alcanzando el 71% al incluir al Callao y tres regiones del norte. De manera alarmante, la región Lima encabezó la lista con un preocupante 53.08% de ciberdelitos de alto riesgo, seguida por Arequipa (5.71%), La Libertad (5.01%) y Lambayeque (4.27%). En dicha situación se registró que el 71.7% pertenecían al fraude informático, el 20.2% a la suplantación de identidad y el 3.6% a los abusos de mecanismos y dispositivos informáticos (Castillo, 2023).

La protección de la información se manifiesta como un factor esencial dentro del contexto de la adopción de soluciones tecnológicas de realidad aumentada en eventos deportivos durante el año 2023. A medida que las organizaciones deportivas adoptan tecnologías sofisticadas para optimizar la experiencia del usuario y la interacción, emergen retos sustanciales en la salvaguarda de datos sensibles. La recopilación y el envío de datos en entornos de realidad aumentada implican potenciales amenazas que podrían comprometer la confidencialidad de los usuarios y la seguridad de la información. Este riesgo genera interrogantes sobre el impacto de la seguridad de datos en la implementación eficiente de herramientas de realidad aumentada en el ámbito deportivo.

El problema en la seguridad de datos ejerce un impacto importante en la ejecución exitosa de aplicaciones de realidad aumentada en eventos deportivos. Las preocupaciones relacionadas con la seguridad generan una serie de obstáculos y desconfianza tanto entre los usuarios finales como en las entidades deportivas. La falta de un marco robusto para salvaguardar la información personal y sensible disminuye la aceptación y adopción de estas aplicaciones, afectando la confianza del público y generando reticencias en los patrocinadores y socios comerciales. La fragilidad de la información puede, en consecuencia, iniciar una serie de consecuencias negativas que ponen en riesgo la implementación eficiente de herramientas de realidad aumentada en el ámbito deportivo.

La protección de la información se convierte en un aspecto crítico en el contexto de la implementación de herramientas de realidad aumentada en eventos deportivos durante el año 2023. A medida que las entidades deportivas adoptan tecnologías avanzadas para optimizar la interacción y la experiencia del usuario, Surgen desafíos significativos en la salvaguarda de datos confidenciales. La captación y el intercambio de datos en entornos de realidad aumentada implican riesgos potenciales que pueden vulnerar la privacidad de los usuarios y comprometer la seguridad de la información. Este riesgo plantea interrogantes sobre la forma en que la seguridad de datos impacta directamente en el despliegue efectivo de aplicaciones de realidad aumentada en el contexto deportivo.

La continuidad del desafío de seguridad de datos en la implementación de aplicaciones de realidad aumentada en eventos deportivos conlleva implicaciones de gran alcance. En primer lugar, la desconfianza generalizada puede llevar a una baja participación de los aficionados y usuarios potenciales, lo que afecta negativamente la rentabilidad y sostenibilidad financiera de los eventos deportivos. Además, la exposición y manipulación no autorizada de datos sensibles podrían generar escándalos de privacidad, erosionando la reputación de las entidades deportivas involucradas. Este escenario amenaza con crear un circulo repetitivo en

La insuficiencia en la protección de datos dificulta la integración de soluciones de realidad aumentada, comprometiendo así el éxito global de los eventos deportivos que buscan aprovechar esta tecnología emergente.

1.3. Formulación del problema

1.3.1. Problema general

¿Cómo se relaciona la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023?

1.3.2. Problemas específicos

- ¿Cómo se relaciona la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023?
- ¿Cómo se relaciona la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023?
- ¿Cómo se relaciona la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023?

1.4. Antecedentes

1.4.1. Antecedentes nacionales

Sosa (2022) llevaron a cabo una investigación denominada “Phishing como modalidad de delitos informáticos: un análisis sobre la usurpación y hurto dirigido a los beneficiarios del subsidio universal en Perú”. Con el fin de obtener la certificación de posgrado, este estudio tiene como objetivo examinar las carencias identificadas.en la definición actual del Phishing en las regulaciones de Perú, Ley N°30096. Resulta destacable que los delincuentes cibernéticos encuentran métodos simples para establecer credibilidad con entidades, como el intercambio de contraseñas y otros datos personales confidenciales. Además, se pretende determinar si la RENIEC, encargada de salvaguardar la información personal como un derecho legal de los ciudadanos beneficiarios, cuenta con un sistema efectivo para protegerla adecuadamente y prevenir la vulneración del derecho a la identidad. La importancia de este estudio se fundamenta en que organismos gubernamentales, como la RENIEC en este contexto, al desarrollar sistemas para que los ciudadanos validen su elegibilidad para recibir bonos, deben asegurar la protección de la información. Sin embargo, la plataforma resultó vulnerable, permitiendo a hackers acceder al mercado negro con los datos de los beneficiarios, afectando a miles de ciudadanos que descubrieron que sus bonos ya habían sido cobrados. Esto configura la figura de suplantación, subrayando la necesidad de abordar estas deficiencias en las leyes y procedimientos de protección de información.

Flores y Uriarte (2023) realizaron una investigación titulada "Influencia de las herramientas tecnológicas en el crimen cibernético de suplantación de identidad en el sector de las telecomunicaciones, Jaén 202", Con el propósito de alcanzar el grado académico de posgrado, esta investigación se desarrolla a partir de la identificación de una problemática específica en la región de Jaén, así como en el contexto peruano, respecto al ciberdCrimen de usurpación de identidad, donde se emplean tecnologías como el principal instrumento. Se

observó que este delito no está específicamente regulado y presenta vacíos normativos, ya que las normas existentes no se adecúan a las nuevas modalidades de estos ciberdelitos innovadores, al depender en gran medida de normativas genéricas. Además, se identificó que las querellas por usurpación de identidad no avanzan y se archivan debido a la falta de agentes policiales, expertos y fiscales especializados en delitos cibernéticos de este tipo en Jaén. El propósito central de esta investigación es examinar de qué manera las soluciones tecnológicas contribuyen a facilitar el delito informático de usurpación de identidad en el ámbito de las telecomunicaciones en Jaén, durante el año 2022. Para alcanzar dicho objetivo, se adoptó un enfoque de investigación cualitativa, utilizando un diseño basado en la teoría fundamentada. Se utilizaron metodologías como el análisis documental y entrevistas con individuos con experiencia para recabar datos pertinentes que respaldaran la premisa general de que los medios tecnológicos efectivamente influyen en el crimen cibernético de usurpación de identidad en el sector de las telecomunicaciones en Jaén en el año 2022.

Chilcon (2019) realizó un estudio titulado "El Delito Informático en la República del Perú y su Influencia en la Defensa Nacional" con el fin de obtener un grado académico avanzado. El objetivo primordial consiste en determinar el efecto del delito informático en la defensa nacional de Perú. En términos metodológicos, Se aplica una metodología de tipo cuantitativo con un enfoque descriptivo-explicativo, basada en un diseño de investigación no experimental. La población analizada está compuesta por líderes y expertos en la gestión de delitos cibernéticos, pertenecientes a entidades como la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial, totalizando 580 funcionarios. La muestra seleccionada incluye a 231 participantes, a quienes se les aplica un cuestionario estructurado con una escala Likert. La validación de las hipótesis se realiza mediante la prueba de Chi Cuadrado. Los resultados del análisis general de la investigación evidencian que el impacto del delito cibernético en Perú tiene una incidencia considerable en la Seguridad Nacional. Como parte de las

recomendaciones finales, se propone la adopción de estrategias para combatir el delito informático.

Chipana et al. (2023) se llevaron a cabo una investigación denominada "El E-mail, como vehículo de infiltración del Engaño y delito cibernético". En los últimos tiempos, el crimen digital ha experimentado un incremento notable en situaciones de fraude cibernético, especialmente a través del correo electrónico empleando la táctica de phishing. Este fenómeno ha generado una preocupación creciente entre los usuarios de esta plataforma digital. El propósito de este análisis fue identificar y examinar los hallazgos más significativos vinculados al correo electrónico y al phishing como métodos de acceso no autorizado, destacándose como una de las modalidades más prominentes de fraude digital. Para realizar la revisión bibliográfica, se consultaron fuentes secundarias siguiendo el enfoque metodológico de análisis sistemático. Se accedió a las bases de datos de Scopus, Scielo, Web of Science, Pro Quest, Redalyc, Ebsco y Latindex, centrando la búsqueda en investigaciones de los últimos 5 años y en idioma español de manera gratuita. Se llevó a cabo la búsqueda y verificación de la producción académica mediante la aplicación de filtros de términos como "correo electrónico", "crimen digital", "phishing" y "delito cibernético", excluyendo los documentos publicados en 2017 o antes, así como aquellos que no estaban disponibles para su descarga sin costo. Los descubrimientos resaltan la relevancia de promover una sensibilización sobre seguridad al utilizar y administrar los correos electrónicos. El estudio enfatiza la necesidad imperiosa de promover una cultura digital que incluya acciones efectivas para evitar los ataques de phishing que impactan tanto a personas como a entidades. Esto se posiciona como una táctica fundamental para reducir las consecuencias del fraude informático, el delito digital más frecuente en el ámbito de la ciberdelincuencia en la actualidad.

Aredo (2021) desarrolló una investigación titulada "La Intercepción y su Influencia en la Infracción de la Salvaguarda de Datos Personales en los Delitos Informáticos" con el

propósito de alcanzar una titulación de posgrado. El objetivo central de este estudio radica en establecer si la interceptación de comunicaciones impacta la protección de los datos personales en el ámbito de los delitos cibernéticos, estableciendo objetivos específicos dirigidos a analizar las dimensiones e implicancias de dicha intercepción en la apropiación indebida de información personal. La protección de datos personales es identificada como esencial para asegurar el derecho a la privacidad, junto con un análisis exhaustivo de los elementos de los delitos informáticos estipulados en el código penal peruano. Este estudio se clasifica como una investigación teórica, centrada en el análisis documental sin implicar aplicaciones prácticas. Los resultados subrayan la necesidad de reformar la normativa vigente, ya que el daño a la persona puede derivar en la comisión de otros delitos. Asimismo, se recomienda la implementación de campañas de sensibilización mediática para promover una cultura preventiva y mitigar la manipulación psicológica. En las conclusiones, se indica que a través de artimañas se explota la falta de conocimientos en informática. Se propone la adopción de mecanismos de validación, como la verificación biométrica y facial, en conjunto con claves digitales enviadas por medio de mensajes de texto, para resguardar los datos personales. Se destaca que los componentes de los delitos informáticos presentan definiciones demasiado amplias que obstaculizan la precisa delimitación del phishing.

García y Guevara (2023) realizaron un estudio denominado "Mitigación del phishing a través de la modificación del sistema de denominación de dominios para prevenir la sustracción de datos en plataformas web de pequeñas empresas en Perú mediante el uso de inteligencia artificial" con el fin de obtener un grado académico avanzado. En los últimos tiempos, los criminales informáticos han perfeccionado sus tácticas para llevar a cabo ataques digitales, especialmente en el ámbito del robo de información confidencial. La manipulación psicológica emerge como la estrategia más recurrentemente utilizada entre los ciberdelincuentes, quienes la emplean para influir en individuos y revelar datos delicados. Un ejemplo de estratagema de

suplantación de identidad es la Manipulación del Sistema de Nombres de Dominio (DNS), una táctica en la que el atacante no apunta a un individuo específico, sino que altera o compromete el servidor DNS, afectando a todos los usuarios que utilizan dicho servicio. A pesar de los esfuerzos de investigación para detectar los ataques de phishing mediante la manipulación del DNS, los delincuentes cibernéticos continúan perfeccionando sus estrategias y presentando nuevos métodos que resultan difíciles de identificar. En este marco, se realizó una investigación enfocada en la identificación de ataques de phishing mediante la alteración del servidor DNS en aplicaciones web. Se emplearon algoritmos de Aprendizaje Automático basados en su precisión validada en investigaciones anteriores. Los resultados revelaron que, entre los algoritmos de detección como Naive Bayes, XGBoost, Random Forest y Perceptrón Multicapa, Naive Bayes demostró la superioridad más significativa, con un índice de precisión del 99.04% en la detección de ataques de corrupción hacia los servidores DNS. La Red Neuronal Multicapa registró una tasa del 80%, superando tanto a XGBoost como a Random Forest, que alcanzaron un 63% y 75% de precisión, respectivamente. Estos hallazgos subrayan la eficacia comprobada de Naive Bayes en la detección de ataques de phishing, resaltando su relevancia en la salvaguarda frente a este tipo de riesgos.

Medina (2022) llevó a cabo una investigación titulada "Centro Deportivo Tradicional como Promotor de la Cohesión Social caso: Zona el avance Carabayllo" con el fin de obtener la titulación universitaria de pregrado. El análisis define los centros deportivos convencionales como instalaciones destinadas a actividades deportivas convencionales, con estructuras especialmente concebidas para la promoción deportiva y la participación en varias disciplinas. Estas instalaciones buscan ofrecer servicios médicos, técnicos y educativos, dirigidos tanto a personas en formación como a promesas emergentes en el ámbito deportivo. Con respecto a la variable 2, se adopta la perspectiva de Foster, Resalta la relevancia de la inclusión comunitaria y la consolidación de espacios públicos como soluciones arquitectónicas para individuos y

colectividades. La integración social, según la conceptualización de Los Santos, implica la unión de personas excluidas socialmente. Los objetivos del estudio se enfocaron en examinar la conexión entre la variable "Infraestructura Deportiva Convencional" y sus aspectos con la variable "Solidaridad Social en Carabayllo en 2019" y sus respectivas dimensiones, utilizando el método hipotético-deductivo. Con un nivel de confianza de 0.880 entre ambas variables, los hallazgos principales revelaron una correlación positiva significativa entre la primera variable. (Infraestructura Deportiva Convencional) y la segunda variable (Solidaridad Social en 2019), así como correlaciones notables en otras asociaciones. En resumen, el estudio reveló que existe una relación moderadamente favorable de 0.752 unidades entre la variable "Infraestructura Deportiva Convencional" y la variable "Solidaridad Social" en Carabayllo en el año 2019.

Egúsquiza (2022) elaboró una investigación titulada "Aplicación de Realidad Aumentada para Mejorar las Competencias Digitales de Profesores en el Campo de Electrotecnia Industrial en un Instituto de Educación Técnica Superior (IEST), Lima 2022", Con el objetivo de cumplir con los requisitos necesarios para obtener el título de pregrado, esta investigación se propuso analizar el impacto de la integración de la realidad virtual en el desarrollo de competencias digitales en profesionales con experiencia en Ingeniería Eléctrica Industrial, en una Institución de Educación Superior en Lima durante el año 2022. Se adoptó un enfoque cuantitativo, clasificado como básico según su propósito, con un diseño no experimental de tipo transversal y correlacional causal. La población objeto de estudio estuvo compuesta por 120 docentes de la mencionada Institución, de los cuales se seleccionó una muestra total de 120 participantes. La investigación empleó la metodología de encuesta, aplicando dos cuestionarios validados y confiables. Los hallazgos revelan que la aplicación de la realidad virtual es considerada satisfactoria para el 38% de los profesores, mientras que el nivel de habilidades digitales se sitúa en un nivel avanzado para el 65% de ellos. En resumen, se concluye que la implementación de la realidad virtual tiene un impacto significativo en las

competencias digitales de los docentes en el Instituto Superior Tecnológico, como lo indica el análisis estadístico de Nageelkerke, con un nivel de eficacia del 27.6%, $p < 0.05$ y Wald > 4.

1.4.2. Antecedentes internacionales

Ospina y Sanabria (2020) condujeron un estudio de análisis denominado "Abordaje Nacional frente a los Desafíos de la Protección Digital en el Contexto Global: Un Estudio para Colombia", con el fin de obtener el título universitario de pregrado. Este informe examina la temática de la salvaguarda de datos a nivel internacional, enfocándose especialmente en las amenazas en línea, a través de un análisis de la coyuntura actual en Colombia. Mediante un enfoque de estudio cualitativo, conceptual, documental y explicativo, se realiza una evaluación histórica de la seguridad digital, explorando áreas como la ciberconfrontación, la cibervigilancia y los crímenes digitales, con un especial interés en el aspecto de protección de la información. Se exploran diversos elementos conexos, tales como entornos, evaluaciones de peligros, plataformas de administración y criterios de excelencia, subrayando los riesgos para organizaciones, la comunidad y naciones, especialmente en el contexto de la pandemia de coronavirus (COVID-19). Se analizan de manera específica los datos relacionados con las acciones gubernamentales en Colombia en respuesta a estas amenazas, así como las directrices de protección digital y los estándares de excelencia adoptados. La conclusión del informe enfatiza los desafíos que enfrenta Colombia en el ámbito de la protección de datos frente a las crecientes amenazas digitales.

Cornejo y Sánchez (2023) llevaron a cabo un estudio titulado "La Preservación de Datos Personales frente a la Práctica Fraudulenta de Acceso a Datos". En este contexto de rápido desarrollo tecnológico y creciente actividad digital, la protección de la información sensible se posiciona como una prioridad esencial para salvaguardar los derechos fundamentales y la privacidad de los individuos en el ámbito digital. El objetivo fundamental de esta investigación es examinar el marco legal vigente en Ecuador orientado a salvaguardar

la confidencialidad de los datos personales frente a accesos no autorizados. Para alcanzar este fin, se llevará a cabo un análisis detallado de la normativa pertinente relacionada con la protección de datos personales, incluyendo la Ley de Protección de Datos Personales y el Código Integral Penal, prestando especial atención al delito de acceso no autorizado a la información, con el fin de determinar cómo estas regulaciones respaldan y protegen la información de los individuos frente a posibles actividades delictivas en el ámbito digital. Surge la duda sobre la efectividad de la legislación ecuatoriana en cuanto a la salvaguardia de los datos personales, así como la pertinencia de recurrir a la vía judicial como medio de protección. Dada la evolución constante del panorama digital, es crucial comprender la amplitud y complejidad de este desafío, así como la importancia de adoptar precauciones adecuadas para mitigar los riesgos asociados. La metodología empleada se basará en enfoques inductivos, documentales y analíticos, con un examen minucioso de las disposiciones legales relevantes en Ecuador. Este estudio aspira a proporcionar una perspectiva holística que pueda actuar como fundamento para el desarrollo de futuras políticas de protección de datos en el país.

Arcos et al. (2023) se realizó un análisis titulado "Comparación de la normativa de protección de datos personales en Ecuador y Colombia desde una perspectiva de seguridad cibernética y delitos digitales". La proliferación de Internet y el progreso tecnológico han transformado nuestra vida diaria y la manera en que ejecutamos nuestras tareas, destacando la importancia de mantener una conectividad permanente. Sin embargo, esta constante interacción ha incrementado el riesgo de exponer información personal, propiciando la ocurrencia de delitos digitales significativos que vulneran los derechos a la protección de datos personales y la privacidad. La carencia de una legislación global eficaz ha dificultado la lucha contra la ciberdelincuencia, lo que ha obligado a los gobiernos a promulgar leyes para proteger a sus ciudadanos. Las organizaciones deben implementar sistemas de seguridad de la

información y adherirse a los procedimientos y políticas pertinentes para gestionar la información que se recopila, procesa y almacena en este contexto. Este documento examina las normativas de Colombia y Ecuador en relación con la protección de datos personales y delitos digitales, así como las propuestas para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que cumpla con los requisitos legales de protección de datos.

Elías (2019) llevó a cabo una investigación titulada "Protección Informática en la Administración de la Información de la Alcaldía de Luján de Cuyo" con el objetivo de obtener un grado académico de doctorado. Este estudio se enfoca en el manejo de la información en la seguridad informática de la Alcaldía de Luján de Cuyo, ubicada en la provincia de Mendoza. Con este propósito, se realiza un análisis exhaustivo del riesgo vinculado a la ocurrencia de diversos tipos de perjuicios informáticos, los cuales son originados por amenazas que explotan las vulnerabilidades y las consecuencias de dichas amenazas. La protección física, la protección lógica y la protección del sistema de administración y comunicación son los tres aspectos principales que se exploran. Se identifican y explican varias modalidades de infracciones informáticas y conductas ilegales llevadas a cabo mediante sistemas. Cada sección comienza con una introducción a los principios y rasgos generales de estos ámbitos, seguida de una descripción pormenorizada de sus aplicaciones específicas en el contexto municipal. Asimismo, se detallan las medidas de resguardo, las políticas de protección y el protocolo de emergencia que han sido establecidos. Se presentan también los procedimientos, procesos y previsiones sugeridos como acciones preventivas, fundamentales para mitigar el riesgo existente a niveles considerados aceptables.

Ochoa (2021) realizó un trabajo de investigación llamado "Desafíos globales del cibercrimen: caso Ecuador periodo 2014–2019" para obtener una maestría. Las transgresiones informáticas o actos de delincuencia digital adoptan configuraciones cada vez más complejas

y evolucionadas para infiltrarse en el ámbito digital y llevar a cabo actividades ilícitas de manera menos detectable conforme avanza el progreso tecnológico. Esta problemática se vuelve un desafío global para todas las naciones. En el contexto de Ecuador, esta cuestión se vuelve compleja, dado que abarca la capacidad institucional, la formulación de políticas de ciberseguridad, así como la implementación de regulaciones y estrategias para combatir el cibercrimen. El objetivo principal de esta investigación es analizar los desafíos globales asociados con la actividad delictiva en el ciberespacio, prestando especial atención a la normativa en Latinoamérica y a las estrategias desarrolladas para contrarrestar dicha actividad. En este contexto, el primer segmento se centra en un análisis teórico del cibercrimen y su clasificación, así como en los retos globales que enfrenta tanto el sector privado como el público, junto con los esfuerzos por implementar medidas de seguridad digital en ambos ámbitos. También se revisan los acuerdos internacionales aplicados en la lucha contra el cibercrimen, para posteriormente contextualizarlos en el marco ecuatoriano. Finalmente, el tercer apartado presenta y evalúa casos específicos relacionados con la sustracción de información personal de ciudadanos ecuatorianos en 2019, así como el caso de Julian Assange.

Carvajal et al. (2021) realizó una investigación titulada "Elaboración de un Esquema de Protección de Datos para el Sistema de Información de la Institución Educativa Gimnasio Los Pinos", con el propósito de obtener el grado de Maestría. La principal meta de este estudio fue desarrollar un manual de protección de datos que asegure la confidencialidad, integridad y disponibilidad de los sistemas de información de la Institución Educativa Gimnasio Los Pinos, situada en Bogotá, D.C. Se utilizó como referencia el Esquema de Protección y Confidencialidad de Datos (EPCD) del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), que se alineaba con las directrices del instructivo número tres de la NORMA TÉCNICA COLOMBIANA ISO 27001. Las tácticas propuestas estaban en sintonía con los estándares ISO 27001, lo que facilitaba la organización eficaz para la puesta

en práctica del plan propuesto. Este enfoque se fundamentó en un análisis explicativo que tenía como propósito comprender el panorama presente en la Institución Educativa Gimnasio Los Pinos, especificando las operaciones, los métodos, la obtención de información y los participantes. Aunque la recolección de datos no fue del todo precisa, posibilitó realizar un examen exhaustivo que mostró las amenazas de seguridad que podrían haber influido en el funcionamiento de la organización. La formulación de una directriz de seguridad demanda atención a diversos elementos fundamentales de un Sistema de Gestión de la Seguridad de la Información en cualquier organización. El análisis de riesgos facilitó la comprensión del estado actual de la empresa en términos de seguridad en el centro de información. Según el análisis de la normativa ISO/IEC 27001:2013, es necesario aplicar un plan y una directriz de seguridad para mitigar los riesgos y las debilidades. La utilización de una herramienta de supervisión, los protocolos de seguridad y la configuración de redes demostraron ser eficaces para disminuir las debilidades de los sistemas y elevarlos a un nivel óptimo de protección. En síntesis, este proyecto logró alcanzar todos sus objetivos.

Guanotasig et al. (2023) realizaron una investigación titulada "Ejecución de un modelo de crecimiento progresivo de programas informáticos que permita la identificación y mitigación de "ataques de ingeniería social a través de técnicas de Aprendizaje Profundo", con el objetivo de obtener su grado académico de posgrado. El propósito del estudio es identificar y mitigar el Shoulder Surfing, un tipo de ataque de ingeniería social, mediante el desarrollo de software avanzado que emplee tecnologías contemporáneas como el Reconocimiento Facial y las Redes Neuronales Convolucionales, complementadas por el Procesamiento de Imágenes y la Visión por Computadora. En el uso de la técnica La metodología SCRUM, conocida por su capacidad para agilizar procesos y producir resultados eficientes y de alta calidad, se utilizó. El método del módulo de reconocimiento facial se basó en un proceso de nueve pasos, desde la carga y extracción de datos de imágenes hasta la detección e identificación de personas, con

pasos adicionales como la reducción, el registro y la notificación. Se realizaron pruebas de experiencia de usuario, evaluaciones de rendimiento de mitigación y evaluaciones de reconocimiento facial. Los hallazgos mostraron que la resolución del video proporcionado al sistema en tiempo real es el principal factor que determina las características de potencia de los dispositivos. Se creó una ecuación para estimar el tiempo de procesamiento del reconocimiento facial, que indica que el tiempo de procesamiento aumenta aproximadamente 3.06 segundos por cada 5 imágenes. Estos resultados tienen el potencial de mejorar significativamente el nivel de ciberseguridad, especialmente en entornos familiares, académicos, comerciales e industriales, ofreciendo una defensa más efectiva contra el surf de hombros y sus posibles efectos financieros, reputacionales y morales.

Mina (2023) llevó a cabo un estudio de investigación titulado "Elaboración de directrices de protección con la aplicación de la Normativa ISO 27001:2013 para resguardar los recursos de datos en la compañía Robtelcom" con el propósito de alcanzar el título académico de pregrado. El objetivo de esta investigación fue elaborar un conjunto de políticas de seguridad de la información que cumplan con los estándares ISO 27001:2013. Este marco tiene como objetivo optimizar la gestión de la base de datos de clientes y el manejo de la información, así como identificar y minimizar las vulnerabilidades y riesgos potenciales relacionados con la divulgación o pérdida de datos. La metodología utilizada incluyó la aplicación de diversos métodos, técnicas e instrumentos para recopilar información y abordar problemas. La propuesta se fundamentó en la normativa ISO 27001:2013 para salvaguardar los activos informativos de la empresa Robtelcom, cumpliendo así con los objetivos planteados en la sección anterior. El análisis de riesgos identificó las principales deficiencias de la empresa y priorizó las etapas de implementación sugeridas. El examen de riesgos facilitó la detección de potenciales amenazas y peligros que podrían impactar las actividades al señalar las principales debilidades de la entidad. La tabla de riesgos posibilitó la priorización de las fases sugeridas

para su ejecución. El alcance inicial del sistema de gestión de seguridad de la información (SGSI), basado en la normativa ISO 27001:2013, se extenderá progresivamente para englobar la totalidad de los recursos de datos de Robtelcom. La tecnología MAGERIT reveló la recurrencia y la magnitud de las amenazas sobre los activos de la organización. Esto condujo a la formulación de políticas adaptadas a las necesidades corporativas y a la creación de un esquema que inicialmente se enfocará en ciertos recursos de información y que se expandirá gradualmente para incluir todos los activos de Robtelcom.

1.5. Justificación de la investigación

Este estudio adquiere fundamentos sólidos al examinar de manera práctica la convergencia entre la protección de datos y la ejecución exitosa de aplicaciones de realidad aumentada en eventos deportivos. En la actualidad, la utilización de la tecnológica emergente como la realidad aumentada ha ganado relevancia en el ámbito deportivo, proporcionando experiencias inmersivas y mejorando la participación de los aficionados. No obstante, este progreso tecnológico implica riesgos Son inherentes a la protección de datos, ya que implican la recopilación y gestión de información sensible tanto de los usuarios como de las propias operaciones internas.

Desde una perspectiva teórica, la investigación se fundamenta en la comprensión de la seguridad de datos y las prácticas óptimas relacionadas con la ejecución de aplicaciones de realidad aumentada en el contexto deportivo. Se explorarán conceptualizaciones y teorías relacionadas con la seguridad de datos en entornos tecnológicos, de la misma manera que los cimientos conceptuales de la realidad aumentada y su aplicación en eventos deportivos. Esta revisión teórica proporcionará un marco conceptual sólido que permitirá entender las complejidades y desafíos de esta interrelación.

Metodológicamente, la investigación se justifica al considerar la necesidad de desarrollar y ajustar herramientas de recopilación de información que posibiliten la evaluación tanto la seguridad de datos como el éxito en la implementación de utilidades de realidad aumentada en eventos deportivos. Se realizará un examen de los factores críticos, reconociendo aspectos e índices pertinentes para valorar la protección de información y el cumplimiento de metas en la implementación de tecnologías de realidad aumentada. Estos instrumentos pasarán por rigurosos procesos de validación y confiabilidad para asegurar la excelencia de la información obtenida, estableciendo así un fundamento robusto para la reproducción de la investigación en entornos análogo. Este exhaustivo análisis proporcionará una perspectiva valiosa que servirá como fundamento preliminar para investigaciones futuras en el campo de la protección de datos y la integración de la realidad aumentada en el ámbito de eventos deportivos'.

1.6. Limitaciones de la investigación

La existencia de información sobre la efectiva ejecución de aplicaciones de realidad aumentada en eventos deportivos puede encontrarse limitada en términos de calidad y cantidad. La carencia de acceso a información específica o detallada acerca de la seguridad de datos en eventos similares podría comprometer la exhaustividad del análisis.

Es fundamental reconocer que tanto la tecnología de aumento de realidad como la protección de datos son ámbitos en constante transformación. Las limitaciones pueden surgir si la tesis no contempla las modificaciones tecnológicas o las nuevas amenazas a la seguridad de datos que puedan surgir durante o después del período de investigación.

1.7. Objetivos

1.7.1. Objetivo general

Determinar cómo se relaciona la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023.

1.7.2. Objetivos específicos

- Identificar como se relaciona la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023
- Determinar la relación entre la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023
- Determinar la relación entre la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023

1.8. Hipótesis

1.8.1. Hipótesis general

Existe una relación significativa entre la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023.

1.8.2. Hipótesis específicas

- Existe una relación significativa entre la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023
- Existe una relación significativa entre la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023
- Existe una relación significativa entre la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023

II. MARCO TEÓRICO

2.1. Marco conceptual

2.1.1. Análisis de Datos

Burbano (2020) el propósito fundamental del análisis de datos en una entidad deportiva es transformar la información cruda en datos valiosos, útiles y procesables. Esto posibilita la toma de decisiones estratégicas, impulsando así un rendimiento financiero superior y una ventaja competitiva sólida y mensurable.

2.1.2. Integración de datos

La integración respalda el análisis de grandes conjuntos de datos al alinear, combinar y presentar información de varios departamentos y fuentes externas. Este proceso busca alcanzar los objetivos planteados por el responsable de la integración. (Power Data, 2023)

2.1.3. Privacidad de los usuarios

Para que los datos de un usuario se mantengan privados, se requiere un control riguroso en su manejo. Los datos personales suelen organizarse de manera que la privacidad del usuario se ve comprometida, ya que pierde el control sobre información que puede ser copiada o compartida sin su consentimiento. (Romero, 2017).

2.1.4. Ciberseguridad

La ciberseguridad abarca una serie de recursos, estrategias, normativas, prácticas, técnicas de gestión de riesgos, educación, estándares, coberturas y tecnologías, orientadas a salvaguardar los activos de una entidad y sus usuarios en el entorno digital. (Cando y Chicaiza, 2021).

2.1.5. Confidencialidad en la transmisión de datos

Cotino (2018) el propósito de la confidencialidad es garantizar la efectividad y el logro exitoso de la mediación. Se busca prevenir el temor o restricción, ya que la información y las comunicaciones generadas en la mediación podrían ser empleadas en su contra en futuros

procedimientos de resolución de disputas. La confianza mutua, facilitada por la confidencialidad, permite que las partes se expresen libremente para encontrar de manera voluntaria la solución que consideren más adecuada.

2.1.6. *Ciberataques*

Martínez (2019) menciona un ciberataque como una acción deliberada llevada a cabo por una persona o un conjunto de individuos con el propósito de atacar el sistema informático de otro individuo u organización. Su objetivo puede ser la destrucción de dispositivos electrónicos o la obtención de ganancias económicas.

2.1.7. Gestión de acceso y permisos

Mora (2016) define como un dispositivo electrónico que regula la entrada o salida de un usuario o conjunto de usuarios a un lugar determinado. Esto se logra verificando la identificación a través de diversos métodos de lectura, al mismo tiempo que administra el acceso mediante un dispositivo eléctrico como un electroimán, cerrojo o motor.

2.1.8. Respaldo y recuperación de datos

Los respaldos de datos se refieren al procedimiento de crear una copia de todos los datos o partes de archivos almacenados en dispositivos como computadoras, servidores u otros medios. Esta acción tiene como objetivo la posibilidad de recuperarlos en cualquier momento en caso de daño o pérdida de los archivos originales. (Clavijo, 2017)

2.1.9. *Cumplimiento normativo*

Cumplimiento Normativo se refiere a la entidad independiente que, mediante políticas y procedimientos idóneos, identifica y controla el riesgo relacionado con el incumplimiento de regulaciones, tanto internas como externas, que conciernen a una organización. (Paagman, 2014)

2.1.10. Espionaje

Mayer y Vera (2020) lo definen como conducta que se vincula con la idea de revelación

indebida de secretos, la cual puede manifestarse al ingresar de forma indebida a información confidencial o al divulgar esa información a terceros, ya sea que se haya obtenido legítimamente o no. En resumen, implica la infracción del secreto, ya sea al conocer la información por cuenta propia o al compartirla con otras personas.

2.2. Estado del arte

2.2.1. Seguridad de datos

Cruz et al. (2022) indica que es un ámbito crucial que se enfoca en la instauración de medidas y tácticas para asegurar que la información almacenada y tratada en los sistemas computarizados sea protegida, fiable y alcanzable. Estas estrategias, que abarcan el encriptado, los sistemas de control de acceso y las evaluaciones, se diseñan para disminuir los riesgos tales como el acceso no autorizado o la manipulación intencionada de los datos. La protección de datos adquiere una importancia creciente en un entorno digital en constante evolución, siendo fundamental para resguardar información crítica y mantener la confianza en la integridad de los sistemas.

Quissanga y Fernandez (2020) añaden que la relevancia de la seguridad de datos se intensifica ante el constante crecimiento de amenazas cibernéticas y la expansión de la interconexión digital. La adopción de tecnologías de vanguardia, combinada con estrategias robustas de protección, emerge como una necesidad ineludible para asegurar una defensa eficaz contra posibles puntos débiles y garantizar la continuidad operativa de las entidades y sistemas en un entorno global cada vez más orientado hacia la información digital.

2.2.1.1. Protección de Datos. Mendoza (2021) indica que se dirige a proteger la confidencialidad y la integridad de la información personal que se procesa y almacena en sistemas informáticos. Esta perspectiva implica la implementación de políticas y medidas destinadas a prevenir el acceso no autorizado, la pérdida accidental o la manipulación maliciosa de datos sensibles. La seguridad de los datos abarca aspectos legales y éticos, incluyendo el

aseguramiento del cumplimiento con normativas de privacidad, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. La protección de datos se establece como un requisito esencial para mantener la confianza del público y garantizar una gestión ética de la información personal en un entorno donde la privacidad está cada vez más amenazada por la interconexión digital.

A. Encriptación de Datos. Solis et al. (2017) añade que se basa en asegurar la confidencialidad y la integridad de la información personal que se procesa y almacena en sistemas informáticos. Esta premisa implica la implementación de políticas y medidas destinadas a prevenir el acceso no autorizado, la pérdida accidental o la manipulación deliberada de datos sensibles. La seguridad de la información comprende consideraciones legales y éticas, incluyendo el cumplimiento de normativas de privacidad como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. La protección de los datos se configura como un requisito esencial para mantener la confianza del público y garantizar un manejo ético de la información personal en un entorno donde la privacidad es cada vez más vulnerable debido a la interconexión digital.

B. Control de Acceso. Rivas (2016) lo define como el conjunto de medidas y políticas diseñadas para regular y limitar la entrada y uso de recursos o información en sistemas informáticos. Este proceso tiene como objetivo principal garantizar que solo usuarios autorizados puedan acceder a determinados datos, sistemas o áreas, mientras se restringe el acceso a aquellos individuos no autorizados. El control de acceso se implementa a través de diversos mecanismos, como la autenticación mediante contraseñas, tarjetas de acceso, biometría u otros métodos de verificación de identidad. Además, se establecen niveles de privilegios que determinan qué acciones o datos pueden ser accedidos por cada usuario autorizado. Este enfoque no solo contribuye a la seguridad de la información, sino que también

desempeña rol en el cumplimiento de regulaciones y normativas de privacidad al limitar el acceso a datos sensibles a aquellos con necesidad y autorización específicas.

C. Respaldo de Datos. Solis et al. (2017) señala que es una práctica importante en el ámbito de la seguridad de la información que consiste en copiar y guardar datos importantes para evitar que se pierdan debido a eventos desfavorables, como fallas técnicas, ataques cibernéticos o errores humanos. Este proceso requiere la creación de copias regulares de datos en un medio de almacenamiento secundario, como discos externos, servidores remotos o servicios en la nube. Su enfoque se dirige a garantizar la confidencialidad y la integridad de la información personal que se procesa y almacena en sistemas informáticos. Esta premisa implica la implementación de políticas y medidas diseñadas para prevenir el acceso no autorizado, la pérdida accidental o la manipulación deliberada de datos sensibles. La seguridad de los datos incluye consideraciones legales y éticas, abarcando el cumplimiento de normativas de privacidad como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. La protección de datos se establece como un requisito fundamental para mantener la confianza del público y asegurar una gestión ética de la información personal en un contexto donde la privacidad es cada vez más vulnerable debido a la interconexión digital.

D. Recuperación de Datos. Salvador y Arquero (2006) se refieren al proceso de restaurar información que ha sido perdida, dañada o comprometida de alguna manera. Este proceso se activa en situaciones que pueden incluir desde errores humanos y fallas técnicas hasta eventos más graves como ataques cibernéticos o desastres naturales. La recuperación de datos implica la utilización de copias de seguridad previamente almacenadas durante la fase de respaldo, así como la aplicación de técnicas especializadas para recuperar datos que no han sido respaldados.

Bordignon y Tolosa (2007) indican que existen diversos enfoques y herramientas disponibles para la recuperación de información, y su eficacia se basa en la naturaleza del

problema y la prontitud con la que se identifica y resuelve la pérdida de datos. La capacidad para recuperar datos de manera efectiva resulta vital tanto en entornos empresariales como personales, con el fin de minimizar los impactos de las interrupciones y asegurar la continuidad de las operaciones. La recuperación de información también constituye un elemento esencial en la gestión de incidentes de seguridad, ya que posibilita la restauración de la integridad y disponibilidad de los datos afectados por sucesos adversos.

2.2.1.2. Integridad de Datos. Rios et al. (2003) señala que representa un principio esencial en la seguridad de la información, asegurando que los datos se mantengan de forma precisa y coherente. Este concepto implica resguardar la información contra modificaciones o errores que puedan afectar su calidad. Se emplean medidas de control de acceso, firmas electrónicas y sistemas de vigilancia para detectar y prevenir cambios no autorizados con el fin de preservar la integridad. La integridad de datos es de suma importancia en entornos críticos, ya que asegura que la información almacenada sea fiable y adecuada para la toma de decisiones. Constituye un elemento indispensable de la gestión de la seguridad de la información.

A. Verificación de Integridad. Rios et al. (2023) añade que es una etapa fundamental en el ámbito de la seguridad de la información, cuyo propósito es verificar la exactitud y la coherencia de los datos almacenados. Este procedimiento se realiza mediante técnicas y herramientas que permiten detectar cualquier modificación no autorizada o error en la información. La verificación de integridad implica comparar datos actuales con versiones anteriores o copias de seguridad, empleando métodos como sumas de verificación, funciones hash o firmas digitales para asegurar que los datos no han sido alterados de manera indebida. Esta práctica es esencial para mantener la fiabilidad de la información en sistemas críticos, proporcionando una capa adicional de seguridad y confianza en la integridad de los datos almacenados.

B. Validación de Datos. Lima (2018) lo define como una etapa indispensable en la gestión de la información que se enfoca en garantizar la exactitud y la coherencia de los datos que ingresan en un sistema. Esta acción se ejecuta mediante la aplicación de normas y criterios previamente definidos, con la meta de garantizar que la información cumpla con determinados estándares y requisitos establecidos. La validación de datos puede incluir la verificación de formatos, rangos, relaciones lógicas, o la comparación con datos previamente almacenados. Este proceso no solo ayuda a mantener la calidad de la información, sino que también ayuda a prevenir errores y garantizar que los datos sean infalibles desde el principio. La validación de datos es crucial en entornos como bases de datos y sistemas de gestión para garantizar que la información almacenada sea confiable y útil.

2.2.1.3. Confidencialidad. Montece et al. (2017) indica que es un principio clave en la seguridad de la información que se enfoca en asegurar que la información sensible o confidencial sea protegida adecuadamente sea accesible únicamente por aquellos que están debidamente autorizados. Este principio implica la implementación de medidas y controles, como el cifrado, la gestión de accesos y políticas de confidencialidad, con el fin de prevenir el acceso no autorizado y la divulgación de datos sensibles. La confidencialidad es crucial en diversos contextos, tales como la salvaguarda de datos personales, secretos empresariales o información estratégica, y su preservación contribuye a la construcción y mantenimiento de la credibilidad en la administración de la información en entornos corporativos y organizacionales.

A. Restricciones de Acceso. Rivas (2016) indica que son medidas adoptadas en el ámbito de la seguridad de la información para restringir y regular el acceso a los recursos, sistemas o datos exclusivamente a los usuarios autorizados. Estas limitaciones se ejecutan mediante la configuración de políticas de gestión de accesos que establecen quiénes tienen permiso para acceder a qué recursos y en qué circunstancias. Las restricciones de acceso se

basan en la autenticación, la autorización y la verificación de identidad, utilizando métodos como contraseñas, tokens de seguridad, y otros mecanismos de autenticación. Es una etapa fundamental en la administración de la información que se centra en asegurar la precisión y la consistencia de los datos que ingresan a un sistema. Esta acción se ejecuta mediante la aplicación de normas y criterios previamente definidos, con la meta de garantizar que la información cumpla con determinados estándares y requisitos establecidos.

B. Gestión de Identidad y Acceso. Valles et al. (2023) señalan que es un sistema completo de procedimientos y tecnologías ideadas para gestionar y salvaguardar las identidades digitales de los usuarios, así como para regular su entrada a recursos y sistemas. Este enfoque se dedica a la autenticación, autorización y validación de la identidad, garantizando que únicamente los usuarios autorizados puedan acceder a datos específicos. La Gestión de Identidades y Accesos (IAM) se ocupa de la creación, modificación y eliminación de cuentas de usuario, la administración de contraseñas, la implementación de políticas de acceso y la supervisión de actividades. Este sistema contribuye a fortalecer la seguridad de la información al garantizar una gestión efectiva de las identidades digitales y proporcionar accesos fundamentados en los principios de necesidad y autorización. Es esencial en entornos empresariales para mitigar riesgos y mantener la integridad y confidencialidad de los datos.

2.2.1.4. Cumplimiento Normativo. Solis (2023) se refieren al proceso de garantizar que una entidad se adhiera a las leyes, regulaciones y estándares pertinentes en su sector industrial o ubicación geográfica. En el contexto de la seguridad de la información, el cumplimiento normativo implica la implementación y observancia de medidas específicas que aseguran que la gestión de datos y la seguridad de la información satisfagan los requisitos legales y las regulaciones aplicables. Esto puede abarcar normativas relacionadas con la privacidad, la protección de datos y la seguridad en línea, entre otros elementos. El cumplimiento normativo no solo evita posibles sanciones legales y multas, sino que también

fomenta la adopción de prácticas sólidas en seguridad de la información, consolidando la confianza de los clientes y la integridad operativa de la organización en un entorno donde la regulación y la conciencia sobre la privacidad son cada vez más significativas.

A. Políticas de Privacidad. Foster (2020) indica que son documentos que establecen las prácticas y procedimientos que una entidad, ya sea una organización o un sitio web, sigue para recopilar, gestionar, y proteger la información personal de los usuarios. Las directrices especifican qué datos se recolectan, cómo se emplean, quién tiene autorización para acceder a ellos y cómo se garantiza su secreto. Además, suelen comunicar a los usuarios sus derechos respecto a sus datos personales y el procedimiento para ejercerlos. Las políticas de confidencialidad son fundamentales para fomentar la transparencia y la confianza en la gestión de la información personal, y en muchos casos, son exigidas por leyes y regulaciones de protección de datos. Su adecuada aplicación no solo facilita el cumplimiento de las normativas, sino que también contribuye a forjar relaciones sólidas y éticas con los usuarios al asegurar un manejo correcto y seguro de la información personal.

B. Ajustes a Estándares de Seguridad. Valencia y Silva (2023) señalan que implican la adaptación y configuración de prácticas, procedimientos y controles de seguridad para cumplir con estándares específicos en un entorno particular. Estos estándares pueden ser dictados por regulaciones gubernamentales, normativas de la industria o mejores prácticas reconocidas. Al llevar a cabo ajustes en los criterios de seguridad, las organizaciones adaptan sus estrategias de protección para cumplir con los requisitos y expectativas establecidos, abordando aspectos como la gestión de identidades, el control de accesos, la encriptación, la protección de datos y otros elementos esenciales. Este proceso tiene como objetivo asegurar que la implementación de medidas de seguridad sea coherente con los estándares pertinentes, garantizando un nivel adecuado de resguardo de la información y promoviendo el cumplimiento normativo. La capacidad de adaptación y la revisión periódica de estos ajustes

son cruciales para mantener la eficacia de las prácticas de seguridad en un entorno tecnológico en constante cambio.

2.2.2. Implementación exitosa de aplicaciones de realidad aumentada

Laurens (2019) señala que implica una cuidadosa definición de objetivos y casos de uso específicos, la elección apropiada de tecnologías y plataformas, y la integración efectiva con sistemas existentes. La implicación activa de los usuarios finale, la recopilación temprana de retroalimentación y ajustes basados en la experiencia del usuario son relevantes. Además, la seguridad de datos y la privacidad deben ser prioridades, junto con la capacitación adecuada para los usuarios. Un plan de mantenimiento continuo asegura la sostenibilidad a largo plazo, garantizando que las aplicaciones de realidad aumentada sigan siendo efectivas y cumplan con las necesidades cambiantes del entorno tecnológico.

2.2.2.1. Desarrollo de Aplicaciones. Vera et al. (2020) señala que abarca un proceso multifacético que implica la planificación, diseño, implementación, prueba y despliegue de software con el objetivo de satisfacer necesidades específicas. Inicia con un análisis detallado de requisitos para comprender las metas y funcionalidades deseadas. Después, se inicia la etapa de planificación de la estructura y la presentación de usuario, seguida por la fase de programación donde se incorporan las funcionalidades establecidas previamente. Se realizan evaluaciones minuciosas para asegurar la calidad y la confiabilidad del software, y finalmente, se inicia la implementación de la aplicación para su uso. El proceso de desarrollo de aplicaciones puede comprender una variedad de enfoques, desde aplicaciones para dispositivos móviles hasta soluciones en línea o sistemas corporativos, y se beneficia de metodologías ágiles para adaptarse eficazmente a cambios en los requerimientos. La seguridad, la capacidad de adaptación y la experiencia del usuario son consideraciones fundamentales a lo largo de todo el proceso para lograr un desarrollo de aplicaciones efectivo y satisfactorio.

A. **Experiencia de Usuario.** Vargas et al. (2021) añade que la percepción del usuario (UX) se relaciona con la interacción global de una persona con un producto, sistema o servicio, y abarca aspectos como la facilidad de uso, la accesibilidad, la efectividad y la satisfacción del usuario. En el ámbito del diseño de aplicaciones y sitios web, la percepción del usuario se vuelve un componente esencial para asegurar la funcionalidad y la adopción del producto. Implica el análisis de usuarios, la elaboración de interfaces intuitivas, el diseño de interacciones eficientes y la consideración de aspectos emocionales para proporcionar una experiencia completa y positiva. La retroalimentación continua de los usuarios y pruebas de usabilidad son esenciales para iterar y mejorar la experiencia de usuario, asegurando que el producto satisfaga de manera eficiente las expectativas y requerimientos de los usuarios. En última instancia, una experiencia de usuario exitosa contribuye a la satisfacción del usuario, la retención y el éxito general de la aplicación o plataforma.

B. ***Interactividad.*** Mercado et al. (2019) señala que viene a ser la capacidad de un sistema, aplicación o entorno para responder a las acciones del usuario, fomentando la participación activa y facilitando una experiencia más dinámica. En la elaboración de interfaces de usuario., la interactividad implica la creación de elementos que permitan a los usuarios realizar acciones, recibir retroalimentación inmediata y explorar contenido de manera intuitiva. Estas interacciones pueden incluir clics, deslizamientos, gestos táctiles y otros comportamientos que enriquecen la experiencia del usuario. La interactividad no solo mejora la usabilidad, sino que también contribuye a la participación y la retención del usuario al proporcionar una experiencia más envolvente y adaptativa. Su implementación efectiva requiere un diseño centrado en el usuario, pruebas iterativas y la consideración de las expectativas del usuario para crear experiencias interactivas significativas y satisfactorias.

C. ***Rendimiento.*** Verona et al. (2016) lo define como la eficacia de las aplicaciones se refiere a su capacidad para desempeñar sus funciones de manera eficiente y sin interrupciones,

asegurando una respuesta ágil y fluida. Factores fundamentales que inciden en esta efectividad abarcan la velocidad de carga, la reactividad de la interfaz de usuario, la optimización en la utilización de recursos del sistema y la estabilidad general. Una evolución eficaz y correctamente adaptada, combinada con una administración apropiada de la memoria y la potencia de procesamiento, son cruciales para lograr un rendimiento óptimo, son vitales para lograr un rendimiento óptimo. Las pruebas exhaustivas, el seguimiento continuo y la optimización basada en datos son estrategias para enfrentar y mejorar el rendimiento de las aplicaciones conforme se ajustan a las exigencias en constante cambio y a las actualizaciones del software. Un rendimiento sólido aporta de manera considerable a la satisfacción del usuario y a la eficacia global del producto.

2.2.2.2. Gestión de Planes. Diaz (2016) se refiere al proceso de concebir, implementar y supervisar planes detallados y cronogramas con el fin de alcanzar metas específicas dentro de un evento, programa o iniciativa. Esta práctica implica definir claramente objetivos, asignar eficientemente recursos, identificar tareas y organizar actividades en un plan minucioso. La gestión de planes es crucial para coordinar las acciones de los equipos, prever posibles desafíos y garantizar un avance continuo hacia los objetivos establecidos. Se recurre a herramientas y técnicas de programación, como los diagramas de Gantt, para visualizar y comunicar el progreso de manera efectiva. Asimismo, implica la actualización y ajuste regular del programa para adecuarse a las transformaciones en el entorno del evento y garantizar una coherencia constante con los propósitos estratégicos. La administración eficiente de programas constituye un componente crucial en la ejecución satisfactoria de eventos y en la maximización de los recursos disponibles.

A. Planificación Eficiente. Miranda et al. (2017) señala que es un proceso estratégico orientado a optimizar la distribución de recursos y tiempo para lograr objetivos específicos de manera eficiente y sin desperdicio. Implica la identificación clara de metas, la evaluación de

recursos disponibles y la elaboración de un plan detallado que minimice los tiempos muertos y maximice la productividad. La planificación eficiente también requiere considerar posibles obstáculos y contingencias, permitiendo una respuesta ágil a cambios inesperados. La aplicación de herramientas y metodologías adecuadas, junto con una colaboración y comunicación efectiva entre los integrantes del equipo, resulta fundamental para asegurar una planificación eficaz que conduzca al logro exitoso de los objetivos establecidos. Este enfoque no solo optimiza la ejecución de eventos, sino que también favorece una administración eficaz de los recursos y la capacidad de adaptación frente a variaciones en el entorno.

B. Gestión de Recursos. Hernández y Martí (2006) indican que es un componente esencial en la planificación y ejecución de eventos , programas o iniciativas, y se enfoca en la distribución eficiente de los recursos disponibles para alcanzar los objetivos fijados. Esto conlleva la identificación y evaluación de los recursos requeridos, como personal, tecnología, tiempo y financiamiento, además de una planificación meticulosa de su utilización a lo largo del ciclo del evento. La gestión de activos tiene como meta mejorar tanto la eficacia como la eficiencia, asegurando una distribución equitativa y una utilización óptima de los recursos para potenciar el desempeño del evento. También involucra una supervisión constante, ajustes según sea necesario y la detección anticipada de posibles restricciones o riesgos en la disponibilidad de recursos. Una gestión de activos eficaz contribuye al logro exitoso de metas, a la reducción de desperdicios y a la habilidad de ajustarse a las variaciones en el entorno del evento.

C. Control de Calidad. Reyes et al. (2022) señalan que es un procedimiento sistemático diseñado para garantizar que los productos o servicios se ajusten a los estándares y requisitos predefinidos, asegurando así la satisfacción del cliente y la efectividad del proceso de producción. Este procedimiento abarca la implementación de estrategias y prácticas para supervisar y analizar la calidad en cada etapa del ciclo de vida del producto o servicio. Esto incluye establecer estándares de calidad precisos, llevar a cabo inspecciones y pruebas, así

como aplicar acciones correctivas en caso de desviaciones. La gestión de calidad no solo se enfoca en detectar y corregir fallos, sino que también busca la mejora continua, la prevención de problemas y la optimización de procesos. En una variedad de sectores, desde la fabricación hasta el desarrollo de software, La garantía de calidad es fundamental para preservar la integridad y la fiabilidad de los productos y servicios ofrecidos.

2.2.2.3. Satisfacción del Usuario. Febres y Mercado (2020) lo describen como un componente fundamental que analiza el grado de satisfacción con respecto a las expectativas establecidas y requisitos de los usuarios con respecto a un producto, servicio o interacción. Está estrechamente relacionado con la percepción positiva que los usuarios tienen sobre la utilidad, facilidad de uso y calidad global de lo que están utilizando. La satisfacción del cliente se fundamenta no solo en la funcionalidad del producto o servicio, sino también en la experiencia completa, que abarca la interfaz, el soporte al cliente y la capacidad de satisfacer sus expectativas. La evaluación constante, las encuestas de retroalimentación y el análisis regular son herramientas esenciales para comprender y mejorar la experiencia del cliente. Un enfoque centrado en el cliente, adaptable y orientado hacia la mejora continua son fundamentales para garantizar la satisfacción del consumidor en contextos tan dinámicos como los contemporáneos. La satisfacción del consumidor no solo se considera un indicador de éxito, sino que también actúa como un elemento esencial para fomentar la fidelidad del cliente y la imagen de la empresa.

A. Facilidad de Uso. Medina et al. (2021) indican que se refiere a la habilidad de un producto, sistema o servicio para ser comprendido, aprendido y utilizado de forma eficiente y efectiva por sus usuarios. Esto implica diseñar interfaces y experiencias que sean intuitivas, accesibles y amigables, con el objetivo de reducir al mínimo la curva de aprendizaje y mitigar la posibilidad de errores por parte del usuario. Los componentes fundamentales de la facilidad de uso comprenden la claridad en el diseño, la coherencia en la interacción y la respuesta

instantánea a las acciones del usuario. La usabilidad, que garantiza que los usuarios puedan realizar sus tareas de manera eficaz y sin frustraciones, es un elemento esencial de la facilidad de uso. Prestar una atención meticulosa a la la usabilidad busca optimizar la satisfacción del usuario, estimular la adopción del producto o servicio, y garantizar una experiencia general favorable.

B. Personalización de Experiencia. Rosales (2015) indica que la personalización de la experiencia se refiere a la adaptación de productos, servicios o sistemas que buscan satisfacer las necesidades y preferencias particulares de los usuarios. Este enfoque busca crear experiencias únicas y relevantes al considerar factores como la ubicación, historial de interacciones, preferencias de usuario y comportamientos anteriores. La personalización puede manifestarse en diversas formas, desde recomendaciones personalizadas hasta ajustes en la interfaz de usuario o en la oferta de productos. La recopilación ética y segura de datos es esencial para lograr una personalización efectiva, y su implementación puede mejorar significativamente la satisfacción del usuario, la retención y la conexión emocional con el producto o servicio. En la actual era digital, la personalización de la experiencia se ha transformado en un diferenciador crucial para ofrecer experiencias más pertinentes y centradas en el usuario.

III. MÉTODO

3.1. Tipo de investigación

Conocida también como investigación pura, este tipo de indagación no tiene como objetivo la resolución de problemas ni contribuye directamente a su solución, en cambio, su función principal radica en proporcionar una base teórica sustancial que pueda servir de cimiento para otros enfoques de investigación (Hadi et al., 2023). Por lo que en este estudio dará a entender la relación existente entre las variables para dar sostén a otras investigaciones. Asimismo, el enfoque es cuantitativo, constituye un método de investigación en el que se emplean técnicas numéricas y estadísticas con el propósito de cuantificar y examinar minuciosamente los datos recolectados (Hadi et al., 2023). Por ende, en este estudio se optó por el análisis estadístico de la información como método principal para abordar las interrogantes planteadas.

Además, los fenómenos se observan en su entorno natural; no se incluye en el estudio ninguna modificación de la variable independiente de acuerdo con el enfoque no experimental (Hernández-Sampieri y Mendoza, 2018). Por lo tanto, en la investigación no se llevó a cabo la manipulación de ninguna de las variables.

El nivel correlacional, según Hernández-Sampieri y Mendoza (2018), tienen como objetivo entender la conexión o relación entre diferentes eventos, fenómenos, conceptos, variables o características, explorando tanto la naturaleza de su la vinculación se define como la ausencia de cualquier relación entre los elementos analizados. En este contexto, el presente estudio tiene como propósito examinar la relación estadística entre dos variables específicas. Por consiguiente, el objetivo principal de esta investigación es determinar la vinculación entre la Protección de la Información y la Eficacia en la Implementación de Aplicaciones de Realidad Aumentada.

3.2. Población y muestra

3.2.1. Población

De acuerdo con Hernández-Sampieri y Mendoza (2018), Una población se caracteriza como un grupo de individuos que satisfacen los estándares predeterminados. Dentro de esta perspectiva, la población objeto de este análisis estuvo conformada por el equipo empleado en actividades deportivas.

3.2.2. Muestra

Para garantizar que los casos elegidos al azar sean representativos de la comunidad investigada, los investigadores utilizarán el censo como base para su estrategia de muestreo (Hernández-Sampieri & Mendoza, 2018). El tamaño de la muestra para esta investigación estuvo compuesto por 50 individuos que ejercen funciones en eventos deportivos.

3.3. Operacionalización de variables

Tabla 1
Operacionalización de las variables

Variable	Dimensión	Indicador
Seguridad de Datos	Protección de Datos	Encriptación de Datos
		Control de Acceso
		Respaldo de Datos
		Recuperación de Datos
	Integridad de Datos	Verificación de Integridad
		Validación de Datos
	Confidencialidad	Restricciones de Acceso
		Gestión de Identidad y Acceso
	Cumplimiento Normativo	Políticas de Privacidad
		Ajustes a Estándares de Seguridad
Implementación Exitosa de Aplicaciones de Realidad Aumentada	Desarrollo de Aplicaciones	Experiencia de Usuario
		Interactividad
		Rendimiento
	Gestión de Planes	Planificación Eficiente
		Gestión de Recursos
		Control de Calidad
	Satisfacción del Usuario	Facilidad de Uso
		Personalización de Experiencia

3.4. Instrumentos

Los instrumentos de investigación son herramientas que los investigadores utilizan para recopilar datos e información para un estudio (Hadi et al., 2023). En el presente estudio, se utilizaron cuestionarios como herramientas de recolección de datos, y la metodología aplicada fue la encuesta, lo que facilitó la obtención de información directa de los participantes sobre las variables analizadas.

Para asegurar la calidad y fiabilidad de la información obtenida, se llevó a cabo un proceso de validación del cuestionario a través de la evaluación por parte de expertos. Estos profesionales colaboraron en la revisión y mejora del contenido del cuestionario. Posteriormente, se llevó a cabo un análisis de los datos utilizando el coeficiente Alfa de

Cronbach, que determina la consistencia interna del instrumento. Es importante señalar que un valor elevado de Alfa de Cronbach, normalmente superior a 0.7, sugiere una fiabilidad significativa en las mediciones realizadas.

3.5. Procedimientos

Durante el transcurso del proceso de investigación, se implementó un procedimiento meticuloso para organizar los datos recopilados mediante el cuestionario. Para iniciar el examen de estos datos, se empleó el programa Excel como herramienta inicial. A continuación, se realizó un análisis más exhaustivo de la información obtenida a través de los cuestionarios, empleando el software estadístico SPSS en su versión 26. Este análisis permitió profundizar en los datos recopilados, facilitando la identificación de patrones y tendencias relevantes en relación con las variables estudiadas. Esta metodología posibilitó una organización eficaz de los datos y facilitó un análisis exhaustivo para obtener conclusiones fundamentadas en el estudio.

3.6. Análisis de datos

Mediante la asistencia del software estadístico SPSS en su edición 26, se procedió a realizar un análisis completo de los datos obtenidos. Se realizó un análisis exhaustivo de las respuestas a cada pregunta formulada, mediante la creación de tablas que mostraron tanto las frecuencias como los porcentajes correspondientes, acompañadas de una interpretación pertinente. De igual manera, se recurrió a la visualización de los resultados mediante gráficos, con el fin de ofrecer una representación clara y accesible desde una óptica visual.

3.7. Consideraciones éticas

Los aspectos éticos considerados son los siguientes:

(a) El cumplimiento de la estructura de tesis indicada por la UNFV;

(b) La búsqueda de generar nuevo conocimiento;

(c) Tesis original y propia del estudiante;

(d) Los resultados deben ser reales sin la manipulación deliberada;

(e) Información citada respetando la autoría.

IV. RESULTADOS

4.1. Análisis inferencial

4.1.1. Hipótesis general

H_0: No existe una relación significativa entre la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023.

H_1: Existe una relación significativa entre la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023.

Tabla 2
Correlación entre la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023.

			Implementación Exitosa de Aplicaciones de Realidad Aumentada
Rho de Spearman	Seguridad de Datos	Coeficiente de correlación	,402**
		Sig. (bilateral)	,004
		N	50

Interpretación: De acuerdo con los resultados obtenidos para validar la hipótesis general, se ha determinado que el coeficiente de correlación Rho de Spearman es de 0,402** y el valor de significancia (bilateral) es de 0,004. Esto nos permite concluir que se cumple la hipótesis alternativa, indicando que existe una relación significativa entre la seguridad de los datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos en 2023.

4.1.2. Hipótesis secundarias

a. Hipótesis específica 1

H_0: No existe una relación significativa entre la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023

H_1: Existe una relación significativa entre la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023

Tabla 3
Correlación entre la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023

			Desarrollo de aplicaciones
Rho de Spearman	Seguridad de Datos	Coeficiente de correlación	,499**
		Sig. (bilateral)	,000
		N	50

Interpretación: De acuerdo con los resultados obtenidos para validar la hipótesis general, se ha establecido que el coeficiente de correlación Rho de Spearman es de 0,499** y el valor de significancia (bilateral) es de 0,000. Esto permite concluir que se acepta la hipótesis alternativa, lo que sugiere que existe una relación significativa entre la seguridad de los datos y el desarrollo de aplicaciones en eventos deportivos en 2023.

b. Hipótesis específica 2

H_0: No existe una relación significativa entre la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023

H_1: Existe una relación significativa entre la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023

Tabla 4
Correlación entre la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023

			Implementación exitosa gestión de planes
Rho de Spearman	Seguridad de Datos	Coeficiente de correlación	,409**
		Sig. (bilateral)	,002
		N	50

Interpretación: Conforme a los resultados obtenidos para validar la hipótesis general, se ha establecido que el coeficiente de correlación Rho de Spearman es de 0,409** y el valor de significancia (bilateral) es de 0,002. Esto permite concluir que se acepta la hipótesis alternativa, lo que indica que existe una relación significativa entre la seguridad de los datos y la gestión exitosa de planes en eventos deportivos en 2023.

c. Hipótesis específica 3

H_0: No existe una relación significativa entre la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023

H_1: Existe una relación significativa entre la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023

Tabla 5
Correlación entre la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023

			Satisfacción del usuario
Rho de Spearman	Seguridad de Datos	Coeficiente de correlación	,389**
		Sig. (bilateral)	,002
		N	50

Interpretación: Conforme a los resultados obtenidos para validar la hipótesis general, se ha determinado que el coeficiente de correlación Rho de Spearman es de 0,389** y el valor de significancia (bilateral) es de 0,002. Esto permite concluir que se acepta la hipótesis alternativa, indicando que existe una relación significativa entre la seguridad de los datos y la satisfacción del usuario en eventos deportivos en 2023.

4.2. Análisis descriptivos

Los resultados de la encuesta muestran una confianza generalizada en la encriptación de datos implementada en la empresa para salvaguardar la privacidad y seguridad de la información confidencial de los clientes y empleados. Un 68% de los encuestados expresó algún grado de acuerdo, con un 32% seleccionando de acuerdo y otro 36% optando por totalmente de acuerdo. Solo un 32% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren un nivel general de confianza en las medidas de seguridad implementadas en la empresa para proteger la información confidencial.

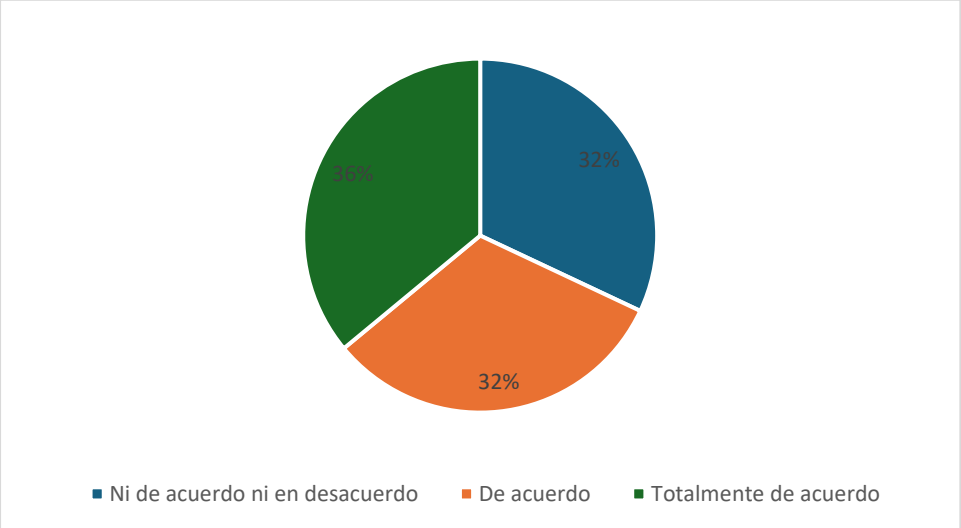
Tabla 6

Frecuencia de Percepciones sobre la Confianza en la Encriptación de Datos Implementada en la Empresa para Salvaguardar la Privacidad y Seguridad de la Información Confidencial de los Clientes y Empleados

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	16	32,0
	De acuerdo	16	32,0
	Totalmente de acuerdo	18	36,0
	Total	50	100,0

Figura 1

Frecuencia de Percepciones sobre la Confianza en la Encriptación de Datos Implementada en la Empresa para Salvaguardar la Privacidad y Seguridad de la Información Confidencial de los Clientes y Empleados



Los resultados de la encuesta revelan que una proporción significativa de los encuestados, correspondiente al 74,0%, manifestó algún grado de acuerdo con la afirmación de que la encriptación de datos desempeña un papel crucial en la integridad y confidencialidad de la información en el entorno laboral. En particular, el 34,0% de los participantes seleccionó "totalmente de acuerdo", mientras que el 40,0% optó por "de acuerdo". Por el contrario, un 26,0% de los encuestados indicó que no estaba ni de acuerdo ni en desacuerdo con dicha afirmación. Estos hallazgos sugieren una percepción favorable dentro de la organización acerca de la importancia de la encriptación de datos en la salvaguarda de la información laboral.

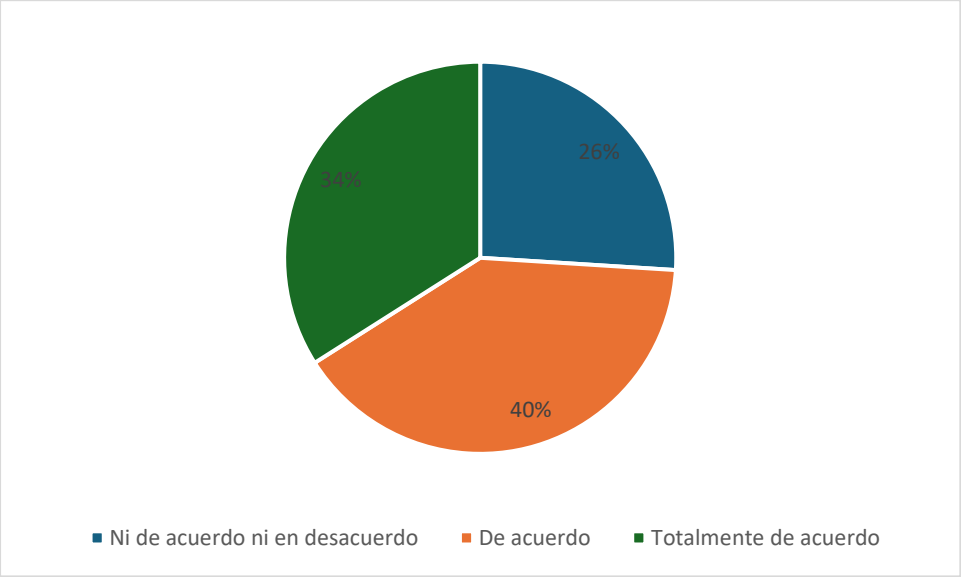
Tabla 7

Frecuencia de Percepciones sobre la Contribución Significativa de la Encriptación de Datos a la Integridad y Confidencialidad de la Información en el Entorno Laboral

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	13	26,0
	De acuerdo	20	40,0
	Totalmente de acuerdo	17	34,0
	Total	50	100,0

Figura 2

Frecuencia de Percepciones sobre la Contribución Significativa de la Encriptación de Datos a la Integridad y Confidencialidad de la Información en el Entorno Laboral



Los resultados de la encuesta indican que existe una percepción mayoritaria respecto a la capacidad del sistema de Control de Acceso para garantizar adecuadamente la seguridad de los datos personales. En concreto, el 68% de los encuestados manifestó algún grado de acuerdo, con un 32% seleccionando "de acuerdo" y un 36% optando por "totalmente de acuerdo". Sin embargo, un 32% indicó que se encuentra en una posición neutral, al manifestar que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos hallazgos sugieren una confianza generalizada en la efectividad del sistema de Control de Acceso en la protección de los datos personales para proteger los datos personales, aunque también se reconoce la necesidad de mejoras o evaluaciones adicionales en ciertos aspectos.

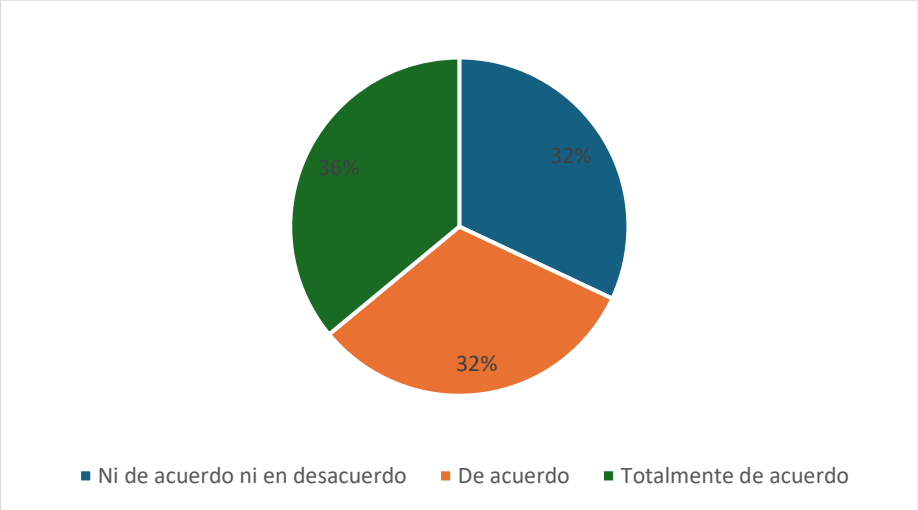
Tabla 8

Frecuencia de Percepciones sobre la Garantía de Seguridad de los Datos Personales por parte del Sistema de Control de Acceso

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	16	32,0
	De acuerdo	16	32,0
	Totalmente de acuerdo	18	36,0
	Total	50	100,0

Figura 3

Frecuencia de Percepciones sobre la Garantía de Seguridad de los Datos Personales por parte del Sistema de Control de Acceso



Los resultados de la encuesta evidencian una percepción mayoritaria de confianza en la efectividad del sistema de control de acceso para proteger la privacidad y confidencialidad de los datos gestionados. Este hallazgo sugiere que los encuestados consideran que las medidas implementadas en el sistema son adecuadas para garantizar la seguridad de la información sensible. El 56% de los encuestados expresaron algún grado de acuerdo, con un 28% seleccionando de acuerdo y otro 28% optando por totalmente de acuerdo. Sin embargo, un 44% indicaron que ni están de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una tendencia positiva en la confianza hacia el sistema de control de acceso, aunque una proporción significativa de encuestados aún tiene dudas o reservas al respecto.

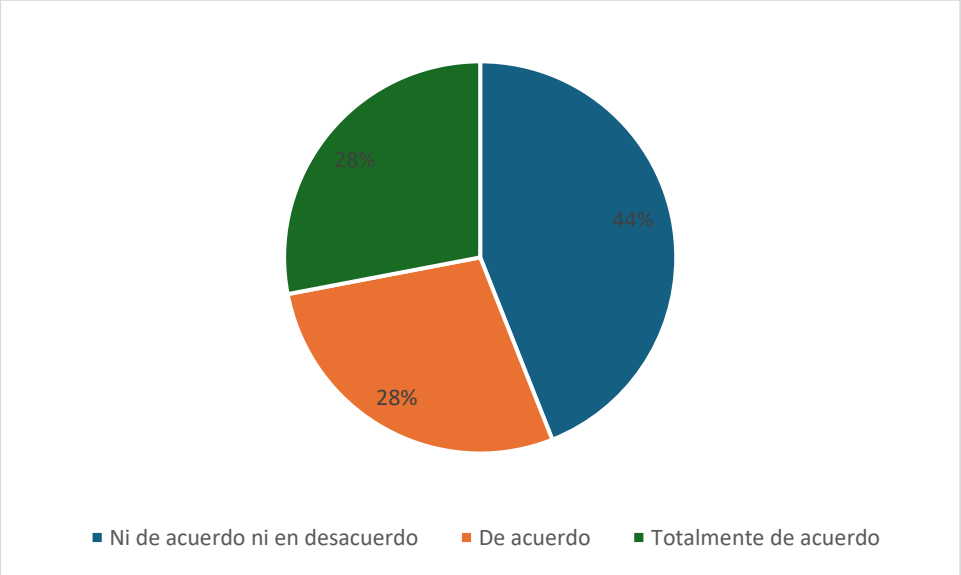
Tabla 9

Frecuencia de Percepciones sobre la Confianza en la Capacidad del Sistema de Control de Acceso para Salvaguardar la Privacidad y Confidencialidad de los Datos Manejados

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	22	44,0
	De acuerdo	14	28,0
	Totalmente de acuerdo	14	28,0
	Total	50	100,0

Figura 4

Frecuencia de Percepciones sobre la Confianza en la Capacidad del Sistema de Control de Acceso para Salvaguardar la Privacidad y Confidencialidad de los Datos Manejados



Los resultados de la encuesta revelan una división en las percepciones respecto a si la empresa ofrece los recursos necesarios para realizar un respaldo de datos efectivo, garantizando así la integridad y disponibilidad de la información. Un 56.0% de los encuestados manifestó algún grado de acuerdo con esta afirmación, desglosándose en un 32.0% que seleccionó "de acuerdo" y un 24.0% que eligió "totalmente de acuerdo". En contraste, un 44.0% expresó que ni está de acuerdo ni en desacuerdo. Estos hallazgos indican que una proporción significativa de los encuestados considera que la empresa podría no estar proporcionando los recursos adecuados para un respaldo eficaz de los datos, lo que podría comprometer la integridad y disponibilidad de la información.

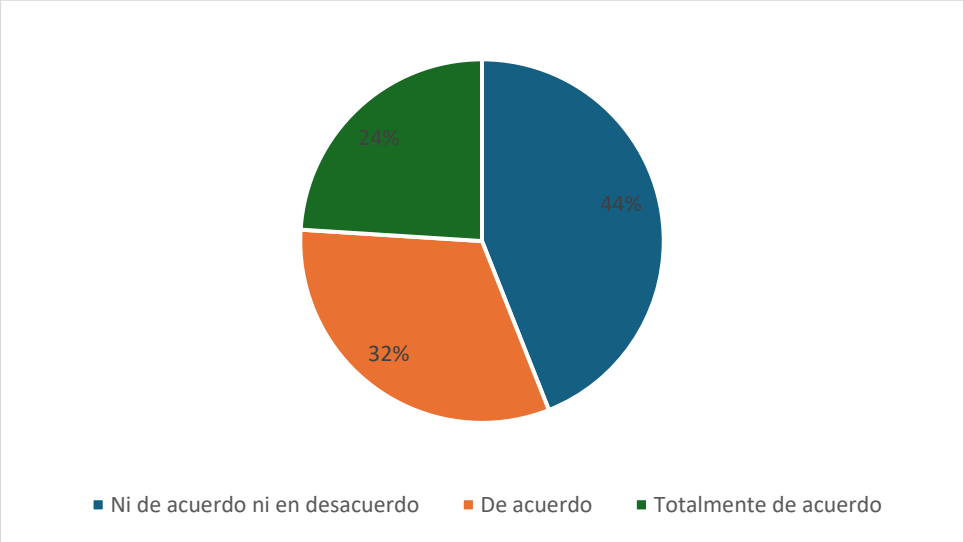
Tabla 10

Frecuencia de Percepciones sobre la Confianza en la Capacidad del Sistema de Control de Acceso para Salvaguardar la Privacidad y Confidencialidad de los Datos Manejados

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	22	44,0
	De acuerdo	16	32,0
	Totalmente de acuerdo	12	24,0
	Total	50	100,0

Figura 5

Frecuencia de Percepciones sobre la Confianza en la Capacidad del Sistema de Control de Acceso para Salvaguardar la Privacidad y Confidencialidad de los Datos Manejados



Los resultados de la encuesta indican que la percepción respecto a la política de respaldo de datos de la empresa es predominantemente positiva, ya que la mayoría de los encuestados manifestó algún nivel de acuerdo con las medidas implementadas. Esto sugiere que los participantes confían en las estrategias adoptadas para garantizar la seguridad y disponibilidad de la información respaldada. Específicamente, el 68.0% de los encuestados indicó estar de acuerdo o totalmente de acuerdo con que la política de respaldo de datos es fácil de entender y seguir, lo que facilita la correcta ejecución de los procedimientos de protección de datos. Un 40.0% seleccionó de acuerdo y un 28.0% optó por totalmente de acuerdo. Solo el 32.0% indicó que ni está de acuerdo ni en desacuerdo. Estos resultados sugieren una percepción general positiva sobre la claridad y la utilidad de la política de respaldo de datos en la empresa.

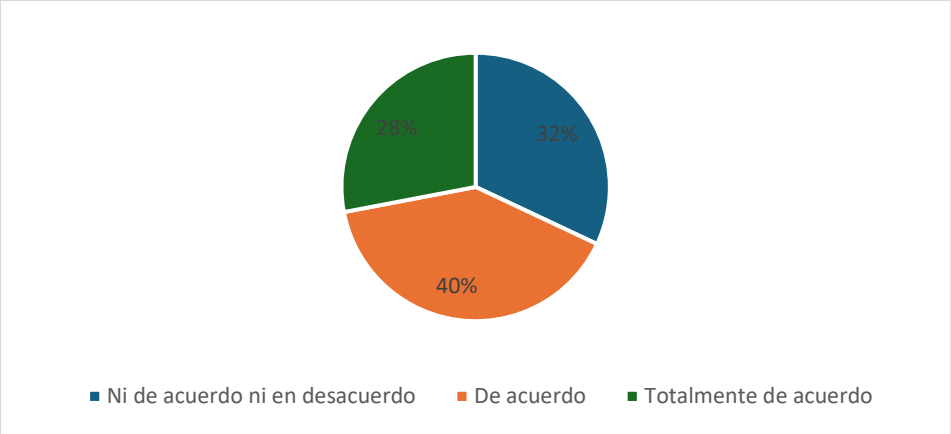
Tabla 11

Frecuencia de Percepciones sobre la Facilidad de Entendimiento y Seguimiento de la Política de Respaldo de Datos de la Empresa, para la Correcta Ejecución de los Procedimientos de Protección de Datos

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	16	32,0
	De acuerdo	20	40,0
	Totalmente de acuerdo	14	28,0
	Total	50	100,0

Figura 6

Frecuencia de Percepciones sobre la Facilidad de Entendimiento y Seguimiento de la Política de Respaldo de Datos de la Empresa, para la Correcta Ejecución de los Procedimientos de Protección de Datos

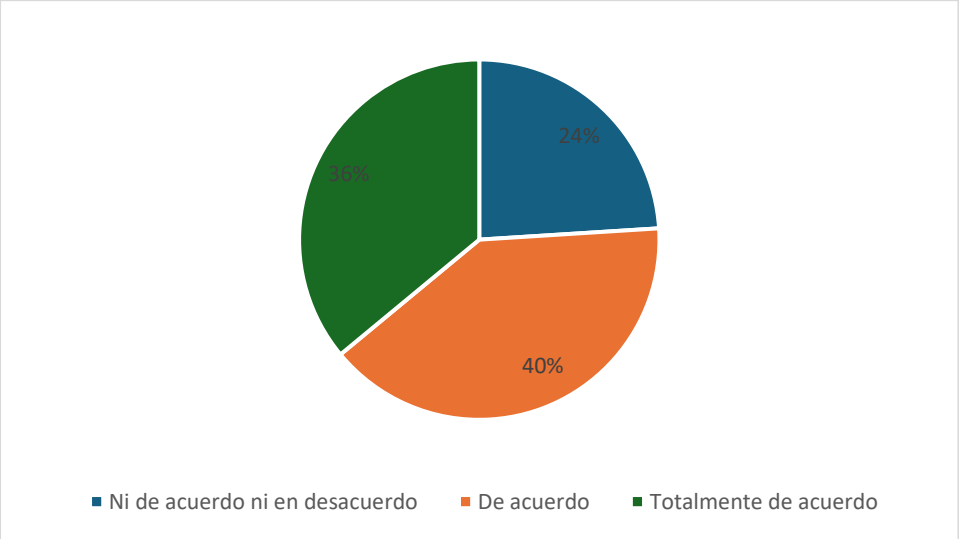


Los resultados de la encuesta muestran que la confianza en la eficacia de los procesos de recuperación de datos implementados por la empresa para garantizar la protección y disponibilidad de la información crítica es notablemente alta, con un 76% de los encuestados expresando algún grado de acuerdo. Específicamente, el 40% seleccionó de acuerdo y el 36% optó por totalmente de acuerdo. Sin embargo, un 24% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una confianza generalizada en los procesos de recuperación de datos implementados por la empresa entre los encuestados.

Tabla 12
Frecuencia de Percepciones sobre la Confianza en la Eficacia de los Procesos de Recuperación de Datos Implementados por la Empresa para Garantizar la Protección y Disponibilidad de la Información Crítica

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	12	24,0
	De acuerdo	20	40,0
	Totalmente de acuerdo	18	36,0
	Total	50	100,0

Figura 7
Frecuencia de Percepciones sobre la Confianza en la Eficacia de los Procesos de Recuperación de Datos Implementados por la Empresa para Garantizar la Protección y Disponibilidad de la Información Crítica



Los resultados de la encuesta reflejan una percepción diversa sobre la capacitación proporcionada sobre los procedimientos de recuperación de datos. Un 62.0% de los encuestados expresaron algún grado de acuerdo con la suficiencia de esta capacitación, con un 34.0% seleccionando de acuerdo y un 28.0% optando por totalmente de acuerdo. Sin embargo, un 38.0% indicó que ni está de acuerdo ni en desacuerdo con la afirmación. Estos resultados sugieren que aunque una mayoría considera que la capacitación es adecuada, aún existe una proporción significativa que no está completamente convencida de su eficacia

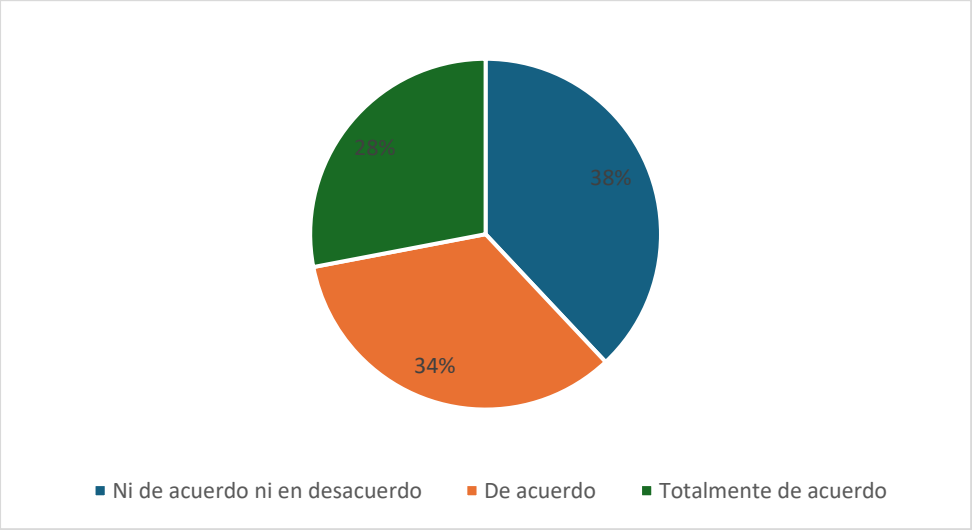
Tabla 13

Frecuencia de Percepciones sobre la Suficiencia de la Capacitación en Procedimientos de Recuperación de Datos para el Entendimiento y Cumplimiento de los Protocolos Establecidos por Todos los Empleados

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	19	38,0
	De acuerdo	17	34,0
	Totalmente de acuerdo	14	28,0
	Total	50	100,0

Figura 8

Frecuencia de Percepciones sobre la Suficiencia de la Capacitación en Procedimientos de Recuperación de Datos para el Entendimiento y Cumplimiento de los Protocolos Establecidos por Todos los Empleados



Los resultados de la encuesta revelan una percepción positiva respecto a la disponibilidad de recursos y herramientas por parte de la empresa para llevar a cabo de manera eficiente las verificaciones de integridad de datos. Un 70,0% de los encuestados expresó algún grado de acuerdo con esta afirmación, desglosándose en un 42,0% que seleccionó "de acuerdo" y un 28,0% que optó por "totalmente de acuerdo". En contraste, un 30,0% indicó que ni está de acuerdo ni en desacuerdo. Estos hallazgos sugieren que la mayoría de los participantes considera que la empresa ofrece los recursos necesarios para realizar de forma efectiva estas verificaciones.las verificaciones de integridad de datos, aunque aún hay una proporción considerable que podría no compartir esta percepción.

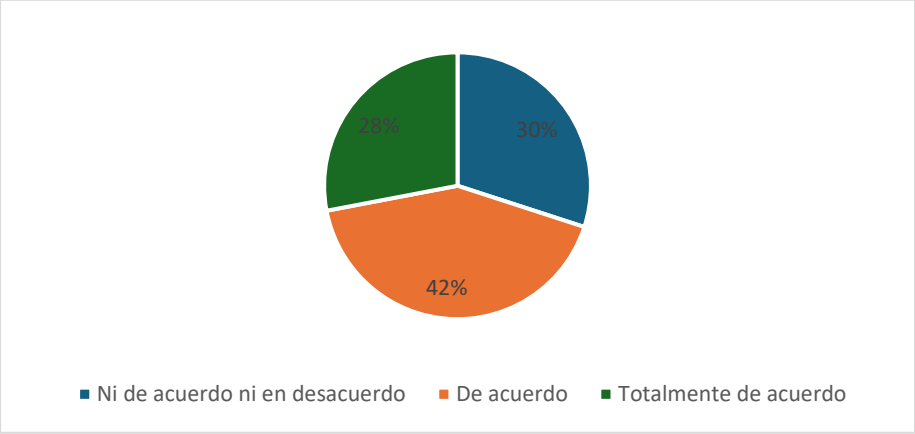
Tabla 14

Frecuencia de Percepciones sobre la Disponibilidad de Recursos y Herramientas para Realizar Eficientemente las Verificaciones de Integridad de Datos en la Empresa

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	15	30,0
	De acuerdo	21	42,0
	Totalmente de acuerdo	14	28,0
	Total	50	100,0

Figura 9

Frecuencia de Percepciones sobre la Disponibilidad de Recursos y Herramientas para Realizar Eficientemente las Verificaciones de Integridad de Datos en la Empresa



Los resultados de la encuesta reflejan una opinión equilibrada sobre si la capacitación y formación proporcionada por la empresa en relación con la verificación de integridad de datos es adecuada para mejorar las habilidades en este ámbito. Un 64.0% de los encuestados expresaron algún grado de acuerdo, con un 32.0% seleccionando de acuerdo y otro 32.0% optando por totalmente de acuerdo. Por otro lado, un 36.0% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren que hay una percepción mixta dentro de la organización sobre la efectividad de la capacitación y formación en la verificación de integridad de datos.

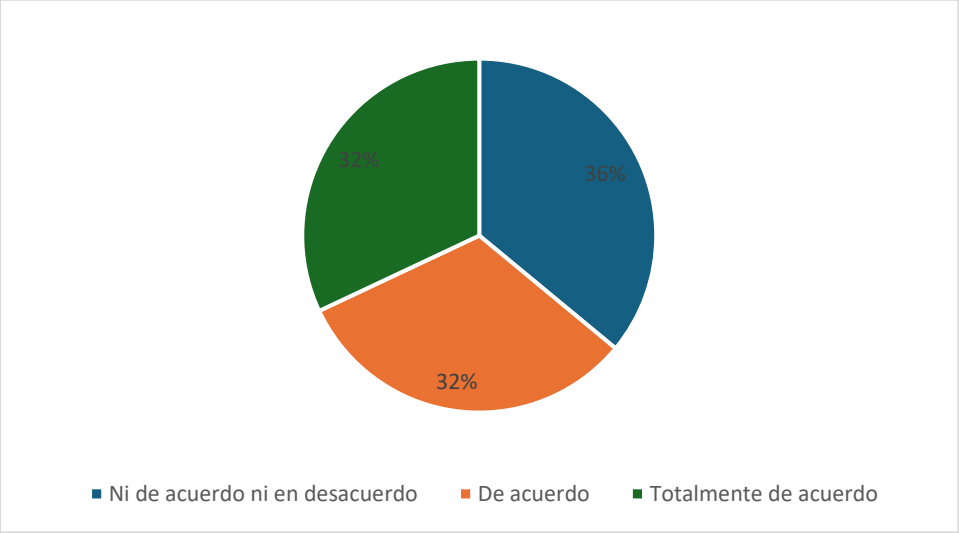
Tabla 15

Frecuencia de Percepciones sobre la Adecuación de la Capacitación y Formación Proporcionada por la Empresa en la Verificación de Integridad de Datos para Mejorar las Habilidades en Este Ámbito

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	18	36,0
	De acuerdo	16	32,0
	Totalmente de acuerdo	16	32,0
	Total	50	100,0

Figura 10

Frecuencia de Percepciones sobre la Adecuación de la Capacitación y Formación Proporcionada por la Empresa en la Verificación de Integridad de Datos para Mejorar las Habilidades en Este Ámbito



Los hallazgos del sondeo revelan una inclinación favorable respecto a la apreciación de la eficacia de las directrices de verificación de datos implementadas por la organización para asegurar la exactitud y confiabilidad de la información empleada en las actividades laborales. Un 56% de los encuestados expresó algún grado de acuerdo, siendo un 24% quienes están de acuerdo y un 32% totalmente de acuerdo. Sin embargo, un 44% indicó que ni está de acuerdo ni en desacuerdo con la efectividad de estas políticas. Estos resultados sugieren una base sólida en la confianza de las políticas de validación de datos, aunque aún queda espacio para mejoras o clarificaciones en ciertas áreas.

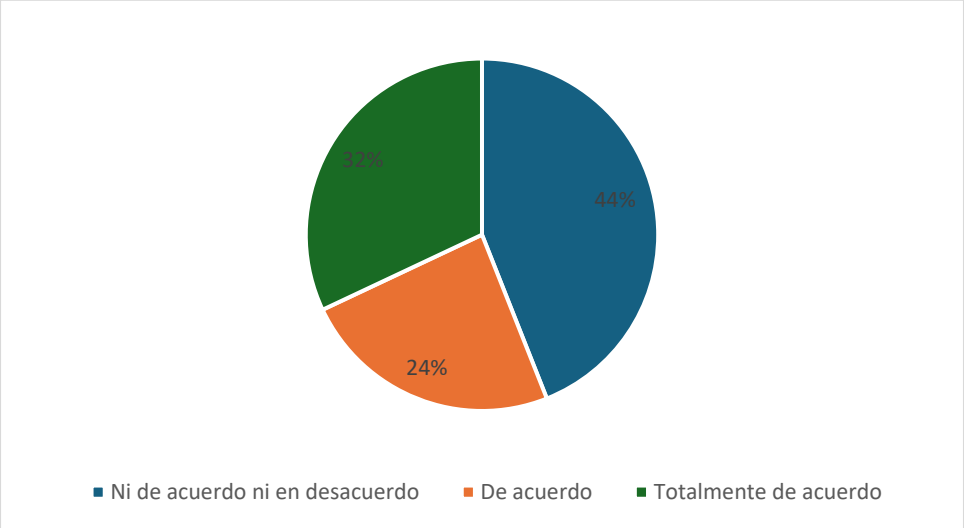
Tabla 16

Frecuencia de Percepciones sobre la Efectividad de las Políticas de Validación de Datos en la Empresa para Garantizar la Integridad y Fiabilidad de la Información Utilizada en las Tareas Laborales

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	22	44,0
	De acuerdo	12	24,0
	Totalmente de acuerdo	16	32,0
	Total	50	100,0

Figura 11

Frecuencia de Percepciones sobre la Efectividad de las Políticas de Validación de Datos en la Empresa para Garantizar la Integridad y Fiabilidad de la Información Utilizada en las Tareas Laborales



Los hallazgos de la encuesta evidencian una dispersión balanceada de opiniones respecto a la influencia de los procedimientos de verificación de datos en la disminución de errores y el aumento de la calidad de la información utilizada en el trabajo diario. Un 64% de los participantes manifestó cierto grado de acuerdo, con un 28% seleccionando de acuerdo y otro 36% optando por totalmente de acuerdo. Por otro lado, un 36% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una diversidad de percepciones dentro de la organización respecto a la efectividad de los procesos de validación de datos en la mejora de la calidad de la información.

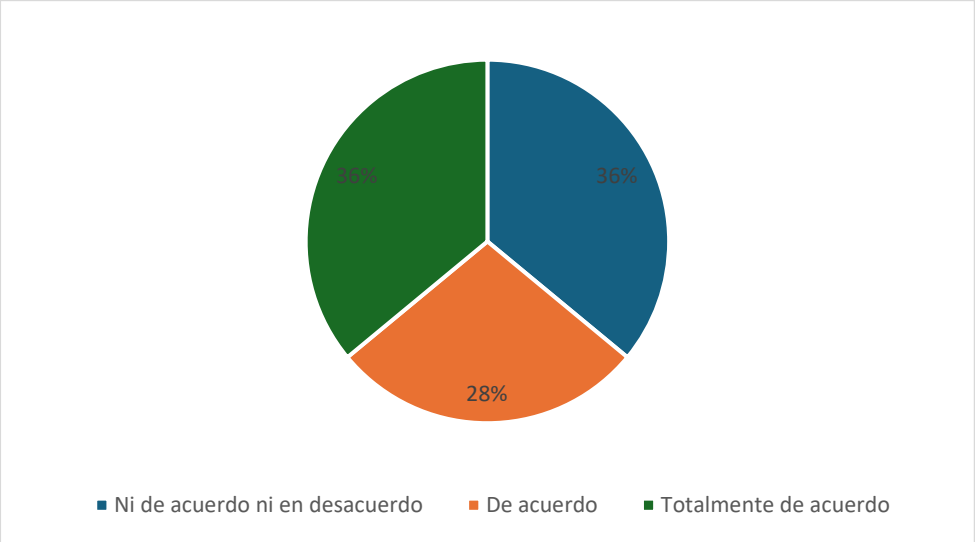
Tabla 17

Frecuencia de Percepciones sobre la Contribución Significativa de los Procesos de Validación de Datos en la Reducción de Errores y la Mejora de la Calidad de la Información

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	18	36,0
	De acuerdo	14	28,0
	Totalmente de acuerdo	18	36,0
	Total	50	100,0

Figura 12

Frecuencia de Percepciones sobre la Contribución Significativa de los Procesos de Validación de Datos en la Reducción de Errores y la Mejora de la Calidad de la Información



Los hallazgos de la encuesta indican una inclinación favorable hacia la eficacia de las estrategias de seguridad adoptadas por la empresa para limitar el acceso no autorizado a datos sensibles. Un 72% de los encuestados expresó algún grado de acuerdo, con un 24% seleccionando de acuerdo y un 48% optando por totalmente de acuerdo. Sin embargo, un 28% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una percepción mayoritariamente favorable hacia la efectividad de las medidas de seguridad en la empresa, aunque también señalan una minoría que no está completamente convencida de su eficacia.

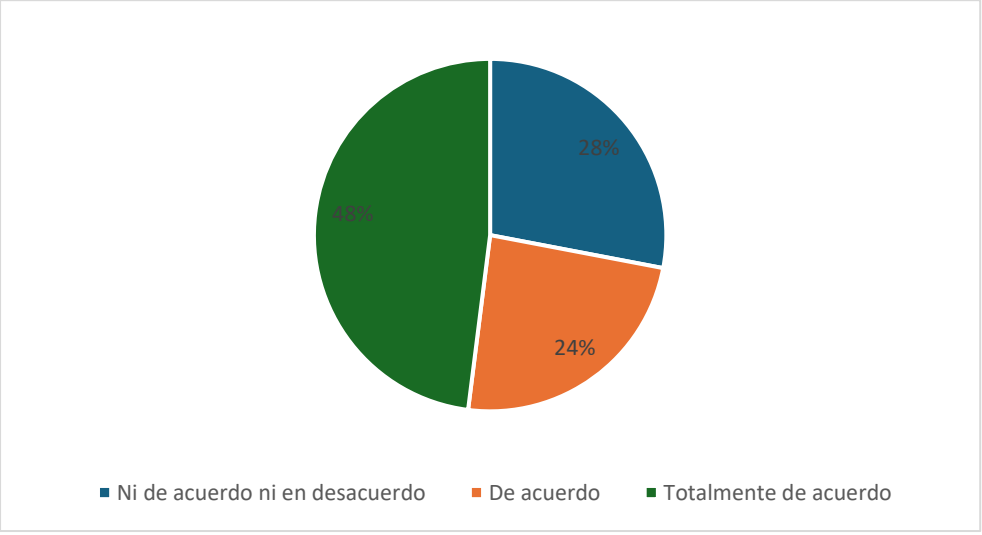
Tabla 18

Frecuencia de Percepciones sobre la Efectividad de las Medidas de Seguridad para Restringir el Acceso No Autorizado a Información Confidencial en la Empresa

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	14	28,0
	De acuerdo	12	24,0
	Totalmente de acuerdo	24	48,0
	Total	50	100,0

Figura 13

Frecuencia de Percepciones sobre la Efectividad de las Medidas de Seguridad para Restringir el Acceso No Autorizado a Información Confidencial en la Empresa



Los hallazgos de la encuesta revelan una distribución equilibrada de opiniones respecto a la suficiencia de las limitaciones de acceso para salvaguardar la privacidad y la confidencialidad de los datos utilizados en el entorno laboral. Un 68% de los encuestados expresó algún grado de acuerdo, con un 38% seleccionando de acuerdo y otro 30% optando por totalmente de acuerdo. Por otro lado, un 32% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una diversidad de percepciones dentro del grupo encuestado sobre la eficacia de las restricciones de acceso para proteger la privacidad y confidencialidad de los datos.

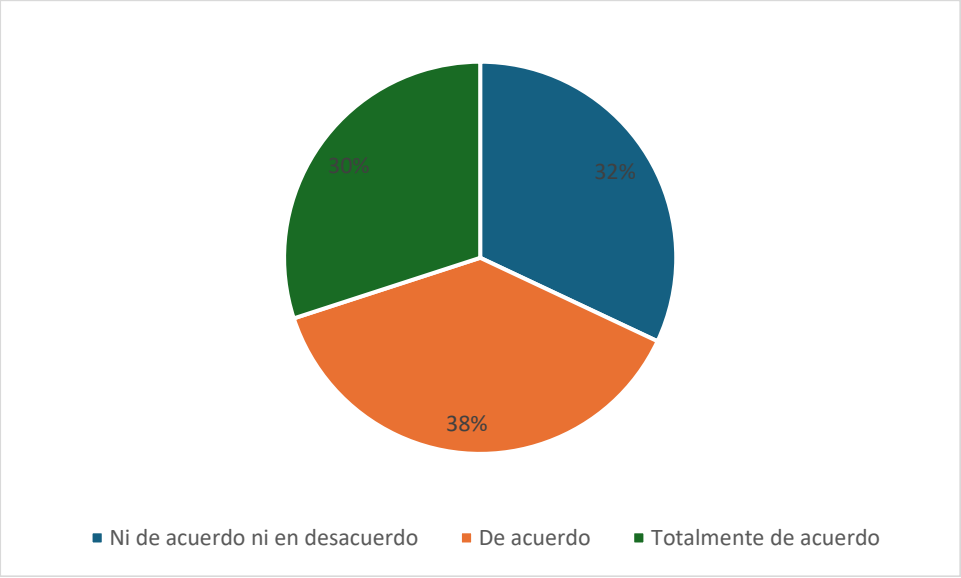
Tabla 19

Frecuencia de Percepciones sobre la Suficiencia de las Restricciones de Acceso para Proteger la Privacidad y Confidencialidad de los Datos Trabajados

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	16	32,0
	De acuerdo	19	38,0
	Totalmente de acuerdo	15	30,0
	Total	50	100,0

Figura 14

Frecuencia de Percepciones sobre la Suficiencia de las Restricciones de Acceso para Proteger la Privacidad y Confidencialidad de los Datos Trabajados



Los hallazgos de la encuesta indican que existe una confianza moderada en la eficacia de las estrategias de Gestión de Identidad y Acceso adoptadas por la empresa para asegurar la confidencialidad de la información. Un 60% de los encuestados manifestó algún grado de acuerdo, distribuyéndose en un 32% que optó por "de acuerdo" y un 28% que eligió "totalmente de acuerdo". No obstante, un 40% expresó que ni está de acuerdo ni en desacuerdo con la efectividad de estas estrategias. Estos resultados sugieren una percepción ambivalente respecto a la efectividad de las medidas de seguridad implementadas en la organización para salvaguardar la confidencialidad de los datos.

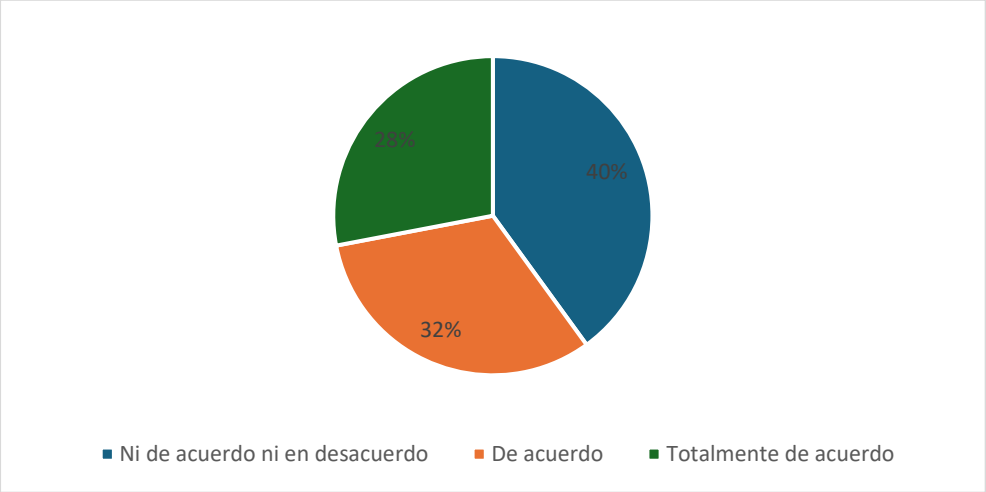
Tabla 20

Frecuencia de Percepciones sobre la Confianza en la Efectividad de las Medidas de Gestión de Identidad y Acceso Implementadas en la Empresa para Mantener la Confidencialidad de los Datos

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	20	40,0
	De acuerdo	16	32,0
	Totalmente de acuerdo	14	28,0
	Total	50	100,0

Figura 15

Frecuencia de Percepciones sobre la Confianza en la Efectividad de las Medidas de Gestión de Identidad y Acceso Implementadas en la Empresa para Mantener la Confidencialidad de los Datos



Los resultados de la encuesta evidencian una distribución balanceada de opiniones en relación con la relevancia de las políticas y procedimientos de Gestión de Identidad y Acceso para asegurar la confidencialidad de la información dentro de la organización. Un 64% de los encuestados expresó algún grado de acuerdo, siendo un 36% totalmente de acuerdo y un 28% de acuerdo. Mientras tanto, un 36% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una diversidad de percepciones dentro de la organización respecto a la efectividad de las políticas y procedimientos en la protección de la confidencialidad de la información.

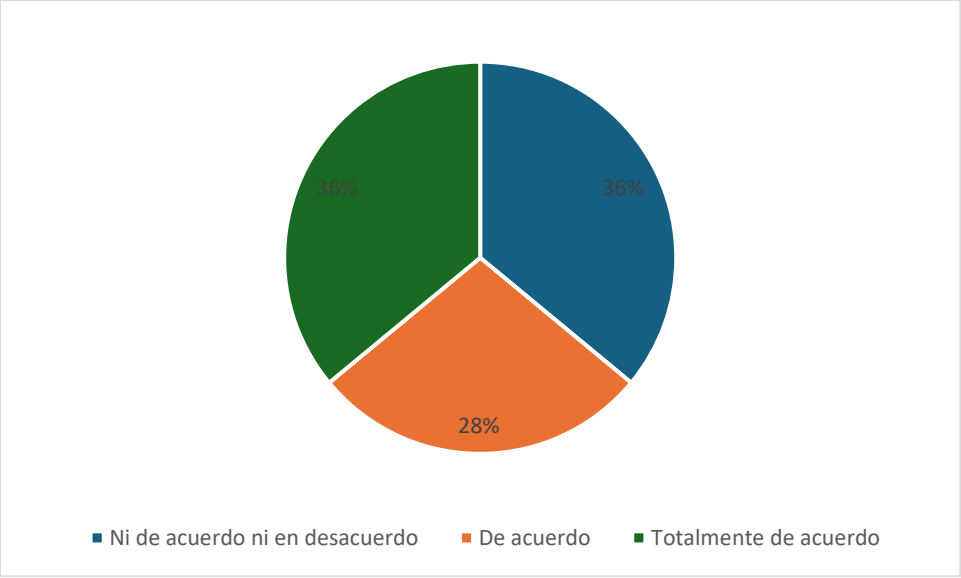
Tabla 21

Frecuencia de Percepciones sobre la Importancia de las Políticas y Procedimientos de Gestión de Identidad y Acceso en la Preservación de la Confidencialidad de la Información

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	18	36,0
	De acuerdo	14	28,0
	Totalmente de acuerdo	18	36,0
	Total	50	100,0

Figura 16

Frecuencia de Percepciones sobre la Importancia de las Políticas y Procedimientos de Gestión de Identidad y Acceso en la Preservación de la Confidencialidad de la Información



Los resultados de la encuesta indican una percepción predominantemente favorable respecto al cumplimiento de las políticas de privacidad establecidas por la empresa con los estándares normativos y legales establecidos. Un 74% de los encuestados expresó algún grado de acuerdo, con un 34% seleccionando de acuerdo y un 40% optando por totalmente de acuerdo. Sin embargo, un 26% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos hallazgos evidencian una confianza generalizada en la conformidad de las políticas de privacidad de la empresa con los estándares normativos y legales establecidos.

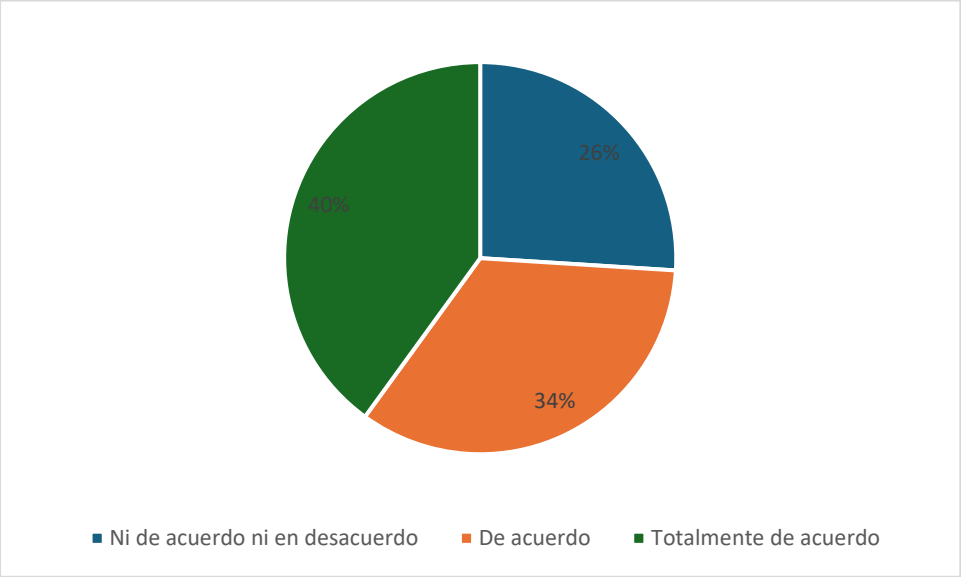
Tabla 22

Frecuencia de Percepciones sobre el Cumplimiento de los Estándares Normativos y Legales en las Políticas de Privacidad de la Empresa

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	13	26,0
	De acuerdo	17	34,0
	Totalmente de acuerdo	20	40,0
	Total	50	100,0

Figura 17

Frecuencia de Percepciones sobre el Cumplimiento de los Estándares Normativos y Legales en las Políticas de Privacidad de la Empresa



Los resultados de la encuesta indican una percepción predominantemente positiva en relación con la claridad y transparencia de las políticas de privacidad de la empresa entre todos los empleados. Un 76.0% de los encuestados manifestó algún grado de acuerdo, con un 40.0% eligiendo "de acuerdo" y un 36.0% seleccionando "totalmente de acuerdo". En contraste, un 24.0% señaló que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos hallazgos sugieren que la mayoría de los empleados consideran que las políticas de privacidad de la empresa son claras y comprensibles.

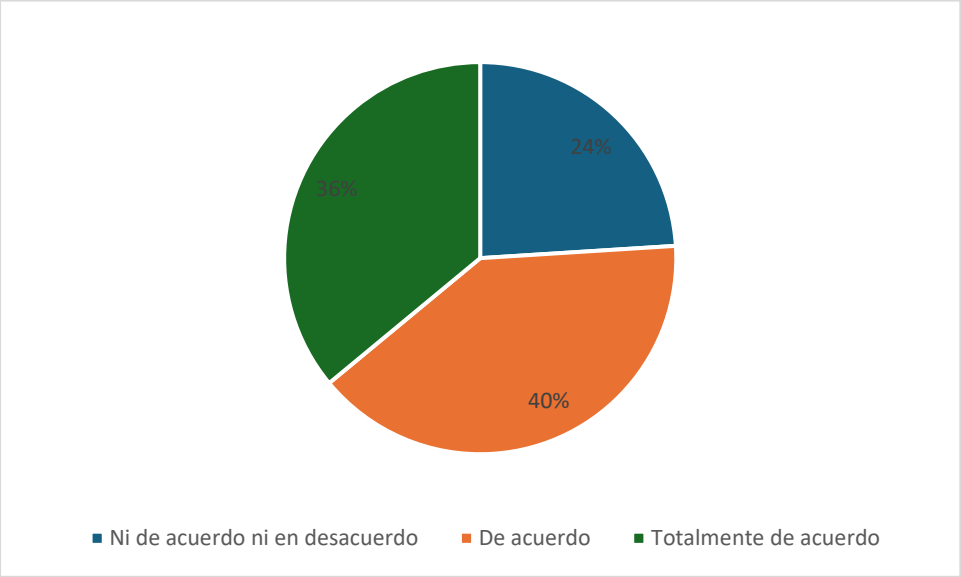
Tabla 23

Frecuencia de Percepciones sobre la Transparencia y Comprensibilidad de las Políticas de Privacidad de la Empresa para Todos los Empleados

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	12	24,0
	De acuerdo	20	40,0
	Totalmente de acuerdo	18	36,0
	Total	50	100,0

Figura 18

Frecuencia de Percepciones sobre la Transparencia y Comprensibilidad de las Políticas de Privacidad de la Empresa para Todos los Empleados



Los resultados de la encuesta revelan una opinión equilibrada respecto a si las modificaciones implementadas en los estándares de seguridad aseguran el cumplimiento normativo en el entorno laboral. Un 72.0% de los encuestados manifestó algún grado de acuerdo, con un 40.0% eligiendo "de acuerdo" y un 32.0% optando por "totalmente de acuerdo". Sin embargo, un 28.0% señaló que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos hallazgos sugieren que, aunque la mayoría de los encuestados considera que los ajustes son beneficiosos para el cumplimiento normativo, persiste un porcentaje significativo que no está completamente convencido.

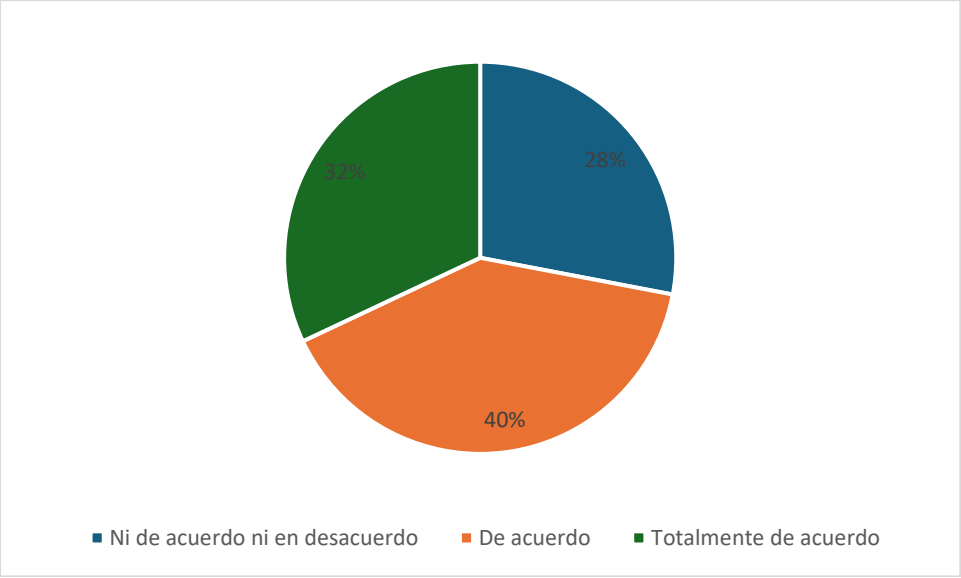
Tabla 24

Frecuencia de Percepciones sobre la Eficacia de los Ajustes a los Estándares de Seguridad en el Cumplimiento Normativo en mi Área de Trabajo

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	14	28,0
	De acuerdo	20	40,0
	Totalmente de acuerdo	16	32,0
	Total	50	100,0

Figura 19

Frecuencia de Percepciones sobre la Eficacia de los Ajustes a los Estándares de Seguridad en el Cumplimiento Normativo en mi Área de Trabajo



Los hallazgos de la encuesta indican que una amplia mayoría de los participantes, que equivale al 76.0%,expresan algún grado de acuerdo en cuanto a la accesibilidad y comprensibilidad de los ajustes a los estándares de seguridad, lo que facilita el cumplimiento normativo en sus tareas diarias. Específicamente, un 34.0% seleccionó de acuerdo y un 42.0% eligió totalmente de acuerdo. Sin embargo, un 24.0% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una percepción generalmente positiva sobre la accesibilidad y comprensibilidad de los ajustes a los estándares de seguridad en la organización.

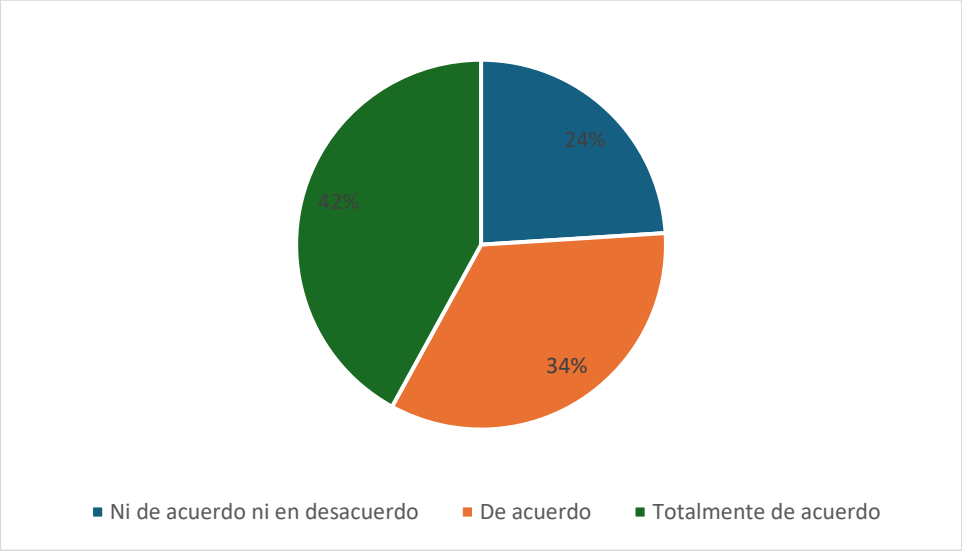
Tabla 25

Frecuencia de Percepciones sobre la Accesibilidad y Comprensibilidad de los Ajustes a los Estándares de Seguridad en la Facilitación del Cumplimiento Normativo en las Tareas Diarias de los Empleados

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	12	24,0
	De acuerdo	17	34,0
	Totalmente de acuerdo	21	42,0
	Total	50	100,0

Figura 20

Frecuencia de Percepciones sobre la Accesibilidad y Comprensibilidad de los Ajustes a los Estándares de Seguridad en la Facilitación del Cumplimiento Normativo en las Tareas Diarias de los Empleados



Los resultados de la encuesta revelan una percepción fragmentada en relación con la navegación dentro de las aplicaciones de la empresa, específicamente en lo que respecta a su intuitividad y facilidad de uso. Un 68.0% de los encuestados manifestó algún grado de acuerdo con esta afirmación, de los cuales un 36.0% seleccionó "de acuerdo" y un 32.0% optó por "totalmente de acuerdo". En contraposición, un 32.0% indicó que ni está de acuerdo ni en desacuerdo con esta evaluación. Estos hallazgos sugieren una diversidad de opiniones respecto a la experiencia del usuario al interactuar con las aplicaciones empresariales.

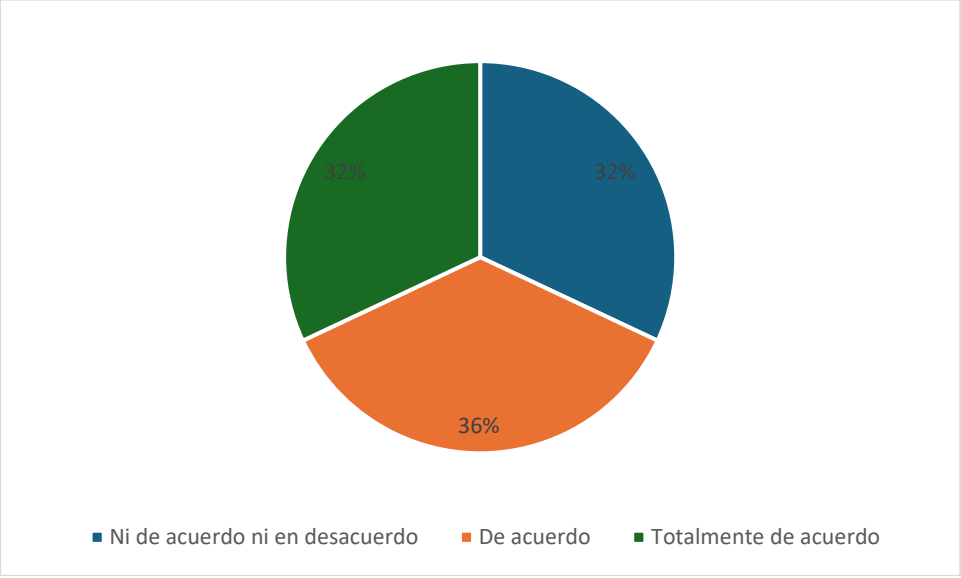
Tabla 26

Frecuencia de Percepciones sobre la Intuitividad y Facilidad de Navegación en las Aplicaciones de la Empresa, y su Impacto en la Experiencia del Usuario

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	16	32,0
	De acuerdo	18	36,0
	Totalmente de acuerdo	16	32,0
	Total	50	100,0

Figura 21

Frecuencia de Percepciones sobre la Intuitividad y Facilidad de Navegación en las Aplicaciones de la Empresa, y su Impacto en la Experiencia del Usuario



Los hallazgos de la encuesta revelan que la opinión respecto a las aplicaciones desarrolladas por la empresa responden de manera efectiva a las necesidades específicas del usuario está dividida entre los encuestados. Un 68% expresó algún grado de acuerdo, con un 32% seleccionando de acuerdo y un 36% optando por totalmente de acuerdo. Mientras tanto, un 32% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una diversidad de opiniones dentro de la organización sobre la efectividad de las aplicaciones desarrolladas en relación con las necesidades del usuario.

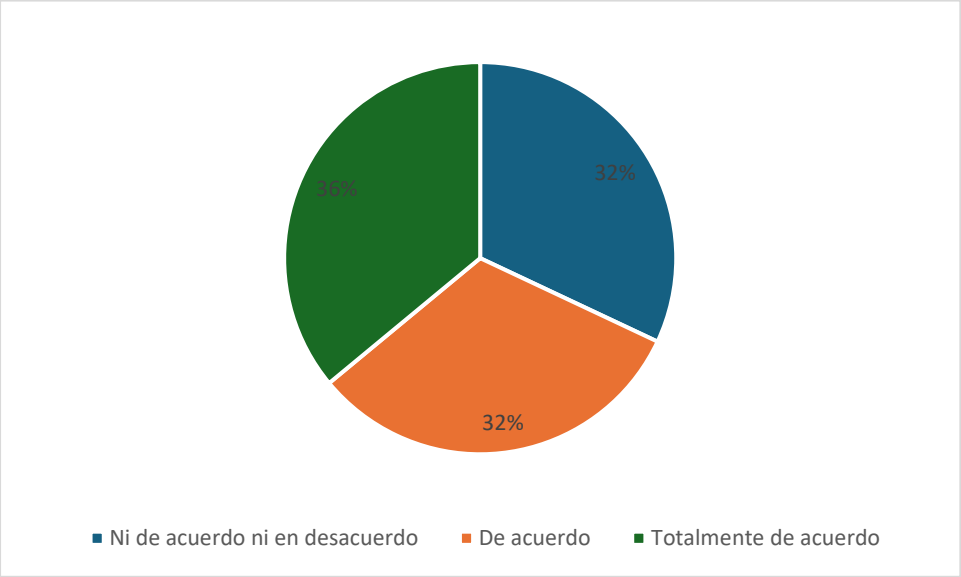
Tabla 27

Frecuencia de Percepciones sobre la Efectividad de las Aplicaciones Desarrolladas por la Empresa en la Respuesta a las Necesidades Específicas del Usuario

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	16	32,0
	De acuerdo	16	32,0
	Totalmente de acuerdo	18	36,0
	Total	50	100,0

Figura 22

Frecuencia de Percepciones sobre la Efectividad de las Aplicaciones Desarrolladas por la Empresa en la Respuesta a las Necesidades Específicas del Usuario



Los resultados de la encuesta revelan una distribución equilibrada de opiniones en torno a si la interactividad de las aplicaciones empleadas en la empresa favorece y optimiza la eficacia en la ejecución de tareas cotidianas. Un 66% de los encuestados manifestó algún nivel de conformidad, con un 32% eligiendo de acuerdo y un 34% optando por totalmente de acuerdo. Por otro lado, un 34% expresó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una diversidad de percepciones dentro de la organización sobre la efectividad de la interactividad de las aplicaciones para mejorar la eficiencia en las actividades diarias.

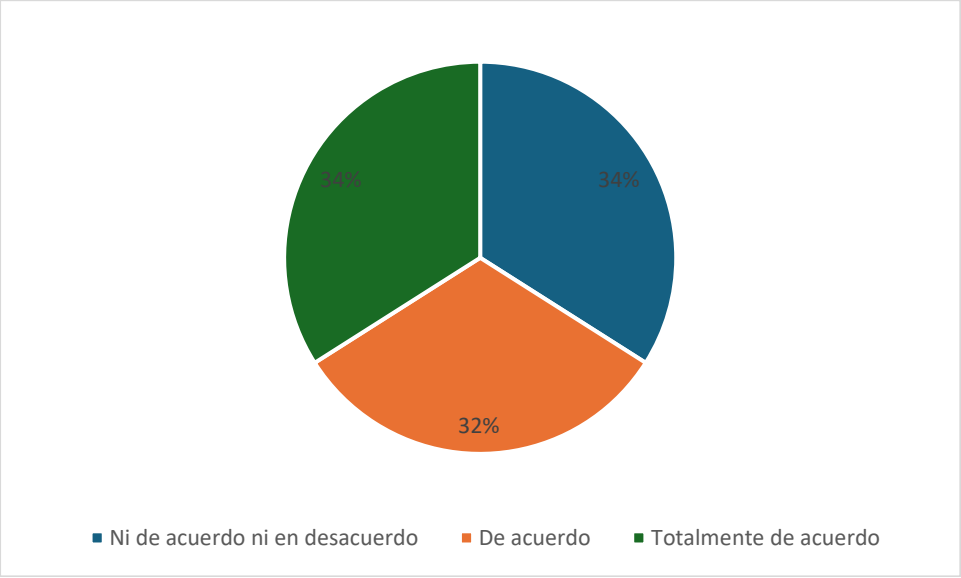
Tabla 28

Frecuencia de Percepciones sobre el Impacto de la Interactividad de las Aplicaciones en la Eficiencia de las Tareas Diarias en la Empresa

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	17	34,0
	De acuerdo	16	32,0
	Totalmente de acuerdo	17	34,0
	Total	50	100,0

Figura 23

Frecuencia de Percepciones sobre el Impacto de la Interactividad de las Aplicaciones en la Eficiencia de las Tareas Diarias en la Empresa



Los resultados de la encuesta reflejan una tendencia favorable en la percepción de la eficacia de la formación brindada para el uso de las aplicaciones desarrolladas internamente. La mayoría de los encuestados, que representan el 68% del total, manifestaron algún nivel de acuerdo con esta afirmación. En concreto, un 32% eligió de acuerdo y otro 36% optó por totalmente de acuerdo. Solo un 32% señaló que ni está de acuerdo ni en desacuerdo. Estos hallazgos sugieren que la mayoría de los encuestados considera que la capacitación ha sido efectiva para mejorar la comprensión y utilización de las funciones interactivas disponibles en las aplicaciones internas creadas.

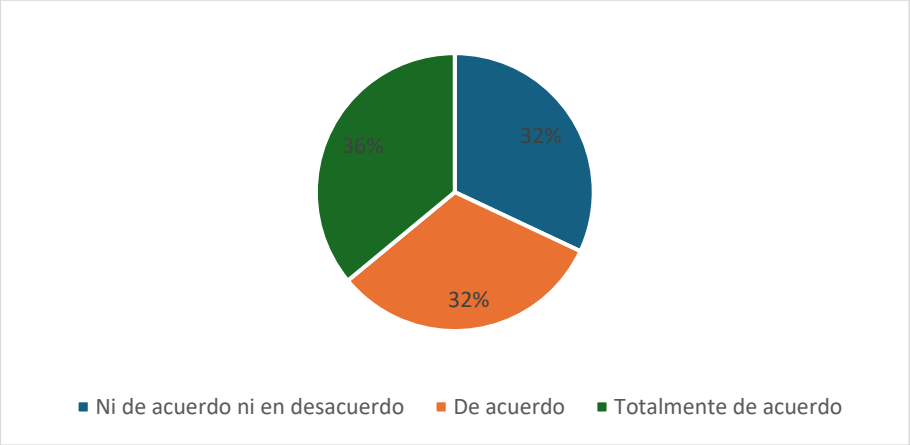
Tabla 29

Frecuencia de Percepciones sobre la Efectividad de la Capacitación para el Uso de Aplicaciones Desarrolladas Internamente en Mejorar la Comprensión y Aprovechamiento de las Funciones Interactivas Disponibles

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	16	32,0
	De acuerdo	16	32,0
	Totalmente de acuerdo	18	36,0
	Total	50	100,0

Figura 24

Frecuencia de Percepciones sobre la Efectividad de la Capacitación para el Uso de Aplicaciones Desarrolladas Internamente en Mejorar la Comprensión y Aprovechamiento de las Funciones Interactivas Disponibles



Los resultados de la encuesta indican que la percepción acerca de la aportación del rendimiento de las aplicaciones al cumplimiento de los objetivos y metas fijados para el desarrollo de eventos es predominantemente favorable. Un 66% de los encuestados expresaron algún grado de acuerdo, con un 28% seleccionando de acuerdo y un 38% eligiendo totalmente de acuerdo. Por otro lado, un 34% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una tendencia favorable hacia la eficacia percibida del rendimiento de las aplicaciones en la consecución de objetivos y metas en el desarrollo de eventos.

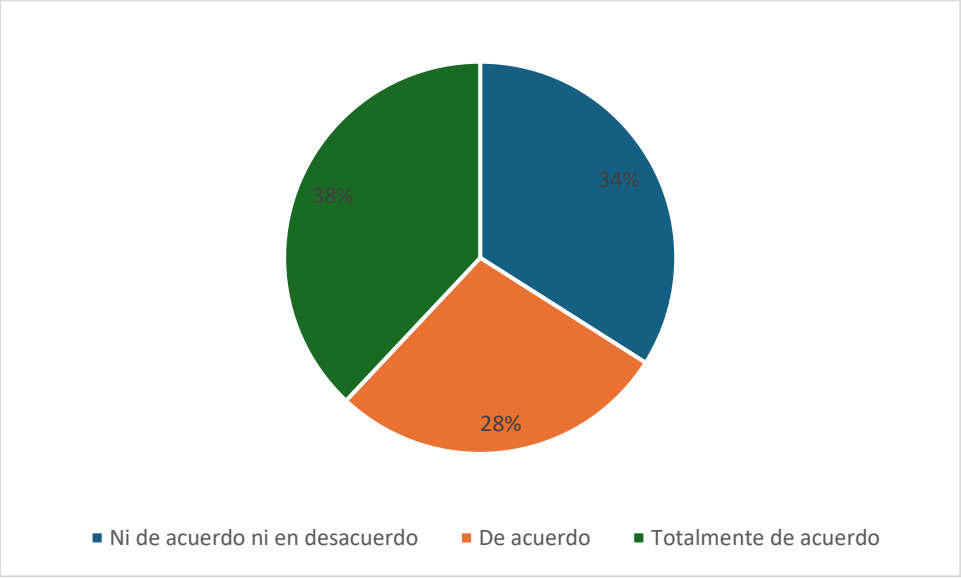
Tabla 30

Frecuencia de Percepciones sobre la Eficacia de la Contribución del Rendimiento de las Aplicaciones en el Logro de Objetivos y Metas para el Desarrollo de Eventos

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	17	34,0
	De acuerdo	14	28,0
	Totalmente de acuerdo	19	38,0
	Total	50	100,0

Figura 25

Frecuencia de Percepciones sobre la Eficacia de la Contribución del Rendimiento de las Aplicaciones en el Logro de Objetivos y Metas para el Desarrollo de Eventos



Los resultados de la encuesta revelan que la mayoría de los participantes, equivalente al 50.0%, indicaron que ni están de acuerdo ni en desacuerdo con la afirmación de que el rendimiento de las aplicaciones ha contribuido a la reducción de errores y fallos durante el proceso de desarrollo e implementación. Sin embargo, un 50.0% expresó algún grado de acuerdo, con un 24.0% seleccionando de acuerdo y un 26.0% eligiendo totalmente de acuerdo. Estos resultados reflejan una diversidad de opiniones sobre el impacto del rendimiento de las aplicaciones en la reducción de errores y fallos durante el proceso de desarrollo e implementación.

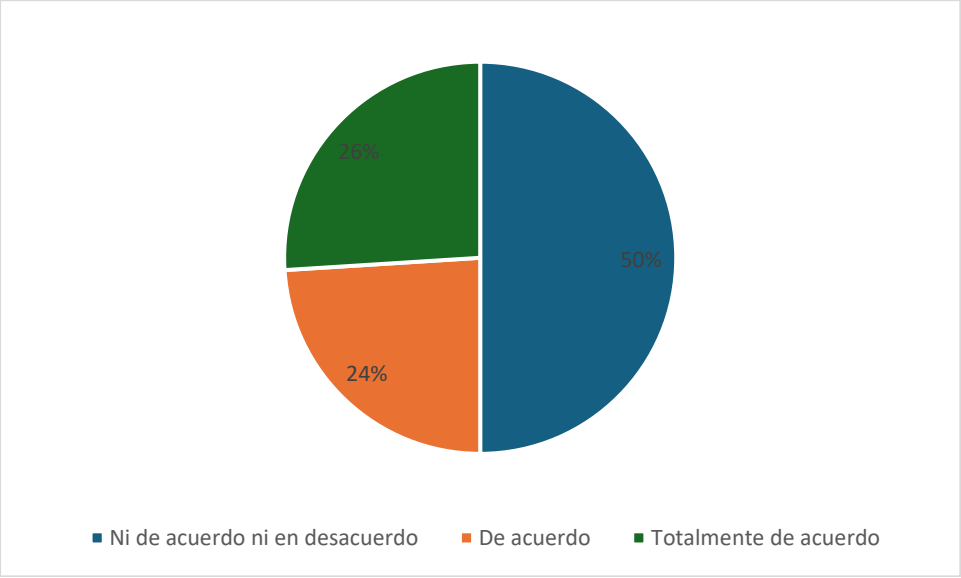
Tabla 31

Frecuencia de Percepciones sobre la Contribución del Rendimiento de las Aplicaciones en la Reducción de Errores y Fallos durante el Proceso de Desarrollo e Implementación

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	25	50,0
	De acuerdo	12	24,0
	Totalmente de acuerdo	13	26,0
	Total	50	100,0

Figura 26

Frecuencia de Percepciones sobre la Contribución del Rendimiento de las Aplicaciones en la Reducción de Errores y Fallos durante el Proceso de Desarrollo e Implementación



Los hallazgos de la encuesta revelan una percepción predominantemente positiva en relación con la eficacia del proceso de planificación de actividades en el contexto de la Gestión de Planes dentro de la empresa. La mayoría de los encuestados, que representa el 76% de las respuestas, manifestó algún nivel de acuerdo con esta afirmación. En detalle, un 48% indicó estar de acuerdo, mientras que un 28% optó por expresar su total conformidad. No obstante, un 24% declaró que ni está de acuerdo ni en desacuerdo respecto a la eficiencia de dicho proceso. Estos resultados sugieren que, aunque la mayoría percibe la existencia de un proceso eficiente para la planificación de actividades, persiste una minoría que no está del todo convencida.

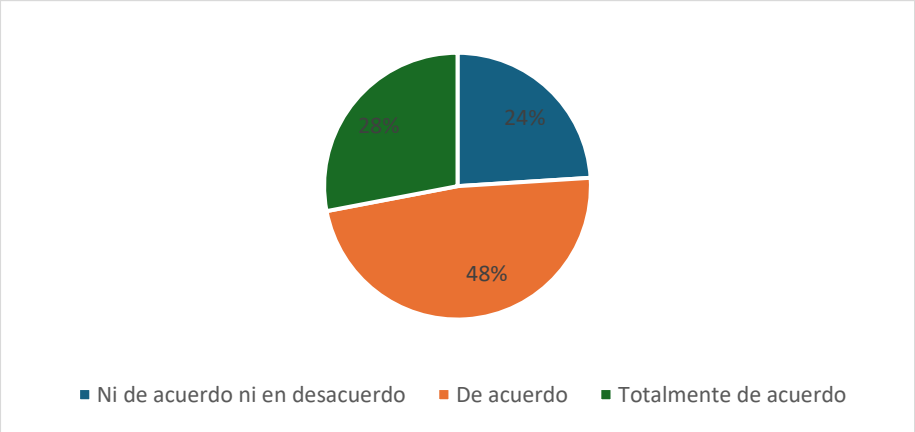
Tabla 32

Frecuencia de Percepciones sobre la Eficiencia del Proceso de Planificación de Actividades en el Ámbito de la Gestión de Planes de la Empresa

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	12	24,0
	De acuerdo	24	48,0
	Totalmente de acuerdo	14	28,0
	Total	50	100,0

Figura 27

Frecuencia de Percepciones sobre la Eficiencia del Proceso de Planificación de Actividades en el Ámbito de la Gestión de Planes de la Empresa



Los resultados de la encuesta muestran que la percepción sobre si la empresa brinda los recursos necesarios para implementar efectivamente los planes estratégicos es bastante equilibrada entre los encuestados. Un 70% de los encuestados expresó algún grado de acuerdo con esta afirmación, con un 36.0% seleccionando de acuerdo y un 34.0% eligiendo totalmente de acuerdo. Mientras tanto, un 30.0% indicó que ni está de acuerdo ni en desacuerdo con esta declaración. Estos resultados sugieren que, si bien una mayoría apreciable percibe que la empresa proporciona los recursos necesarios, aún existe un segmento significativo que podría tener reservas al respecto.

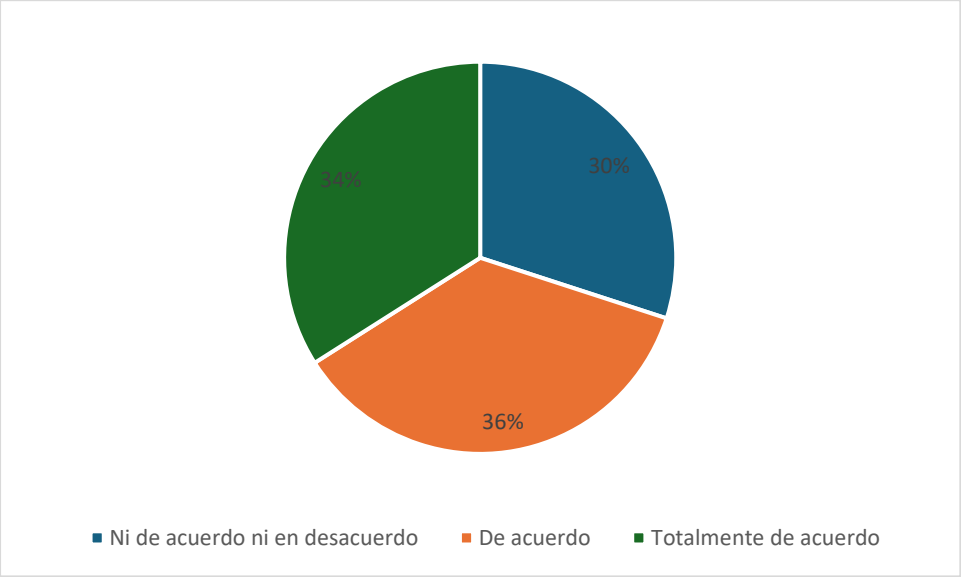
Tabla 33

Frecuencia de Percepciones sobre la Disponibilidad de Recursos de la Empresa para la Implementación Efectiva de Planes Estratégicos

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	15	30,0
	De acuerdo	18	36,0
	Totalmente de acuerdo	17	34,0
	Total	50	100,0

Figura 28

Frecuencia de Percepciones sobre la Disponibilidad de Recursos de la Empresa para la Implementación Efectiva de Planes Estratégicos



Los hallazgos de la encuesta sugieren que la percepción acerca de la efectividad de la empresa en la distribución de recursos para lograr los objetivos establecidos es predominantemente favorable. Un 72.0% de los encuestados expresó algún grado de acuerdo, con un 38.0% seleccionando de acuerdo y un 34.0% optando por totalmente de acuerdo. Por otro lado, un 28.0% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una confianza generalizada en la capacidad de la empresa para gestionar eficazmente sus recursos en pos de sus objetivos planificados.

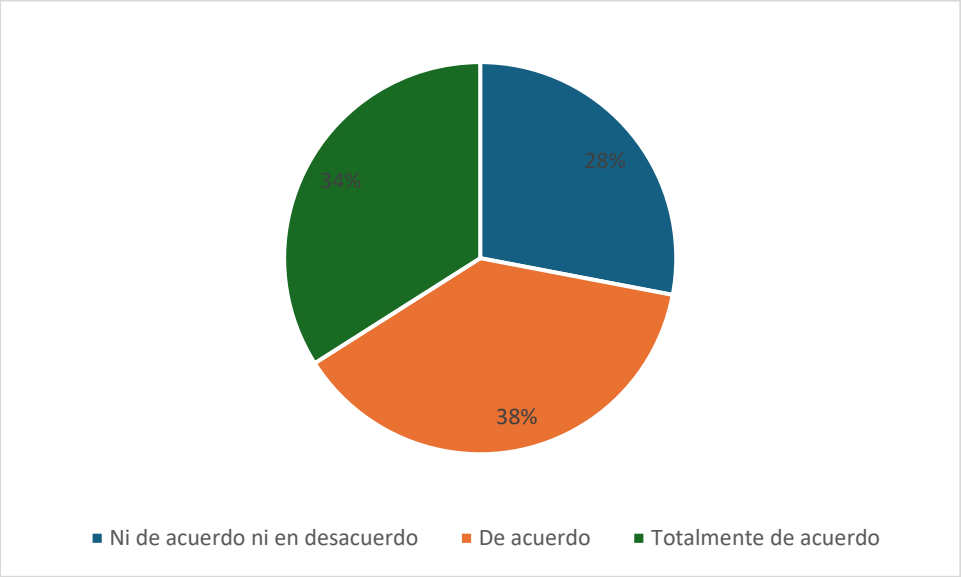
Tabla 34

Frecuencia de Percepciones sobre la Disponibilidad de Recursos para la Implementación Efectiva de Planes Estratégicos en la Empresa

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	14	28,0
	De acuerdo	19	38,0
	Totalmente de acuerdo	17	34,0
	Total	50	100,0

Figura 29

Frecuencia de Percepciones sobre la Disponibilidad de Recursos para la Implementación Efectiva de Planes Estratégicos en la Empresa



Los hallazgos de la encuesta revelan una dispersión equilibrada de opiniones respecto a si la empresa emplea los recursos disponibles para responder a cambios inesperados o situaciones de crisis en el entorno empresarial. Un 70.0% de los encuestados expresó algún grado de acuerdo, con un 40.0% seleccionando de acuerdo y otro 30.0% optando por totalmente de acuerdo. Por otro lado, un 30.0% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una percepción general positiva sobre la capacidad de la empresa para adaptarse a cambios imprevistos o crisis en su entorno empresarial, aunque existe un segmento que no está completamente convencido.

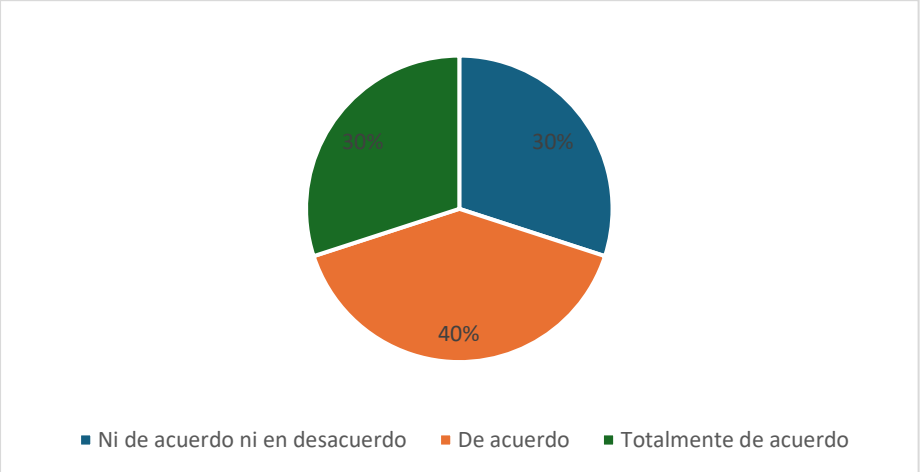
Tabla 35

Frecuencia de Percepciones sobre la Disponibilidad de Recursos para la Implementación Efectiva de Planes Estratégicos en la Empresa

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	15	30,0
	De acuerdo	20	40,0
	Totalmente de acuerdo	15	30,0
	Total	50	100,0

Figura 30

Frecuencia de Percepciones sobre la Disponibilidad de Recursos para la Implementación Efectiva de Planes Estratégicos en la Empresa



Los resultados de la encuesta reflejan una percepción favorable respecto a la eficacia del sistema de Control de Calidad en la administración de planes dentro de la empresa. La mayoría de los participantes, que representa el 72% del total, expresó algún nivel de acuerdo con esta afirmación. En particular, un 38% manifestó estar de acuerdo y un 34% eligió la opción de totalmente de acuerdo. No obstante, un 28% de los encuestados se mostró neutral, seleccionando la opción de ni de acuerdo ni en desacuerdo. Estos hallazgos sugieren una inclinación hacia una percepción positiva sobre la efectividad del sistema de Control de Calidad en la gestión de planes, aunque una proporción significativa de los encuestados permanece indecisa al respecto.

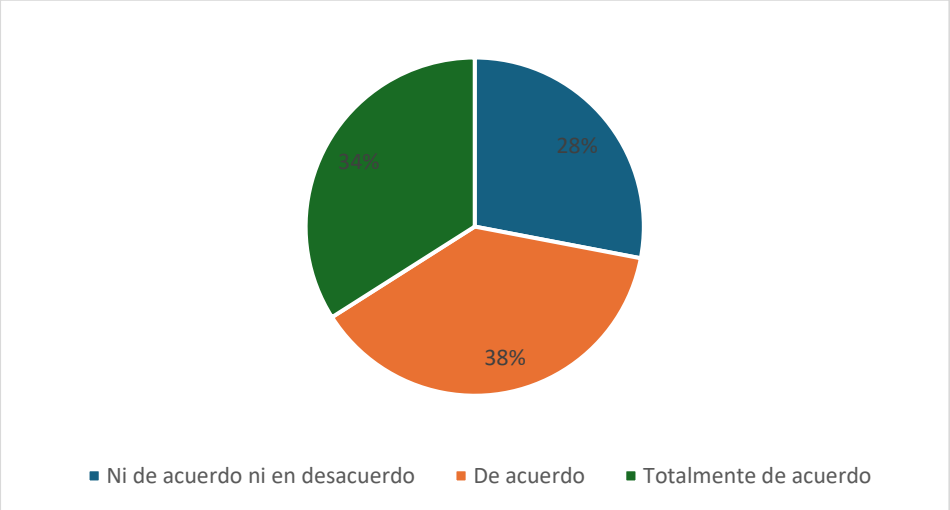
Tabla 36

Frecuencia de Percepciones sobre la Efectividad del Sistema de Control de Calidad en la Gestión de Planes de la Empresa

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	14	28,0
	De acuerdo	19	38,0
	Totalmente de acuerdo	17	34,0
	Total	50	100,0

Figura 31

Frecuencia de Percepciones sobre la Efectividad del Sistema de Control de Calidad en la Gestión de Planes de la Empresa



Los resultados de la encuesta revelan una discrepancia en las opiniones respecto al compromiso de la empresa con el Control de Calidad en la implementación de los planes estratégicos. A pesar de que un 66% de los encuestados manifestó algún grado de acuerdo, con un 38% indicando estar de acuerdo y un 28% optando por totalmente de acuerdo, un 34% expresó que se encuentra en una posición neutral, seleccionando ni de acuerdo ni en desacuerdo. Estos hallazgos sugieren una diversidad de percepciones en la organización sobre el compromiso de la empresa con el Control de Calidad en la ejecución de sus planes estratégicos.

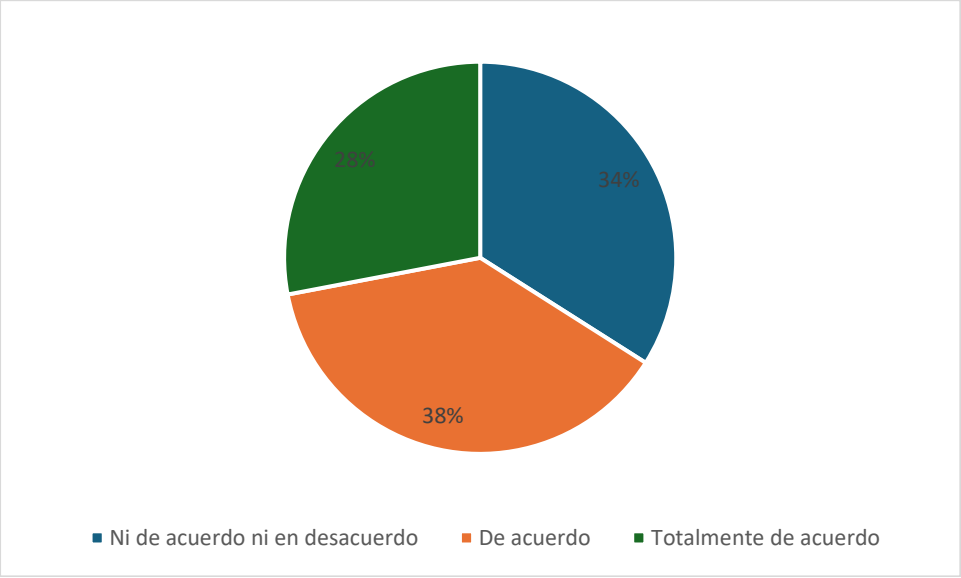
Tabla 37

Frecuencia de Percepciones sobre el Compromiso de la Empresa con el Control de Calidad en la Ejecución de los Planes Estratégicos

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	17	34,0
	De acuerdo	19	38,0
	Totalmente de acuerdo	14	28,0
	Total	50	100,0

Figura 32

Frecuencia de Percepciones sobre el Compromiso de la Empresa con el Control de Calidad en la Ejecución de los Planes Estratégicos



Los resultados de la investigación evidencian una notable predisposición hacia una valoración positiva de la accesibilidad de las plataformas y aplicaciones, considerándola un elemento que potencia la eficiencia. Un 66% de los individuos encuestados expresó algún grado de acuerdo, desglosándose en un 44% que seleccionó la opción "totalmente de acuerdo" y un 22% que eligió "de acuerdo". Únicamente un 34% de los participantes adoptó una postura neutra respecto a esta afirmación. Estos hallazgos sugieren que la mayoría de los encuestados aprecian la accesibilidad de las plataformas y aplicaciones como un factor beneficioso que contribuye a la optimización de la eficiencia en sus operaciones.

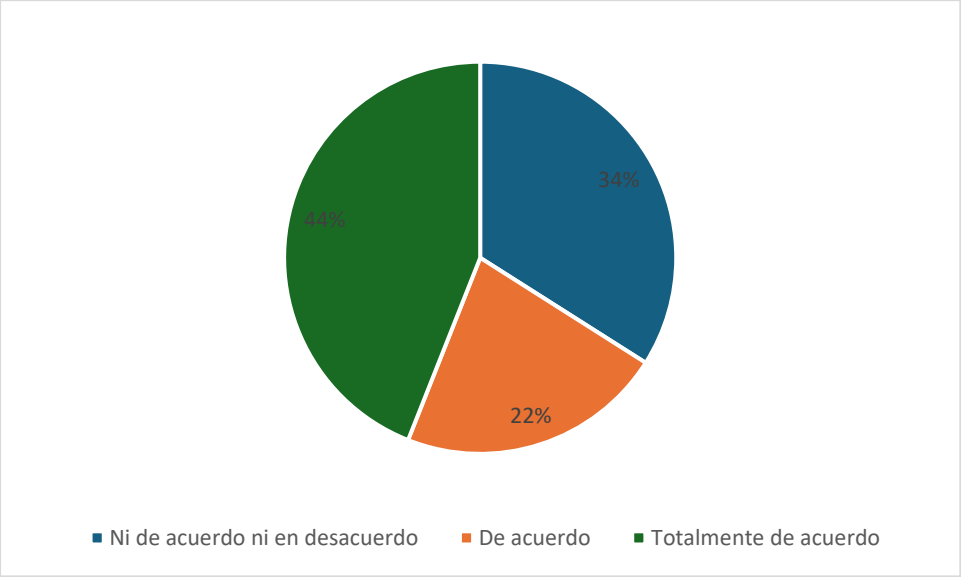
Tabla 38

Frecuencia de Percepciones sobre la Importancia de la Accesibilidad de Plataformas y Aplicaciones para la Eficiencia

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	17	34,0
	De acuerdo	11	22,0
	Totalmente de acuerdo	22	44,0
	Total	50	100,0

Figura 33

Frecuencia de Percepciones sobre la Importancia de la Accesibilidad de Plataformas y Aplicaciones para la Eficiencia



Los resultados de la encuesta muestran que una gran mayoría de los encuestados, representando el 72% de las respuestas, confían en la simplicidad y claridad de las herramientas. Específicamente, un 42% de los encuestados indicaron estar totalmente de acuerdo con esta afirmación, mientras que un 30% estuvo de acuerdo. Sin embargo, un 28% expresó que ni está de acuerdo ni en desacuerdo. Estos resultados sugieren que la mayoría de los encuestados perciben las herramientas como simples y claras, lo que puede ser un aspecto positivo en su utilización.

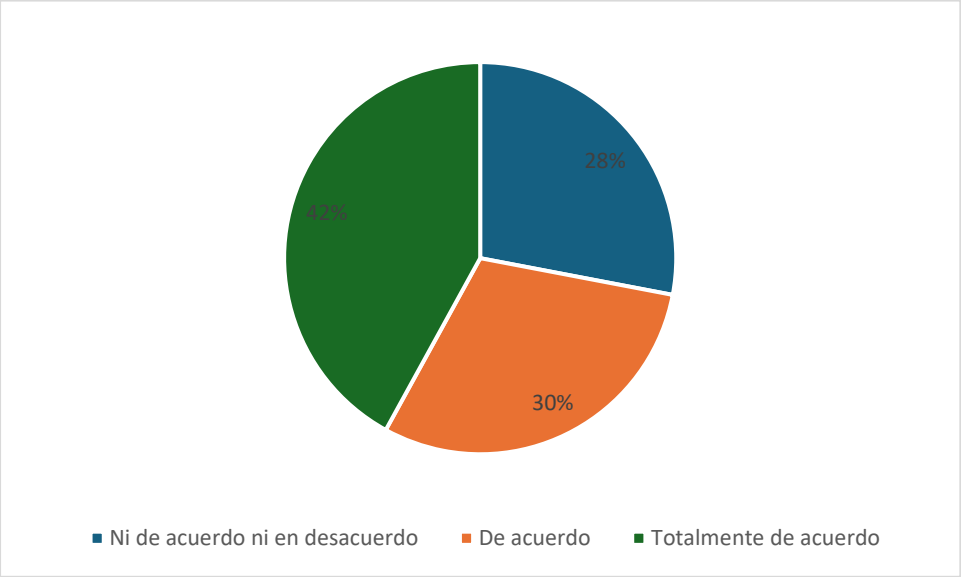
Tabla 39

Frecuencia de Percepciones sobre la Confianza en la Simplicidad y Claridad de las Herramientas

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	14	28,0
	De acuerdo	15	30,0
	Totalmente de acuerdo	21	42,0
	Total	50	100,0

Figura 34

Frecuencia de Percepciones sobre la Confianza en la Simplicidad y Claridad de las Herramientas



Los resultados de la encuesta muestran una distribución equitativa de opiniones sobre si la personalización de las políticas de desarrollo profesional se alinea con las metas y expectativas. Un 70% de los encuestados expresó algún grado de acuerdo, con un 40% seleccionando de acuerdo y otro 30% optando por totalmente de acuerdo. Por otro lado, un 30% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados sugieren una diversidad de perspectivas dentro de la organización sobre la alineación de las políticas de desarrollo profesional con las metas y expectativas individuales.

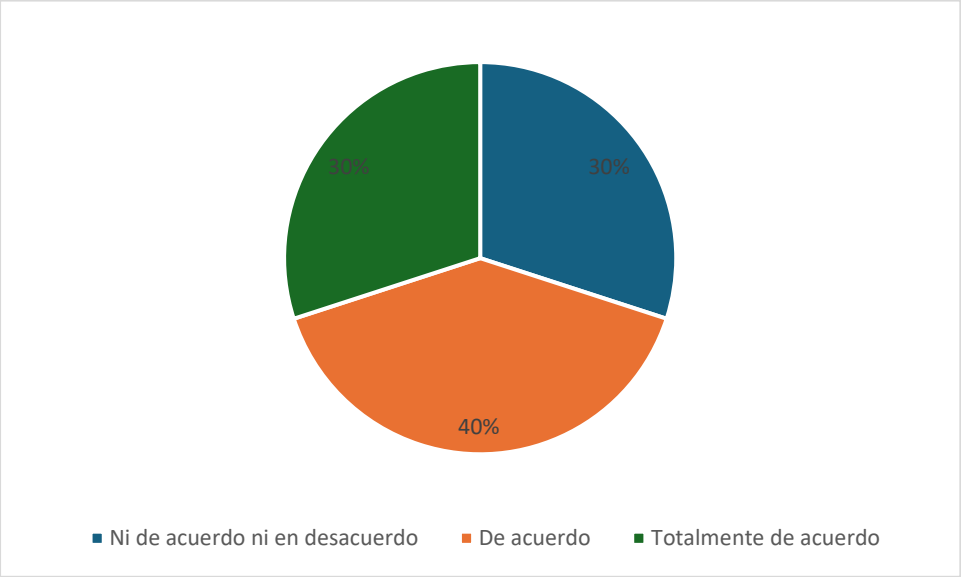
Tabla 40

Frecuencia de Percepciones sobre la Alineación de las Metas y Expectativas con la Personalización de las Políticas de Desarrollo Profesional

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	15	30,0
	De acuerdo	20	40,0
	Totalmente de acuerdo	15	30,0
	Total	50	100,0

Figura 35

Frecuencia de Percepciones sobre la Alineación de las Metas y Expectativas con la Personalización de las Políticas de Desarrollo Profesional



Los resultados de la encuesta reflejan que la percepción sobre si la personalización de la comunicación interna, adaptada a las necesidades y preferencias, contribuye a la satisfacción del usuario, varía entre los encuestados. Un 56% expresó algún grado de acuerdo, con un 24% seleccionando de acuerdo y un 32% optando por totalmente de acuerdo. Sin embargo, un 44% indicó que ni está de acuerdo ni en desacuerdo con esta afirmación. Estos resultados muestran una diversidad de opiniones dentro de la organización sobre la contribución de la personalización de la comunicación interna a la satisfacción del usuario.

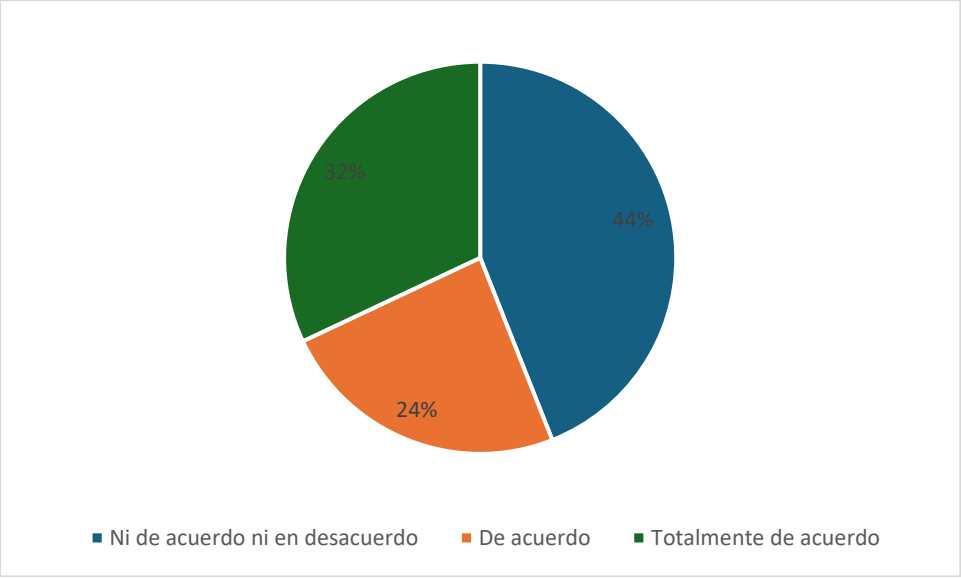
Tabla 41

Frecuencia de Percepciones sobre la Contribución de la Personalización de la Comunicación Interna, Adaptada a las Necesidades y Preferencias, en la Satisfacción del Usuario

		Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	22	44,0
	De acuerdo	12	24,0
	Totalmente de acuerdo	16	32,0
	Total	50	100,0

Figura 36

Frecuencia de Percepciones sobre la Contribución de la Personalización de la Comunicación Interna, Adaptada a las Necesidades y Preferencias, en la Satisfacción del Usuario



V. DISCUSIÓN DE RESULTADOS

Sosa (2022) destaca que los delincuentes informáticos encuentran fácilmente maneras de generar confianza en entidades, la investigación también busca examinar cómo se comparten contraseñas y otra información confidencial de datos personales, y además, indagar si la RENIEC, responsable de proteger los datos personales como un bien jurídico de los ciudadanos beneficiarios, dispone de un sistema efectivo para su adecuada protección y para prevenir la violación del derecho a la identidad. Lo importante de esta investigación radica en que entidades estatales, como la RENIEC en este caso, al diseñar plataformas para que los ciudadanos puedan verificar su elegibilidad para el cobro de bonos, deben asegurar la seguridad de los datos. No obstante, la plataforma resultó vulnerable, lo que permitió a hackers acceder al mercado negro con los datos de los beneficiarios, afectando a miles de ciudadanos que descubrieron que sus bonos ya habían sido cobrados. Esto subraya la urgente necesidad de evaluar de manera minuciosa l La eficacia de las medidas de seguridad adoptadas por la RENIEC y otras instituciones gubernamentales para proteger la información confidencial de los ciudadanos es crucial. A lo largo de este análisis, se determinó un coeficiente de correlación Rho de Spearman de 0.402** y un valor de significancia (bilateral) de 0.004. Estos resultados demuestran una correlación positiva significativa entre las variables examinadas, lo que indica que al fortalecer las medidas de seguridad, es factible que se alcance una mejora en la salvaguarda de la información personal. La protección de datos es esencial para la ejecución exitosa de aplicaciones de realidad aumentada en eventos deportivos durante el año 2023. Se observa una relación directa entre la solidez de las medidas de seguridad y la confianza del usuario en dichas aplicaciones, lo cual repercute significativamente en la experiencia global del evento.

Flores y Uriarte (2023) la finalidad principal de este estudio es establecer de qué forma las herramientas tecnológicas aportan al delito informático de suplantación de identidad en el

ámbito de las telecomunicaciones en Jaén para el año 2022. Esto incluye investigar cómo la escasa presencia de policías, profesionales y fiscales especializados en casos de ciberdelitos como este en Jaén puede influir en el manejo y resolución de denuncias por suplantación de identidad, las cuales tienden a no prosperar y ser archivadas. Con el propósito de alcanzar este propósito, se aplicó una metodología de análisis cualitativo de categoría esencial, implementando el diseño de teoría arraigada. Se utilizaron métodos como el examen documental y la interacción con individuos experimentados para adquirir datos pertinentes que ratificaran la premisa principal de que los recursos tecnológicos efectivamente promueven la infracción cibernética de usurpación de identidad en el ámbito de las telecomunicaciones en Jaén durante el año 2022. En este análisis, se calculó un coeficiente de correlación Rho de Spearman que arroja un valor de 0.409** y un nivel de significancia (bilateral) de 0.002. Se concluye que la ejecución exitosa de la gestión de planes en eventos deportivos durante el año 2023 está fuertemente ligada a la seguridad de datos. La aptitud para resguardar la información pertinente, como los horarios, las locaciones y los detalles de los participantes, aporta de manera significativa a la eficiencia operativa y al logro de los objetivos del evento.

Elías (2019) en su investigación, se analiza el nivel de protección cibernética que posee la Municipalidad de Luján de Cuyo, situada en la provincia de Mendoza, en lo concerniente a la administración de la información. Para este propósito, se realiza un análisis detallado del riesgo asociado a la generación de diversos tipos de daños informáticos, los cuales son originados por las amenazas que actúan sobre las vulnerabilidades y el impacto resultante de dichas amenazas. Estas facetas se exploran en tres áreas esenciales: protección física, seguridad informática y seguridad en el sistema de gestión y comunicación. Se analizan y detallan diversos tipos de actividades delictivas relacionadas con la informática, así como las prácticas dañinas realizadas a través de sistemas. En esta investigación, se ha determinado un coeficiente de correlación Rho de Spearman que muestra un valor de 0.402** y un nivel de significancia

(bilateral) de 0.004. Esto sugiere que la protección de datos desempeña un papel crucial en la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos durante el año 2023. Se evidencia una correlación directa entre la robustez de las medidas de seguridad y la confianza del usuario en estas aplicaciones, lo que influye en la experiencia general del evento.

Ochoa (2021) indica que en el contexto particular de Ecuador, esta problemática se plantea como un tema de gran envergadura en lo que respecta a la capacidad gubernamental, La elaboración de políticas en el ámbito de la seguridad digital y la toma de decisiones para regular y enfrentar el cibercrimen es esencial. Este estudio se centra en examinar los desafíos globales derivados de la delincuencia cibernética, particularmente en relación con la legislación latinoamericana y las políticas destinadas a su prevención. En el primer apartado, se lleva a cabo un análisis teórico acerca del cibercrimen y sus categorías, abordando los desafíos globales que enfrentan tanto el sector comercial como las instituciones gubernamentales, así como las iniciativas para implementar medidas de seguridad digital en ambos ámbitos. Se examinan los tratados internacionales aplicables en la lucha contra el cibercrimen y se lleva a cabo una comparación legislativa en América Latina, contextualizándola en el marco ecuatoriano. En la sección final, se presentan y analizan casos concretos, como los de Julian Assange, Ola Bini y el incidente de sustracción de datos personales de ciudadanos ecuatorianos en 2019. Al finalizar este estudio, se obtuvo un coeficiente de correlación Rho de Spearman con un valor de 0.402** y un nivel de significancia (bilateral) de 0.004, lo que indica una correlación positiva significativa entre las variables examinadas. Se concluye que la salvaguarda de la información resulta fundamental en la adecuada fusión de las aplicaciones de realidad aumentada en eventos deportivos durante el año 2023. Se observa una conexión directa entre la solidez de las precauciones de seguridad y la confianza del usuario en dichas aplicaciones, lo que impacta en la experiencia global del evento.

Carvajal et al. (2021) tuvo como objetivo primordial de este proyecto consiste en desarrollar un manual de protección informática para asegurar la confidencialidad, integridad y disponibilidad de los sistemas de información. en el Colegio Gimnasio Los Pinos, ubicado en Bogotá DC. Este manual se basa en el Esquema de Seguridad y Confidencialidad de Datos (ESCD) de MINTIC y sigue las pautas del instructivo número tres de la NORMA TECNICA COLOMBIANA ISO 27001. La elaboración de una directriz de seguridad abarca una amplia variedad de aspectos, siendo fundamental para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI) eficaz en cualquier organización. Este análisis de riesgos ofreció una comprensión integral del estado actual de la entidad en relación con la seguridad en el entorno del centro de datos. La evaluación se realizó conforme a los estándares establecidos por la norma ISO/IEC 27001:2013, subrayando la necesidad urgente de implementar una estrategia y política de protección para mitigar los riesgos y vulnerabilidades identificados. La integración de un sistema de monitoreo, junto con la adopción de medidas de seguridad y la ejecución de la segmentación de la red existente, demostró ser efectiva para reducir las vulnerabilidades de los sistemas, elevándolos a un nivel de protección óptimo. En conclusión, este proyecto logró cumplir plenamente con todos los objetivos planteados. En esta evaluación, se determinó un coeficiente de correlación Rho de Spearman que alcanzó un valor de 0.409**, con un nivel de significancia (bilateral) de 0.002. Se infiere que la eficacia en la gestión de eventos deportivos en 2023 está significativamente relacionada con la protección de los datos. La capacidad para salvaguardar información crucial, como los cronogramas, es esencial para garantizar un desarrollo adecuado y sin contratiempos, ubicaciones y detalles de los participantes, contribuye de manera significativa a la eficacia operativa y al logro de los objetivos del evento.

VI. CONCLUSIONES

6.1. Los hallazgos indican un coeficiente de correlación Spearman Rho de 0.402**, acompañado de un nivel de significancia bilateral de 0.004. Cabe subrayar que la protección de la información ejerce una función determinante en la implementación efectiva de soluciones basadas en realidad aumentada dentro de escenarios deportivos durante el año 2023. Se evidencia una correlación directa entre la robustez de las medidas de seguridad y la confianza del usuario en estas aplicaciones, lo que influye en la experiencia general del evento.

6.2. Los resultados evidencian un coeficiente de correlación Spearman Rho de 0.499**, con un nivel de significancia bilateral de 0.000. Esto indica una relación considerable entre el desarrollo de software para eventos deportivos en 2023 y la protección de datos. La salvaguarda de la confidencialidad y la integridad de la información resulta fundamental en este contexto del usuario es fundamental para asegurar el éxito de dichas aplicaciones y para preservar la confianza tanto de los usuarios como de las partes interesadas involucradas en el evento.

6.3. Los hallazgos revelan un coeficiente de correlación Spearman Rho de 0.409**, acompañado de un nivel de significancia bilateral de 0.002. Se concluye que la implementación exitosa de la gestión de planes en eventos deportivos durante 2023 está significativamente influenciada por estos factore. La aptitud para salvaguardar la información pertinente, como horarios, ubicaciones y detalles de los participantes, contribuye significativamente a la eficiencia operativa y al cumplimiento de los objetivos del evento.

6.4. Los resultados indican un coeficiente de correlación Spearman Rho de 0.389**, con un nivel de significancia bilateral de 0.002; la satisfacción del usuario en eventos deportivos en 2023 está directamente vinculada a la seguridad de datos. Los usuarios

esperan que sus datos personales estén protegidos de manera efectiva durante su participación en el evento, y cualquier fallo en la seguridad puede impactar negativamente en la experiencia y percepción del usuario.

VII. RECOMENDACIONES

7.1. Establecer como principal enfoque la incorporación de medidas de seguridad robustas en cada etapa de creación y operación de las aplicaciones de realidad aumentada destinadas a eventos deportivos. Esto incluye la encriptación de datos, la verificación de identidad de usuarios y la realización regular de evaluaciones de seguridad, integrar protocolos de seguridad robustos desde las primeras etapas del desarrollo de aplicaciones para eventos deportivos, asegurando la participación de expertos en seguridad de datos en todo el proceso de desarrollo.

7.2. Establecer directrices y procedimientos detallados para garantizar la protección de datos en la gestión de programas vinculados a actividades deportivas, lo cual requiere entrenar al equipo en métodos seguros de manejo de información y emplear tecnologías de seguridad de vanguardia.

7.3. Realizar revisiones periódicas de seguridad de datos y pruebas de intrusión para identificar posibles debilidades y reducir riesgos en eventos deportivos, otorgando importancia principal a la salvaguardia de los datos personales y confidenciales de los participantes.

7.4. Fomentar la franqueza y la comunicación anticipada con los usuarios sobre las medidas de protección ejecutadas, con el fin de elevar la confiabilidad y el grado de complacencia del usuario en acontecimientos deportivos. Esto puede incluir la publicación de políticas de privacidad detalladas y la provisión de canales de contacto para reportar inquietudes relacionadas con la seguridad de datos.

VIII. REFERENCIAS

Arcos, M., Matute, K., y Fernández, M. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informativos. *Revista Ibérica de Sistemas y Tecnología de información, (S60),* 100–114. https://www.proquest.com/openview/d29c2f8f2bdc11ccd4644ff0be3d8b56/1?pq-origsite=gscholar&cbl=1006393

Aredo, L. (2021). *El phishing y su vulneración a la protección de datos personales en los delitos informáticos*. [Tesis de maestría, Universidad Cesar Vallejo]. Repositorio UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/80920/Aredo_LLA-SD.pdf?sequence=1&isAllowed=y

Bordignon, F. y Tolosa, G. (2007). Recuperación de información: un área de investigación en crecimiento. *Ciencias de la Información, 38*(1-2), 13-24. https://www.redalyc.org/pdf/1814/181414865002.pdf

Carvajal, J., Vega, E. y García, R. (2021). *Diseño de un plan de seguridad informativa para el sistema de información de Colegio Gimnasio Los Pinos.* [Tesis de maestría, Universidad Cooperativa de Colombia]. Repositorio UCC. https://repository.ucc.edu.co/server/api/core/bitstreams/cea12143-38ff-40c1-b716-233316570ba7/content#page=24&zoom=100,148,114

Castillo, P. (2023). L*a ciberdelincuencia en el Perú: Estrategias y retos del Estado*. Defensoría del Pueblo. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Chilcon, M. (2019). *El Cibercrimen en el Perú y su incidencia en la Seguridad Nacional.* [Tesis de maestría, Centro de Altos Estudios Nacionales]. Repositorio CAEN - EPG. https://renati.sunedu.gob.pe/handle/sunedu/393223.

Chipana, Y., Osco, M., Quispe, R., Nieto, G., García, G., y Aliaga, D. (2023). El correo electrónico, como medio de intrusión del Phishing y fraude informático. *Revista de Climatología Edición Especial Ciencias Sociales. 23,* 1139. https://rclimatol.eu/wp-content/uploads/2023/07/Articulo-CS23-Yolanda-maribel.pdf

Cornejo, S. y Sánchez, X. (2023). La protección de datos de carácter personal frente al delito de intercepción ilegal de datos. *Código Científico Revista de Investigación 4(E2*), 984 - 1023. https://revistacodigocientifico.itslosandes.net/index.php/1/article/view/192/401

Cruz, I., Delgado, E., Ponce, B., y Marcillo, J. (2022). Riesgos de seguridad de los datos en la web. *Journal TechInnovation, 1*(2), 43–49. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.43-49

Diaz, C. (2016). *Gestión del cambio en las organizaciones: efectos sobre la actividad y las personas. Revista OpenEdition, 12*(2). https://journals.openedition.org/laboreal/2314

EasyDMARC. (2022). *Phishing Statistics: EasyDMARC Report*. Reporte estadístico. https://assets.easydmarc.com/static/phishing-statistics-2022-07-06.pdf

Egúsquiza, R. (2022). *Realidad aumentada en las competencias digitales de los docentes del área de Electrotecnia Industrial de un ISTP, Lima 2022.* [Tesis de maestría, Universidad Cesar Vallejo]. Repositorio UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/97252/Eg%FAsquiza_CRG-SD.pdf?sequence=4

El Peruano. (2021). *Ciberdelitos en el Perú: se elevan denuncias de fraude informático y suplantación de identidad*. Ciencia y Tecnología. https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad

Elías, N. (2019). *Seguridad informática en el manejo de la información de la Municipalidad de Lujan de Cuyo.* [Tesis de doctorado, Universidad Nacional de Cuyo]. Repositorio UNC. http://videla-rivero.bdigital.uncu.edu.ar/objetos_digitales/15984/elias-fce.pdf.

Febres, R., y Mercado, R. (2020). Satisfacción del usuario y calidad de atención del servicio de medicina interna del Hospital Daniel Alcides Carrión. Huancayo - Perú. *Revista de la Facultad de Medicina Humana, 20*(3), 397-403. https://dx.doi.org/10.25176/rfmh.v20i3.3123.

Flores, M. y Uriarte, G. (2023). *Contribución de los medios tecnológicos en el delito informativo de la suplantación de identidad en las telecomunicaciones, Jaén 2022.* [Tesis de maestría, Universidad Cesar Vallejo]. Repositorio UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/113122/Flores_MMA-Uriarte_PGS-SD.pdf?sequence=1&isAllowed=y#page=7&zoom=100,109,94

Foster, M. (2020). Protección y privacidad de la información. Análisis de riesgo y (des)conocimiento en usuarios de TICs de la ciudad de La Plata [Tesis de maestría, Universidad Nacional de La Plata]. Repositorio de la Universidad Nacional de La Plata. https://sedici.unlp.edu.ar/bitstream/handle/10915/124284/Documento_completo.pdf?sequence=1&isAllowed=y

Garcia, K. y Guevara, C. (2023). *Detención de phishing por envenenamiento del servidor de nombre de dominio para evitar el robo de información en aplicaciones web de microempresas peruanas utilizando aprendizaje de máquina.* [Tesis de maestría,

Universidad Señor de Sipán]. Repositorio USS. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/11546/Garcia%20Gutierrez%20Kevin%20-%20Guevara%20Ramirez%20Cesar.pdf?sequence=1&isAllowed=y

Guanotasig, B. David, S. Zurita, B. y Fuertes, W. (2022). *Implementación de un modelo de desarrollo evolutivo de software que permita detectar y mitigar ataques de ingeniería social utilizando técnicas de Deep Learning.* [Tesis de maestría, Universidad Católica San Pablo]. Repositorio UCSP. https://repositorio.espe.edu.ec/bitstream/21000/37443/3/T-ESPE-058415.pdf.

Guarneros, F. (2022). *Los daños a la ciberseguridad crecen 144% cada año y esto se espera para 2023*. Diario Expansión. https://expansion.mx/tecnologia/2022/12/30/que-espera-2023-en-ciberataques

Hadi, M., Martel, C., Huayta, F., Rojas, C. y Arias, J. (2023). *Metodología de la Investigación*. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C.

Hernández, F., y Martí, Y. (2006). Conocimiento organizacional: la gestión de los recursos y el capital humano. *ACIMED, 14*(1). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352006000100003&lng=es&tlng=es.

Hernández, R., y Mendoza, C. (2018). *Metodología de la investigación las rutas cuantitativa, cualitativa y mixta*. Ciudad de México: Mc Graw Hill Education.

Instituto Nacional de Ciberseguridad [INCIBE]. (2023). *INCIBE gestionó más de 118.000 incidentes de ciberseguridad durante 2022, un 9% más que en 2021*. Sala de Prensa. https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-115000-incidentes-ciberseguridad-durante-2022-9-mas

Kolesnikov, N. (2023). *Más de 50 Estadísticas de Ciberseguridad para el 2023 que debes Conocer: Dónde, Quiénes y Qué se Encuentra en el punto de Mira*. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Laurens, L. (2019). *REALIDAD AUMENTADA: PROPUESTA METODOLÓGICA PARA LA DIDÁCTICA DE DISEÑO INDUSTRIAL EN EL ÁMBITO UNIVERSITARIO. Revista científica electrónica de Educación y Comunicación en la Sociedad del Conocimiento. 19*(2). https://dialnet.unirioja.es/descarga/articulo/7183646.pdf

Lima, C. (2018). *Validación de integridad de un data warehouse a través de un método de watermarking de distorsión controlada Confidencialidad.* [Tesis de maestría, Instituto Nacional de Astrofísica, Óptica y Electrónica]. https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/1723/1/LimaRCD.pdf

Lubeck, L. (2021). *En 2020 se duplicaron las detecciones de ataques de ingeniería social*. ESET. https://www.welivesecurity.com/la-es/2021/01/07/2020-duplico-detecciones-ataques-ingenieria-social/

Medina, J. (2022). *Instalación deportiva convencional como generador de la integración social caso: Sector el progreso Carabayllo, 2019.* [Tesis de maestría, Universidad Cesar Vallejo]. Repositorio UCV. https://hdl.handle.net/20.500.12692/81604

Medina, J., Ábrego, D., y Echeverría, O. (2021). Satisfacción, facilidad de uso y confianza del ciudadano en el gobierno electrónico. *Investigación administrativa, 50*(127), 12704. https://doi.org/10.35426/iav50n127.04.

Mendoza, O. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS, 15*(48), 179-207. https://doi.org/10.35487/rius.v15i48.2021.743

Mercado, W., Guarnieri, G., y Rodriguez, G. (2019). *Análisis y evaluación de procesos de interactividad en entornos virtuales de aprendizaje. Trilogía Ciencia Tecnología Sociedad, 11*(20). pp. 63-99. https://www.redalyc.org/journal/5343/534367764004/html/

Micucci, M. (2023). *Desafíos de la seguridad asociados a la realidad virtual y aumentada*. ESET. https://www.welivesecurity.com/es/otros-temas/seguridad-realidad-virtual-aumentada/

Mina, R. (2023). *Diseñar políticas de seguridad aplicando la Norma ISO 27001:2013 para la protección de los activos de la información en la empresa Robtelcom.* [Tesis de pregrado, Universidad de Guayaquil]. Repositorio UG. https://repositorio.ug.edu.ec/server/api/core/bitstreams/4b796613-8505-40de-a257-81b6e9a828d6/content

Ministerio Público Fiscalía de la Nación [MPFN]. (2023). *¿Qué es la seguridad de la información?* Plataforma digital única del Estado Peruano. https://www.gob.pe/23391-que-es-la-seguridad-de-la-informacion

Miranda, P., Aguayo, V., y Villalva, G. (2017). La planificación estratégica y la gestión de recursos de la información. *Dominio de las Ciencias, 3*(4), 1044-1059. https://dialnet.unirioja.es/servlet/articulo?codigo=6325530

Montece, F., Verdesoto, A., y Vargas, H. (2017). Software de seguridad que permita la confidencialidad de los datos del sistema de gestión y servicios académicos para planteles de educación media (SiViSA). *Dominio de las Ciencias, 3*(3), 91-107. http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.3.jun.91-107

Ochoa, A. (2021). *Desafíos globales del cibercrimen: caso Ecuador periodo 2014 - 2019.* [Tesis de Maestría, Universidad Andina Simón Bolivar]. Repositorio UASB.

https://repositorio.uasb.edu.ec/bitstream/10644/7919/1/T3432-MRI-Ochoa-Desafios.pdf

Ospina, M. y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*(2), 199 – 217. http://www.scielo.org.co/scielo.php?pid=S1794-31082020000200199&script=sci_arttext

Quissanga, F. y Fernandez, R. (2020). Importancia de la seguridad de la información en las empresas de tecnología de información corporativa. *Project Design and Management, 2*(1). https://doi.org/10.35992/pdm.v2i1.431

Reyes, D., Cadena, A, y Rivera, G. (2022). El Sistema de Gestión de Calidad y su relación con la innovación. *Inter disciplina, 10*(26), 217-240. https://doi.org/10.22201/ceiich.24485705e.2021.25.80975.

Ríos, A., Vásquez, Y., y Mendoza, C. (2023). Métodos emergentes de auditoría en integridad de datos en la nube: Una revisión sistemática de las últimas tendencias. *Investigación & Desarrollo, 23*(1), 107-116. https://doi.org/10.23881/idupbo.023.1-8i

Rivas, M. (2016). *Implementación de un sistema de control de acceso para mejorar la seguridad de la información de la empresa SNX S.A.C.* [Tesis de pregrado, Universidad Nacional Mayor de San Marcos]. Repositorio UNMSM. https://core.ac.uk/download/pdf/323348923.pdf)

Rodríguez, G., Jofré, N., Alvarado, Y., Fernández, J. y Guerrero, R. (2020). Realidades alternativas como soporte para el desarrollo sostenible. *XXII Workshop de Investigadores en Ciencias de la Computación*, 313-317. https://sedici.unlp.edu.ar/handle/10915/103730

Rosales, J. (2015). Percepción y Experiencia. *EPISTEME, 35*(2), 21-36. http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S0798-43242015000200002&lng=es&tlng=es.

Salvador, A., y Arquero, R. (2006). Una aproximación al concepto de recuperación de información en el marco de la ciencia de la documentación. *Investigación bibliotecológica, 20*(41), 13-43. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2006000200002&lng=es&tlng=es

Seminario Interdiocesano de Caracas [SIC]. (2023). Ciberseguridad, seguridad de la información y privacidad. *Securmática, 156*. https://revistasic.es/sic156/revistasic156.pdf

Solis, D. (2023). Importancia del cumplimiento normativo en México. Implementación del compliance en las empresas mexicanas. *MLS Law and International Politics*, *2*(1). https://doi.org/10.58747/mlslip.v2i1.2200

Solis, F., Pinto, D., y Solís, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA. *Enfoque UTE, 8*(1), 160-171. https://doi.org/10.29019/enfoqueute.v8n1.123

Sosa, O. (2022). *Phishing como modalidad de delitos informáticos: a propósito de la suplantación y robo a los Beneficiarios del Bono Universal en el Perú.* [Tesis de Posgrado, Universidad Nacional de Piura]. Repositorio UNP. https://repositorio.unp.edu.pe/handle/20.500.12676/3559.

Valencia, J., y Silva, D. (2023). *Gestión de seguridad en riesgos, mantenimiento preventivo y análisis de costos en la empresa RENOVA S.A.C.* [Tesis de pregrado, Universidad Nacional de San Agustín de Arequipa]. *Repositorio de Tesis de la Universidad Nacional*

de San Agustín de Arequipa. https://repositorio.unsa.edu.pe/server/api/core/bitstreams/239a12ee-479c-43a5-8f47-f4f4061c1b72/content

Valles, M., Riascos, J., y Hernandez, E. (2020). Gestión de la identidad digital del investigador y su efecto en el ranking webométrico de una universidad amazónica peruana. *Revista Cubana de Información en Ciencias de la Salud, 31*(2). https://acimed.sld.cu/index.php/acimed/article/view/1406/985

Vargas, B., Inga, L., y Maldonado, M. (2021). Design Thinking aplicado al Diseño de Experiencia de Usuario. *Innovación y Software, 2*(1), 6-19 https://www.redalyc.org/journal/6738/673870838001/html/

Vera, P., Rodriguez, R., y Carrau, M. (2020). Experiencias en el Desarrollo de Aplicaciones Móviles con Interfaces basadas en la Interacción Física. *ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, 9*(1), 1-16. https://www.redalyc.org/journal/5122/512267930002/html/

Verona, S., Perez, Y., Torres, L., Delgado, M., y Yañez, C. (2016). Pruebas de rendimiento a componentes de software utilizando programación orientada a aspectos. *Ingeniería Industrial, 37*(3), 278-285. https://dialnet.unirioja.es/servlet/articulo?codigo=5712242

IX. ANEXOS

Anexo A: Matriz de Consistencia

Título de la investigación	RELACIÓN ENTRE LA SEGURIDAD DE DATOS Y LA IMPLEMENTACIÓN EXITOSA DE APLICACIONES DE REALIDAD AUMENTADA EN EVENTOS DEPORTIVOS, 2023						
Problema	**Objetivo**	**Hipótesis**	**Variable**	**Dimensión**	**Indicador**	**Ítems**	**Metodología**
Problema general ¿Cómo se relaciona la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023? **Problemas específicos** ¿Cómo se relaciona la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023? ¿Cómo se relaciona la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023? ¿Cómo se relaciona la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023?	**Objetivo general** Determinar cómo se relaciona la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023 **Objetivos específicos** Identificar como se relaciona la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023 Determinar la relación entre la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023 Determinar la relación entre la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023	**Hipótesis general** Existe una relación significativa entre la seguridad de datos y la implementación exitosa de aplicaciones de realidad aumentada en eventos deportivos, 2023 **Hipótesis especificas** Existe una relación significativa entre la seguridad de datos y el desarrollo de aplicaciones en eventos deportivos, 2023 Existe una relación significativa entre la seguridad de datos y la implementación exitosa gestión de planes en eventos deportivos, 2023 Existe una relación significativa entre la seguridad de datos y la satisfacción del usuario en eventos deportivos, 2023	Seguridad de Datos	Protección de Datos	Encriptación de Datos	1-8	Diseño: no experimental Tipo: descriptivo Nivel: correlacional
					Control de Acceso		
					Respaldo de Datos		
					Recuperación de Datos		
				Integridad de Datos	Verificación de Integridad	9-12	
					Validación de Datos		
				Confidencialidad	Restricciones de Acceso	13-16	
					Gestión de Identidad y Acceso		
				Cumplimiento Normativo	Políticas de Privacidad	17-20	
					Ajustes a Estándares de Seguridad		
			Implementación Exitosa de Aplicaciones de Realidad Aumentada	Desarrollo de Aplicaciones	Experiencia de Usuario	1-6	
					Interactividad		
					Rendimiento		
				Gestión de Planes	Planificación Eficiente	7-12	
					Gestión de Recursos		
					Control de Calidad		
				Satisfacción del Usuario	Facilidad de Uso	13-16	
					Personalización de Experiencia		

Anexo B: Instrumento de recolección de datos

Al completar el instrumento con escala de Likert, por favor, lee cada pregunta con atención para comprenderla completamente antes de seleccionar tu respuesta en la escala. Utiliza la gama de opciones, desde "Totalmente en desacuerdo" hasta "Totalmente de acuerdo", para expresar con precisión tu opinión. Sé honesto y sincero al responder, basando tus elecciones en tus experiencias y percepciones personales. Evita respuestas neutras siempre que sea posible y, por favor, no omitas ninguna pregunta, incluso si algunas te resultan desafiantes. Tu participación es esencial para obtener datos significativos y apreciamos sinceramente tu colaboración en este proceso. ¡Gracias!

ITEMS		Totalmente en desacuerdo	En Desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
Variable Independiente: Seguridad de Datos						
DIMENSION: Protección de Datos						
1	Confías en la encriptación de datos implementada en la empresa para salvaguardar la privacidad y seguridad de la información confidencial de los clientes y empleados					
2	La encriptación de datos contribuye de manera significativa a la integridad y confidencialidad de la información que se maneja en el entorno laboral					
3	Considero que el sistema de Control de Acceso garantiza adecuadamente la seguridad de los datos personales.					
4	Confias en la capacidad del sistema de control de acceso para salvaguardar la privacidad y confidencialidad de los datos que se maneja					
5	Consideras que la empresa proporciona los recursos necesarios para llevar a cabo un respaldo de datos adecuado, asegurando así la integridad y disponibilidad de la información					

6	Crees que la política de respaldo de datos de la empresa es fácil de entender y seguir, facilitando la correcta ejecución de los procedimientos de protección de datos					
7	Confías en la eficacia de los procesos de recuperación de datos implementados por la empresa para garantizar la protección y disponibilidad de la información crítica					
8	Crees que la capacitación proporcionada sobre los procedimientos de recuperación de datos es suficiente para que todos los empleados comprendan y puedan seguir correctamente los protocolos establecidos					
DIMENSION: Integridad de Datos						
9	Consideras que la empresa brinda suficientes recursos y herramientas para llevar a cabo eficientemente las verificaciones de integridad de datos					
10	Crees que la capacitación y formación proporcionada por la empresa en relación con la verificación de integridad de datos es adecuada para mejorar las habilidades en este ámbito					
11	Crees que las políticas de validación de datos de la empresa son efectivas para garantizar la integridad y fiabilidad de la información que utilizas en tus tareas laborales					
12	Los procesos de validación de datos han contribuido significativamente a la reducción de errores y la mejora de la calidad de la información con la que se trabaja cotidianamente					
DIMENSION: Confidencialidad						
13	Consideras que las medidas de seguridad implementadas en la empresa son efectivas en cuanto a restringir el acceso no autorizado a información confidencial					
14	Crees que las restricciones de acceso son suficientes para proteger la privacidad y confidencialidad de los datos con los que se trabaja					
15	Confías que la efectividad de las medidas de Gestión de Identidad y Acceso implementadas en la empresa para mantener la confidencialidad de los datos					

16	Consideras que las políticas y procedimientos de Gestión de Identidad y Acceso establecidos en la organización son fundamentales para preservar la confidencialidad de la información					
DIMENSION: Cumplimiento Normativo						
17	Crees que las políticas de privacidad de la empresa cumplen con los estándares normativos y legales establecidos					
18	Consideras que las políticas de privacidad de la empresa son transparentes y comprensibles para todos los empleados					
19	Consideras que los ajustes realizados a los estándares de seguridad garantizan el cumplimiento normativo en mi área de trabajo					
20	Crees que los ajustes a los estándares de seguridad son fácilmente accesibles y comprensibles para todos los empleados, facilitando el cumplimiento normativo en sus tareas diarias					

ITEMS		Totalmente en desacuerdo	En Desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
Variable Dependiente: Implementación Exitosa de Aplicaciones de Realidad Aumentada						
DIMENSION: Desarrollo de Aplicaciones						
1	Crees que la navegación dentro de las aplicaciones de la empresa es intuitiva y fácil de comprender, facilitando así la experiencia del usuario					
2	Consideras que las aplicaciones desarrolladas por la empresa responden de manera efectiva a las necesidades específicas del usuario					
3	Consideras que la interactividad de las aplicaciones utilizadas en la empresa facilita y mejora la eficiencia en la realización de tareas diarias					
4	Consideras que la capacitación proporcionada para el uso de las aplicaciones desarrolladas internamente ha sido efectiva en mejorar la comprensión y aprovechamiento de las funciones interactivas disponibles					
5	Consideras que la contribución del rendimiento de las aplicaciones es eficaz en el logro de los objetivos y metas establecidos para el desarrollo de eventos					
6	Consideras que el rendimiento de las aplicaciones ha contribuido a la reducción de errores y fallos durante el proceso de desarrollo y implementación					
DIMENSION: Gestión de Planes						
7	Consideras que la empresa tiene un proceso eficiente para la planificación de actividades en el ámbito de la Gestión de Planes					
8	Consideras que la empresa brinda los recursos necesarios para implementar de manera efectiva los planes estratégicos					

9	Consideras que la empresa ha demostrado eficacia en la asignación de recursos para alcanzar los objetivos planificados					
10	La empresa utiliza los recursos disponibles para responder a cambios inesperados o situaciones de crisis en el entorno empresarial					
11	Consideras que la empresa tiene un sistema efectivo de Control de Calidad en la gestión de planes					
12	La empresa demuestra un compromiso sólido con el Control de Calidad en la ejecución de los planes estratégicos					
DIMENSION: Satisfacción del Usuario						
13	Considera que la accesibilidad de las plataformas y aplicaciones es un factor positivo para la eficiencia					
14	Confía en la simplicidad y claridad de las herramientas					
15	Crees que la personalización de las políticas de desarrollo profesional se alinea con las metas y expectativas					
16	Consideras que la personalización de la comunicación interna, adaptada a las necesidades y preferencias, contribuye a la satisfacción del usuario					

Anexo C: Validación de juicio de expertos

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
ESCUELA UNIVERSITARIA DE POSGRADO

Ficha de Validación
(Juicio de Experto)

I. DATOS GENERALES

1.1. Apellidos y Nombres: Anicama Flores Luis Miguel
1.2. Grado académico: Doctor en Ingeniería
1.3. Cargo e Institución donde labora: Docente de EUPG-UNFV
1.4. Nombre del instrumento motivo de evaluación: Cuestionario
1.5. Título de la Investigación: "RELACIÓN ENTRE LA SEGURIDAD DE DATOS Y LA IMPLEMENTACIÓN EXITOSA DE APLICACIONES DE REALIDAD AUMENTADA EN EVENTOS DEPORTIVOS, 2023"
1.6. Autor(a) del Instrumento: Minaya Isique, Jesus Francisco

II. ASPECTOS DE VALIDACIÓN

Criterios	Indicadores	Deficiente 0-20%	Baja 21-50%	Regular 51-70%	Buena 71%-90%	Muy buena 91%-100%
1. Claridad	Está formulado con lenguaje apropiado.				90%	
2. Objetividad	Está expresado en conductas observables				90%	
3. Actualidad	Adecuado al avance de la especialidad				90%	
4. Organización	Existe una organización lógica				90%	
5. Suficiencia	Comprende los aspectos en cantidad y calidad.				90%	
6. Intencionalidad	Adecuado para valorar la investigación				90%	
7. Consistencia	Basado en aspectos teóricos científicos.				90%	
8. Coherencia	Entre lo descrito en dimensiones e indicadores				90%	
9. Metodología	La formulación responde a la investigación				90%	
10. Pertinencia	Es útil y adecuado para la investigación				90%	

III. PROMEDIO DE VALORACIÓN: 90%

a) Deficiente [ ] **b) Baja** [ ] **c) Regular** [ ] **d) Buena** [X] **e) Muy Buena** [ ]

IV. OPINIÓN DE APLICABILIDAD: El Instrumento es aplicable en la investigación.

Lima, Febrero del 2025

MG. ANICAMA FLORES LUIS MIGUEL
Código ORCID: 0000-0002-0494-3212

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
ESCUELA UNIVERSITARIA DE POSGRADO

Ficha de Validación
(Juicio de Experto)

I. DATOS GENERALES

1.1. Apellidos y Nombres: Bazán Ramírez Wilfredo

1.2. Grado académico: Magister en Ingeniería

1.3. Cargo e Institución donde labora: Docente de EUPG-UNFV

1.4. Nombre del instrumento motivo de evaluación: Cuestionario

1.5. Título de la Investigación: "RELACIÓN ENTRE LA SEGURIDAD DE DATOS Y LA IMPLEMENTACIÓN EXITOSA DE APLICACIONES DE REALIDAD AUMENTADA EN EVENTOS DEPORTIVOS, 2023"

1.6. Autor(a) del Instrumento: Minaya Isique, Jesus Francisco

II. ASPECTOS DE VALIDACIÓN

Criterios	Indicadores	Deficiente 0-20%	Baja 21-50%	Regular 51-70%	Buena 71%-90%	Muy buena 91%-100%
1. Claridad	Está formulado con lenguaje apropiado.				90%	
2. Objetividad	Está expresado en conductas observables				90%	
3. Actualidad	Adecuado al avance de la especialidad				90%	
4. Organización	Existe una organización lógica				90%	
5. Suficiencia	Comprende los aspectos en cantidad y calidad.				90%	
6. Intencionalidad	Adecuado para valorar la investigación				90%	
7. Consistencia	Basado en aspectos teóricos científicos.				90%	
8. Coherencia	Entre lo descrito en dimensiones e indicadores				90%	
9. Metodología	La formulación responde a la investigación				90%	
10. Pertinencia	Es útil y adecuado para la investigación				90%	

III. PROMEDIO DE VALORACIÓN: 90%

a) Deficiente [ ] **b) Baja** [ ] **c) Regular** [ ] **d) Buena** [X] **e) Muy Buena** [ ]

IV. OPINIÓN DE APLICABILIDAD: El Instrumento es aplicable en la investigación

Lima, Febrero del 2025

DR. WILFREDO BAZAN RAMIREZ
Código ORCID: 0000-0002-2685-8254

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
ESCUELA UNIVERSITARIA DE POSGRADO

Ficha de Validación
(Juicio de Experto)

I. DATOS GENERALES

1.1. Apellidos y Nombres: Zuñiga Diaz, Walter Benjamin

1.2. Grado académico: Magister en Ingeniería

1.3. Cargo e Institución donde labora: Docente de EUPG-UNFV

1.4. Nombre del instrumento motivo de evaluación: Cuestionario

1.5. Título de la Investigación: "RELACIÓN ENTRE LA SEGURIDAD DE DATOS Y LA IMPLEMENTACIÓN EXITOSA DE APLICACIONES DE REALIDAD AUMENTADA EN EVENTOS DEPORTIVOS, 2023"

1.6. Autor(a) del Instrumento: Minaya Isique, Jesus Francisco

II. ASPECTOS DE VALIDACIÓN

Criterios	Indicadores	Deficiente 0-20%	Baja 21-50%	Regular 51-70%	Buena 71%-90%	Muy buena 91%-100%
1. Claridad	Está formulado con lenguaje apropiado.				90%	
2. Objetividad	Está expresado en conductas observables				90%	
3. Actualidad	Adecuado al avance de la especialidad				90%	
4. Organización	Existe una organización lógica				90%	
5. Suficiencia	Comprende los aspectos en cantidad y calidad.				90%	
6. Intencionalidad	Adecuado para valorar la investigación				90%	
7. Consistencia	Basado en aspectos teóricos científicos.				90%	
8. Coherencia	Entre lo descrito en dimensiones e indicadores				90%	
9. Metodología	La formulación responde a la investigación				90%	
10. Pertinencia	Es útil y adecuado para la investigación				90%	

III. PROMEDIO DE VALORACIÓN: 90%

a) Deficiente [ ] **b) Baja** [ ] **c) Regular** [ ] **d) Buena** [X] **e) Muy Buena** [ ]

IV. OPINIÓN DE APLICABILIDAD: El Instrumento es aplicable en la investigación.

Lima, Febrero del 2025

MG. WALTER BENJAMÍN ZÚÑIGA DÍAZ
código ORCID: 0000- 0001-6860-7456