Modelo para la integración de Seguridad de la Información en la Gestión de Proyectos de TI

Juan David García Carrillo

Mary Paz Domínguez Palencia

Gustavo Adolfo Paredes González

Universidad EAN

Facultad de Ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá D.C., Colombia

31/marzo/2026

Modelo para la integración de Seguridad de la Información en la Gestión de Proyectos de TI

Juan David García Carrillo

Mary Paz Domínguez Palencia

Gustavo Adolfo Paredes González

Trabajo de grado presentado como requisito para optar al título de:

Magister en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Director (a):

Luis Armando Cobo Campo

Modalidad:

Trabajo Dirigido

Universidad EAN

Facultad de Ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá D.C., Colombia

31/marzo/2026

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Bogotá D.C, día/mes/año

“El conocimiento no es el destino alcanzado, sino la herramienta con la que hemos decidido esculpir nuestra propia libertad.”

A nosotros, arquitectos de nuestro propio camino. Esta obra representa la culminación de un proceso académico y la hazaña de haber sostenido el equilibrio cuando el tiempo parecía insuficiente y el horizonte lejano.

Nos dedicamos esta meta por la disciplina inquebrantable, por la madurez hallada en la incertidumbre y por la convicción de que el crecimiento profesional es, ante todo, un acto de voluntad personal y trascendencia del ser.

A nuestras familias, quienes fueron testigos, soporte y cómplices silenciosos en cada etapa de este proyecto. Hoy celebramos la libertad que otorga el conocimiento y la profunda satisfacción del deber cumplido con nosotros mismos.

Agradecimientos

Expresamos nuestra más profunda gratitud a **OSP INTERNATIONAL CALA S.A.S.**, organización líder en el sector de las Tecnologías de la Información y las Comunicaciones, por abrir sus puertas y permitir la realización de esta consultoría. Su disposición para el intercambio de conocimientos y su enfoque en la generación de valor agregado fueron pilares fundamentales para el éxito de este trabajo de grado.

Resumen

La creciente dependencia de sistemas de información y la aceleración de la transformación digital han posicionado la seguridad de la información como factor estratégico en la gestión de proyectos TI. No obstante, en muchas organizaciones su integración sigue siendo parcial y reactiva. En este contexto, el trabajo tuvo como objetivo diseñar un modelo para integrar la seguridad de la información en la gestión de proyectos TI en OSP INTERNATIONAL CALA S.A.S., orientado a fortalecer la trazabilidad, el cumplimiento normativo y la continuidad operativa.

La investigación se desarrolló bajo un enfoque mixto, con diseño no experimental, descriptivo y correlacional, mediante estudio de caso único. Se emplearon encuestas tipo Likert, entrevistas semiestructuradas, revisión documental, observación no participante y bitácoras de campo, permitiendo la triangulación de los hallazgos. Los resultados evidenciaron capacidades técnicas relevantes, pero también brechas en la estandarización de controles, subregistro de incidentes, ausencia de métricas y débil articulación entre niveles estratégico y operativo.

Como respuesta, se propuso un modelo basado en gobernanza, gestión metodológica y operación técnica, articulado con estándares internacionales. Se concluye que la organización requiere consolidar y formalizar sus capacidades existentes, para integrar la seguridad como un criterio transversal, verificable y sostenible en la gestión de proyectos TI.

Palabras clave: seguridad de la información, gestión de proyectos, gobernanza de TI, gestión de riesgos, DevSecOps, modelos de integración.

Abstract

The increasing reliance on information systems and the acceleration of digital transformation have positioned information security as a strategic factor in IT project management. However, in many organizations, its integration remains partial and reactive. In this context, this study aimed to design a model to integrate information security into IT project management at OSP INTERNATIONAL CALA S.A.S., oriented toward strengthening traceability, regulatory compliance, and operational continuity.

The research was conducted under a mixed-methods approach, with a non-experimental, descriptive, and correlational design, through a single case study. Data collection methods included Likert-scale surveys, semi-structured interviews, document review, non-participant observation and field logs, enabling the triangulation of findings.

The results revealed relevant technical capabilities, but also gaps in control standardization, incident underreporting, lack of systematic metrics, and weak alignment between strategic and operational levels. In response, a model based on governance, methodological management, and technical operation was proposed, aligned with international standards. It is concluded that the organization needs to consolidate and formalize its existing capabilities to integrate security as a transversal, verifiable, and sustainable criterion in IT project management.

Keywords: information security, project management, IT governance, risk management, DevSecOps, integration models.

Tabla de Contenido

Pág.

Lista de Figuras

Pág.

Lista de Tablas

Introducción

La gestión de proyectos ha evolucionado de un enfoque operativo a una disciplina estratégica enfocada en la competitividad empresarial. Según el Project Management Institute (PMI) (2013), la gestión de proyectos permite alinear iniciativas con objetivos organizacionales. En este contexto, la digitalización ha impulsado metodologías híbridas que mejoran la eficiencia y adaptabilidad (Lee, 2018), así como la adopción de tecnologías como inteligencia artificial y computación en la nube, que exigen una cultura organizacional basada en la innovación y el aprendizaje continuo (Hasan, Alzoud & Al Jasime, 2025). No obstante, estos avances han introducido nuevos desafíos en la seguridad de la información.

La transformación digital ha aumentado la exposición a ciberataques y vulnerabilidades (Siebel, 2020). Los ataques cibernéticos han aumentado en frecuencia y complejidad afectando la continuidad operativa de las organizaciones (Ali & Zain, 2021). En América Latina, las organizaciones enfrentan un promedio de 2.569 ciberataques semanales, cifra aproximadamente 40% superior al promedio global (CCIT, 2024 & Policía Nacional, 2024). En Colombia, se registraron más de 70.000 incidentes cibernéticos en 2024, con un incremento sostenido frente a los 59.000 reportados en 2023 (Centro Cibernético Policial, 2024). Entre las principales amenazas se encuentran el ransomware, las vulnerabilidades de software y los ataques de denegación de servicio distribuido (DDoS), que pueden generar pérdidas económicas y afectar la reputación corporativa (Maimon & Liao, 2020).

La gestión de proyectos TI (Tecnologías de la Información) requiere un enfoque integral que considere la seguridad de la información en todas las fases del ciclo de vida del proyecto (Molina & Chacón, 2022). Sin embargo, la seguridad sigue tratándose de

manera aislada, sin alineación efectiva con los procesos de gestión de proyectos y sin garantizar cumplimiento normativo de marcos como ISO/IEC 27001, Reglamento General de Protección de Datos (GDPR) y estándares del Instituto Nacional de Estándares y Tecnología (NIST) (Calder & Watkins, 2017). En Colombia, estudios en pymes del sector TIC (Tecnologías de la Información y las Comunicaciones) evidencian brechas entre la importancia reconocida de la seguridad y su implementación real (Buriticá & López, 2018), mientras que en América Latina el 30% de las organizaciones ha sufrido incidentes de ciberseguridad (ESET, 2024).

Este es el caso de OSP INTERNATIONAL CALA S.A.S, una empresa con 57 empleados con presencia en 4 ciudades de Colombia, que a pesar de contar con certificaciones como ISO 9001:2008, ISO 9001:2015 e ITMARK, carece de un proceso formal de seguridad de la información en la gestión de proyectos. Según entrevista con el líder de desarrollo, se evidencia que la empresa enfrenta desafíos en la gestión de proyectos, incumplimientos en plazos y una segmentación ineficiente de responsabilidades, dado que un solo ingeniero de soporte asume múltiples funciones. Esta sobrecarga incrementa los riesgos de seguridad y afecta la calidad de los proyectos.

La problemática se acentúa debido a la ausencia de indicadores de gestión de proyectos a nivel organizacional. Actualmente, la organización únicamente cuenta con métricas operativas, tales como número de bugs, incidentes, solicitudes de soporte y mantenimiento. Adicionalmente, se ha evidenciado la materialización de un riesgo crítico, reflejado en la pérdida aproximada del 70% de la información del área de calidad, asociada a fallas en los controles de respaldo, verificación y restauración de la información (backup/restore).

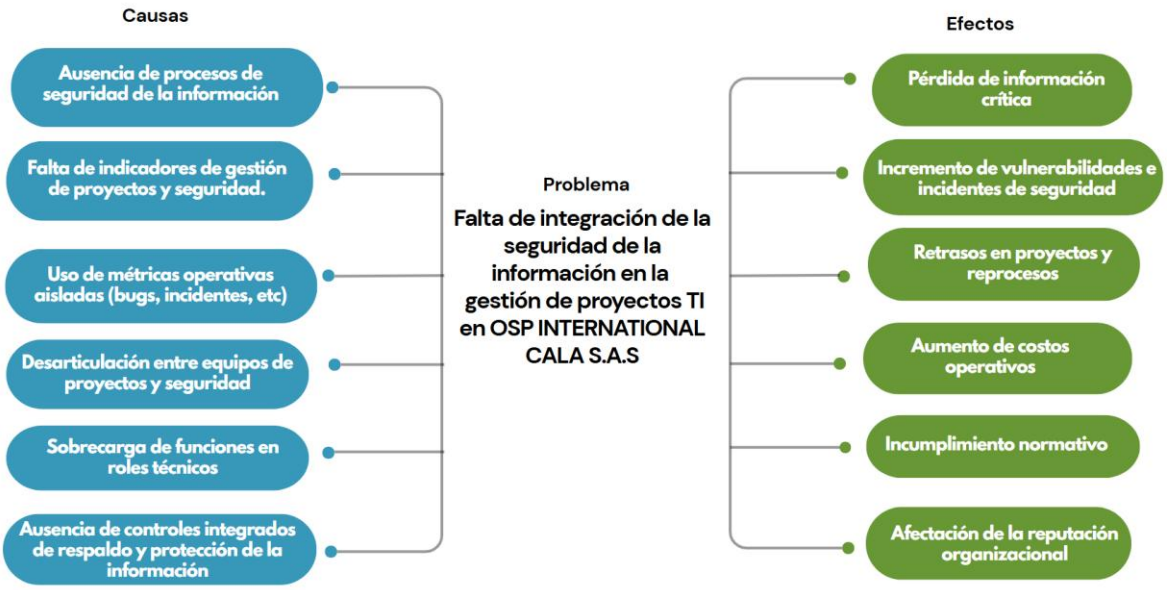
Las consecuencias de esta falta de integración se evidencian en impactos financieros, operativos y reputacionales. El costo promedio de una brecha de datos en América

Latina alcanzó los 2.76 millones de dólares en 2024 (IBM Security, 2024), mientras que las pérdidas económicas por ciberataques en empresas colombianas pueden oscilar entre 120 millones y 5.000 millones de pesos según el tamaño de la organización (CCIT, 2024). Según Giordano (2020), las brechas de seguridad afectan negativamente el valor para los accionistas y la percepción pública, mientras que la falta de estrategias de prevención y respuesta puede derivar en sanciones regulatorias, pérdidas económicas y deterioro de la confianza de clientes y socios comerciales.

En el contexto regional, algunos casos evidencian la magnitud del impacto: Air-e, empresa distribuidora de energía en Colombia, sufrió un ataque de ransomware en septiembre de 2024 que paralizó sus sistemas operativos, causó retrasos en atención al cliente y detuvo la gestión financiera y logística (WeLiveSecurity, 2024). En Perú, Interbank experimentó un incidente donde un atacante accedió a datos sensibles de más de 3 millones de clientes mediante ingeniería social, exigiendo un rescate de 4 millones de dólares (WeLiveSecurity, 2024).

Figura 1.

Representación gráfica del problema



Nota. Elaboración propia con base en el diagnóstico organizacional de OSP INTERNATIONAL CALA S.A.S.

La adopción de enfoques integrados que articulen la gestión de proyectos con la seguridad de la información se convierte en una necesidad estratégica pueden contribuir a reducir los riesgos asociados y garantizar la continuidad operativa. De esta manera, se propone la siguiente pregunta de investigación ¿Qué estrategias permiten integrar la seguridad de la información en la gestión de proyectos TI para la empresa OSP INTERNATIONAL CALA S.A.S, asegurando la continuidad operativa y el cumplimiento normativo en cada fase del ciclo de vida del proyecto?

El presente trabajo se estructura en apartados que permiten la comprensión progresiva del estudio. Se inicia con los objetivos y la justificación, que delimitan el propósito y la relevancia de la investigación. Posteriormente, se desarrollan los marcos institucional, conceptual y legal, como sustento teórico y normativo del análisis. A continuación, se presenta el diseño metodológico, seguido del diagnóstico organizacional y los resultados de la propuesta de solución. Finalmente, se exponen las conclusiones y recomendaciones, complementadas con las referencias y anexos que lo respaldan.

Objetivos

Objetivo general

Diseñar un modelo para la integración de la seguridad de la información en la gestión de proyectos TI para la empresa OSP INTERNATIONAL CALA S.A.S, durante el periodo 2025-2026.

Objetivos específicos

Planificar (P)

1. Analizar el impacto de la falta de integración de la seguridad de la información en la gestión de proyectos TI en OSP INTERNATIONAL CALA S.A.S, identificando las principales brechas, desafíos y riesgos operativos.
2. Evaluar el grado de adopción y efectividad de metodologías de gestión de proyectos (ágiles, híbridas y/o tradicionales) en la mitigación de riesgos de seguridad de la información dentro de la empresa.
3. Identificar marcos de gobernanza y herramientas de gestión que faciliten la alineación entre los objetivos estratégicos de la organización y la gestión operativa de TI, asegurando la protección de la información.

Hacer (H)

4. Diseñar estrategias para la incorporación de controles de seguridad de la información en cada fase del ciclo de vida de los proyectos TI que garanticen su trazabilidad y cumplimiento normativo en la empresa.
5. Proponer y validar mediante la técnica Delphi un modelo de integración de seguridad de la información en la gestión de proyectos TI para la empresa OSP INTERNATIONAL CALA S.A.S.

Verificar (V)

Nota: La fase de verificación se encuentra incorporada en el OE5 mediante el proceso de validación con expertos (técnica Delphi).

Actuar (A)

Nota: La fase de actuar se deriva de los resultados de la validación del modelo propuesto, orientando su mejora y aplicabilidad en la organización.

Justificación

En OSP INTERNATIONAL CALA S.A.S la gestión de proyectos TI presenta relevancia estratégica, dado que la competitividad de la organización depende de sus sistemas tecnológicos. En este contexto, la empresa busca optimizar la ejecución de sus proyectos tecnológicos para mantenerse a la vanguardia digital. Sin embargo, en la auditoría TI realizada en 2023 se identificaron múltiples deficiencias en la gestión de la seguridad de la información (SI), evidenciando vulnerabilidades críticas que comprometen la confidencialidad, integridad y disponibilidad de los datos. A pesar de estos hallazgos, solo se aplican medidas correctivas ante exigencias del cliente y únicamente para cumplir lo solicitado

Las principales novedades identificadas comprenden la gestión deficiente de accesos privilegiados, incrementando el riesgo de alteración, eliminación o fuga de información, así como la ausencia de controles en la gestión de cambios afecta la integridad y continuidad de los procesos. Asimismo, la falta de procedimientos para la gestión de copias de respaldo limita la capacidad de recuperación ante incidentes. De igual forma, el incumplimiento en la protección de datos personales expone a la organización a riesgos regulatorios y reputacionales, mientras que la desalineación entre la estrategia TI y los objetivos de negocio restringe la capacidad de innovación y crecimiento institucional.

Ante la situación descrita, se requiere el diseño de un modelo de integración de seguridad de la información en la gestión de proyectos TI, que garantice la aplicación de controles de seguridad en cada fase del ciclo de vida. Con ello, se pretende fortalecer la protección de activos digitales, reducir riesgos y garantizar la continuidad operativa frente a incidentes tecnológicos. En este sentido, se proyecta una reducción estimada del 30% en los costos asociados a reprocesos, incidentes y fallos de seguridad en proyectos TI

durante el primer año de implementación del modelo. Al respecto, IBM Security (2024) demuestra que organizaciones con gestión proactiva de seguridad reducen en promedio un 33% el costo de las brechas frente a aquellas con enfoque reactivo, reforzando la pertinencia del modelo propuesto.

La relevancia del estudio se amplía al sector TIC colombiano, donde según MinTIC y la OEA (2024), las PyMEs tecnológicas presentan los mayores rezagos en ciberseguridad: mientras el 67,2% de las grandes empresas cuenta con estrategias de protección, solo el 37,1% de las PyMEs las ha implementado. El modelo es transferible a organizaciones similares, en un contexto donde Colombia registró más de 70.000 incidentes cibernéticos en 2024 y el sector TIC genera anualmente más de 15.000 empleos que requieren competencias en seguridad de la información (MinTIC, 2024).

Este estudio contribuirá al fortalecimiento de la gobernanza y la seguridad de la información, promoviendo la articulación de la gestión de proyectos y el cumplimiento normativo con una asignación más eficiente de recursos. Adicionalmente, impulsa el desarrollo de competencias en ciberseguridad, donde el 48% de las vacantes TI en Latinoamérica no se cubren por falta de talento especializado (Netser Group, 2024). La integración de metodologías de proyectos con estándares de seguridad permitirá adoptar un enfoque preventivo que favorezca la resiliencia organizacional ante los desafíos tecnológicos actuales.

Viabilidad del proyecto

En la siguiente tabla se detalla la factibilidad de cada uno los criterios del proyecto

Tabla 1.

Criterios de factibilidad del proyecto.

Criterio	Factibilidad (siendo 1 menor y 5 mayor)
Acceso a la información.	5
Apoyo e interés de la alta dirección.	5

Disponibilidad de recursos requeridos.	4
Probabilidad de avance en el tiempo establecido.	4
Tamaño de la empresa para soportar y desarrollar el plan de mejora a proponer.	4
Disponibilidad de tecnología.	4,5
Impacto ambiental.	4,5
Promedio	**4,4**

Nota. Elaboración propia.

El análisis de factibilidad del proyecto refleja una viabilidad moderada, con un promedio de 4,4, lo que indica condiciones favorables para su ejecución, aunque con algunos desafíos que deben ser gestionados. Uno de los factores positivos de alta relevancia es el acceso a la información y el apoyo de la alta dirección, ambos con una calificación de 5. Contar con el respaldo de los directivos facilita la disponibilidad de datos clave y asegura el compromiso organizacional para la implementación del modelo de integración de seguridad de la información.

Asimismo, la disponibilidad de tecnología, con una puntuación de 4,5, es un punto fuerte que minimiza riesgos operativos. La empresa cuenta con la infraestructura tecnológica y los insumos necesarios, lo que permite avanzar sin restricciones en términos de hardware, software y herramientas especializadas. Asimismo, el impacto ambiental, con el mismo puntaje representa un aspecto favorable, ya que se trata de un proyecto enfocado en procesos digitales y optimización interna, sin generación directa de residuos o afectaciones al entorno físico.

Sin embargo, la probabilidad de avance en el tiempo establecido, con una puntuación de 4, sugiere que podrían presentarse retrasos debido a los tiempos de gestión internos. El tamaño de la empresa y disponibilidad de recursos, con un puntaje de 4, confirma que la organización tiene la capacidad para desarrollar el modelo propuesto, aunque su éxito dependerá de una adecuada asignación de recursos humanos dada la situación financiera de la empresa y su enfoque en reducción de costos.

Marco Institucional

OSP INTERNATIONAL CALA S.A.S. es una empresa dedicada a la generación de valor agregado, con énfasis en tecnologías de la información y las comunicaciones aplicadas al mejoramiento de procesos y servicios. La compañía inicio sus labores en Colombia en el año 2002, con aportes de capital mexicano, americano y colombiano, con el objetivo de desarrollar e integrar productos y servicios de tecnología para el mercado de Latinoamérica. Desde su formación la compañía ha centrado sus esfuerzos en áreas de Investigación y Desarrollo, con alianzas estratégicas como la co-investigación con la Universidad de Antioquia.

La empresa ha desarrollado soluciones tecnológicas de verificación, inventario y diagnóstico de redes e infraestructura, soluciones de software para automatización de procesos, con reconocimiento en Telcos de Latinoamérica (más de 15 operadores en 8 países) y presencia comercial en la mayoría de países de la región. Entre sus principales clientes se encuentran UNE, ETB, Emcali, ICETEX, Ministerio TIC, Ministerio de Cultura, Servicios Postales Nacionales, Empresas Públicas de Cundinamarca, Grupo Energía Bogotá, Universidad Católica de Colombia y Fondo Nacional del Ahorro. Además, cuentan con la certificación de Gestión de Calidad ISO 9001 versión 2015 y están afiliados a FEDESOFT (Colombia).

Referentes estratégicos

Misión: OSP INTERNATIONAL CALA S.A.S provee soluciones y servicios en la industria de tecnologías de la información y las comunicaciones, con énfasis en innovación, satisfaciendo las necesidades y expectativas de sus clientes. Con un equipo humano competente, a través de procesos eficaces y alianzas estratégicas, desarrollando soluciones de alto valor agregado y estándares de calidad.

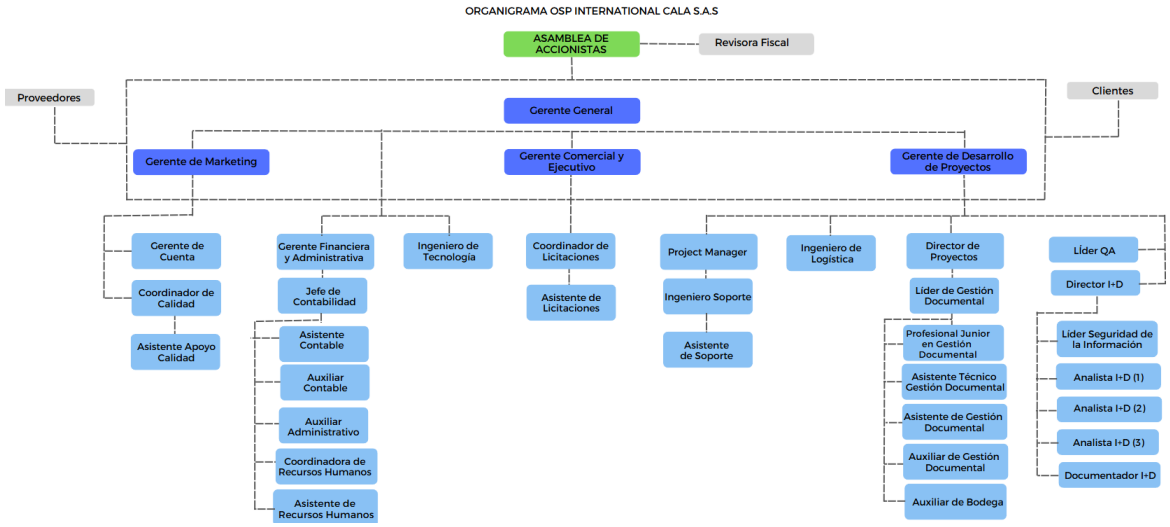
Visión: OSP INTERNATIONAL CALA S.A.S será una organización líder del mercado, con alto reconocimiento por sus soluciones y servicios en la industria TIC. Será promotor de la investigación y desarrollo en la industria a través de alianzas tecnológicas, generará valor para sus grupos de interés, con responsabilidad social.

Estructura organizacional

La estructura organizacional se encuentra diseñada para garantizar la eficiencia operativa, la innovación y la excelencia en el servicio y productos. Se cuenta con un equipo multidisciplinario de 57 personas altamente capacitadas que trabaja de manera coordinada para ofrecer soluciones tecnológicas de alto impacto en transformación digital, consultoría en TI, automatización y desarrollo de software.

Figura 2.

Organigrama OSP INTERNATIONAL CALA S.A.S.



Nota. Adaptado de Planeación estratégica – Documento 07 versión 29, por OSP INTERNATIONAL CALA S.A.S. (2019). Sistema de Gestión de Calidad. [Documento interno PE-D-07-V29].

Relación entre las características institucionales y la problemática

Las características institucionales de OSP INTERNATIONAL CALA S.A.S amplifican la problemática de seguridad identificada en la auditoría TI de 2023. Su tamaño limita la posibilidad de contar con roles exclusivos de seguridad de la información, concentrando funciones en personal técnico que simultáneamente atiende desarrollo, soporte e infraestructura. La orientación a múltiples líneas de servicio incrementa la complejidad en la gestión de riesgos, al requerir controles diferenciados según la naturaleza de cada proyecto y las exigencias normativas de clientes del sector público y privado.

Adicionalmente, la reducción de ingresos del 27% en 2023 ha restringido la inversión en herramientas de seguridad y programas de capacitación. La ausencia de una estructura formal de seguridad, sumada a la desarticulación entre equipos y la falta de indicadores, se materializa en hallazgos como: administración inadecuada de accesos privilegiados, ausencia de controles en gestión de cambios, deficiencias en copias de respaldo y brechas en protección de datos personales.

Productos y/o servicios ofertados

OSP INTERNATIONAL CALA S.A.S ofrece soluciones en transformación digital, consultoría en TI, automatización y desarrollo de software, y servicios diseñados para potenciar la eficiencia, la seguridad y la innovación en cada proyecto:

- **Transformación digital:** soluciones en gestión documental, seguridad de la información y carpeta ciudadana, abarcando todas las etapas del ciclo de gestión de la información. Se especializa en la administración eficiente de grandes volúmenes de información con altos estándares de seguridad, destacando los servicios de gestión documental y custodia en entornos corporativos y gubernamentales.

- **Consultoría / servicios:** amplio conocimiento en tecnologías de la información, redes de telecomunicaciones, integración de plataformas y automatización de procesos, posicionándose como proveedor de soluciones de valor agregado para consultorías, interventorías y gerencia de proyectos.
- **Gestión / Automatización:** la experiencia en redes de telecomunicaciones y sistemas Scada permitió desarrollar la plataforma SIPLEX MANAGEMENT, con soluciones como SMNET, SMQR, SM-SCADA, SMNET-EWSD, SMPRO, SMVER, SMIVR y dispositivos electrónicos.
- **Software:** desarrollo de soluciones de software desde 2002, incluyendo firmware, aplicaciones informáticas y sistemas integrados de gestión. La oferta se complementa con herramientas de diagnóstico centralizado, gestión de tiquetes e indicadores, y alianzas estratégicas con Tableau, Splunk, Syncsort y Trustwave.

Información financiera

De acuerdo con los estados financieros del cierre contable, en el año 2023 la compañía reportó ventas por $10.136.806.171 COP, en comparación con los resultados del año anterior representó una disminución respecto a los $13.931.056.619 COP. La variación se debe a un ajuste en la dinámica comercial de la empresa, influenciado principalmente por factores de mercado y servicios ofertados.

En términos de rentabilidad, la utilidad bruta para 2023 se situó en $2.133.382.706 COP, con una utilidad operativa de $996.283.455 COP. Sin embargo, se observa una reducción respecto al año anterior, cuando estos valores alcanzaron $3.249.595.899 COP y $1.765.543.125 COP, respectivamente.

La utilidad neta del ejercicio 2023 fue de $302.254.377 COP, significativamente menor en comparación con la del 2022, que ascendió a $1.092.448.225 COP. La diminución se

presentó por incrementos en costos operativos, ajustes en estrategias comerciales y la distribución de dividendos, que en 2023 ascendió a $600.000.000 COP.

La empresa cerró el año con un total de activos de $8.950.437.216 COP, compuesto por activos corrientes y no corrientes. A su vez, los pasivos totales sumaron $3.262.531.221 COP. El patrimonio neto de la compañía se ubicó en $5.687.905.995 COP, consolidando su estabilidad financiera. La revisión de los estados financieros confirma la presencia activa de la empresa en el mercado y su compromiso con la transformación digital, incluyendo servicios clave como gestión documental y custodia.

Análisis del sector

El sector TIC en Colombia ha logrado impulsar ventajas competitivas derivadas del constante crecimiento de proyectos tecnológicos y de las exigencias de la transformación digital. Este enfoque representa una ventaja estratégica frente a alternativas estandarizadas, adoptadas por grandes compañías para seguir con el flujo de la innovación en el mercado. Sin embargo, las medianas y pequeñas empresas no siempre logran el mismo nivel de adaptación. Por ello, algunos de los principales factores diferenciales del sector radican en su capacidad especializada y personalización en la oferta de servicios con el fin de ajustarse con mayor precisión a las necesidades específicas de sus clientes.

Asimismo, el sector ha evidenciado una alta capacidad de integración con otros sectores como salud, educación, transporte e industria, lo que amplía las oportunidades en el mercado y posicionado al sector TIC como aliado de la gestión de proyectos y desarrollo intersectorial. La proyección laboral continúa creciendo y se adoptan nuevos marcos de trabajo como el teletrabajo y los modelos híbridos, los cuales han potenciado la competitividad del sector al permitir mayor atracción de talento especializado, reducir las barreras geográficas y ampliar las oportunidades laborales en los entornos digitales.

Contexto del sector

El sector de TIC en Latinoamérica ha experimentado un crecimiento exponencial impulsado por la transformación digital, la automatización y la demanda de soluciones para la gestión de datos y la seguridad de la información. OSP INTERNATIONAL CALA S.A.S. se posiciona en la región a partir de su enfoque en innovación y desarrollo de soluciones especializadas.

La digitalización en sectores como el gubernamental, financiero, educativo e industrial ha generado un entorno competitivo, impulsado por políticas públicas y planes de modernización tecnológica. Sin embargo, este crecimiento también plantea desafíos en competencia, cumplimiento normativo y adaptación al mercado. De acuerdo con el Ministerio TIC (2023), aunque el país ha avanzado en tecnologías emergentes, persisten falencias en infraestructura y capacidades organizativas, así como brechas en la adopción de soluciones en la nube, inteligencia artificial, big data y automatización de procesos.

Análisis PESTEL

Siguiendo a Porter (2008), quien señala que valuar el entorno permite determinar el lugar que ocupa la organización en el mercado, se identifican los siguientes factores que condicionan la operación de OSP INTERNATIONAL CALA S.A.S:

- **Político**: las políticas de transformación digital impulsadas por MinTIC y el Plan Nacional de Desarrollo Digital incentivan la modernización del sector público, generando oportunidades de contratación que exigen cada vez más certificaciones y estándares de seguridad.
- **Económico:** la reducción del 27% en ingresos entre 2022 y 2023 refleja la variabilidad en la demanda de servicios tecnológicos y la presión sobre márgenes operativos, limitando la inversión en ciberseguridad.

- **Social:** la brecha de talento especializado en seguridad de la información en Colombia dificulta la incorporación de competencias específicas en los equipos de trabajo.
- **Tecnológico:** la rápida evolución hacia enfoques como DevSecOps, inteligencia artificial y automatización de pruebas de seguridad demanda actualización continua de herramientas y metodologías.
- **Ecológico:** la adopción de servicios en la nube y prácticas digitales reduce el consumo de recursos físicos, alineándose con objetivos de sostenibilidad.
- **Legal:** el cumplimiento de la Ley 1581 de 2012 de protección de datos personales, el Decreto 1377 de 2013 y estándares como ISO/IEC 27001 constituyen obligaciones que, de no gestionarse adecuadamente, exponen a la empresa a sanciones de la Superintendencia de Industria y Comercio (SIC).

Competencia

En el mercado TIC colombiano, la organización compite con empresas de consultoría tecnológica, desarrollo de software y transformación digital. Entre los competidores se encuentran Heinsohn Business Technology, con más de 40 años de experiencia y certificaciones en desarrollo de software para sectores financiero y gubernamental; InterGrupo, especializada en infraestructura TI y servicios gestionados con certificaciones CMMI; Asesoftware, enfocada en software a la medida con presencia regional; y multinacionales como SONDA y Stefanini, con operaciones en múltiples países y estructuras consolidadas de gobernanza y seguridad. En comparación, OSP presenta fortalezas en innovación, I+D propio y personalización de soluciones, pero enfrenta retos en la integración formal de la seguridad en la gestión de proyectos, lo que puede afectar su posicionamiento frente a competidores con mayor madurez en ciberseguridad.

Posicionamiento

OSP INTERNATIONAL CALA S.A.S. se ha consolidado como un actor relevante en el sector TIC en Colombia, con presencia en más de 4 regiones del país y ciudades como Cali, Bogotá, Medellín y Pamplona. Su estrategia de diferenciación se basa en la investigación y desarrollo (I+D), para ofrecer soluciones tecnológicas innovadoras para la gestión de redes, automatización de procesos y seguridad de la información.

Un factor clave ha sido su capacidad de establecer relaciones de confianza con sus clientes, basada en la excelencia operativa y la entrega de soluciones adaptadas a necesidades específicas. Además, la empresa cuenta con un equipo altamente especializado en desarrollo y adaptación de tecnologías, que otorga una ventaja competitiva frente a otras empresas del sector. Aunque la organización ha logrado optimizar su operación mediante el mantenimiento de infraestructura arrendada, aún enfrenta retos de expansión y reducción de costos operativos.

Tendencias del sector y oportunidades

- **Transformación digital:** la creciente digitalización en empresas y entidades gubernamentales impulsa la demanda de gestión documental y automatización de procesos, áreas donde la empresa tiene sólida experiencia.
- **Seguridad de la información:** el aumento de ciberataques y regulaciones más estrictas en protección de datos han convertido a la ciberseguridad en prioridad, representando una oportunidad para fortalecer el posicionamiento de OSP.
- **Automatización y redes inteligentes:** sistemas SCADA y plataformas como SIPLEX MANAGEMENT permiten la optimización de redes y monitoreo en tiempo real en sectores como telecomunicaciones, energía e industria.

- **Desarrollo de software y soluciones a medida:** la demanda de integración de plataformas y soluciones personalizadas representa oportunidad para tecnologías escalables y adaptables.
- **Políticas gubernamentales favorables:** El Plan Nacional de Desarrollo Digital prioriza la modernización tecnológica y abre espacios para proyectos de infraestructura digital y servicios gubernamentales.

Desafíos del Sector

El crecimiento del sector TIC también trae desafíos estructurales y estratégicos:

- La rápida evolución tecnológica exige innovación constante, actualización de servicios y capacitación continua para mantener la competitividad.
- El uso no regulado de tecnologías emergentes como la inteligencia artificial ha incrementado la exposición a amenazas cibernéticas, afectando la integridad, confidencialidad y disponibilidad de la información.
- La adaptación continua a normativas locales e internacionales sobre protección de datos y ciberseguridad supone un desafío constante.
- En algunos ambientes corporativos persiste baja disposición para adoptar tecnologías emergentes, por limitaciones económicas, falta de experticia y estructuras operativas tradicionales.

Ventajas competitivas

El sector TIC se destaca como uno de los más dinámicos y con mayor proyección laboral, impulsado por la transformación digital y la inversión en nuevas tecnologías.

Entre las ventajas más importantes se destacan:

- Alta generación de empleo en Colombia, dada la constante necesidad de perfiles capacitados en análisis de datos, gestión de proyectos tecnológicos y desarrollo de software.

- Apoyo institucional del Ministerio TIC para la formación del talento humano mediante programas de formación gratuita, certificaciones internacionales y programas de becas como "Un Ticket para el futuro" (Mintic, 2022), con el objetivo de disminuir la brecha de talento y fortalecer la empleabilidad.
- Expansión del teletrabajo y flexibilidad laboral, permitiendo la vinculación de profesionales en diferentes regiones y facilitando el acceso a mayores oportunidades.
- Promoción de altos estándares con marcos internacionales como ISO/IEC 27001 e ITIL, mejorando la credibilidad, sostenibilidad y confianza del sector.
- Crecimiento sostenido del ecosistema digital con avance en infraestructura tecnológica, plataformas digitales y servicios en la nube, generando estabilidad laboral y proyectos de larga duración.

Marco de referencia

La construcción del modelo para la integración de la seguridad de la información en la gestión de proyectos de tecnologías de la información (TI) exige el análisis de conceptos provenientes de la ingeniería de sistemas, la gestión de proyectos, la seguridad informática y la gobernanza organizacional. A continuación, se presenta el fundamento teórico organizado por ejes temáticos, con el propósito de articular teorías, modelos y marcos conceptuales que sustenten la propuesta metodológica.

a) Gestión de proyectos

Según el PMI (2021), un proyecto es "un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único", caracterizado por su temporalidad y unicidad. Nicholas y Steyn (2020) complementan esta definición al señalar que un proyecto es una unidad organizacional temporal que debe alinearse con los objetivos estratégicos de la empresa y los intereses de sus partes interesadas. Kerzner (2017) precisa que la gestión de proyectos consiste en la aplicación de conocimientos, habilidades, herramientas y técnicas para cumplir los objetivos del proyecto dentro de límites de tiempo, presupuesto, costo y calidad.

La gestión de proyectos se organiza en cinco grupos de procesos: iniciación, planificación, ejecución, monitoreo y control, y cierre (PMI, 2021; Heagney, 2022). El PMI (2021) identifica diez áreas de conocimiento que debe dominar todo director de proyectos: integración, alcance, cronograma, costos, calidad, recursos, comunicaciones, riesgos, adquisiciones e interesados. Estas áreas proporcionan una estructura sistemática desde la concepción hasta la finalización del proyecto (Heagney, 2022).

Un aspecto central es el manejo de las restricciones PCTS: desempeño (performance), costo, tiempo y alcance. Estas dimensiones están interrelacionadas; si se

modifica una, las demás se ven afectadas. El director de proyecto debe determinar la cuarta variable en función de las tres fijadas por el patrocinador (Heagney, 2022).

El ciclo de vida del proyecto comprende las fases de concepto, definición, planificación, ejecución, control y cierre. Una definición imprecisa del problema o una planificación deficiente comprometen el éxito desde los primeros pasos. La calidad de la planificación resulta un factor crítico: muchas organizaciones no dedican suficiente tiempo a esta etapa, lo que conduce a gestión reactiva, retrabajo y conflictos con los interesados (Heagney, 2022).

El control de cambios es igualmente relevante. A lo largo del ciclo de vida pueden surgir desviaciones o necesidades no previstas; por ello, es indispensable un proceso definido que evalúe el impacto en alcance, presupuesto o cronograma antes de su aprobación. Una gestión inadecuada del cambio genera el fenómeno conocido como scope creep, que compromete el éxito del proyecto (Heagney, 2022).

En el sector TI, la gestión de proyectos adquiere una dimensión estratégica. Según Salinas (2021), implica aplicar conocimientos, habilidades y herramientas para organizar, ejecutar y dar seguimiento a iniciativas tecnológicas mediante planificación detallada, ejecución coordinada y monitoreo continuo. El rol del director de proyectos trasciende la coordinación técnica: debe ejercer liderazgo, resolver conflictos, gestionar recursos limitados y actuar como facilitador ante los diversos interesados (Heagney, 2022).

b) Metodologías de gestión de proyectos

Metodologías tradicionales

Las metodologías tradicionales se caracterizan por su enfoque predictivo y secuencial, donde el desarrollo del proyecto se estructura en fases definidas que se ejecutan de forma lineal: iniciación, planificación, ejecución, control y cierre (Riaño Nossa, 2021). La

modelo cascada establece requisitos fijos desde el inicio, prioriza la documentación exhaustiva y se basa en un diseño detallado antes de pasar a etapas posteriores.

Entre las metodologías tradicionales más representativas se encuentran: PMBOK (Project Management Body of Knowledge), que ofrece un compendio de buenas prácticas estructuradas en cinco grupos de procesos y diez áreas de conocimiento, ampliamente reconocido y adaptable a proyectos con requisitos claros y estables (Riaño Nossa, 2021); PRINCE2 (Projects in Controlled Environments), que enfatiza la gestión por procesos y principios, con roles definidos, fases de control y una justificación constante del negocio (Riaño Nossa, 2021); y otras como el modelo en espiral, el modelo en V y el proceso racional unificado (RUP), todas con énfasis en la planificación y control como mecanismos para mitigar riesgos (Velásquez et al., 2019).

Las ventajas de estas metodologías radican en su claridad de procesos, trazabilidad documental y facilidad para aplicar controles de calidad (Riaño Nossa, 2021). No obstante, su rigidez ante cambios, el alto costo de adaptación y la poca flexibilidad las hacen menos idóneas para entornos cambiantes (Velásquez et al., 2019).

Metodologías ágiles

Las metodologías ágiles surgen como respuesta a las limitaciones del enfoque tradicional en proyectos caracterizados por la volatilidad y la evolución constante de requerimientos (Riaño Nossa, 2021). El Manifiesto para el Desarrollo Ágil de Software, redactado en 2001 por diecisiete expertos, estableció cuatro valores fundamentales: individuos e interacciones sobre procesos y herramientas; software funcional sobre documentación extensiva; colaboración con el cliente sobre negociación contractual; y respuesta ante el cambio sobre seguir un plan (Beck et al., 2001; Velásquez et al., 2019).

Entre las metodologías ágiles más destacadas se encuentran: Scrum, que organiza el trabajo en sprints con roles definidos (Scrum Master, Product Owner y equipo de

desarrollo) y fuerte orientación a la retroalimentación y mejora continua; Kanban, que utiliza tableros visuales para gestionar el flujo de trabajo y limitar tareas en proceso; Programación Extrema (XP); DSDM; Crystal; AUP; OpenUP; y FDD (Feature-Driven Development) (Velásquez et al., 2019; PMI, 2021). Estas metodologías han demostrado mayor efectividad en proyectos con requisitos cambiantes y promueven equipos autogestionados, mejora continua y orientación al cliente, aunque requieren altos niveles de disciplina y colaboración constante (Riaño Nossa, 2021).

Enfoques híbridos y antecedentes

Acuña et al. (2022) evidenciaron, mediante un análisis mixto basado en encuestas a expertos, que las organizaciones enfrentan el desafío de seleccionar metodologías según las características específicas de cada proyecto y que no existe una metodología universalmente aplicable. Los enfoques híbridos, que combinan elementos de metodologías tradicionales y ágiles, han sido adoptados por diversas organizaciones en entornos dinámicos, muchas veces de forma inconsciente. El estudio resalta la importancia de considerar el perfil del equipo, los objetivos del proyecto y el entorno como factores clave en la toma de decisiones metodológicas.

Viveros et al. (2019) propusieron Scrum+, una guía escalada para la gestión ágil de proyectos globales de desarrollo de software en entornos multimodelo. La investigación busca la armonización entre Scrum y modelos como ISO/IEC 15504, ISO 9001 y CMMI-DEV. La validación se realizó mediante grupos focales con expertos y evaluación de agilidad con el método 4-DAT; los resultados confirman la claridad, adecuación y agilidad de la guía. Este antecedente respalda que, en entornos tecnológicos cambiantes, las organizaciones requieren marcos que comprendan la complejidad contextual y la diversidad metodológica.

Janampa, Vilca y Meneses (2023) propusieron un modelo híbrido denominado Scrumban/XP, que integra Scrum, Kanban y Programación Extrema (XP). El modelo fue validado en un caso real -el desarrollo de un sistema de pago- y demostró mejoras en la planificación, ejecución y calidad del producto final. La combinación estructurada de marcos ágiles permite superar las limitaciones individuales de cada metodología en contextos organizacionales dinámicos.

Metodologías para proyectos de impacto social

Según Rojas Escobar (2024), la selección adecuada de metodologías permite a las organizaciones integrar elementos sociales, normativos y estratégicos en todas las fases del ciclo de vida del proyecto. Las principales metodologías analizadas incluyen: PM4R, desarrollada por el BID, centrada en resultados tangibles e integración de aspectos sociales (ponderación SIA: 88); PMDPro, especializada en proyectos de desarrollo en entornos humanitarios (81); ISO 21500, con directrices internacionales flexibles (77); PRINCE2, con estructura orientada a procesos (76); PMBOK (75); P2M, con visión estratégica de innovación empresarial (69); ICB IPMA, basada en competencias (68); Scrum (60); e ITIL (58).

Tabla 2.

Resumen comparativo de metodologías de gestión de proyectos.

Metodología	Descripción general	Principales fortalezas	Ponderación (SIA)
PM4R.	Metodología orientada a resultados, promovida por el BID.	Alta alineación con objetivos sociales, gestión adaptativa, transparencia, participación activa.	88
PMDPro.	Enfoque especializado en proyectos de desarrollo y ayuda humanitaria.	Evaluación contextual, participación comunitaria, enfoque en sostenibilidad.	81
ISO 21500.	Estándar internacional para gestión de proyectos	Flexibilidad, alineación con normas internacionales, orientación a procesos.	77

	aplicable a múltiples sectores.		
PRINCE2.	Metodología estructurada basada en procesos, común en Europa.	Gestión de riesgos, justificación continua del negocio, informes detallados.	76
PMBOK.	Marco global del PMI con enfoque en áreas de conocimiento.	Gestión de riesgos, definición de indicadores, estructura robusta.	75
P2M.	Enfoque japonés centrado en innovación organizacional.	Visión estratégica e integradora, enfoque sistémico.	69
ICB IPMA.	Modelo basado en competencias para gestión de proyectos, programas y portafolios.	Evaluación integral de habilidades técnicas y comportamentales.	68
SCRUM.	Metodología ágil e iterativa, ampliamente usada en desarrollo de software.	Adaptabilidad, seguimiento continuo, entrega incremental.	60
ITIL.	Marco para la gestión de servicios TI.	Mejora continua del servicio, estandarización operativa.	58

Nota. Adaptado de (Rojas Escobar, 2024). La ponderación representa el nivel de adecuación de cada metodología para proyectos de desarrollo e impacto social, según los 10 elementos clave del enfoque SIA.

c) Gobernanza de TI

La gobernanza de TI representa un conjunto de estructuras, procesos y mecanismos que aseguran que la gestión de TI respalde y extienda las estrategias y objetivos corporativos. Según ISACA (2019), funciona como orientación del uso eficiente y responsable de recursos tecnológicos, con la capacidad de tomar decisiones informadas, reducir riesgos y maximizar el valor entregado. Su integración en la gestión de proyectos TI evita desviaciones y reprocesos, al articular decisiones tecnológicas con la estrategia empresarial.

De Haes y Van Grembergen (2015) precisan que la gobernanza empresarial de TI es un componente esencial de la gobernanza corporativa, cuyo propósito es definir e

incorporar procesos y estructuras organizacionales que permitan a las áreas de negocio y de tecnología ejecutar sus responsabilidades, maximizar el valor de las inversiones habilitadas por TI y alcanzar el alineamiento estratégico entre ambas dimensiones.

COBIT 2019

COBIT (Control Objectives for Information and Related Technologies), desarrollado por ISACA, se ha consolidado como el marco más adoptado para la gobernanza y gestión empresarial de la información y la tecnología. Su versión COBIT 2019 ofrece un modelo integral que articula 40 objetivos de gobernanza y gestión, organizados en cinco dominios que abarcan desde la evaluación y dirección estratégica hasta la entrega, el servicio y el soporte operativo (ISACA, 2018).

Según la revisión sistemática de Putra et al. (2025), la implementación de COBIT 2019 en diversos sectores demuestra beneficios consistentes en el alineamiento de TI con las estrategias de negocio, la optimización de recursos y la gestión de riesgos, aunque evidencia desafíos relacionados con la complejidad del marco y la necesidad de formación continua.

La integración de COBIT con otros marcos normativos es una característica central de su arquitectura. Incluye áreas focales específicas para seguridad de la información, riesgo tecnológico y DevOps, y proporciona guías para la implementación del Marco de Ciberseguridad del NIST (ISACA, 2020). Esta capacidad de articulación con ISO 27001, ISO 27005 y NIST refuerza su pertinencia al ofrecer el marco evaluativo y directivo necesario para asegurar que las decisiones de seguridad estén alineadas con los objetivos institucionales.

TOGAF

TOGAF (The Open Group Architecture Framework) proporciona un enfoque estructurado para diseñar, planificar, implementar y gobernar sistemas de información

alineados con los objetivos del negocio. Su componente central, el método ADM (Architecture Development Method), organiza el desarrollo arquitectónico en fases iterativas que incluyen la definición de la visión, el diseño de la arquitectura de negocio, datos, aplicaciones y tecnología, así como su implementación y gobierno. Según Putra et al. (2025), TOGAF ADM permite integrar la gestión de riesgos desde las etapas iniciales del diseño arquitectónico, especialmente cuando se articula con modelos de gobernanza como COBIT 2019.

Principios de gobernanza ISO/IEC 38500

La norma ISO/IEC 38500 establece los principios para la gobernanza corporativa de TI, orientando a la alta dirección en la evaluación, dirección y monitoreo del uso de las tecnologías de la información. Su enfoque se basa en principios como responsabilidad, estrategia, desempeño y conformidad, que permiten asegurar la alineación entre TI y los objetivos organizacionales, así como la gestión adecuada de riesgos y el cumplimiento normativo (ISO, 2024). En el contexto de la gestión de proyectos TI, este marco refuerza la necesidad de definir roles claros y de integrar la gobernanza desde las etapas iniciales, complementando marcos como COBIT y TOGAF desde una perspectiva estratégica y de control (ISO, 2024).

d) Modelos de madurez

Los modelos de madurez son herramientas metodológicas que miden el grado de formalización, consistencia y optimización de prácticas organizacionales (CMMI Institute, 2018). Se estructuran en niveles progresivos —generalmente cinco— que van desde procesos informales y reactivos hasta procesos optimizados y mejorados de forma continua, lo que permite diagnosticar brechas y orientar mejoras. La madurez organizacional, según Huang (2024), se vincula con la capacidad institucional para desarrollar y consolidar progresivamente procesos internos, en alineación con objetivos

estratégicos. La alineación estratégica refleja el grado en que los esfuerzos tecnológicos se integran con la estrategia organizacional, con mejoras en desempeño, eficiencia de procesos y capacidad de respuesta ante cambios del entorno (Huang, 2024).

En el ámbito de la seguridad, el modelo ISM3 (Information Security Management Maturity Model) distingue cinco niveles de madurez y 45 procesos con un enfoque práctico orientado a objetivos de negocio (Altamirano Di Luca, 2019). Este autor propuso un modelo integral que sintetiza controles de ISO 27001 y NIST SP 800-53 en un enfoque integrado que reduce complejidad, maximiza la automatización de controles y opera bajo un ciclo cerrado de mejora continua PHVA.

e) Seguridad de la información

La seguridad de la información constituye un eje estratégico en las organizaciones contemporáneas. Se define como el conjunto de políticas, procedimientos y controles destinados a proteger los activos de información frente a amenazas, con el propósito de preservar su confidencialidad, integridad y disponibilidad - la tríada CIA o CID - (Samaniego & Ponce, 2021; Chai & Zolkipli, 2021). En el marco normativo, la ISO/IEC 27001 (2022) establece que la seguridad abarca la protección de activos informacionales en cualquier formato o medio.

Principios de la seguridad de la información

La confidencialidad garantiza el acceso a la información únicamente a individuos o sistemas autorizados, mediante controles de acceso, autenticación robusta y técnicas criptográficas (Samaniego & Ponce, 2021). Chai y Zolkipli (2021) advierten que el crecimiento exponencial del uso de redes y dispositivos móviles ha incrementado los riesgos asociados a este principio.

La integridad asegura que la información no haya sido modificada de manera indebida y permanezca completa y fiel a su estado original. Se protege mediante funciones hash,

auditorías periódicas y sistemas de control de cambios (Samaniego & Ponce, 2021). En entornos distribuidos, técnicas como la replicación de datos o el cifrado de texto dinámico refuerzan este principio (Chai & Zolkipli, 2021).

La disponibilidad establece que la información debe estar accesible para los usuarios autorizados cuando la requieran. Su garantía implica respaldos periódicos, balanceadores de carga, infraestructura redundante y protección contra ataques de denegación de servicio (Samaniego & Ponce, 2021). En la nube, se aplican técnicas como la verificación homomórfica para mantener el acceso seguro y eficiente (Chai & Zolkipli, 2021).

Modelo AAA: Autenticación, Autorización y Auditoría

La gestión de acceso se articula mediante el modelo AAA. La autenticación verifica la identidad de los usuarios a través de credenciales, tokens o datos biométricos; la autorización define los permisos según el rol del usuario; y la auditoría registra las actividades para análisis forense y cumplimiento normativo (Samaniego & Ponce, 2021). Lopez-Gomez et al. (2025) proponen la arquitectura SDN-AAA, que utiliza redes definidas por software para la gestión centralizada y automatizada de configuraciones de AAA, con adaptación dinámica ante fallas o variaciones de tráfico.

La efectividad de estas infraestructuras técnicas requiere un marco de gobernanza que defina la participación humana. Ferdiansyah et al. (2023) sostienen que la integración de una Matriz RACI (Responsible, Accountable, Consulted, Informed) permite determinar con precisión los actores idóneos para implementar estrategias de seguridad, con asignación clara de responsabilidades que fortalezca la toma de decisiones estratégicas.

Principio de menor privilegio

Este principio establece que todo usuario o proceso debe contar únicamente con los permisos mínimos indispensables para ejecutar sus funciones. Su implementación reduce la superficie de ataque, limita el impacto de intrusiones y previene errores humanos o maliciosos (Samaniego & Ponce, 2021). Los modelos basados en roles (RBAC) y en atributos (ABAC) permiten gestionar privilegios de forma granular; en infraestructuras más complejas, la arquitectura SDN-AAA asigna permisos dinámicamente según el comportamiento del usuario o las condiciones del entorno (López-Gómez et al., 2025).

Mecanismos de control

La protección de los sistemas se complementa con tres tipos de mecanismos. Los preventivos buscan evitar incidentes mediante firewalls, autenticación multifactor, cifrado y segmentación de red. Los detectivos identifican accesos no autorizados o comportamientos anómalos a través de sistemas de detección de intrusos (IDS), supervisión de registros (log monitoring) y sistemas de correlación de eventos (SIEM). Los correctivos contienen y mitigan los efectos de incidentes mediante restauración de respaldos, aplicación de parches y bloqueo de accesos comprometidos (Samaniego & Ponce, 2021). Estos mecanismos, junto con el principio de menor privilegio y el modelo AAA, conforman un conjunto de criterios necesarios para la protección de sistemas informáticos, respaldado por la ISO/IEC 27001.

f) Ciberseguridad

Según el NIST (2018), la ciberseguridad es la práctica de proteger sistemas informáticos, redes y dispositivos frente a accesos no autorizados, alteraciones maliciosas y ataques intencionados, mediante tecnologías específicas, buenas prácticas operativas y procesos de respuesta. Mientras la seguridad de la información adopta una

visión amplia centrada en datos en cualquier formato, la ciberseguridad actúa como su componente técnico especializado en el entorno digital.

NIST Cybersecurity Framework (CSF)

El NIST Cybersecurity Framework (CSF) es uno de los marcos más reconocidos para la gestión de riesgos de ciberseguridad. Desde su primera versión en 2014, ha sido adoptado por organizaciones de todos los tamaños y sectores. En 2024, el NIST publicó la versión 2.0, que introduce actualizaciones significativas para responder a los desafíos de gobernanza digital, amenazas emergentes y protección de la cadena de suministro tecnológica (Lanz, 2024).

El CSF se estructura en seis funciones: Identificar, Proteger, Detectar, Responder, Recuperar y Gobernar - esta última incorporada en la versión 2.0 -. La función Gobernar fortalece el rol de la alta dirección en el establecimiento de políticas, roles y estrategias de ciberseguridad, e integra la gestión de riesgos en la cadena de suministro digital. Con ello, el marco trasciende el enfoque técnico-operativo para alinearse con la gobernanza organizacional y la gestión estratégica de riesgos (NIST, 2024).

Su enfoque modular y adaptable permite la integración con otros marcos como COBIT, ISO/IEC 27001, COSO ERM e ITIL. Ofrece herramientas como guías de inicio rápido, perfiles por tipo de organización y niveles de madurez (tiers), lo que facilita su adopción en diversos contextos. Desde la perspectiva de la gestión de proyectos TI, el CSF puede integrarse en el diseño, planificación y control de proyectos con altas exigencias de cumplimiento, protección de datos o dependencia tecnológica; su enfoque por funciones permite mapear controles específicos a lo largo del ciclo de vida del proyecto (Lanz, 2024).

Security by Design

El principio de Security by Design establece que la seguridad debe incorporarse como requisito fundamental desde las fases iniciales de concepción y diseño de sistemas, en lugar de tratarse como un componente añadido tras el desarrollo (McGraw, 2006). Este enfoque se sustenta en la premisa de que los sistemas operan en entornos potencialmente hostiles; su arquitectura debe anticipar ataques y minimizar la superficie de exposición. Según el NIST SP 800-160 Vol. 1 Rev. 1, la ingeniería de seguridad de sistemas establece principios, conceptos, actividades y tareas para el desarrollo de sistemas confiables y seguros, con aplicabilidad transversal a diversos tipos de sistemas y etapas del ciclo de vida (NIST, 2022).

DevSecOps

DevSecOps constituye una evolución del paradigma DevOps que incorpora la seguridad como responsabilidad compartida y transversal a lo largo de todo el ciclo de vida del desarrollo de software, en contraposición al enfoque que trata la seguridad como actividad posterior (Myrbakken y Colomo-Palacios, 2017). Se fundamenta en el principio de shift-left security, que propone desplazar las actividades de seguridad hacia las fases más tempranas del ciclo de desarrollo para identificar y remediar vulnerabilidades de manera proactiva, con la consecuente reducción de costos de corrección en fases posteriores (Rajapakse et al., 2022).

Su implementación se articula mediante controles de seguridad automatizados en las canalizaciones de integración y entrega continua (CI/CD). Según Ramaj et al. (2024), las prácticas abarcan: planificación con modelado de amenazas y definición de requisitos de seguridad; desarrollo con análisis estático de código; construcción con verificación de dependencias; pruebas con análisis dinámico y pruebas de penetración; despliegue con escaneos de conformidad; y monitoreo continuo en operación.

Controles de seguridad en proyectos TI

Los security gates (puertas de seguridad) constituyen puntos de control formales que evalúan si un artefacto de software o entregable cumple con criterios de seguridad predefinidos antes de avanzar a la siguiente fase del desarrollo (Rindell et al., 2021). Estos puntos incorporan criterios como la ausencia de vulnerabilidades críticas, el cumplimiento de estándares de codificación segura y la conformidad con políticas organizacionales de seguridad (Uzunova et al., 2024).

El baseline de seguridad se define como el conjunto mínimo de configuraciones y controles que un sistema debe satisfacer para ser considerado aceptable en un contexto organizacional determinado. Según el NIST SP 800-53B (2020), los baselines se establecen conforme a la categorización de seguridad del sistema y se adaptan mediante procesos de ajuste basados en la evaluación de riesgos, los requisitos de cumplimiento normativo y las condiciones operativas de la organización.

g) Marcos normativos y estándares

ISO/IEC 27001

La ISO/IEC 27001 es el estándar internacional más reconocido para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Adopta el modelo de mejora continua basado en el ciclo PDCA (Plan-Do-Check-Act) y define requisitos generales que incluyen el establecimiento de políticas, la asignación de responsabilidades, el tratamiento de riesgos, la concienciación del personal y la revisión continua de la eficacia de los controles (Robayo Bautista, 2020).

Su Anexo A integra controles de seguridad clasificados en 14 dominios, desde la política de seguridad hasta la gestión de incidentes y la continuidad del negocio. La norma enfatiza la identificación y protección de los activos de información - entendidos como documentos, bases de datos, personas, procesos y tecnologías -, lo que permite

abordar la seguridad desde una perspectiva integral, tanto lógica como física (Robayo Bautista, 2020). En el contexto de las pruebas de seguridad de software, los lineamientos de ISO/IEC 27001 pueden incorporarse como parte de una guía de buenas prácticas para la validación de aplicaciones web (Robayo Bautista, 2020).

Gestión de riesgos: ISO 31000, ISO 27005 y NIST RMF

La ISO 31000:2018 define el riesgo como el "efecto de la incertidumbre sobre los objetivos" y establece un marco articulado en tres componentes: principios que orientan la gestión de riesgos, un marco organizacional que la incorpora a la gobernanza y la estrategia, y un proceso analítico que comprende la identificación, el análisis, la evaluación, el tratamiento y el monitoreo de riesgos (ISO/IEC, 2018). Esta estructura tripartita resulta coherente con la arquitectura de tres dimensiones del modelo propuesto.

La ISO 27005 proporciona directrices para la gestión de riesgos de seguridad de la información en proyectos TI, con la identificación de activos, amenazas y vulnerabilidades, y la estimación del nivel de riesgo mediante la evaluación de probabilidad e impacto sobre los objetivos de confidencialidad, integridad y disponibilidad (ISO/IEC, 2022). Su integración con el proceso de gestión de riesgos del PMBOK permite articular los riesgos de seguridad con los riesgos del proyecto en un registro unificado.

El NIST Risk Management Framework (RMF), documentado en el NIST SP 800-37, complementa esta perspectiva con un proceso estructurado de seis pasos: categorizar, seleccionar, implementar, evaluar, autorizar y monitorear, que conecta la gestión de riesgos con la autorización de sistemas y el monitoreo continuo de seguridad (NIST, 2018). La articulación del RMF con el ciclo de vida del proyecto permite establecer criterios objetivos de aceptación de riesgo en cada security gate.

Riesgos tecnológicos en proyectos TI

Los riesgos tecnológicos se definen como la posibilidad de afectación negativa de activos organizacionales, procesos o capacidad operativa por amenazas asociadas al uso de TI (ISO/IEC 27005, 2022). Las organizaciones enfrentan ciberataques, errores humanos o fallos de sistemas que requieren un enfoque que combine medidas administrativas, técnicas y físicas para proteger datos y minimizar vulnerabilidades (ISO 31000, 2018; ISO/IEC 27002, 2022).

h) Estado del arte: integración de la seguridad en proyectos TI

La revisión bibliográfica evidencia que la falta de integración de la seguridad de la información en la gestión de proyectos TI constituye un problema multidimensional, documentado desde perspectivas normativas, organizacionales y técnicas.

Coque Vásquez y Kujundzic Riveros (2018) identificaron una brecha crítica en el PMBOK al demostrar que sus grupos de procesos carecen de mecanismos formales para la gestión de seguridad de la información, y propusieron un mapeo de controles de ISO/IEC 27002 a los grupos de procesos del PMBOK para crear un marco híbrido con especial relevancia para MiPymes.

Fattah Ys, Parga Zen y Wasitarini (2023) evaluaron la implementación de ISO 27001 en la Biblioteca Nacional de Indonesia y evidenciaron riesgos físicos y operativos no resueltos, activos no identificados, sobrecarga de funciones y escasez de personal, lo que refleja un nivel de madurez inicial en la gestión de seguridad.

Fiore, Facin y Muniz Jr. (2023) analizaron la integración de ISO 27001 con ISO 9001 e identificaron cinco factores habilitadores críticos —integración de estándares, recursos humanos, disponibilidad de recursos, aspectos de los estándares y modelo de implementación— y concluyeron que el factor humano (resistencia al cambio y falta de competencias internas) es la barrera más crítica.

Kitsios, Chatzidimitriou y Kamariotou (2023) documentaron la implementación de ISO 27001 en una consultora TI internacional basada en proyectos; el estudio evidenció beneficios en imagen, disponibilidad de infraestructura, reducción de costos y soporte a la gobernanza, y conectó ISO 27001 con ISO 15504 como modelo de madurez de procesos software.

Kamil, Lund e Islam (2023) exploraron la legitimidad de ISO 27001 desde la perspectiva de stakeholders del sector privado sueco y concluyeron que la certificación por sí sola no satisface las expectativas de los clientes, que las amenazas dinámicas superan la velocidad de actualización del estándar, y que la cultura de seguridad resulta crítica para una implementación efectiva.

Mesquida, Mas, San Feliu y Arcilla (2014) desarrollaron el marco MIN-ITs para la integración simultánea de ISO/IEC 9001, ISO/IEC 20000-1 e ISO/IEC 27001, con base en los procesos de ISO/IEC 15504. Los resultados evidencian que una implementación integrada reduce esfuerzo, tiempo y costos, mejora la trazabilidad y la coherencia en la ejecución de proyectos TI, y promueve una visión holística que articula la seguridad como componente transversal y estratégico.

Valencia y Orozco (2017) propusieron una metodología para la implementación de un SGSI basada en la familia ISO/IEC 27000, con cinco fases -desde la aprobación directiva hasta el diseño del SGSI- y un enfoque sistémico que considera tanto los activos tecnológicos como la información como recursos estratégicos. La investigación concluye que, pese a la complejidad derivada del amplio número de normas involucradas, es posible establecer una ruta metodológica que oriente a las organizaciones en la construcción de un SGSI efectivo y contextualizado.

Lara y Corella (2018) señalan que marcos normativos como ISO/IEC 27001, NIST, COBIT e ITIL aportan lineamientos valiosos para la gestión responsable de la seguridad,

pero deben adaptarse a la cultura organizacional. La ausencia de un proceso formal de seguridad refleja una falta de integración estratégica y de conciencia transversal.

Rahman, Williams y Kazman (2022) advierten que la implementación de seguridad en entornos ágiles requiere cambios culturales, entrenamiento técnico y colaboración efectiva entre desarrolladores y especialistas en seguridad. La falta de habilidades específicas en los equipos dificulta la toma de decisiones informadas, particularmente en contextos donde la coordinación entre agilidad y seguridad exige enfoques flexibles y colaborativos.

Schwaber (2004) señala que, en entornos cambiantes como el tecnológico, se requieren marcos metodológicos que vayan más allá de lo operativo, que comprendan el contexto organizacional y acompañen su evolución. En conjunto, estos estudios confirman que: (a) ISO 27001 es un eje articulador fundamental pero insuficiente por sí solo; (b) la seguridad debe integrarse desde el diseño y no añadirse con posterioridad; (c) el factor humano es la variable más subestimada; (d) la automatización y la medición objetiva constituyen diferenciadores de madurez organizacional; y (e) las organizaciones requieren marcos que articulen la seguridad como valor transversal, más allá del cumplimiento técnico.

Marco Legal

El marco legal busca que el desarrollo y la ejecución del proyecto se realicen cumpliendo con las normativas pertinentes. Se alinea con las leyes, reglamentos y estándares sobre protección de datos, seguridad de la información, ciberseguridad y gestión de proyectos. Dada la naturaleza sensible de la información involucrada y el contexto tecnológico actual, es fundamental seguir las normativas, tanto nacionales como internacionales, que garantizan la legalidad, integridad y efectividad del proyecto.

Contexto Legal del Proyecto

El proyecto se sitúa en un entorno legal que cada vez es más exigente en cuanto a la protección de datos personales y la seguridad de la información. En Colombia, hay varias leyes y regulaciones que establecen criterios mínimos para el manejo adecuado de la información. Al mismo tiempo, estándares internacionales como la ISO/IEC 27001 ofrecen un marco técnico y de gestión que refuerza los sistemas de información. Igualmente, regulaciones como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea tienen un impacto que puede alcanzar a entidades en Colombia que procesan datos de ciudadanos europeos.

Leyes y reglamentos aplicables

La Ley 1581 de 2012 es la normativa general que regula el tratamiento de datos personales en Colombia. Su objetivo principal es desarrollar el derecho constitucional que tienen todas las personas “a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos” (Congreso de la República, 2012, art. 1). Además, se busca garantizar el respeto de los demás derechos fundamentales como la intimidad, el buen nombre y el derecho a la información.

Esta ley se aplica a toda operación de recolección, almacenamiento, uso, circulación o supresión de datos personales, ya sea por parte de entidades públicas o privadas, y establece principios rectores como la legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad, los cuales deben ser observados por todos los responsables y encargados del tratamiento (Ley 1581, art. 4).

Tal como lo menciona Ruiz Garzón y Aguirre Olmos (2020), “la Ley 1581 de 2012 obliga a las compañías colombianas que manejan datos personales a establecer e implementar políticas, procedimientos y controles con este propósito” (p. 18). De igual manera, la Superintendencia de Industria y Comercio (SIC), entidad delegada para la vigilancia y control del cumplimiento de esta norma, ha impuesto sanciones por más de 21 mil millones de pesos debido a infracciones relacionadas con el uso inadecuado de datos personales, como lo son reportes erróneos o sin autorización a centrales de riesgo, o falta de actualización de información (SIC, 2017).

En el contexto de los proyectos TI, el cumplimiento de esta ley implica la implementación de un enfoque preventivo que integre la seguridad de la información desde la fase de diseño hasta la operación de cada proyecto. El enfoque se alinea con el principio de seguridad, que según la Ley 1581 “obliga al responsable del tratamiento a adoptar las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros” (Ley 1581, art. 19). En palabras de Ruiz Garzón y Aguirre Olmos (2020), “la seguridad informática puede mejorar la aplicabilidad de la norma en cualquier organización” (p. 19), garantizando la protección de los datos durante todo su ciclo de vida (recolección, procesamiento, almacenamiento y eliminación).

Asimismo, esta normativa fue parcialmente reglamentada por los Decretos 1377 de 2013, Decreto 886 de 2014 y el Decreto Único Reglamentario 1074 de 2015, los cuales refuerzan el deber de implementar un Registro Nacional de Bases de Datos, establecer

canales de atención para los titulares y aplicar medidas de seguridad acordes al nivel de riesgo. El Decreto 1377 de 2013 complementa la Ley 1581 de 2012 al establecer disposiciones prácticas sobre el consentimiento para el tratamiento de datos personales recolectados. Entre sus aportes más relevantes se encuentra la habilitación de mecanismos alternativos para obtener la autorización de los titulares, en casos donde no sea posible contactarlos directamente, siempre que se respeten los principios legales de protección de datos como la seguridad, la confidencialidad y la finalidad. Además, resalta la obligación de los responsables del tratamiento de informar a los titulares sobre sus derechos y las finalidades del uso de sus datos, fortaleciendo así el principio de transparencia (Congreso de la República, 2013).

Por otro lado, la Ley 1273 de 2009 introdujo en el Código Penal colombiano un nuevo bien jurídico: la protección de la información y de los datos. Su objetivo principal es sancionar penalmente conductas delictivas relacionadas con el acceso no autorizado, la interceptación de datos, la alteración de información y la propagación de software malicioso. Así, esta ley reconoce que la información y los datos digitales se han convertido en activos estratégicos cuya vulneración puede causar daños económicos, reputacionales y sociales (Jiménez-Almeira & López, 2023).

La Ley 1273 de 2009 respondió a la creciente sofisticación de los delitos informáticos y al incremento en la dependencia de las tecnologías digitales tanto por parte del sector público como del privado. Además, se alinea con compromisos internacionales, como el Convenio de Budapest sobre ciberdelincuencia, al adoptar estándares internacionales para combatir el cibercrimen y mejorar la cooperación entre países (Guzmán, citado en Jiménez-Almeira & López, 2023). Según varios estudios, esta ley ha sido fundamental para fortalecer el ecosistema normativo colombiano en materia de ciberseguridad, y ha motivado la creación de grupos especializados como el Centro Cibernético Policial,

encargado de prevenir, detectar y judicializar conductas asociadas a delitos informáticos (Policía Nacional de Colombia, 2022)

En el contexto de la gestión de proyectos TI, la normatividad actual contempla implicaciones concretas para la planificación e implementación de sistemas y plataformas tecnológicas. Las organizaciones deben diseñar medidas de control que aseguren la confidencialidad, integridad y disponibilidad de los datos, no solo por razones técnicas o éticas, sino también por obligaciones legales que, de ser incumplidas, pueden conllevar consecuencias penales.

La Estrategia Nacional Digital de Colombia 2023–2026, formulada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), se presenta como una hoja de ruta integral para promover el desarrollo digital del país de manera segura, inclusiva y sostenible. El gobierno colombiano reconoce que el avance tecnológico conlleva riesgos que deben ser gestionados, por lo cual uno de sus ejes centrales es la seguridad y confianza digital (MinTIC, 2023).

Dentro de este documento, la ciberseguridad se plantea como un elemento transversal y habilitador para la transformación digital. La estrategia promueve la adopción de prácticas orientadas a proteger infraestructuras críticas, garantizar la privacidad de la información, y fomentar una cultura de prevención frente a amenazas digitales. Asimismo, resalta la necesidad de fortalecer las capacidades institucionales para la detección y respuesta ante incidentes, a través de la cooperación entre entidades del Estado, el sector privado y la ciudadanía.

Como señala el documento oficial, la estrategia articula múltiples políticas y planes previos, como la Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020), y busca consolidar un entorno digital seguro que garantice los derechos de los ciudadanos y promueva la innovación responsable (MinTIC, 2023).

No obstante, en el contexto internacional se cuenta con el Reglamento General de Protección de Datos (GDPR), adoptado por la Unión Europea en 2016 y vigente desde 2018, el cual constituye uno de los marcos normativos más exigentes en materia de protección de datos personales a nivel mundial. Aunque se trata de una normativa europea, su ámbito de aplicación se extiende extraterritorialmente, afectando a cualquier empresa, sin importar su ubicación geográfica, que procese datos de ciudadanos de la Unión Europea. De esta manera, involucra a organizaciones colombianas que, directa o indirectamente, traten información personal de ciudadanos europeos.

El GDPR establece principios como la licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad. Además, exige mecanismos de responsabilidad proactiva que implica que las organizaciones deban cumplir con la norma y ser capaces de demostrar dicho cumplimiento (Parlamento Europeo y Consejo de la Unión Europea, 2016). Según el estudio de Méndez Velandia (2024), la legislación colombiana, representada por la Ley 1581 de 2012, presenta avances significativos, pero aún existen brechas frente al enfoque preventivo y sancionatorio del GDPR. Por ejemplo, el reglamento europeo contempla derechos como el de portabilidad, el derecho al olvido y la notificación obligatoria ante brechas de seguridad, los cuales no están plenamente desarrollados en el contexto colombiano.

Diseño Metodológico

El presente estudio se orienta a responder la pregunta de investigación: ¿Qué estrategias permiten integrar la seguridad de la información en la gestión de proyectos TI para la empresa OSP INTERNATIONAL CALA S.A.S, asegurando la continuidad operativa y el cumplimiento normativo en cada fase del ciclo de vida del proyecto? Para ello, se ha estructurado una ruta metodológica coherente con los objetivos del trabajo, que combina el análisis cuantitativo con la profundidad interpretativa del enfoque cualitativo, en un marco de investigación aplicada. La selección del diseño metodológico se orienta en lo expuesto por Haro et al. (2024) y obedece a la necesidad de comprender a fondo los procesos actuales de la empresa en materia de gestión de proyectos y seguridad de la información, así como de recolectar evidencia empírica que permita identificar brechas, validar buenas prácticas y formular un modelo de integración efectivo. De esta manera, se busca describir y correlacionar variables relevantes como el nivel de madurez, los riesgos operativos o los controles existentes, así como proponer soluciones prácticas para garantizar la pertinencia y aplicabilidad de los hallazgos.

Diseño de la investigación

El diseño de esta investigación se clasifica como no experimental, de tipo descriptivo y correlacional, enmarcado dentro de un enfoque aplicado. La clasificación responde a la intención de comprender, caracterizar y relacionar distintos aspectos del problema sin manipular deliberadamente variables independientes. Se prevalece la observación de los fenómenos en el contexto natural de la empresa OSP INTERNATIONAL CALA S.A.S.

La investigación es no experimental dado a que no manipula intencionadamente variables, ni asigna tratamientos o condiciones específicas a los participantes, por lo tanto, no cumple los requisitos de un diseño experimental. En cambio, se observa y

analiza la realidad tal como ocurre en los proyectos actuales de la empresa, donde se extraen conclusiones a partir de datos existentes, percepciones del personal (encuestas y entrevistas) y registros históricos de seguridad de la información. Además, existen restricciones éticas y prácticas que impiden intervenir en los procesos operativos críticos de la organización, lo cual reafirma la pertinencia de un diseño no experimental observacional.

Se utiliza la investigación descriptiva para identificar y caracterizar de forma sistemática los elementos vinculados a la integración de la seguridad de la información en la gestión de proyectos TI. En este estudio se busca analizar aspectos como el nivel de madurez de la gestión, la existencia de políticas de seguridad, los controles implementados, las metodologías de gestión adoptadas y la percepción organizacional sobre los riesgos de seguridad. La descripción detallada permite generar un diagnóstico del estado actual y establecer una línea base para futuras mejoras.

La investigación es correlacional ya que busca explorar las relaciones entre variables clave. Aunque no se pretende establecer causalidad, el análisis permite identificar patrones que fundamentan el diseño de estrategias y recomendaciones. La correlación facilita una comprensión más profunda de cómo interactúan los factores organizacionales y técnicos dentro del ciclo de vida de los proyectos TI.

Las principales variables consideradas en el estudio se definen a continuación:

Madurez en la gestión de proyectos TI: Evalúa el grado de formalización, estandarización y optimización de los procesos de gestión de proyectos en OSP INTERNATIONAL CALA S.A.S. Es coherente con el objetivo de analizar el impacto de la falta de integración de la seguridad en la gestión de proyectos y permite identificar brechas estructurales.

Controles de seguridad de la información: Grado en el que se han implementado medidas técnicas y organizativas (según ISO 27001, NIST o COBIT) en las distintas fases del ciclo de vida del proyecto. Directamente relacionado con el diseño de estrategias de integración de seguridad en el ciclo de vida del proyecto.

Percepción de cumplimiento normativo: Opinión del personal técnico y directivo sobre el cumplimiento de la empresa con normas locales (como la Ley 1581 de 2012 en Colombia) e internacionales. Aporta una dimensión subjetiva elemental para interpretar el compromiso regulatorio, alineado con el objetivo de garantizar cumplimiento normativo.

Adopción de metodologías de gestión de proyectos: Evalúa qué marcos de trabajo se utilizan (ágiles, tradicionales, híbridos), su grado de formalidad y su relación con la gestión de seguridad. Responde al objetivo de evaluar la efectividad de metodologías en la mitigación de riesgos de seguridad.

Frecuencia e impacto de incidentes de seguridad: Registro de eventos adversos relacionados con la seguridad en proyectos TI (pérdida de datos, accesos no autorizados, etc.) y su efecto operativo. Esta variable sirve para evaluar riesgos y brechas existentes.

Cultura de seguridad de la información: Conjunto de creencias, actitudes y comportamientos del personal respecto a la protección de datos e información sensible. Es un factor cualitativo para medir el éxito de la sostenibilidad del modelo propuesto; asociado a la alineación estratégica y cambio organizacional.

Enfoque metodológico

El presente estudio adopta un enfoque metodológico mixto, al integrar elementos cuantitativos y cualitativos. Según el problema de investigación propuesto, se exige comprender no solo la frecuencia y relación entre variables como la madurez en gestión de proyectos o la implementación de controles de seguridad (cuantitativo), sino también

explorar percepciones, barreras y facilitadores en el contexto organizacional (cualitativo). Teniendo en cuenta lo anterior, el enfoque mixto permite generar una visión integral y contextualizada que articula evidencias estadísticas con interpretaciones para sustentar el diseño de un modelo aplicable en la empresa OSP INTERNATIONAL CALA S.A.S.

Tipo de estudio

Este trabajo se desarrolla bajo la modalidad de un estudio de caso único, centrado en la empresa OSP INTERNATIONAL CALA S.A.S, lo cual permite un análisis detallado y contextualizado de su realidad organizacional en materia de gestión de proyectos TI y seguridad de la información. El estudio tiene un alcance transversal, dado que la recolección de datos se realizará en un solo punto en el tiempo, facilitando un diagnóstico situacional sin necesidad de seguimiento longitudinal. Además, incorpora un enfoque prospectivo, en la medida en que los resultados permitirán proyectar estrategias y diseñar un modelo aplicable a futuros proyectos. También, el modelo permite las mejoras en términos de continuidad operativa y cumplimiento normativo.

Método

El método adoptado para esta investigación es de carácter observacional, con apoyo en las estrategias documental y de campo. Se opta por una aproximación no experimental, en la que los fenómenos se analizan tal como ocurren en su contexto natural, sin manipulación de variables. El componente documental permitirá examinar políticas internas, auditorías, lecciones aprendidas y registros de proyectos previos, mientras que el trabajo de campo incluirá la aplicación de encuestas y entrevistas a personal clave de la organización. Como se mencionó anteriormente, esta combinación resulta adecuada para desarrollar datos objetivos e interpretaciones cualitativas, con el propósito de tener una base sólida para el diseño del modelo de integración propuesto.

Población y muestra

La población objeto de estudio está conformada por los colaboradores de OSP INTERNATIONAL CALA S.A.S vinculados directamente a los procesos de gestión de proyectos TI y seguridad de la información. Se considera el personal de áreas técnicas como el desarrollo de software, soporte técnico, gestión documental, automatización e infraestructura TI. También se considera al personal que participa en procesos de toma de decisiones estratégicas o que tiene responsabilidad sobre la implementación de controles de seguridad y cumplimiento normativo.

Dado que se trata de un estudio de caso único con enfoque mixto y alcance aplicado, se utilizará un muestreo probabilístico simple y no probabilístico por criterio o juicio. La selección del segundo tipo de muestreo se justifica en seleccionar intencionadamente a aquellos participantes que poseen conocimientos, experiencia o responsabilidades clave en relación con las variables de interés del estudio. Se priorizarán colaboradores con roles directivos, técnicos y operativos que intervienen en las fases del ciclo de vida de los proyectos TI y que pueden aportar información relevante sobre las prácticas actuales y las oportunidades de mejora.

Muestreo probabilístico simple

El muestreo probabilístico simple permitirá obtener una muestra representativa de la población, lo que facilitará la generalización de los hallazgos cuantitativos a la totalidad de los colaboradores relevantes dentro de la empresa.

Tamaño de la Población (N): 57 colaboradores de la empresa.

Nivel de Confianza Z (1 - α): 95% (Alpha = 0.05).

Margen de error (e): Error esperado 10%

Proporción estimada (P): 41/57 = 0,72 colaboradores de la empresa vinculados directamente a los procesos de gestión de proyectos TI y seguridad de la información. Así mismo, se identificó que la población se encuentra organizada en tres grandes

grupos según la naturaleza de sus funciones, se aplicó una asignación proporcional de la muestra a cada estrato:

Técnicos / Desarrollo / Soporte / QA / Analistas: 41 personas

Administrativos / Archivo / Bodega / Contabilidad / Auxiliares: 12 personas

Gerencia / Jefaturas / Dirección: 4 personas

Figura 3.

Cálculo del tamaño de la muestra.

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{e^2(N-1) + Z^2 \cdot p \cdot q}$$

$$n = \frac{57 \cdot (1.96)^2 \cdot 0.72 \cdot 0.28}{0.1^2(57-1) + (1.96)^2 \cdot 0.72 \cdot 0.28} \approx \frac{58.07}{1.76} \approx 33$$

Nota. Elaboración propia procesado con lenguaje de programación Latex.

Tamaño de muestra

El tamaño de muestra calculado es de aproximadamente 33 personas para obtener resultados representativos de la población objetivo (57 personas), con un nivel de confianza del 95%, un margen de error del 10%, y una proporción estimada del 72% de participación directa en los procesos relevantes. Sin embargo, dado que la población total es pequeña y accesible, se optó por aplicar la encuesta a la totalidad de los colaboradores (censo completo).

Muestreo No probabilístico por criterio o juicio

Paralelamente al muestreo probabilístico, se empleará un muestreo no probabilístico por criterio o juicio para la selección de participantes en la fase cualitativa del estudio. De acuerdo con este método, se seleccionarán intencionadamente aquellos colaboradores

que poseen conocimientos, experiencia o responsabilidades clave en relación con las variables de interés del estudio.

Criterios de Selección

Los participantes para la fase cualitativa serán seleccionados en base a los siguientes criterios:

Rol y Nivel Jerárquico: Se incluirán colaboradores en roles directivos para comprender la visión estratégica, roles técnicos para conocer las prácticas operativas y los desafíos técnicos, y roles operativos para entender la implementación y el impacto en el día a día.

Experiencia: Se priorizará a aquellos colaboradores con una trayectoria mayor a 1 año dentro de la empresa y/o experiencia relevante en gestión de proyectos TI y seguridad de la información.

Responsabilidades: Se seleccionarán personas que tengan responsabilidades directas en la toma de decisiones estratégicas, la implementación de controles de seguridad, la gestión de proyectos críticos o la supervisión de áreas técnicas relevantes.

Conocimiento Específico: Se buscará la participación de colaboradores que posean un conocimiento profundo sobre los procesos, las herramientas, las políticas y los desafíos relacionados con las variables de interés del estudio.

El tamaño de la muestra para la fase cualitativa se determinará por saturación teórica, es decir, hasta que la información obtenida no revele nuevas perspectivas o temas relevantes para la investigación. Se estima inicialmente la participación de 6 a 9 colaboradores que puede ser ajustado según el desarrollo de la relación de datos.

Técnicas e instrumentos de recolección de información

Para garantizar la validez y confiabilidad de los datos que sustenten el diagnóstico y el diseño del modelo propuesto, se emplearán técnicas de investigación cualitativa y cuantitativa.

Tabla 3.

Técnicas e instrumentos para la recolección de datos.

Técnica	Instrumento	Variables / categorías clave
Encuesta online (Likert 1-5).	Cuestionario adaptado de CMMI-DEV & ISO 27001.	• Nivel de madurez de gestión de proyectos • Controles de seguridad implementados • Percepción de riesgos.
Entrevistas semiestructuradas.	Guion con 10-12 preguntas abiertas.	• Barreras y facilitadores • Cultura de seguridad • Expectativas sobre el modelo
Revisión documental.	Matriz de extracción.	• Políticas, procedimientos, informes de auditoría TI • Lecciones aprendidas de proyectos previos.
Observación no participante.	Lista de verificación en reuniones de proyecto.	• Prácticas reales de integración de seguridad en cada fase PMBOK/ágil.

Nota. Elaboración propia. Los instrumentos diseñados para la recolección de información (cuestionario, guía de entrevista, matriz documental y lista de verificación) se presentan en detalle en los anexos del documento.

Técnica de análisis de datos

Además de las técnicas anteriormente descritas, se incorporarán los siguientes criterios y estrategias complementarias para reforzar la calidad metodológica del estudio:

1. Validación de encuesta: Para el cuestionario cuantitativo, se tomará una prueba piloto con una muestra reducida (n=5) para verificar la claridad, relevancia y confiabilidad de las preguntas. A partir de esta aplicación preliminar, se realizaron ajustes menores en la redacción de algunas preguntas para mejorar su interpretación. Posteriormente, se calculará el alfa de Cronbach para garantizar consistencia interna del instrumento.

2. Análisis comparativo por roles: Dado que los participantes ocupan diferentes niveles jerárquicos (directivos, técnicos, operativos), se realizará un análisis comparativo de respuestas por tipo de rol. Esto permitirá identificar posibles brechas o divergencias en la percepción de la seguridad de la información y su integración en los proyectos TI.
3. Codificación cualitativa: Las entrevistas semiestructuradas serán transcritas y analizadas mediante codificación temática. Se utilizará codificación doble (dos investigadores) y se calculará el coeficiente Kappa de Cohen o el acuerdo intercodificador (≥ 0.8) para asegurar objetividad en el análisis de las categorías emergentes.
4. Inclusión de bitácora de campo: Durante la aplicación de entrevistas, se mantendrá una bitácora de campo en la que se registrarán impresiones del investigador, incidentes durante la recolección de datos y reflexiones analíticas preliminares. Esta práctica cualitativa permitirá capturar información contextual que complemente los datos explícitamente recogidos.
5. Triangulación metodológica: Se aplicará una triangulación de tipo metodológica y de fuentes para contrastar los hallazgos cualitativos y cuantitativos, asegurando la validez de los resultados. Por ejemplo, las percepciones recogidas en entrevistas se contrastarán con evidencia documental y datos de encuestas. Esta estrategia contribuirá a reducir sesgos y aumentar la credibilidad del análisis.
6. Validación del modelo: El modelo de integración de seguridad de la información en la gestión de proyectos TI será sometido a un proceso de

validación de contenido por juicio de expertos en gestión de proyectos y seguridad de la información.

Fases del proceso metodológico

A continuación, se presenta la estructura metodológica del estudio, organizada en seis fases secuenciales que guían el desarrollo del proyecto de intervención. Cada etapa responde a una lógica progresiva, asegurando la coherencia entre los objetivos del proyecto, la participación de los actores clave y la rigurosidad en la recolección, análisis e interpretación de la información. La ruta metodológica inicia con la planificación, el aval institucional y la sensibilización organizacional, continúa con la captación de participantes y la aplicación de instrumentos de recolección de datos tanto cuantitativos como cualitativos. Posteriormente, se realiza el análisis, la triangulación de resultados y el diseño del modelo de integración, que será sometido a validación técnica. Finalmente, se incluye una fase de evaluación del impacto, seguimiento y socialización de resultados, buscando garantizar la aplicabilidad, pertinencia y sostenibilidad de la propuesta.

Figura 4.

Fases del proceso metodológico.

Nombre	Duracion	Inicio	Terminado	Predecesores
Cronograma OSP - Medologico	186 da...	14/7/25, 8:00	8/4/26, 17:00	
Fase 1. Planificación, aval, sensibilización	3 days?	14/7/25, 8:00	16/7/25, 17...	
Socialización del proyecto (Alta dirección y líderes)	1 day?	14/7/25, 8:00	14/7/25, 17:00	
Solicitud y obtención del aval	2 days	15/7/25, 8:00	16/7/25, 17:00	3
Documentación de desiciones metodológicas	1 day?	15/7/25, 8:00	15/7/25, 17:00	3
Fase 2. Captación	2 days?	17/7/25, 8:00	18/7/25, 17...	
Sensibilización alta dirección y personal interno	1 day?	17/7/25, 8:00	17/7/25, 17:00	4
Taller corto de sensibilización en seguridad de la información	1 day?	18/7/25, 8:00	18/7/25, 17:00	7
Fase 3. Recolección de datos (Cuantitativos y Cualitativo	29 days	21/7/25, 8:00	1/9/25, 17:00	
Diseño y validación de instrumentos (Encuestas y guión de e	3 days	21/7/25, 8:00	23/7/25, 17:00	8
Aplicación de encuesta online (Typeform / Google Forms)	10 days	24/7/25, 8:00	6/8/25, 17:00	10
Recordatorio y cierre de encuesta	16 days	7/8/25, 8:00	1/9/25, 17:00	11
Realización de entrevistas semiestructuradas	15 days	24/7/25, 8:00	14/8/25, 17:00	10
Transcripción y organización de entrevistas (asistidas por IA)	2 days	15/8/25, 8:00	19/8/25, 17:00	13
Observación no participante en reuniones clave	2 days	24/7/25, 8:00	25/7/25, 17:00	10
Revisión documental y extracción sistematica de información	2 days	20/8/25, 8:00	21/8/25, 17:00	14
Fase 4. Análisis de datos y triangulación	8 days?	22/8/25, 8:00	2/9/25, 17:00	
Análisis estadístico de encuestas	3 days	22/8/25, 8:00	26/8/25, 17:00	16
Análisis temático de entrevistas y observaciones	3 days	22/8/25, 8:00	26/8/25, 17:00	16
Preparación de datos para análisis estadístico (SPSS)	2 days	22/8/25, 8:00	25/8/25, 17:00	16
Análisis estadístico descriptivo (SPSS)	1 day?	26/8/25, 8:00	26/8/25, 17:00	20
Pruebas de correlación de variables (SPSS)	2 days	27/8/25, 8:00	28/8/25, 17:00	21
Triangulación convergente de resultados	3 days	29/8/25, 8:00	2/9/25, 17:00	22
Fase 5. Diseño y validación del modelo de integración	23 days?	3/9/25, 8:00	3/10/25, 17...	
Workshop participativo para diseño preliminar del modelo	5 days	3/9/25, 8:00	9/9/25, 17:00	23
Definición de indicadores SMART para validación	5 days	10/9/25, 8:00	16/9/25, 17:00	25
Validación interna del modelo (Tecnica Delphi) sesión 1	1 day?	17/9/25, 8:00	17/9/25, 17:00	26
Validación interna del modelo (Tecnica Delphi) sesión 2	1 day?	19/9/25, 8:00	19/9/25, 17:00	27
Ajuste final del modelo	10 days	22/9/25, 8:00	3/10/25, 17:00	28
Fase 6. Evaluación del impacto y seguimiento	128 days	6/10/25, 8:00	8/4/26, 17:00	
Aplicación de pre-test/post-test de KPIs de proyectos TI	15 days	6/10/25, 8:00	27/10/25, 17:00	29
Medición de impacto en la implementación del modelo	3 days	28/10/25, 8:00	30/10/25, 17:00	31
Planificación de seguimiento longitudinal	3 days	31/10/25, 8:00	5/11/25, 17:00	32
Proyección segundo seguimiento (6 meses)	3 days	6/4/26, 8:00	8/4/26, 17:00	33
Fase 7. Documentación y Socialización	6 days?	6/11/25, 8:00	13/11/25, 1...	
Redacción del informe final	5 days	6/11/25, 8:00	12/11/25, 17:00	33
Socialización de resultados con alta dirección y equipos	1 day?	13/11/25, 8:00	13/11/25, 17:00	36

Nota. Elaboración propia en Project.

De acuerdo con la imagen anterior, se observa que en la fase 6 se ha incorporado una actividad adicional correspondiente a un segundo seguimiento, programado para realizarse seis meses después de la entrega de los resultados a la alta dirección. Esta actividad fue incluida a solicitud expresa de la empresa, con el fin de evaluar la sostenibilidad y aplicación práctica del modelo propuesto. No obstante, los resultados de dicho seguimiento no serán contemplados en el presente trabajo de investigación, ya que se encuentran fuera del cronograma definido para la ejecución del proyecto. Los resultados completos, se pueden visualizar en el Project adjunto, (ver Anexo 1).

Consideración y limitaciones del diseño.

Para el desarrollo del presente estudio se atenderá los principios éticos fundamentales y tendrá en cuenta las limitaciones prácticas que se pueden derivar del contexto organizacional. La implementación de las técnicas de recolección y análisis de la información, se regirán a través de lineamientos éticos y metodológicos que aseguren la protección e integridad de los datos obtenidos.

Consideraciones éticas.

- **Consentimiento informado**: Previo a la participación en encuestas o entrevistas, los colaboradores serán informados sobre el propósito del estudio, su carácter voluntario, el manejo confidencial de la información y la posibilidad de retirarse en cualquier momento.
- **Anonimato**: Para preservar la privacidad de los participantes, se aplicará un sistema de codificación alfanumérica en los registros, evitando la exposición de nombres o cargos en los informes.
- **Custodia segura de la información**: Toda la información recolectada se almacenará en medios digitales protegidos con acceso restringido exclusivamente a los investigadores.

- **Cumplimiento legal:** Se acatarán los lineamientos de la Ley 1581 de 2012 y el Decreto 1377 de 2013, referentes a la protección de datos personales en Colombia. La información será utilizada exclusivamente con fines académicos, en el marco del proyecto de intervención empresarial.
- **Principio de no daño:** Se garantizará que la participación en el estudio no represente riesgo alguno para los colaboradores ni afecte sus condiciones laborales. No se evaluarán desempeños individuales ni se emitirán juicios sobre su conducta profesional.
- **Libre retiro**: Cualquier persona podrá abstenerse o retirarse del proceso de recolección de información sin necesidad de justificar su decisión y sin que esto implique consecuencias para su relación con la empresa.

Limitaciones del diseño metodológico

- **Alta carga operativa del personal:** Una de las principales restricciones previstas en la ejecución del estudio es la limitada disponibilidad del talento humano de OSP INTERNATIONAL CALA S.A.S., debido a la alta carga operativa diaria. Esta novedad puede dificultar la participación oportuna y completa en entrevistas, encuestas y sesiones de observación. Para mitigar el riesgo, se planificaran las actividades con antelación, se dispondrá de espacios cortos, y se ofrecerán facilidades de diligenciamiento de la información a través de formatos digitales.
- **Cambios organizacionales imprevistos**: La dinámica empresarial puede generar modificaciones en la disponibilidad de equipos, cronogramas o recursos durante el desarrollo del estudio. Aplica la estrategia mencionada anteriormente con la comunicación constante con la alta dirección para facilitar la continuidad del proceso.

- **Acceso de documentación sensible:** Dada la naturaleza del estudio, algunos documentos pueden estar sujetos a restricciones de confidencialidad interna.
- **Sesgos de deseabilidad social corporativa:** Existe el riesgo de que algunos participantes proporcionen respuestas socialmente aceptables o alineadas con lo que se espera institucionalmente, lo cual podría afectar la objetividad de los datos. Para mitigar este sesgo, se garantizará el anonimato, se utilizarán preguntas indirectas y se validará la información mediante múltiples fuentes.

Contribuciones originales esperadas

El presente trabajo aporta contribuciones en cuatro dimensiones. A nivel organizacional, el modelo propuesto ofrece una solución para OSP INTERNATIONAL CALA S.A.S., basada en una arquitectura por capas (gobernanza, gestión metodológica y operación técnica). Este enfoque mejora la trazabilidad de los controles de seguridad mediante Security Gates, matriz de trazabilidad y baseline mínimo obligatorio, y refuerza el cumplimiento normativo a través de ISO/IEC 27001, NIST e ISO 27034.

Además, aborda el subregistro de incidentes identificado en el diagnóstico, e integra la seguridad como criterio verificable en la gestión de proyectos, con una disminución estimada del 30% en los costos asociados a reprocesos e incidentes. A nivel sectorial, es un referente transferible para PyMEs del sector TIC colombiano que facilita su adopción progresiva.

En términos de conocimiento, el trabajo integra ISO/IEC 27001, enfoques DevSecOps (automatización de pruebas en CI/CD) y metodologías ágiles e híbridas, validadas mediante técnica Delphi, como aporte a la gerencia de sistemas de información. A nivel social, fortalece el empleo en el sector TI, promueve competencias transversales en seguridad de la información y fomenta una cultura de protección de activos digitales.

Finalmente, se evidencia la aplicación de conocimientos de la Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos: gobernabilidad y buenas prácticas en TI, gestión de riesgos, aseguramiento de la información, gestión del ciclo de vida de proyectos (PMI), estándares de calidad y seguridad (ISO) y gestión de stakeholders mediante validación Delphi, reflejado en la articulación entre formación académica y solución de problemáticas organizacionales reales.

Diagnóstico Organizacional

El diagnóstico organizacional se desarrolló en coherencia con el enfoque metodológico mixto, estructurado en etapas secuenciales que permitieron asegurar la rigurosidad y validez de los resultados. Previo a la recolección de la información, se obtuvo la autorización formal por parte de la empresa para la ejecución del estudio (ver Anexo 2). Posteriormente, se llevó a cabo un taller de sensibilización en seguridad de la información, con el propósito de contextualizar a los participantes y fortalecer la calidad de sus aportes (ver Anexo 3).

Una vez realizada la motivación, se desarrolló la fase de recolección de información mediante la aplicación de técnicas cuantitativas y cualitativas, que incluyeron encuesta tipo Likert fundamentadas en referentes como CMMI-DEV e ISO 27001, entrevistas semiestructuradas aplicadas a una muestra seleccionada mediante muestreo no probabilístico por criterio, así como revisión documental y observación no participante. En primer lugar, se llevó a cabo la planificación del proceso y la definición de la población objetivo, conformada por 57 colaboradores para la aplicabilidad técnica cuantitativa (encuesta). Aunque inicialmente se planteó un censo completo, se obtuvo una participación efectiva de 45 respuestas.

En la fase cualitativa, los participantes fueron seleccionados de manera intencional con base en su rol, experiencia, responsabilidades y nivel de conocimiento, logrando la participación de seis colaboradores, sin embargo, debido a limitaciones en la disponibilidad del personal y restricciones organizacionales de la empresa, no fue posible ampliar la muestra, por lo que no se alcanzó la saturación teórica.

De manera posterior, se realizó el análisis de la información mediante estrategias como la triangulación metodológica y de fuentes, la codificación temática con validación

intercodificador y el análisis comparativo por niveles jerárquicos. Este proceso fue complementado con la validación de instrumentos y el registro en bitácora de campo. Finalmente, los hallazgos obtenidos permitieron consolidar un diagnóstico integral que sirvió como base para el diseño y validación del modelo propuesto, garantizando la pertinencia y alineación con las necesidades identificadas.

Procesamiento estadístico de datos

Encuesta online (Likert 1-5).

En el componente cuantitativo, correspondiente a la encuesta tipo Likert compuesta por 45 ítems, se inició con la validación del instrumento mediante el análisis de su confiabilidad interna, con el propósito de garantizar que las preguntas diseñadas midieran de manera consistente la gestión de la seguridad de la información. Para ello, se aplicó el coeficiente alfa de Cronbach, el cual permite evaluar el grado de correlación entre los ítems del instrumento, determinando si estos presentan coherencia y homogeneidad con la medición objeto de estudio.

El procesamiento estadístico se realizó mediante el software IBM SPSS Statistics (versión 27.0.1). Inicialmente, se llevó a cabo la depuración de la base de datos, se verificó la existencia de valores atípicos, datos faltantes y posibles inconsistencias en la digitación. Dado que la recolección se efectuó a través de un formulario digital, no se evidenciaron errores de registro; sin embargo, se realizó la revisión general de las respuestas obtenidas para garantizar la integridad de la información.

Posteriormente, se efectuó la codificación de las variables, asignando valores numéricos a cada una de las opciones de respuesta de la escala Likert (1 = Nunca, 2 = Raramente, 3 = Ocasionalmente, 4 = Frecuentemente, 5 = Siempre). Esta estandarización permitió la aplicación de técnicas estadísticas descriptivas y el análisis de consistencia interna del instrumento.

Para ello, se aplicó el coeficiente alfa de Cronbach, el cual permite evaluar el grado de correlación entre los ítems del instrumento, determinando si estos presentan coherencia y homogeneidad con la medición objeto de estudio (Cronbach, 1951). De acuerdo con criterios ampliamente aceptados en la literatura, valores iguales o superiores a 0,70 indican un nivel adecuado de consistencia interna (Hair et al., 2014). El alfa de Cronbach se calcula como:

$$\alpha = \frac{k}{k-1}\left(1-\frac{\sum Var(i)}{Var(total)}\right)$$

Donde:

- k= número de ítems
- $Var(i)$= varianza de cada ítem
- $Var(total)$= varianza del puntaje total

Figura 5.

Resultado alfa de Cronbach

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	45	100,0
	Excluido[a]	0	,0
	Total	45	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,918	40

Nota. Elaboración propia con base en el análisis de confiabilidad interna mediante el coeficiente alfa de Cronbach, realizado en IBM SPSS Statistics (versión 27.0.1), a partir de las respuestas del cuestionario tipo Likert aplicado (n = 45). Para el cálculo del coeficiente, se consideraron únicamente los ítems de la escala Likert, excluyendo las preguntas de caracterización (ítems 1 a 4) y la pregunta abierta final, por no corresponder al constructo evaluado ni presentar una escala homogénea de medición. En consecuencia, el análisis se realizó sobre un total de 40 ítems.

En relación con la confiabilidad, el coeficiente alfa de Cronbach obtenido fue de 0,918, lo cual indica un nivel de consistencia interna excelente, de acuerdo con los criterios establecidos en la literatura. Este resultado evidencia que los ítems del instrumento presentan una alta correlación y contribuyen de manera coherente a la medición del constructo evaluado.

De manera complementaria, se realizó un análisis exploratorio de los ítems, revisando su comportamiento estadístico general; no obstante, no fue necesario eliminar ítems, manteniéndose la estructura original del cuestionario para el análisis posterior.

Una vez validado el instrumento, se procedió al procesamiento de los ítems correspondientes a la escala Likert, con base en las 45 respuestas válidas disponibles. El análisis se desarrolla en dos niveles: descriptivo (frecuencias, porcentajes, medidas de tendencia central y gráficos por pregunta) y analítico (construcción de índices por componente, lectura organizacional y síntesis de brechas). Se verificó la consistencia de la base de datos, observándose 45 registros completos para cada uno de los ítems analizados. Los resultados fueron organizados en tablas y representados mediante gráficos, facilitando la visualización de la distribución de las respuestas.

Es importante precisar que variables como la marca temporal y la dirección de correo electrónico fueron consideradas únicamente como datos de control del instrumento,

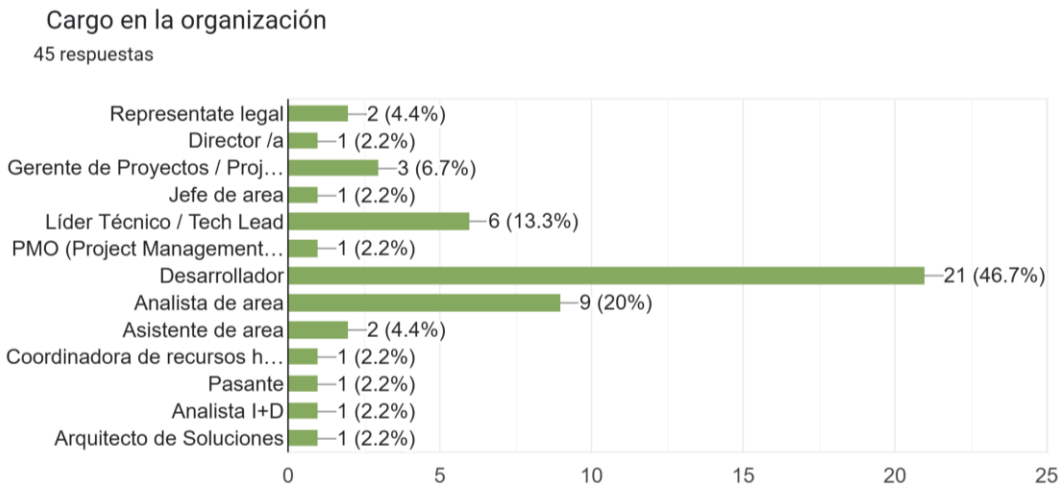
utilizados para la validación del registro y la trazabilidad de la información, por lo que no hicieron parte del análisis estadístico ni del proceso de caracterización de la muestra.

Datos de caracterización.

Este componente tiene como propósito describir las características generales de los participantes y contextualizar los resultados del estudio; por tanto, no genera índices cuantitativos ni hace parte del cálculo de confiabilidad del instrumento.

Figura 6.

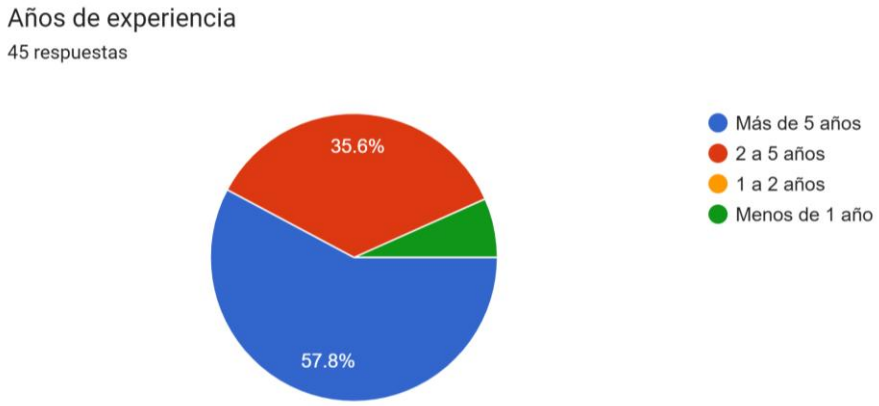
Pregunta 1. Cargo en la organización



La distribución de los participantes evidencia una alta concentración en roles operativos y técnicos, especialmente desarrolladores (46,7%) y analistas (20%), lo que sugiere que la percepción sobre la integración de la seguridad de la información está principalmente influenciada por quienes ejecutan directamente los proyectos. Esta configuración puede generar un sesgo hacia aspectos técnicos, limitando la visión estratégica y de gobernanza, lo cual resulta relevante al interpretar los resultados relacionados con riesgo, cultura y madurez organizacional.

Figura 7.

Pregunta 2. Años de experiencia



Los resultados evidencian que el 93,4% de los participantes cuenta con más de dos años de experiencia en proyectos TI, destacándose un 57,8% con más de cinco años. Esto indica que la muestra está compuesta principalmente por personal altamente experimentado, lo cual fortalece la confiabilidad de los resultados. Sin embargo, la baja representación de perfiles junior puede limitar la diversidad de perspectivas, especialmente en la adopción de nuevas prácticas y enfoques innovadores en seguridad de la información.

Figura 8.

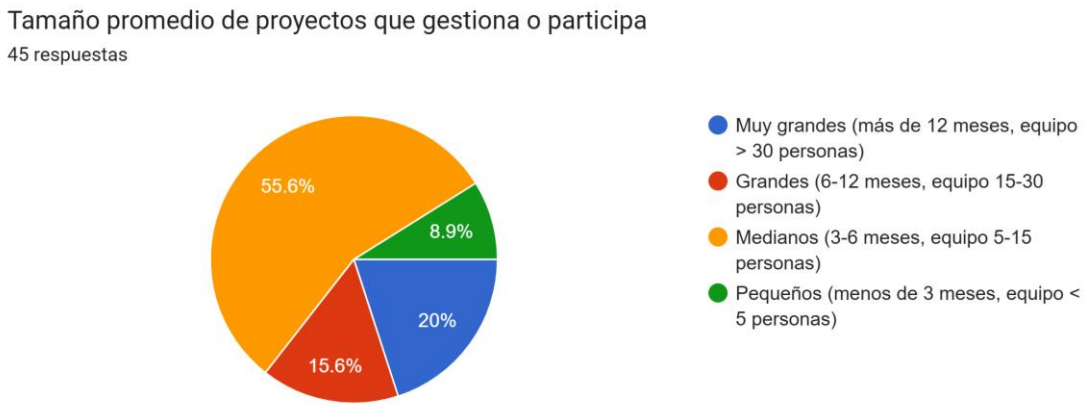
Pregunta 3. Metodología Principal en su Proyecto

Los resultados evidencian que el 46,7% de los participantes utiliza metodologías híbridas, seguido por un 35,6% que emplea enfoques ágiles, lo que refleja una tendencia

hacia modelos de gestión flexibles y adaptativos. Este escenario favorece la integración continua de la seguridad de la información; no obstante, también plantea desafíos en términos de control, estandarización y formalización de prácticas, especialmente si no se cuenta con un enfoque estructurado como DevSecOps.

Figura 9.

Pregunta 4. Tamaño promedio de proyectos que gestiona o participa



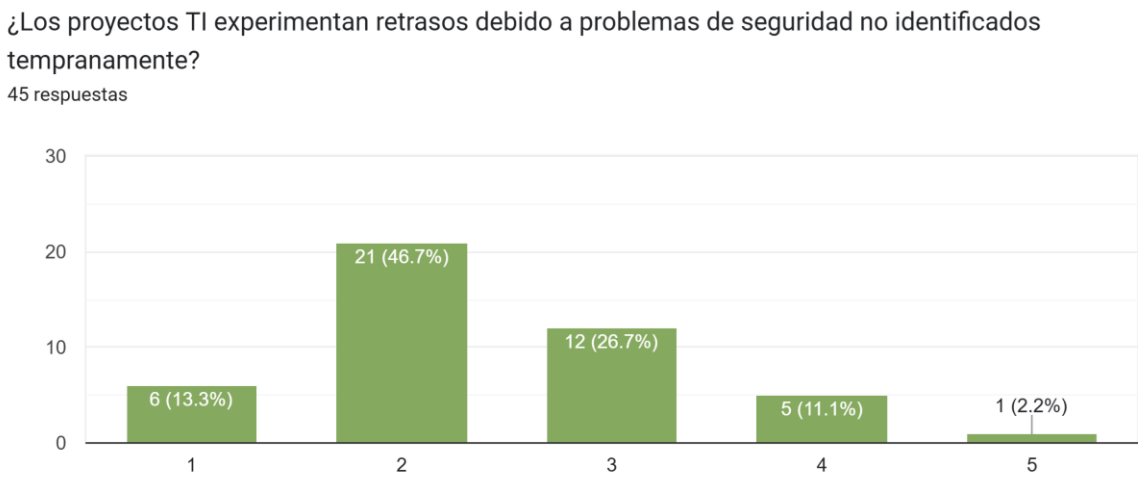
Los resultados muestran que el 55,6% de los participantes trabaja en proyectos de tamaño mediano, seguido por un 35,6% en proyectos grandes y muy grandes, lo que evidencia un entorno organizacional caracterizado por una complejidad operativa significativa. Este tipo de proyectos requiere una integración estructurada de la seguridad de la información a lo largo de todo el ciclo de vida; sin embargo, si dicha integración es limitada, se incrementa el riesgo de afectaciones en costos, tiempos y calidad de los entregables.

Datos de medición (Likert).

Impacto de la falta de integración de seguridad

Figura 10.

Pregunta 5. ¿Los proyectos TI experimentan retrasos debido a problemas de seguridad no identificados tempranamente?



La distribución se concentra en las categorías 1 y 2 (60.0%), con una media de 2.42. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel. El resultado favorece al componente «impacto de la falta de integración de seguridad», porque sugiere que los proyectos TI experimentan retrasos debido a problemas de seguridad no identificados tempranamente no constituye una fuente crítica de afectación en la organización.

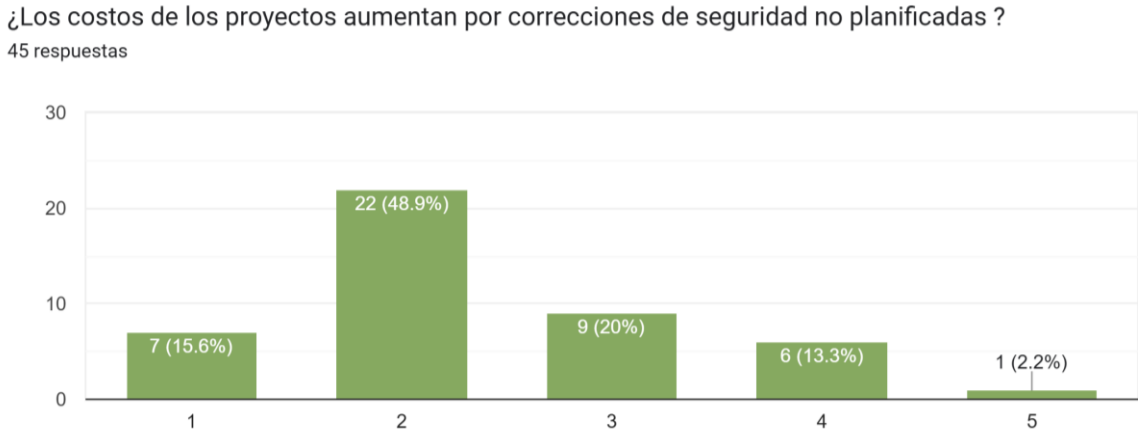
Figura 11.

Pregunta 6. ¿Se detectan vulnerabilidades de seguridad en fases avanzadas del proyecto (Implementación/Producción)?

La distribución se concentra en las categorías 1 y 2 (51.1%), con una media de 2.42. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel. El resultado favorece al componente «impacto de la falta de integración de seguridad», porque sugiere que se detectan vulnerabilidades de seguridad en fases avanzadas del proyecto (Implementación/Producción) no constituye una fuente crítica de afectación en la organización.

Figura 12.

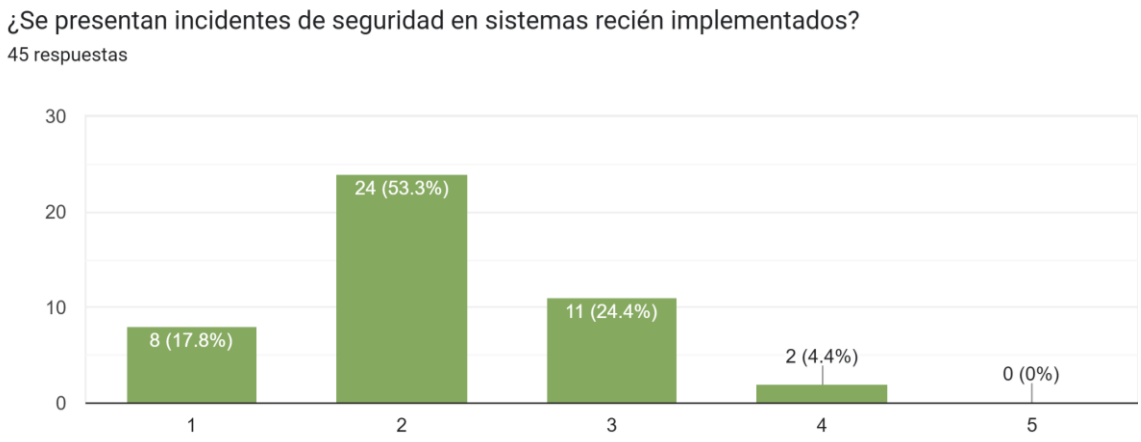
Pregunta 7. ¿Los costos de los proyectos aumentan por correcciones de seguridad no planificadas?



La distribución se concentra en las categorías 1 y 2 (64.5%), con una media de 2.38. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel. El resultado favorece al componente «impacto de la falta de integración de seguridad», porque sugiere que los costos de los proyectos aumentan por correcciones de seguridad no planificadas no constituye una fuente crítica de afectación en la organización.

Figura 13.

Pregunta 8. ¿Se presentan incidentes de seguridad en sistemas recién implementados?

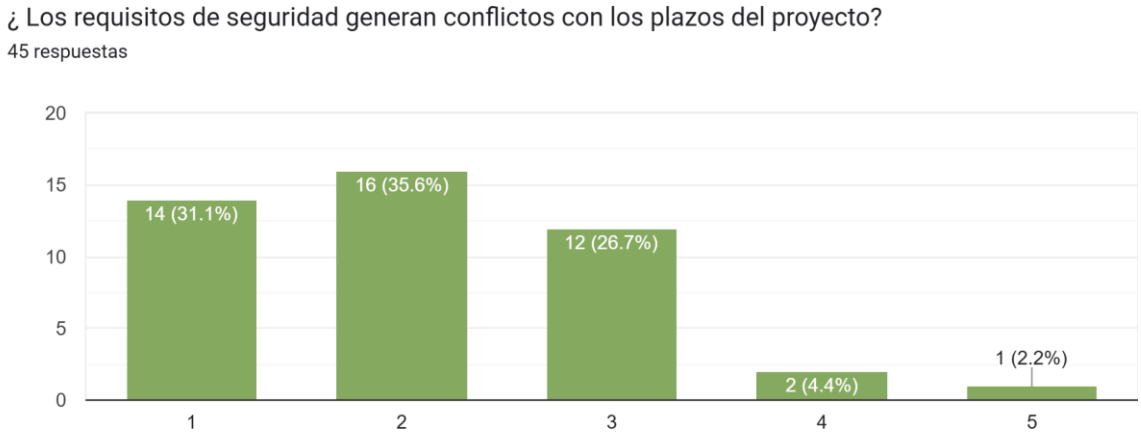


La distribución se concentra en las categorías 1 y 2 (71.1%), con una media de 2.16. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel. El resultado favorece al componente «impacto de la falta de integración de seguridad»,

porque sugiere que se presentan incidentes de seguridad en sistemas recién implementados no constituye una fuente crítica de afectación en la organización.

Figura 14.

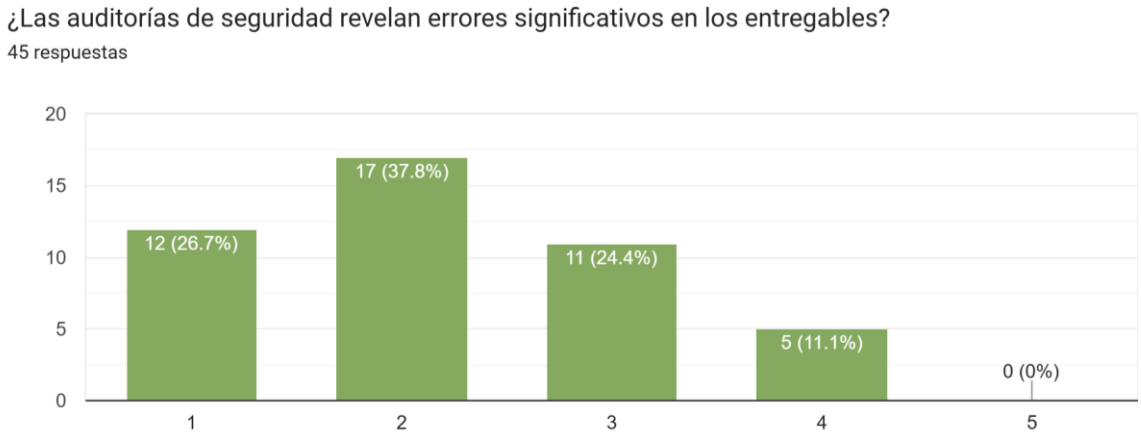
Pregunta 9. ¿Los requisitos de seguridad generan conflictos con los plazos del proyecto?



La distribución se concentra en las categorías 1 y 2 (66.7%), con una media de 2.11. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel. El resultado favorece al componente «impacto de la falta de integración de seguridad», porque sugiere que los requisitos de seguridad generan conflictos con los plazos del proyecto no constituye una fuente crítica de afectación en la organización.

Figura 15.

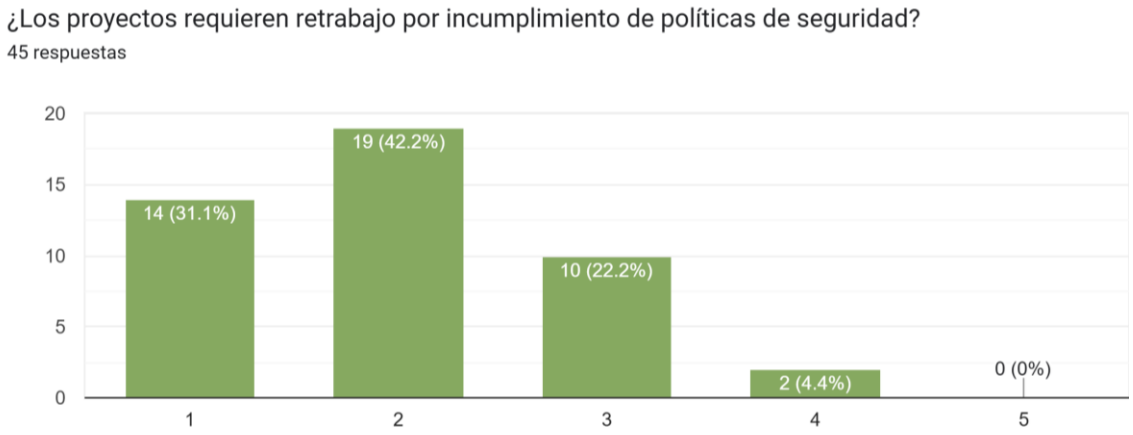
Pregunta 10. ¿Las auditorías de seguridad revelan errores significativos en los entregables?



La distribución se concentra en las categorías 1 y 2 (64.5%), con una media de 2.20. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel. El resultado favorece al componente «impacto de la falta de integración de seguridad», porque sugiere que las auditorías de seguridad revelan errores significativos en los entregables no constituye una fuente crítica de afectación en la organización.

Figura 16.

Pregunta 11. ¿Los proyectos requieren retrabajo por incumplimiento de políticas de seguridad?



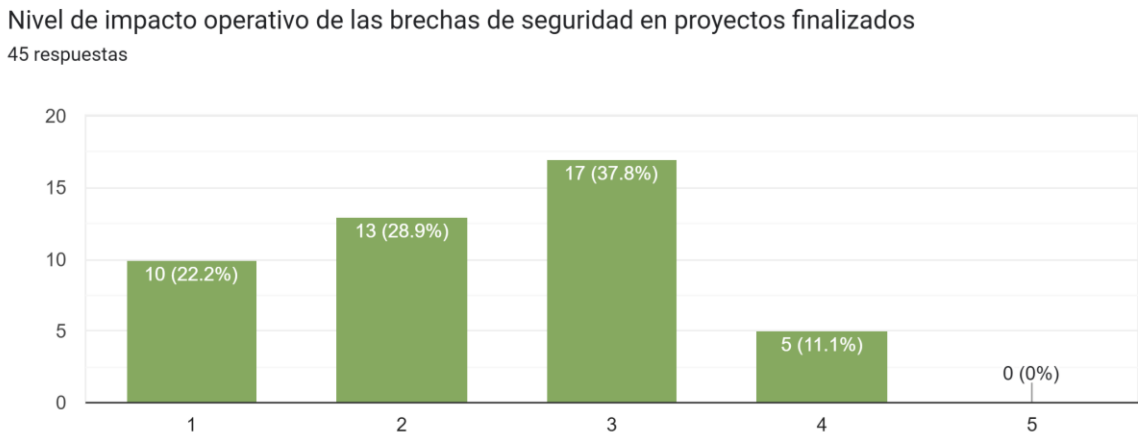
La distribución se concentra en las categorías 1 y 2 (73.3%), con una media de 2.00. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel.

Analíticamente, este resultado favorece al componente «impacto de la falta de integración de seguridad», porque sugiere que los proyectos requieren retrabajo por incumplimiento de políticas de seguridad no constituye una fuente crítica de afectación en la organización.

Nivel Organizacional de Riesgo y Exposición.

Figura 17.

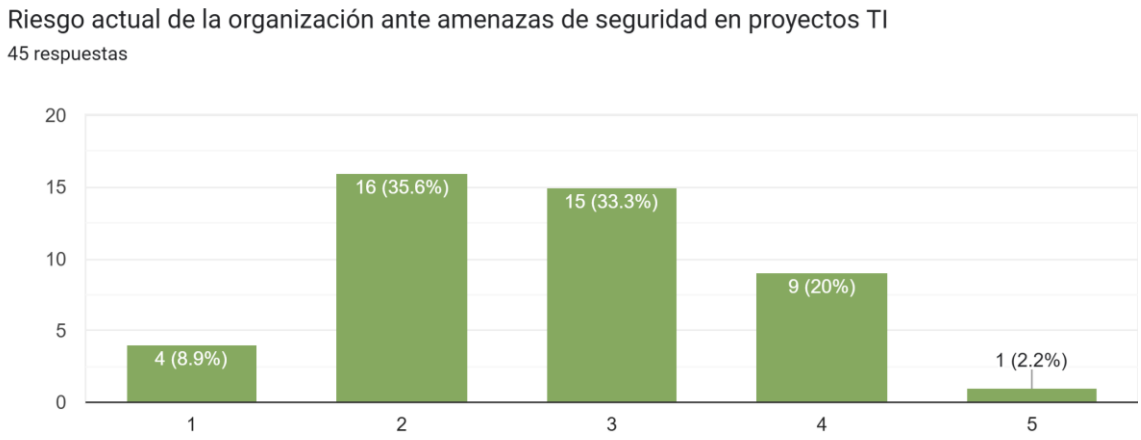
Pregunta 12. Nivel de impacto operativo de las brechas de seguridad en proyectos finalizados



La distribución se concentra en las categorías 1 y 2 (51.1%), con una media de 2.38. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel. El resultado favorece al componente «nivel organizacional de riesgo y exposición», porque sugiere que nivel de impacto operativo de las brechas de seguridad en proyectos finalizados no constituye una fuente crítica de afectación en la organización.

Figura 18.

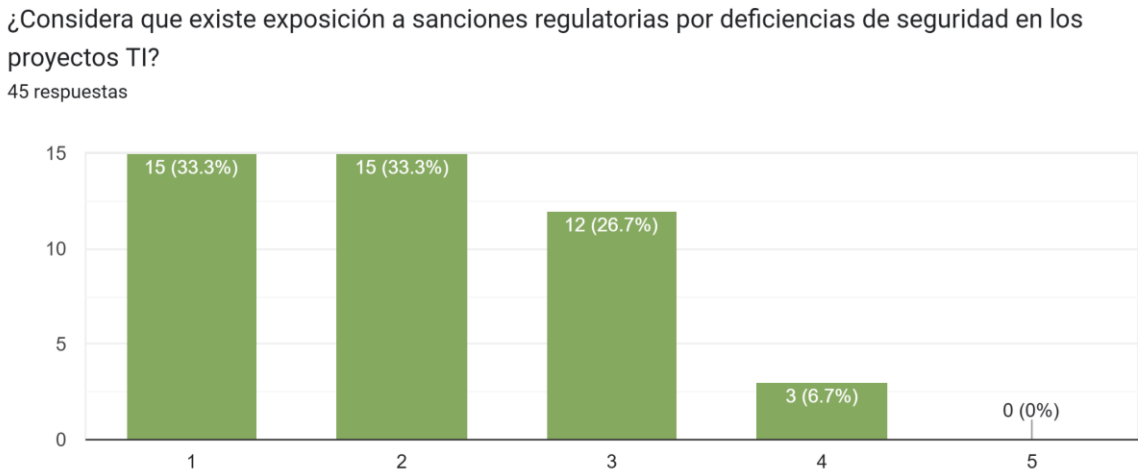
Pregunta 13. Riesgo actual de la organización ante amenazas de seguridad en proyectos TI



Las respuestas muestran una presencia intermedia del fenómeno: 33.3% se ubicó en el valor 3 y la media fue de 2.71. Esto sugiere ocurrencia ocasional o nivel moderado. Desde el plano analítico, el ítem señala una brecha de atención intermedia dentro del componente «nivel organizacional de riesgo y exposición». El comportamiento observado indica que riesgo actual de la organización ante amenazas de seguridad en proyectos TI puede materializarse bajo ciertas condiciones del proyecto y debería tratarse mediante controles tempranos y coordinación transversal.

Figura 19.

Pregunta 14. ¿Considera que existe exposición a sanciones regulatorias por deficiencias de seguridad en los proyectos TI?

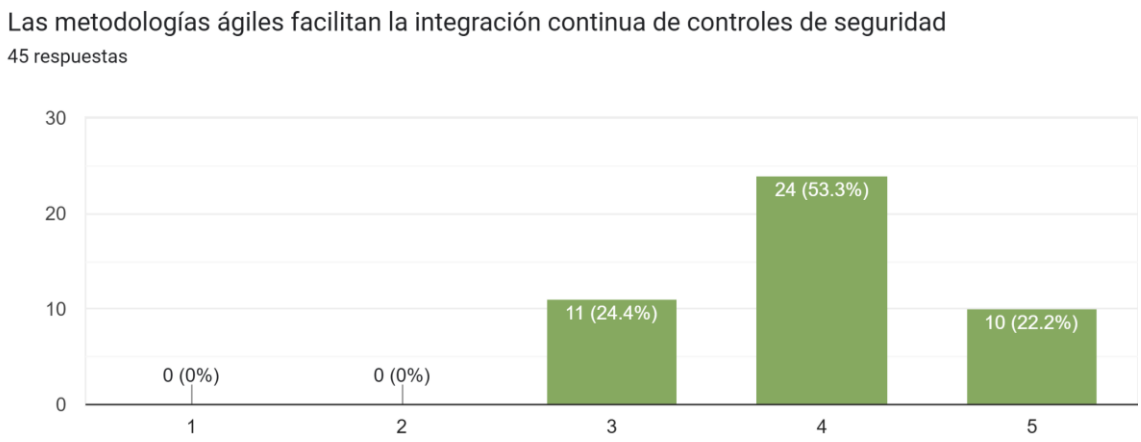


La distribución se concentra en las categorías 1 y 2 (66.6%), con una media de 2.07. Esto indica que la situación evaluada se percibe con baja frecuencia o bajo nivel. El resultado favorece al componente «nivel organizacional de riesgo y exposición», porque sugiere que considera que existe exposición a sanciones regulatorias por deficiencias de seguridad en los proyectos TI no constituye una fuente crítica de afectación en la organización.

Adopción de metodologías y mitigación de riesgos

Figura 20.

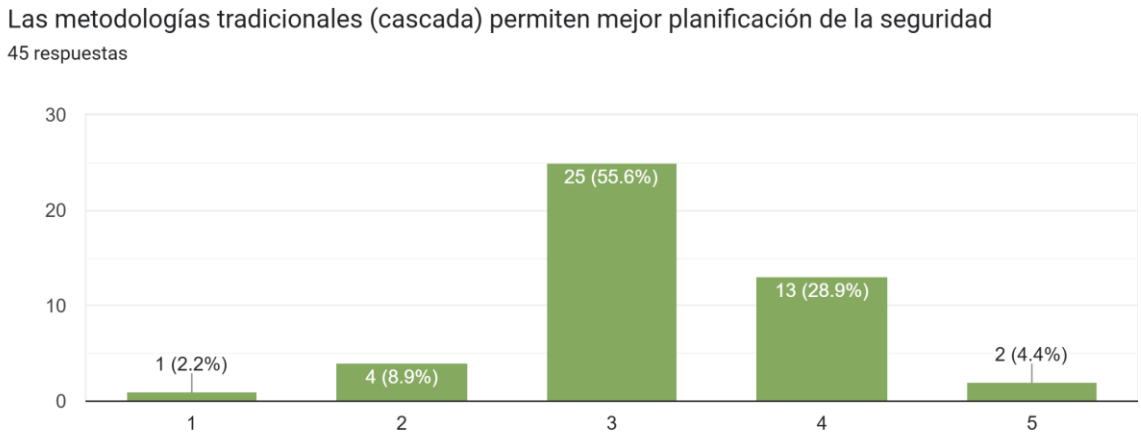
Pregunta 15. ¿Las metodologías ágiles facilitan la integración continua de controles de seguridad?



Predominan las categorías 4 y 5 (75.5%), con una media de 3.98. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «adopción de metodologías y mitigación de riesgos», porque muestra que las metodologías ágiles facilitan la integración continua de controles de seguridad está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 21.

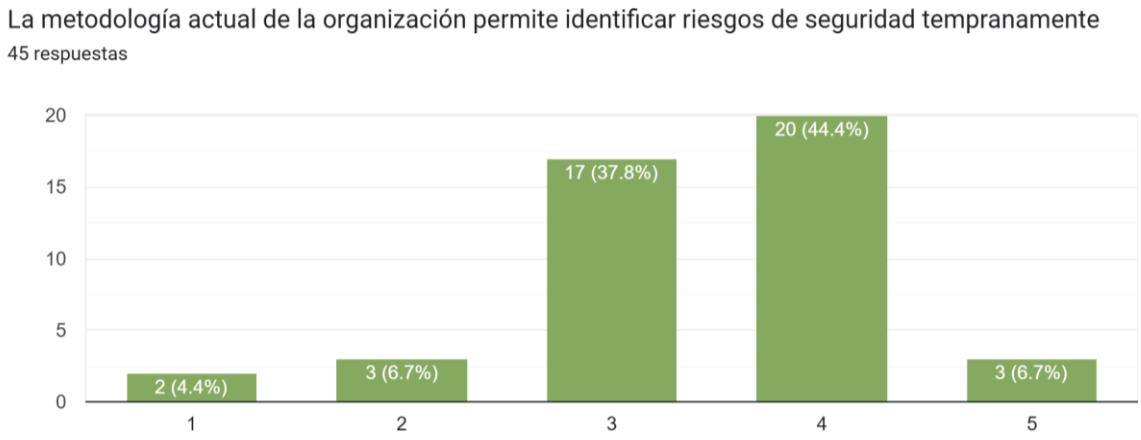
Pregunta 16. Las metodologías tradicionales (cascada) permiten mejor planificación de la seguridad



La distribución se concentra en posiciones intermedias, con 55.6% en la categoría 3 y una media de 3.24. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «adopción de metodologías y mitigación de riesgos». Aunque existe alguna práctica asociada a las metodologías tradicionales (cascada) permiten mejor planificación de la seguridad, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 22.

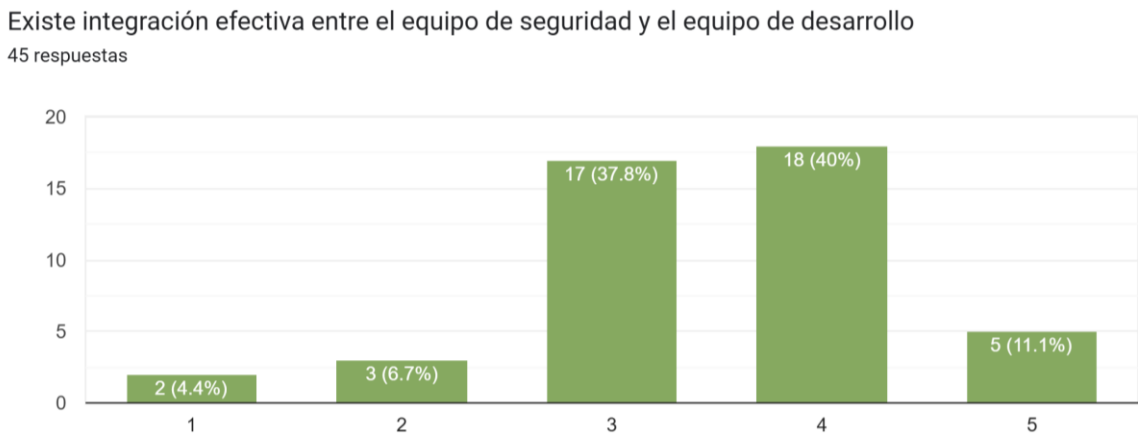
Pregunta 17. La metodología actual de la organización permite identificar riesgos de seguridad tempranamente



La distribución se concentra en posiciones intermedias, con 37.8% en la categoría 3 y una media de 3.42. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «adopción de metodologías y mitigación de riesgos». Aunque existe alguna práctica asociada a la metodología actual de la organización permite identificar riesgos de seguridad tempranamente, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 23.

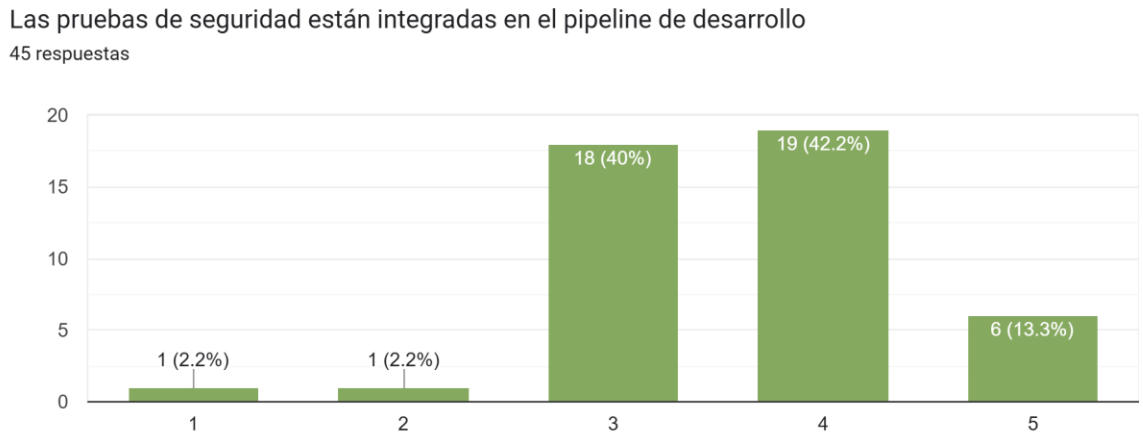
Pregunta 18. Existe integración efectiva entre el equipo de seguridad y el equipo de desarrollo



La distribución se concentra en posiciones intermedias, con 37.8% en la categoría 3 y una media de 3.47. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «adopción de metodologías y mitigación de riesgos». Aunque existe alguna práctica asociada a existe integración efectiva entre el equipo de seguridad y el equipo de desarrollo, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 24.

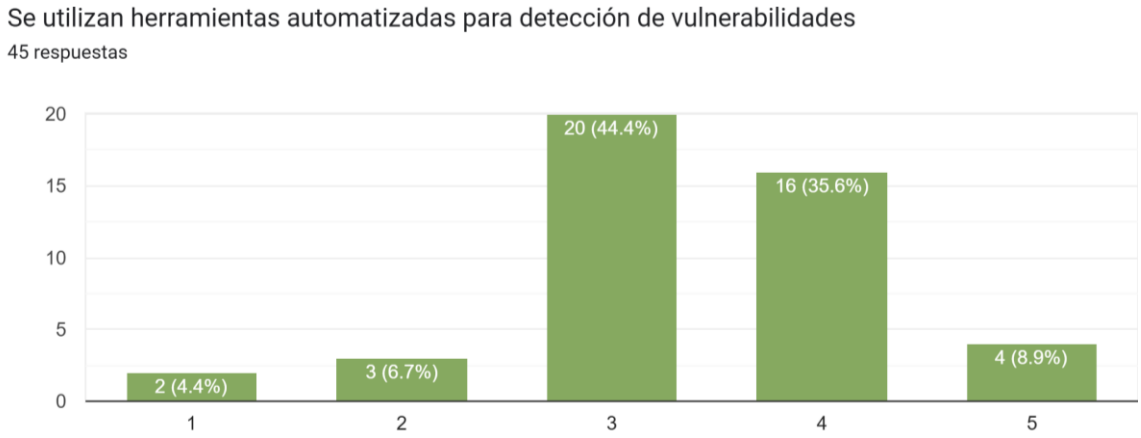
Pregunta 19. Las pruebas de seguridad están integradas en el pipeline de desarrollo



Predominan las categorías 4 y 5 (55.5%), con una media de 3.62. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. En términos analíticos, el resultado fortalece el componente «adopción de metodologías y mitigación de riesgos», porque muestra que las pruebas de seguridad están integradas en el pipeline de desarrollo está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 25.

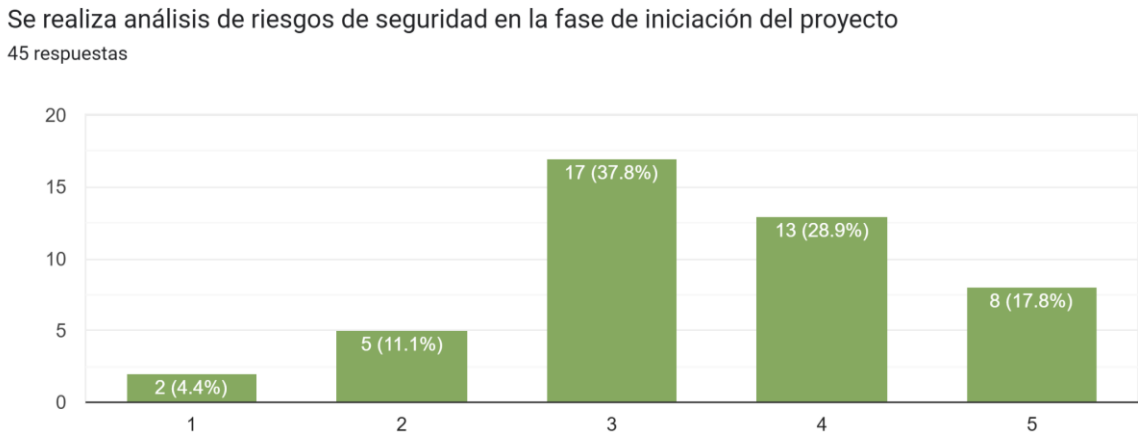
Pregunta 20. Se utilizan herramientas automatizadas para detección de vulnerabilidades



La distribución se concentra en posiciones intermedias, con 44.4% en la categoría 3 y una media de 3.38. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «adopción de metodologías y mitigación de riesgos». Aunque existe alguna práctica asociada a se utilizan herramientas automatizadas para detección de vulnerabilidades, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 26.

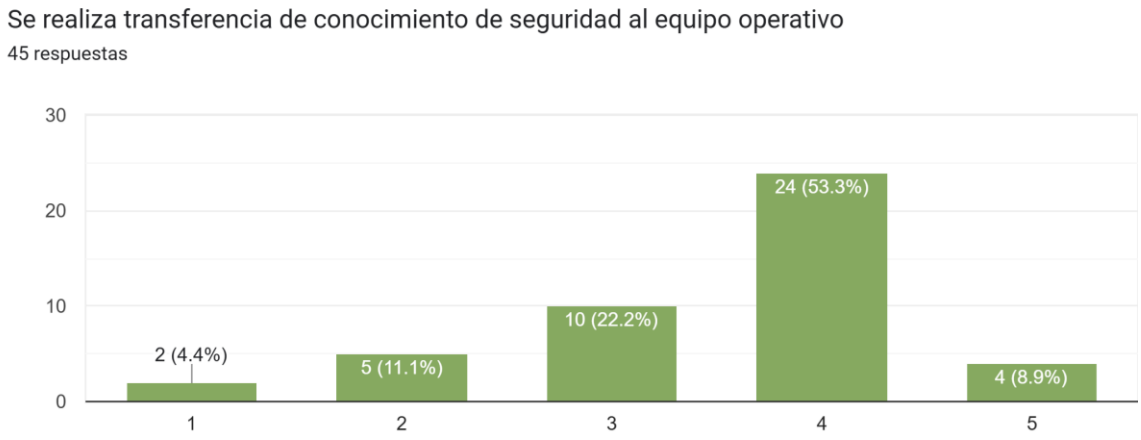
Pregunta 21. Se realiza análisis de riesgos de seguridad en la fase de iniciación del proyecto



La distribución se concentra en posiciones intermedias, con 37.8% en la categoría 3 y una media de 3.44. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «adopción de metodologías y mitigación de riesgos». Aunque existe alguna práctica asociada a se realiza análisis de riesgos de seguridad en la fase de iniciación del proyecto, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 27.

Pregunta 22. Se realiza transferencia de conocimiento de seguridad al equipo operativo e realiza análisis de riesgos de seguridad en la fase de iniciación del proyecto

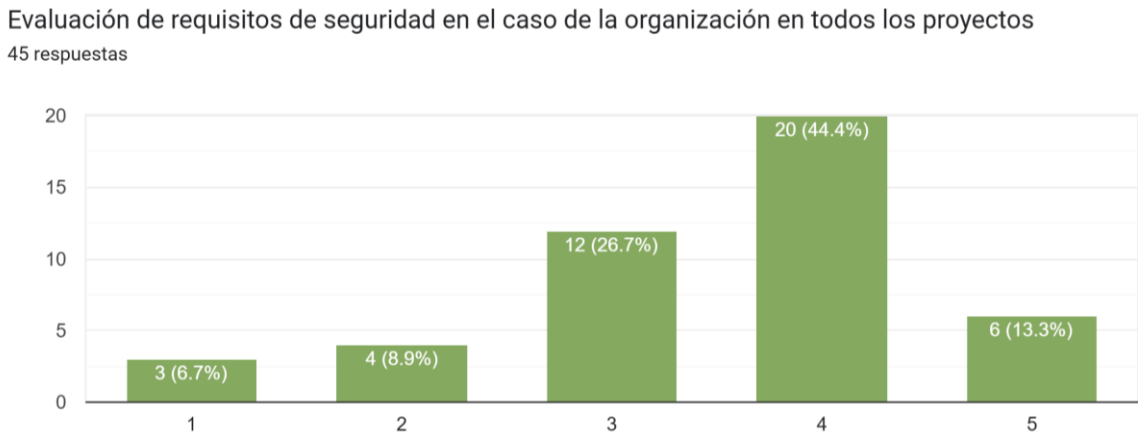


Predominan las categorías 4 y 5 (62.2%), con una media de 3.51. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «adopción de metodologías y mitigación de riesgos», porque muestra que se realiza transferencia de conocimiento de seguridad al equipo operativo está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Controles de seguridad en el ciclo de vida del proyecto

Figura 28.

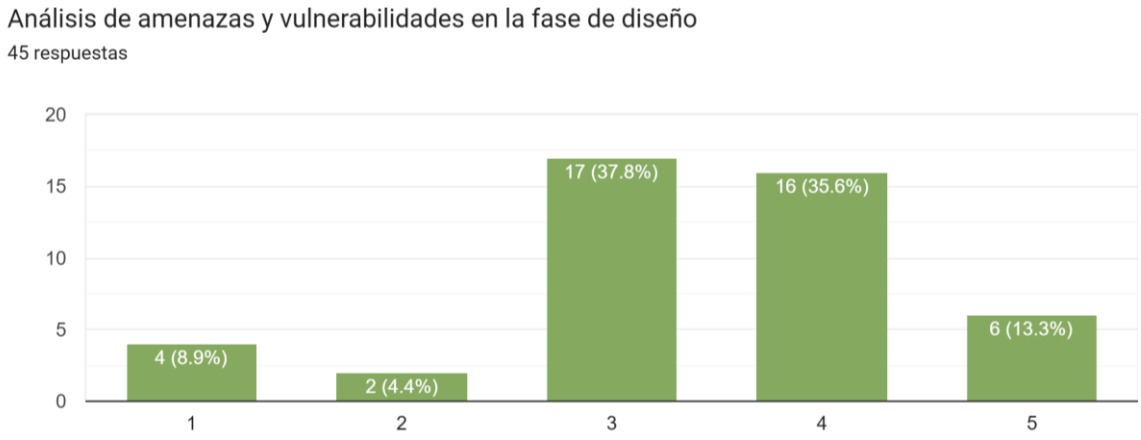
Pregunta 23. Evaluación de requisitos de seguridad en el caso de la organización en todos los proyectos



La distribución se concentra en posiciones intermedias, con 26.7% en la categoría 3 y una media de 3.49. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «controles de seguridad en el ciclo de vida del proyecto». Aunque existe alguna práctica asociada a evaluación de requisitos de seguridad en el caso de la organización en todos los proyectos, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 29.

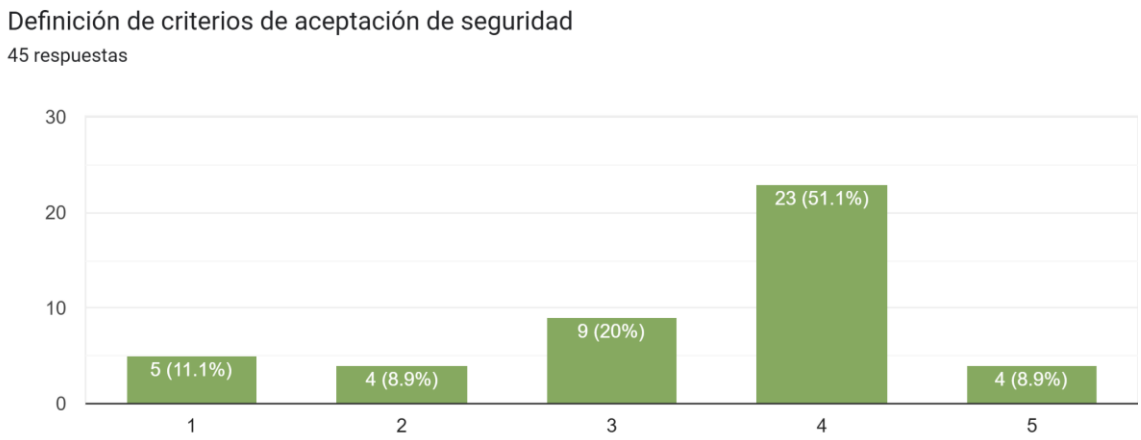
Pregunta 24. Análisis de amenazas y vulnerabilidades en la fase de diseño



La distribución se concentra en posiciones intermedias, con 37.8% en la categoría 3 y una media de 3.40. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «controles de seguridad en el ciclo de vida del proyecto». Aunque existe alguna práctica asociada a análisis de amenazas y vulnerabilidades en la fase de diseño, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 30.

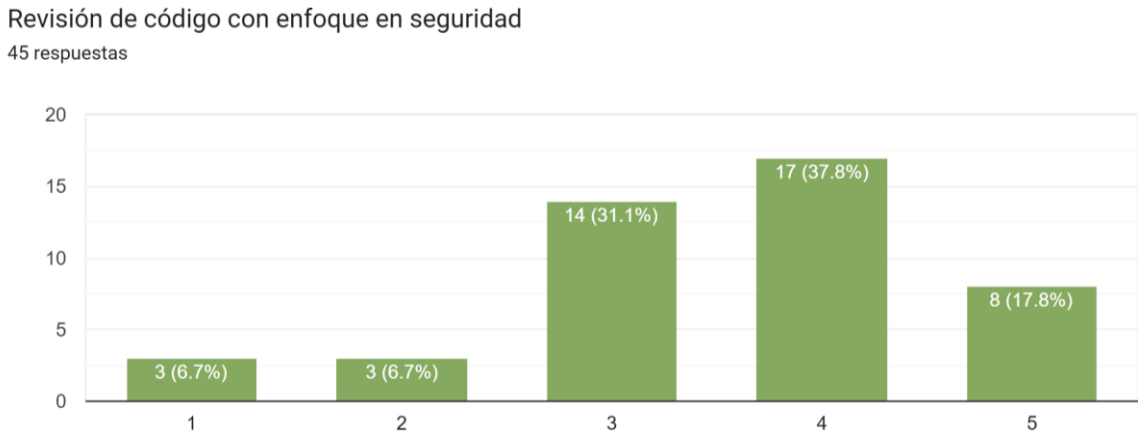
Pregunta 25. Definición de criterios de aceptación de seguridad



La distribución se concentra en posiciones intermedias, con 20.0% en la categoría 3 y una media de 3.38. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «controles de seguridad en el ciclo de vida del proyecto». Aunque existe alguna práctica asociada a definición de criterios de aceptación de seguridad, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 31.

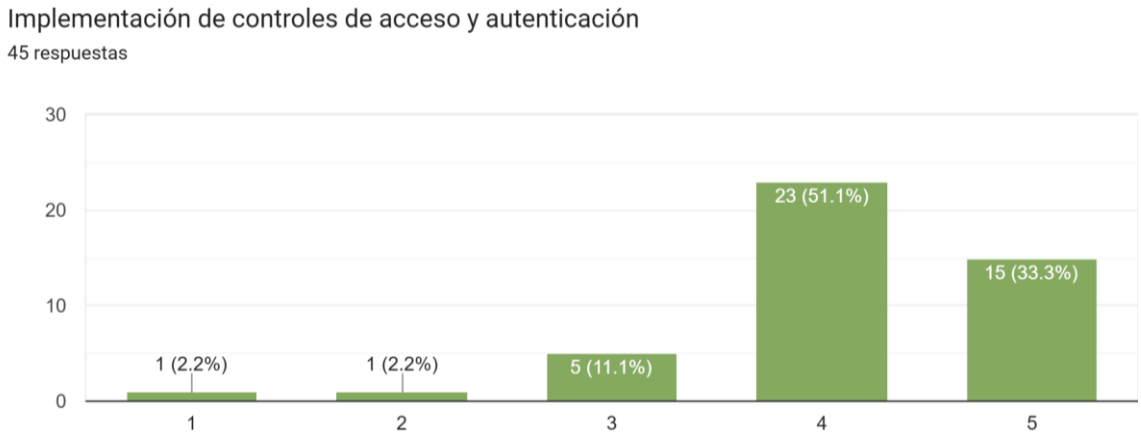
Pregunta 26. Revisión de código con enfoque en seguridad



Predominan las categorías 4 y 5 (55.6%), con una media de 3.53. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «controles de seguridad en el ciclo de vida del proyecto», porque muestra que revisión de código con enfoque en seguridad está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 32.

Pregunta 27. Implementación de controles de acceso y autenticación



Predominan las categorías 4 y 5 (84.4%), con una media de 4.11. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «controles de seguridad en el ciclo de vida del proyecto», porque muestra que implementación de controles de acceso y autenticación está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

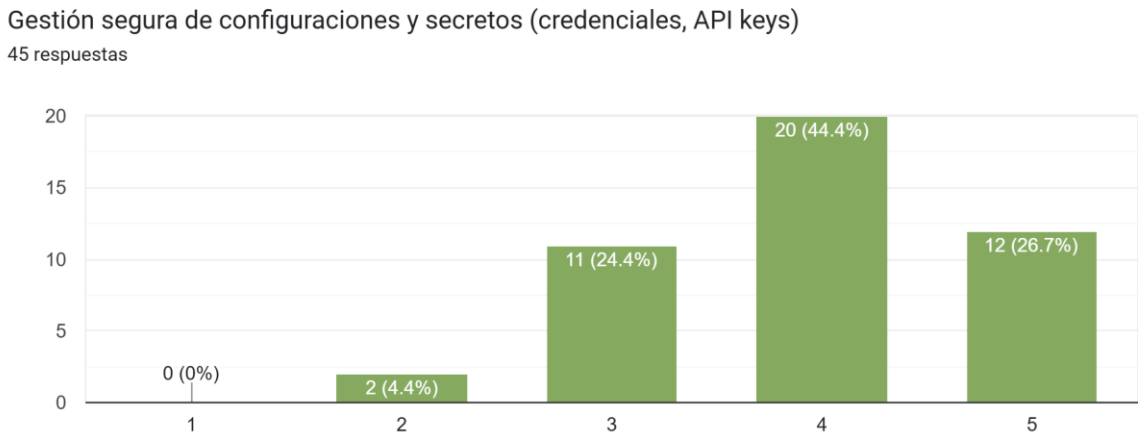
Figura 33.

Pregunta 28. Cifrado de datos sensibles en tránsito y en reposo

Predominan las categorías 4 y 5 (64.5%), con una media de 3.82. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «controles de seguridad en el ciclo de vida del proyecto», porque muestra que cifrado de datos sensibles en tránsito y en reposo está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 34.

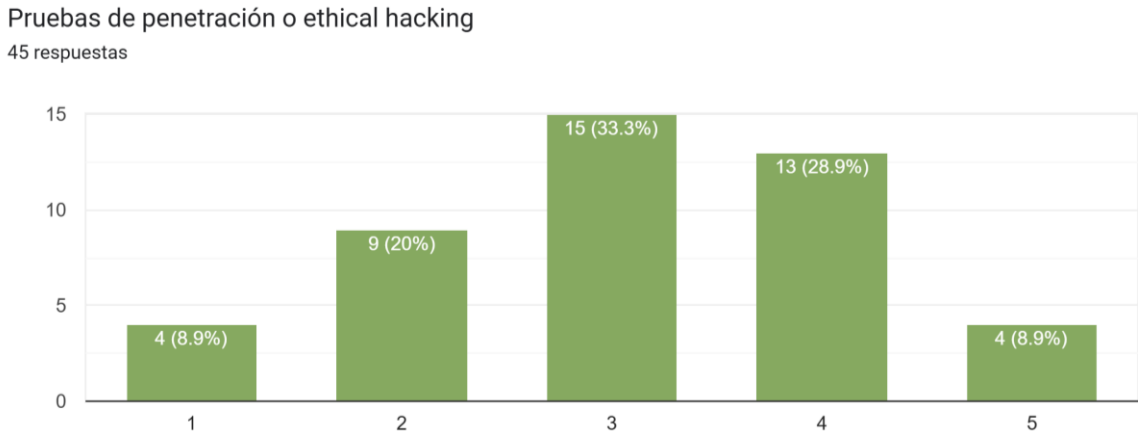
Pregunta 29. Gestión segura de configuraciones y secretos (credenciales, API keys)



Predominan las categorías 4 y 5 (71.1%), con una media de 3.93. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «controles de seguridad en el ciclo de vida del proyecto», porque muestra que gestión segura de configuraciones y secretos (credenciales, API keys) está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 35.

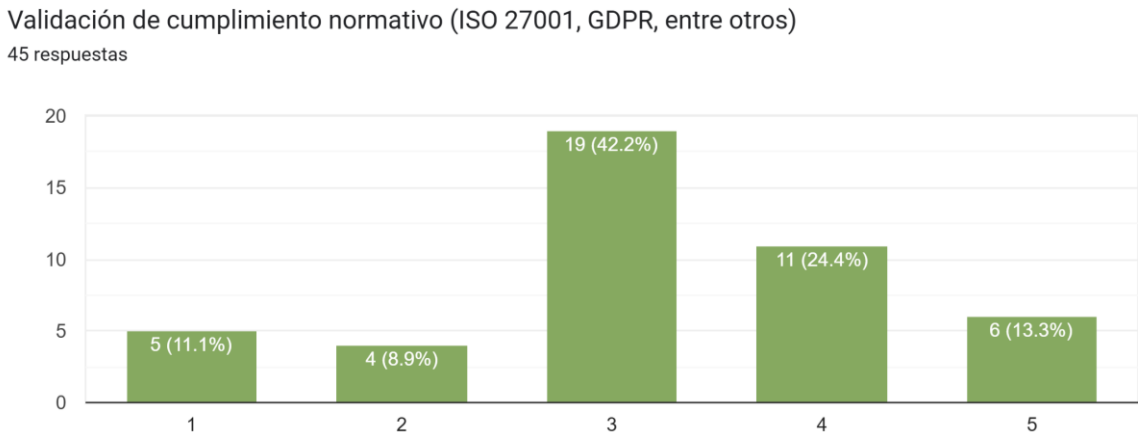
Pregunta 30. Pruebas de penetración o ethical hacking



La distribución se concentra en posiciones intermedias, con 33.3% en la categoría 3 y una media de 3.09. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «controles de seguridad en el ciclo de vida del proyecto». Aunque existe alguna práctica asociada a pruebas de penetración o ethical hacking, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 36.

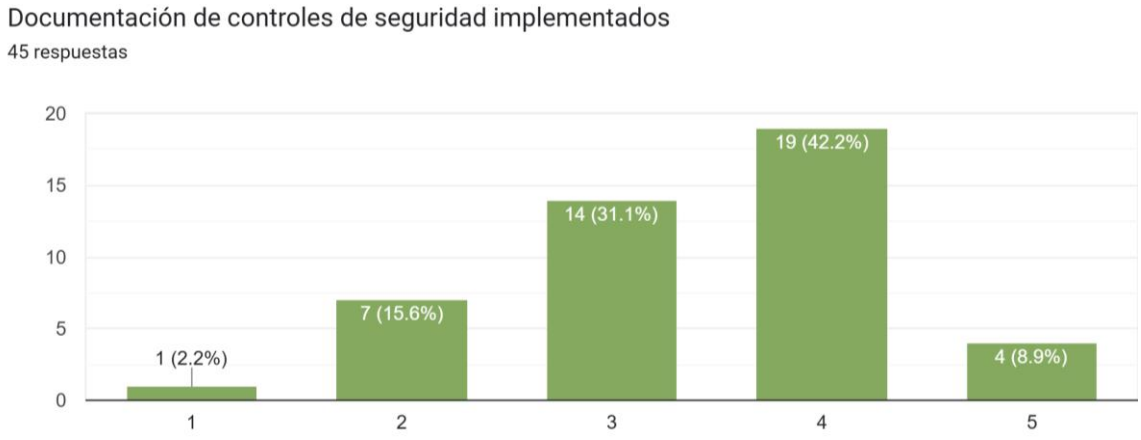
Pregunta 31. Validación de cumplimiento normativo (ISO 27001, GDPR, entre otros)



La distribución se concentra en posiciones intermedias, con 42.2% en la categoría 3 y una media de 3.20. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «controles de seguridad en el ciclo de vida del proyecto». Aunque existe alguna práctica asociada a validación de cumplimiento normativo (ISO 27001, GDPR, entre otros), su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 37.

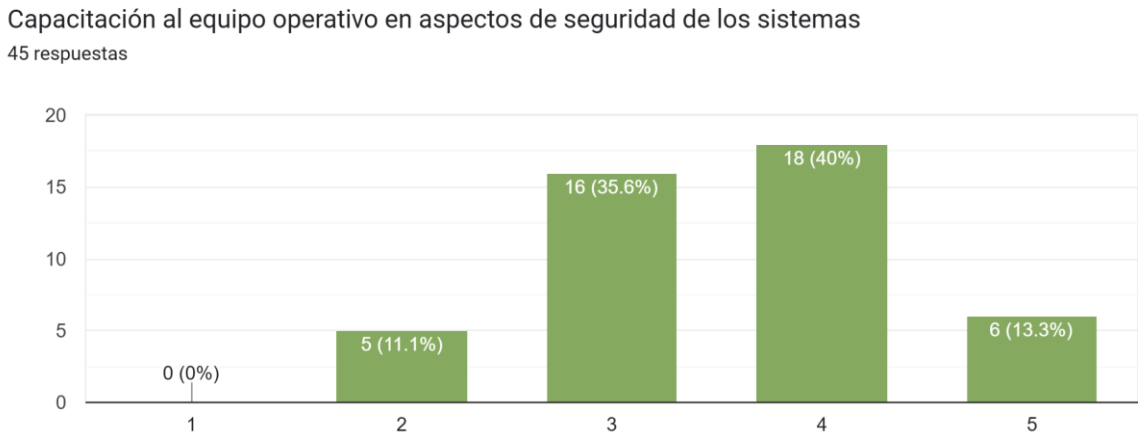
Pregunta 32. Documentación de controles de seguridad implementados



La distribución se concentra en posiciones intermedias, con 31.1% en la categoría 3 y una media de 3.40. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «controles de seguridad en el ciclo de vida del proyecto». Aunque existe alguna práctica asociada a documentación de controles de seguridad implementados, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 38.

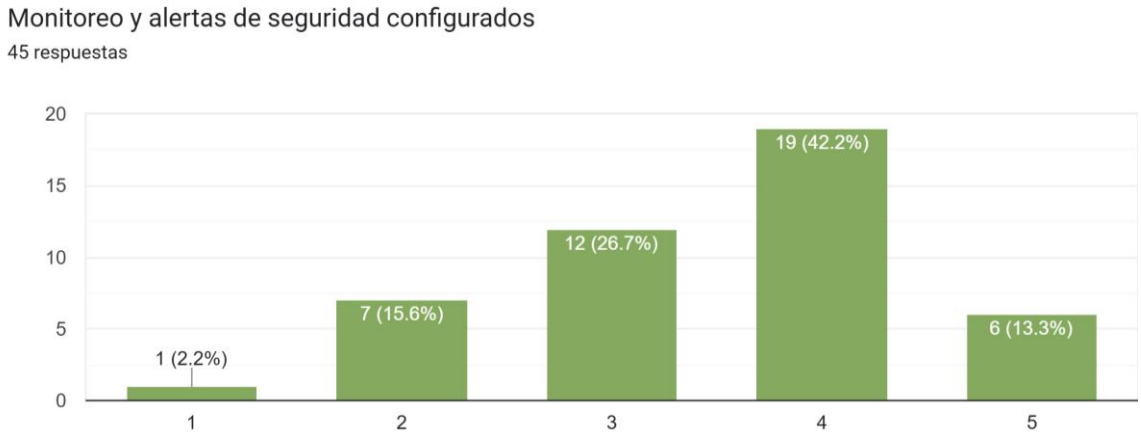
Pregunta 33. Capacitación al equipo operativo en aspectos de seguridad de los sistemas



Predominan las categorías 4 y 5 (53.3%), con una media de 3.56. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «controles de seguridad en el ciclo de vida del proyecto», porque muestra que capacitación al equipo operativo en aspectos de seguridad de los sistemas está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 39.

Pregunta 34. Monitoreo y alertas de seguridad configurados

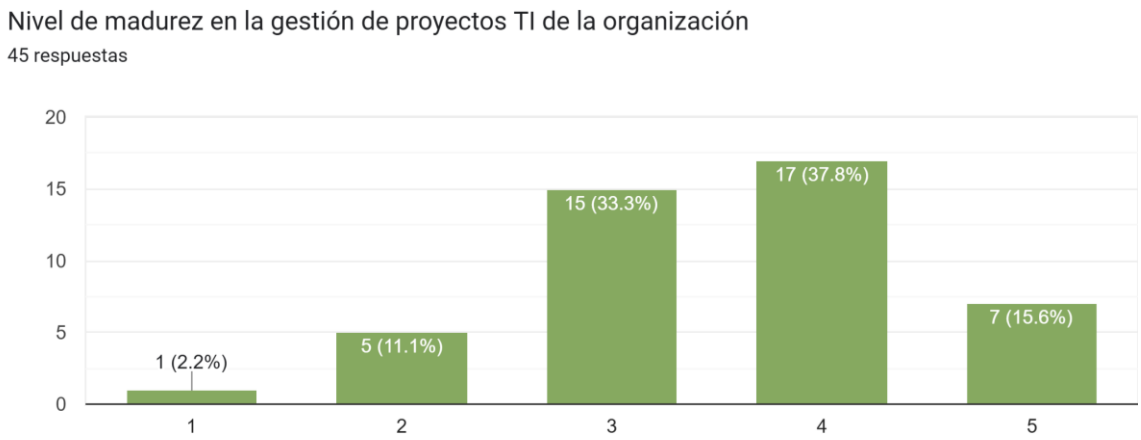


La distribución se concentra en posiciones intermedias, con 26.7% en la categoría 3 y una media de 3.49. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «controles de seguridad en el ciclo de vida del proyecto». Aunque existe alguna práctica asociada a monitoreo y alertas de seguridad configurados, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Nivel de madurez (CMMI-DEV)

Figura 40.

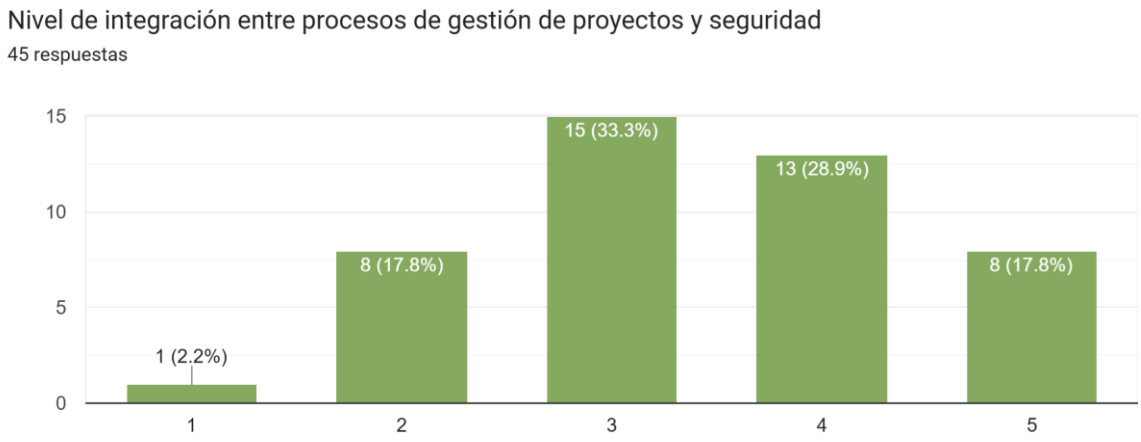
Pregunta 35. Nivel de madurez en la gestión de proyectos TI de la organización



Predominan las categorías 4 y 5 (53,4%), lo que refleja una percepción mayoritariamente favorable; sin embargo, la media de 3,53 indica que este nivel de madurez no es homogéneo en toda la organización. Aunque existen avances significativos asociados a prácticas de niveles superiores, no se alcanza una consolidación plena del nivel 4, sino una madurez intermedia con variabilidad en su aplicación. En este sentido, el componente «nivel de madurez (CMMI-DEV)» se ve fortalecido al evidenciar que la gestión de proyectos TI incorpora elementos estructurados. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 41.

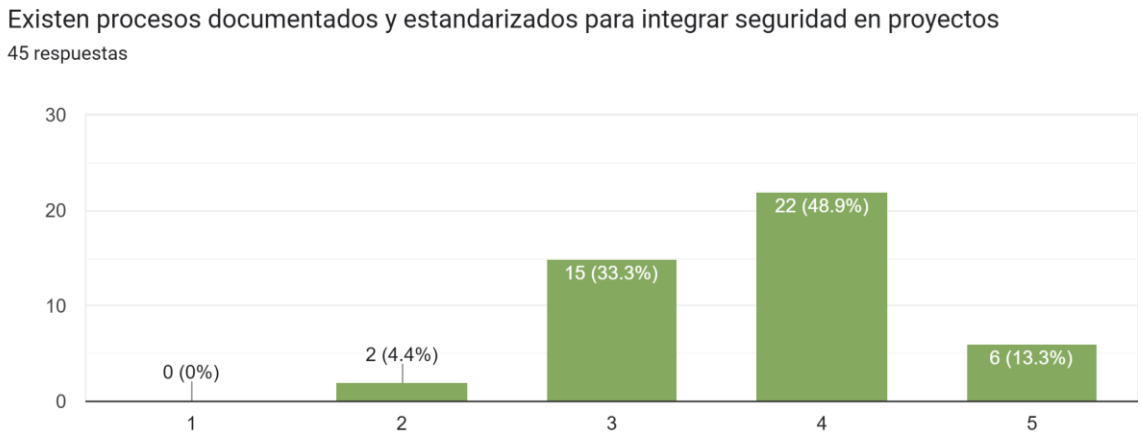
Pregunta 36. Nivel de integración entre procesos de gestión de proyectos y seguridad



La distribución se concentra en posiciones intermedias, con 33.3% en la categoría 3 y una media de 3.42. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «nivel de madurez (cmmi-dev)». Aunque existe alguna práctica asociada a nivel de integración entre procesos de gestión de proyectos y seguridad, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 42.

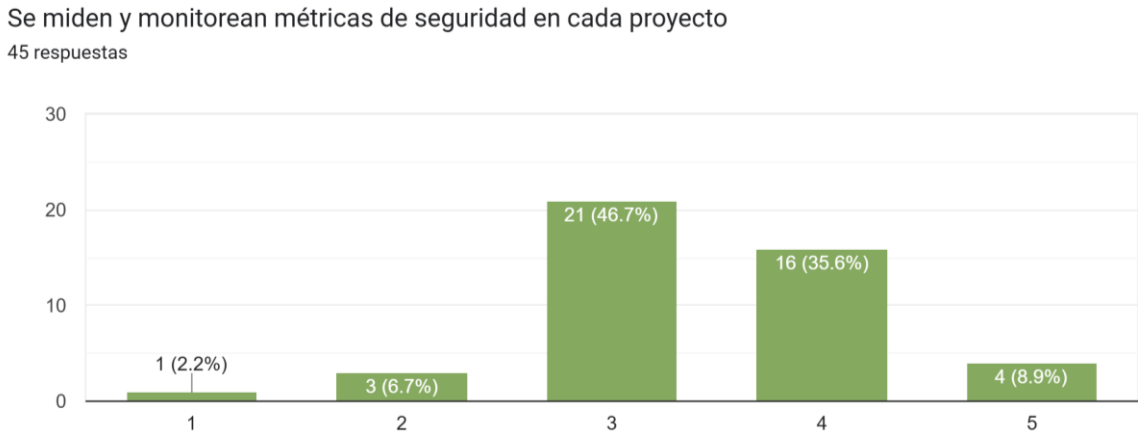
Pregunta 37. Existen procesos documentados y estandarizados para integrar seguridad en proyectos



Predominan las categorías 4 y 5 (62.2%), con una media de 3.71. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «nivel de madurez (cmmi-dev)», porque muestra que existen procesos documentados y estandarizados para integrar seguridad en proyectos está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 43.

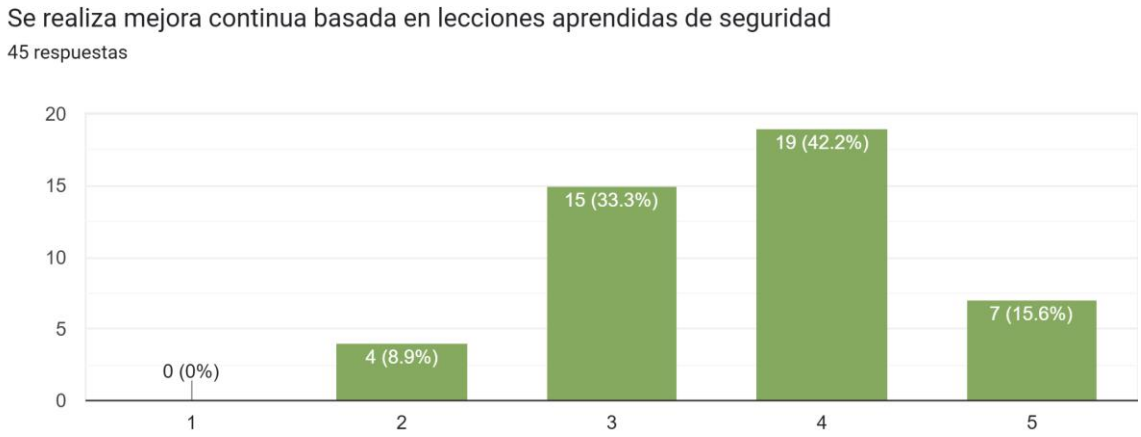
Pregunta 38. Se miden y monitorean métricas de seguridad en cada proyecto



La distribución se concentra en posiciones intermedias, con 46.7% en la categoría 3 y una media de 3.42. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «nivel de madurez (cmmi-dev)». Aunque existe alguna práctica asociada a se miden y monitorean métricas de seguridad en cada proyecto, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 44.

Pregunta 39. Se realiza mejora continua basada en lecciones aprendidas de seguridad



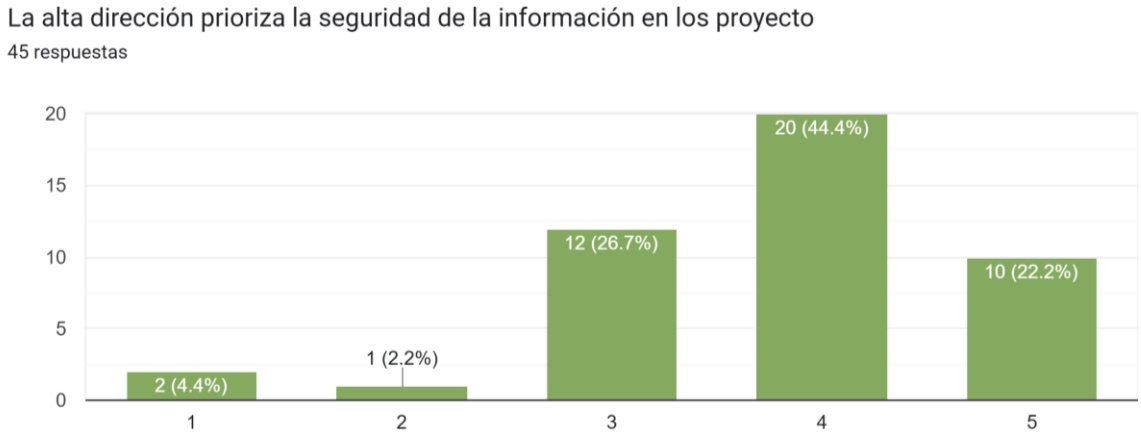
Predominan las categorías 4 y 5 (57.8%), con una media de 3.64. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El

resultado fortalece el componente «nivel de madurez (cmmi-dev)», porque muestra que se realiza mejora continua basada en lecciones aprendidas de seguridad está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Cultura y percepción de seguridad

Figura 45.

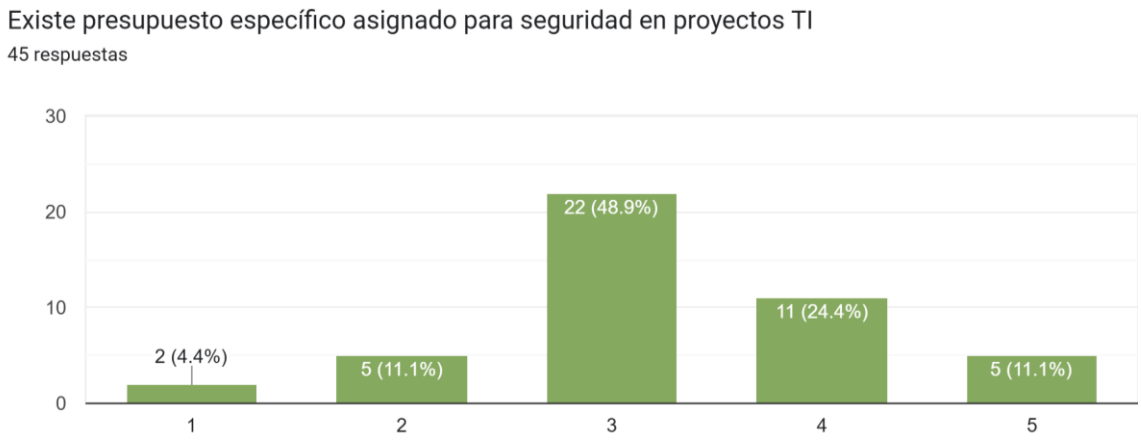
Pregunta 40. La alta dirección prioriza la seguridad de la información en los proyectos



Predominan las categorías 4 y 5 (66.6%), con una media de 3.78. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «cultura y percepción de seguridad», porque muestra que la alta dirección prioriza la seguridad de la información en el proyecto está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 46.

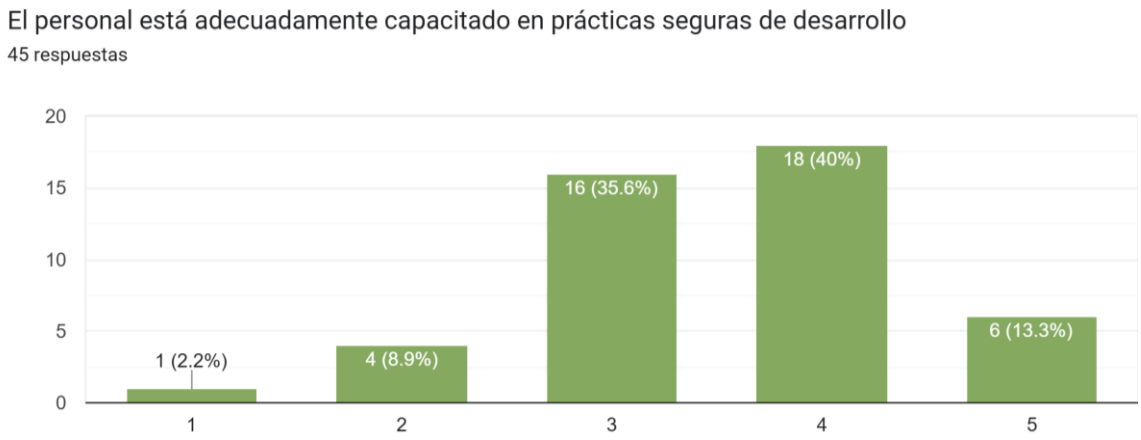
Pregunta 41. Existe presupuesto específico asignado para seguridad en proyectos TI



La distribución se concentra en posiciones intermedias, con 48.9% en la categoría 3 y una media de 3.27. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «cultura y percepción de seguridad». Aunque existe alguna práctica asociada a existe presupuesto específico asignado para seguridad en proyectos TI, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 47.

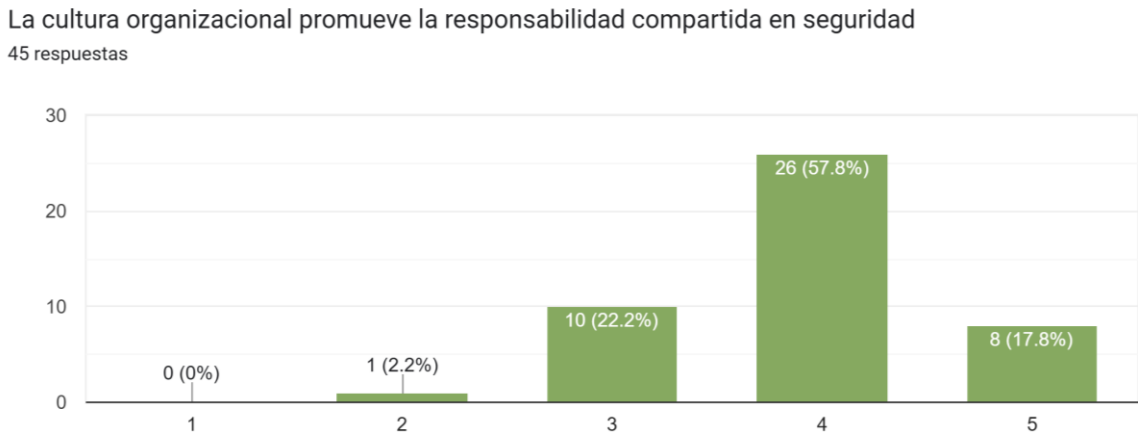
Pregunta 42. El personal está adecuadamente capacitado en prácticas seguras de desarrollo



Predominan las categorías 4 y 5 (53.3%), con una media de 3.53. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «cultura y percepción de seguridad», porque muestra que el personal está adecuadamente capacitado en prácticas seguras de desarrollo está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 48.

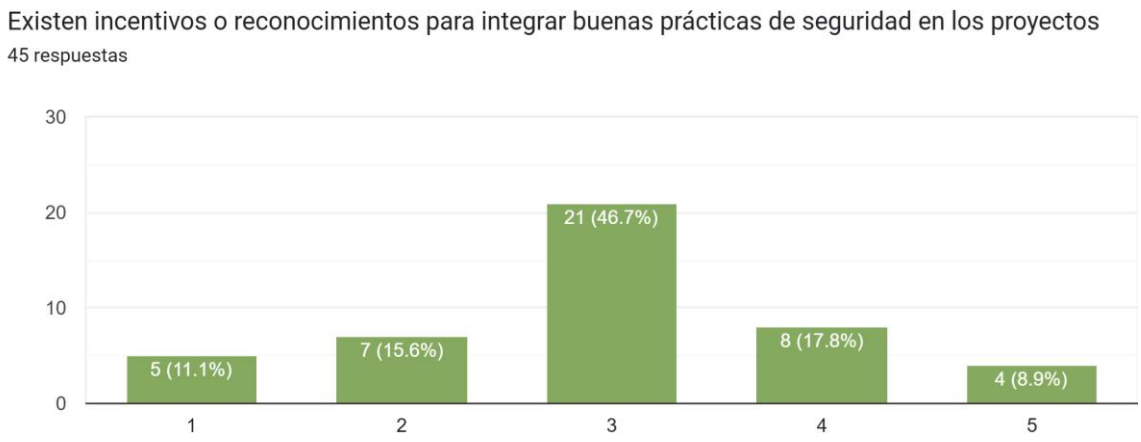
Pregunta 43. La cultura organizacional promueve la responsabilidad compartida en seguridad



Predominan las categorías 4 y 5 (75.6%), con una media de 3.91. Esto evidencia un nivel favorable de acuerdo, implementación o madurez en el aspecto evaluado. El resultado fortalece el componente «cultura y percepción de seguridad», porque muestra que la cultura organizacional promueve la responsabilidad compartida en seguridad está relativamente incorporado en la gestión de proyectos. Aun así, el desafío consiste en sostener y estandarizar esta práctica entre áreas y tipos de proyecto.

Figura 49.

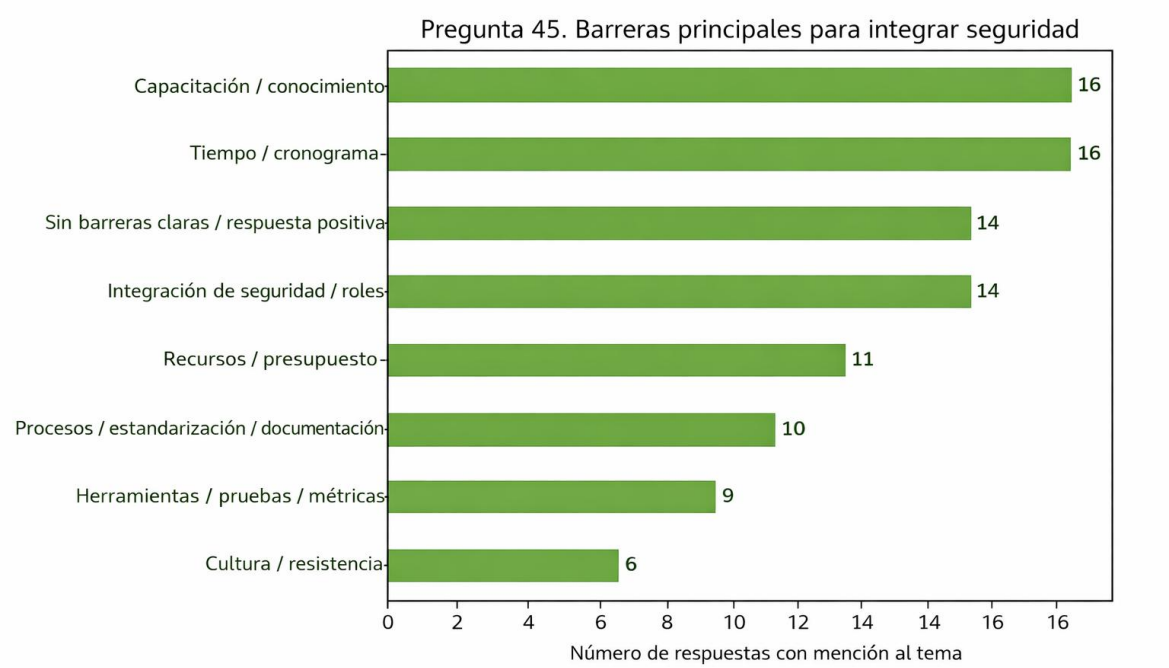
Pregunta 44. Existen incentivos o reconocimientos para integrar buenas prácticas de seguridad en los proyectos



La distribución se concentra en posiciones intermedias, con 46.7% en la categoría 3 y una media de 2.98. El resultado sugiere un desarrollo parcial o una efectividad moderada. El ítem evidencia un avance parcial dentro del componente «cultura y percepción de seguridad». Aunque existe alguna práctica asociada a existen incentivos o reconocimientos para integrar buenas prácticas de seguridad en los proyectos, su desarrollo todavía luce heterogéneo y dependiente del contexto del proyecto.

Figura 50.

Pregunta 45. ¿Cuáles considera que son las 3 principales barreras para integrar seguridad de la información en la gestión de proyectos TI en OSP INTERNATIONAL CALA S.A.S.?



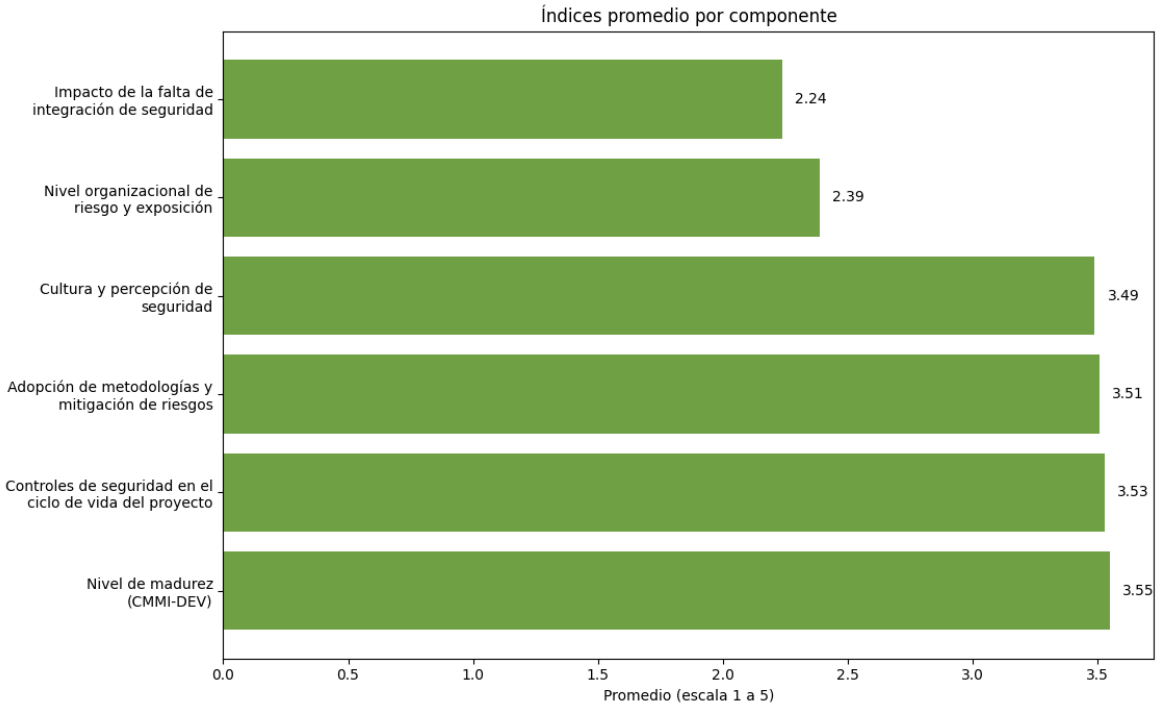
La pregunta abierta fue analizada mediante codificación temática no excluyente. Las barreras más recurrentes fueron «Tiempo / cronograma» (16 menciones), «Capacitación / conocimiento» (16 menciones) y «Integración de seguridad / roles» (14 menciones). La evidencia cualitativa confirma que las principales tensiones no se explican solo por la existencia de controles técnicos, sino por restricciones de tiempo, capacidades, articulación organizacional y formalización de procesos. También se identificaron 14 respuestas sin barreras claras o con valoración positiva del estado actual, lo que sugiere percepciones diferenciadas entre áreas y niveles de responsabilidad.

Índice promedio por componente.

Los resultados evidencian que la organización ha avanzado en la integración de la seguridad en la gestión de proyectos TI, reflejado en niveles medios-altos en madurez (3,55), controles (3,53) y metodologías (3,51). Sin embargo, estos avances no se traducen completamente en resultados operativos, dado que el riesgo y exposición (2,39) y el impacto (2,24) presentan niveles bajos.

Figura 51.

índices promedio por componente



Esto indica que la seguridad se gestiona de forma parcial o reactiva, evidenciado en eventos ocasionales como vulnerabilidades tardías, retrabajos y afectaciones en proyectos. Entre las principales barreras se identifican la falta de capacitación, limitaciones de tiempo, recursos insuficientes y debilidades en procesos y herramientas.

Por otro lado, las metodologías ágiles se destacan como un facilitador clave para la integración continua de la seguridad. En resumen, la organización se encuentra en una etapa de transición, con bases sólidas, pero con la necesidad de fortalecer la integración temprana y efectiva de la seguridad para reducir riesgos e impactos.

La siguiente tabla presenta el resumen de los índices promedio por componente, a partir de las respuestas del cuestionario aplicado. Cada componente agrupa preguntas relacionadas con dimensiones clave de la integración de la seguridad en proyectos TI.

Tabla 4.

Resumen de índices por componentes.

Componente	Preguntas	Índice	Nivel	Lectura analítica breve
Impacto de la falta de integración de seguridad.	5 - 11	2.24	Bajo impacto.	Fortaleza principal: P5. Aspecto con menor valoración: P9.
Nivel organizacional de riesgo y exposición.	12 - 14	2.39	Baja exposición.	Fortaleza principal: P13. Aspecto con menor valoración: P12.
Adopción de metodologías y mitigación de riesgos.	15 - 22	3.51	Alta efectividad.	Fortaleza principal: P15. Aspecto con menor valoración: P20.
Controles de seguridad en el ciclo de vida del proyecto.	23 - 34	3.53	Nivel 3 (Definido).	Fortaleza principal: P27. Aspecto con menor valoración: P31.
Nivel de madurez percibida (CMMI-DEV).	35 - 39	3.55	Nivel 3 (Definido).	Fortaleza principal: P37. Aspecto con menor valoración: P36.
Cultura y percepción de seguridad.	40 - 45	3.49	Cultura en Desarrollo.	Fortaleza principal: P43. Aspecto con menor valoración: P41.

Nota. Elaboración propia con base en los resultados de la aplicabilidad del formato Anexo 4. Cuestionario Likert adaptado de CMMI-DEV & ISO 27001.

Los índices, medidos en una escala de 1 a 5, permiten identificar el nivel de desempeño de cada componente, mientras que la lectura analítica destaca fortalezas y aspectos por mejorar. En conjunto, la tabla ofrece una visión general del estado actual de la integración de la seguridad y sirve como base para la interpretación de resultados y la formulación de mejoras.

Análisis comparativo por roles.

Dado que los participantes del estudio ocupan diferentes niveles jerárquicos dentro de la organización, se realizó un análisis comparativo de las respuestas en función del tipo de rol desempeñado, con el fin de identificar posibles variaciones en la percepción de la gestión de la seguridad de la información. Para este análisis, los cargos fueron agrupados en tres categorías: nivel directivo, nivel técnico y nivel operativo, considerando criterios como el grado de responsabilidad, la participación en la toma de decisiones y la naturaleza de las funciones desempeñadas.

Nivel directivo (10 participantes):

- Gerente de Proyectos / Project Manager (3)
- Representante legal (2)
- Coordinadora de recursos humanos (1)
- Scrum Master / Agile Coach (1)
- PMO (Project Management Office) (1)
- Director de TI / CIO (1)
- Coordinadora de Calidad y Cumplimiento (1)

Nivel técnico (32 participantes):

- Desarrolladores (incluye senior)
- Analistas de área
- Analista I+D
- Analista de Seguridad de la Información
- Líder Técnico / Tech Lead
- Arquitecto de Soluciones
- Roles mixtos (Desarrollador - Analista, Tech Lead - Desarrollador)

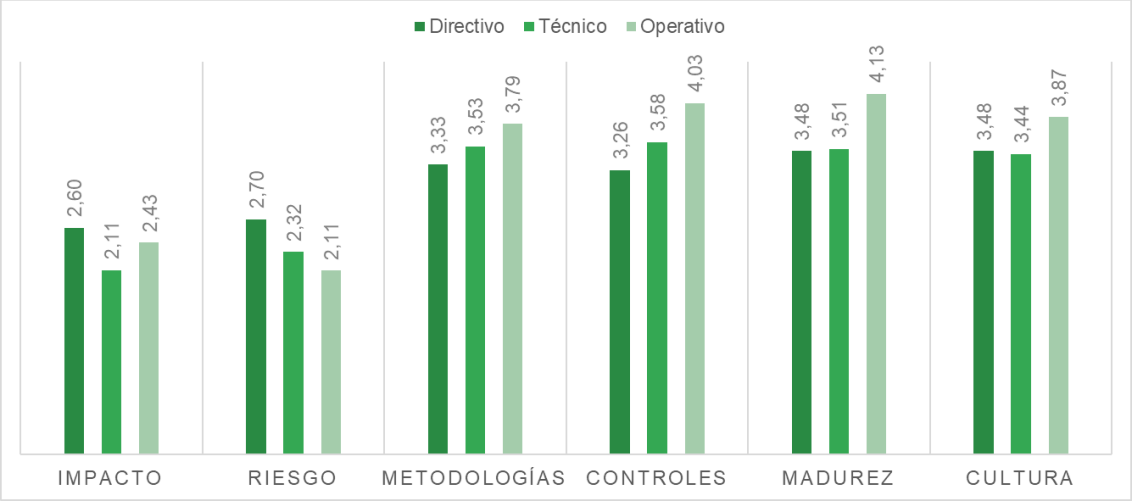
Nivel operativo (3 participantes):

- Asistente de área (2)

- Pasante (1)

Figura 52.

Comparativo promedio por componentes y roles



Nota. Elaboración propia.

Impacto de la falta de integración de seguridad: Los resultados muestran que el nivel directivo presenta una mayor percepción del impacto (2,60), en comparación con el nivel operativo (2,43) y, especialmente, con el nivel técnico (2,11), que registra la valoración más baja. La diferencia sugiere que los directivos tienen una visión más amplia de las consecuencias organizacionales asociadas a la falta de integración de la seguridad, en aspectos como retrasos en proyectos, costos adicionales y afectaciones reputacionales. Por su parte, los niveles técnicos tienden a percibir el impacto como bajo o manejable, lo que puede estar relacionado con su enfoque en la resolución operativa de incidentes.

Nivel organizacional de riesgo y exposición: En este componente se mantiene un patrón similar, donde el nivel directivo presenta la mayor valoración (2,70), seguido del nivel técnico (2,32) y el nivel operativo (2,11). Lo anterior indica que los directivos tienen una mayor sensibilidad frente al riesgo organizacional, mientras que los niveles técnicos

y operativos tienden a subestimar la exposición. Esta situación puede deberse a que los perfiles técnicos se enfocan en la gestión de incidentes una vez ocurren, más que en su prevención.

Adopción de metodologías y mitigación de riesgos: En contraste con los componentes anteriores, el nivel operativo presenta la valoración más alta (3,79), seguido del nivel técnico (3,53) y el nivel directivo (3,33). Este resultado evidencia que los roles más cercanos a la ejecución perciben una mayor efectividad en la aplicación de metodologías, especialmente en entornos ágiles e híbridos. Sin embargo, los directivos presentan una visión más moderada, posiblemente influenciada por la evaluación de resultados organizacionales.

Controles de seguridad en el ciclo de vida del proyecto: Los resultados muestran una diferencia significativa entre roles, donde el nivel operativo alcanza la valoración más alta (4,03), seguido del nivel técnico (3,58) y el nivel directivo (3,26). Esto sugiere que los niveles operativos perciben una alta presencia de controles en su trabajo cotidiano, mientras que los directivos presentan una valoración más crítica, posiblemente asociada a la efectividad real de dichos controles en el cumplimiento de objetivos organizacionales.

Nivel de madurez (CMMI-DEV): En este componente, el nivel operativo presenta nuevamente la valoración más alta (4,13), seguido del nivel técnico (3,51) y el nivel directivo (3,48). Si bien estos resultados reflejan una percepción general de madurez organizacional, la diferencia entre roles sugiere que los niveles operativos pueden estar evaluando la madurez en función de la existencia de procesos, mientras que los niveles directivos consideran aspectos más estratégicos y de resultados.

Cultura y percepción de seguridad: En cuanto a la cultura organizacional, el nivel operativo presenta la valoración más alta (3,87), seguido del nivel directivo (3,48) y el nivel técnico (3,44). Este resultado indica que los niveles operativos perciben una cultura

de seguridad más consolidada en su entorno inmediato, mientras que los niveles técnico y directivo presentan una visión más equilibrada.

Análisis de correlación de variables

Para fortalecer el análisis, se aplicó la correlación bivariada mediante el coeficiente de Spearman, con el fin de identificar relaciones entre los componentes evaluados. La elección de esta prueba no paramétrica se fundamenta en la naturaleza ordinal de las variables de escala Likert y en su capacidad para medir asociaciones monótonas entre instrumentos (Hernández-Sampieri y Mendoza, 2018).

Previamente, se calcularon los promedios de puntuación por componente para cada participante, a partir de los ítems agrupados en cada dimensión del instrumento (impacto, riesgo, metodologías, controles, madurez y cultura). Los resultados se interpretaron considerando tanto la magnitud del coeficiente como su nivel de significancia estadística ($\rho < 0,05$).

Figura 53.

Resultado de correlación bivariada mediante el coeficiente de Spearman.

Correlaciones

			Impacto Promedio	Riesgo Promedio	Metodologías Promedio	Controles Promedio	Madurez Promedio	Cultura Promedio
Rho de Spearman	Impacto Promedio	Coeficiente de correlación	1,000	,629**	-,321*	-,357*	-,428**	-,334*
		Sig. (bilateral)	.	<,001	,032	,016	,003	,025
		N	45	45	45	45	45	45
	Riesgo Promedio	Coeficiente de correlación	,629**	1,000	-,351*	-,386**	-,443**	-,480**
		Sig. (bilateral)	<,001	.	,018	,009	,002	<,001
		N	45	45	45	45	45	45
	Metodologías Promedio	Coeficiente de correlación	-,321*	-,351*	1,000	,723**	,744**	,775**
		Sig. (bilateral)	,032	,018	.	<,001	<,001	<,001
		N	45	45	45	45	45	45
	Controles Promedio	Coeficiente de correlación	-,357*	-,386**	,723**	1,000	,843**	,728**
		Sig. (bilateral)	,016	,009	<,001	.	<,001	<,001
		N	45	45	45	45	45	45
	Madurez Promedio	Coeficiente de correlación	-,428**	-,443**	,744**	,843**	1,000	,821**
		Sig. (bilateral)	,003	,002	<,001	<,001	.	<,001
		N	45	45	45	45	45	45
	Cultura Promedio	Coeficiente de correlación	-,334*	-,480**	,775**	,728**	,821**	1,000
		Sig. (bilateral)	,025	<,001	<,001	<,001	<,001	.
		N	45	45	45	45	45	45

**. La correlación es significativa en el nivel 0,01 (bilateral).

*. La correlación es significativa en el nivel 0,05 (bilateral).

Nota. Elaboración propia con base en el análisis de correlación bivariada realizado en IBM SPSS Statistics (versión 27.0.1), a partir de las respuestas del cuestionario tipo Likert aplicado (n = 45).

Los resultados evidencian la existencia de relaciones estadísticamente significativas entre las variables analizadas ($p < 0,05$), lo que permite interpretar el comportamiento sistémico de la gestión de la seguridad de la información en la organización.

En primer lugar, se identificó una correlación positiva fuerte entre el nivel de riesgo y el impacto ($\rho = 0,629$), lo que indica que el incremento en la exposición al riesgo se traduce directamente en mayores afectaciones en los proyectos, evidenciando la materialización de amenazas en consecuencias operativas.

Por otra parte, los componentes asociados a la capacidad organizacional (metodologías, controles, madurez y cultura) presentan correlaciones positivas altas entre sí, destacándose la relación entre controles y madurez ($\rho = 0,843$), así como entre cultura y madurez ($\rho = 0,821$). Esto sugiere que la madurez organizacional en seguridad depende tanto de la implementación de controles como del fortalecimiento de la cultura organizacional.

Asimismo, se observaron correlaciones negativas entre estos componentes y las variables de riesgo e impacto. En particular, la madurez presenta una relación inversa con el impacto ($\rho = -0,428$), mientras que la cultura organizacional muestra una relación negativa con el riesgo ($\rho = -0,480$), lo que evidencia que el fortalecimiento de estos elementos contribuye a la reducción de la exposición y sus consecuencias.

Finalmente, las metodologías presentan correlaciones positivas fuertes con todos los componentes organizacionales ($\rho > 0,70$), lo que permite inferir que actúan como un eje articulador en la integración de la seguridad dentro de los proyectos TI. Sin embargo, pese a estos avances, la persistencia de niveles de riesgo e impacto evidencia una

brecha entre la implementación de prácticas y su efectividad real, lo que sugiere la necesidad de fortalecer la integración temprana y estratégica de la seguridad.

Entrevistas semiestructuradas.

En el componente cualitativo, se realizaron seis entrevistas semiestructuradas a profesionales del área de investigación y desarrollo (I+D), seleccionados bajo un criterio de diversidad de roles, niveles de experiencia y responsabilidades organizacionales. Las entrevistas semiestructuradas fueron transcritas y analizadas mediante un enfoque de codificación temática, orientado a identificar patrones, categorías emergentes y relaciones entre los discursos de los participantes. El análisis se estructuró a partir de seis ejes analíticos previamente definidos:

1. Impacto de la falta de integración de seguridad
2. Nivel organizacional de riesgo y exposición
3. Adopción de metodologías y mitigación de riesgos
4. Controles de seguridad en el ciclo de vida del proyecto
5. Nivel de madurez de gestión
6. Percepción y cultura de seguridad

La unidad de análisis correspondió a cada evidencia cualitativa identificada (citas o paráfrasis relevantes extraídas de las entrevistas), tal como se presenta en las tablas de evidencias de cada video.

Se aplicó un proceso de codificación doble independiente, en el cual dos investigadores analizaron las mismas unidades de significado:

- **Codificador A:** enfoque interpretativo (mayor sensibilidad al contexto)
- **Codificador B**: enfoque descriptivo (mayor apego a definiciones estrictas)

Cada codificador asignó de manera independiente una categoría a cada evidencia, sin interacción previa.

Los resultados de la codificación se consolidaron en una matriz estructurada, en la cual cada fila representa una unidad de análisis (evidencia) y cada columna corresponde a la codificación realizada por cada investigador. Esta matriz fue diseñada para su procesamiento en software estadístico (SPSS), con el fin de calcular el nivel de acuerdo intercodificador.

Para evaluar la consistencia entre codificadores, se empleará el coeficiente Kappa de Cohen (1960), el cual permite medir el grado de acuerdo corregido por el azar. Se estableció como criterio de aceptación un valor de kappa mayor a 0,80, el cual es considerado como un nivel de acuerdo casi perfecto o alto, siguiendo los criterios de Landis y Koch (1977). En caso de obtener valores inferiores, se contempla una fase de revisión y consenso para ajustar el esquema de codificación y asegurar la fiabilidad de los datos.

Tabla 5.

Matriz de codificación temática y concordancia intercodificador inicial

ID	Entrevista	Evidencia resumida	Cod_A	Cod_B
1	Video 1	Certificación ISO 9001 e IT Mark.	5	5
2	Video 1	Uso de Scrum + PMI.	3	3
3	Video 1	Uso de VPN y repositorios.	4	4
4	Video 1	Comité de seguridad.	5	5
5	Video 1	Resistencia del equipo a seguridad.	6	6
6	Video 2	Seguridad en todo el ciclo.	4	4
7	Video 2	Falta de certificación individual.	5	5
8	Video 2	Uso de VPN remoto.	4	4
9	Video 2	Presión de tiempo reduce seguridad.	3	6
10	Video 2	Enfoque en herramientas.	4	4
11	Video 3	Uso de IT Mark, PMBOK, ITIL.	5	5
12	Video 3	No ISO 27001.	5	5
13	Video 3	Seguridad como costo alto (teórico).	6	6
14	Video 3	Herramientas proactivas (SonarQube).	4	4
15	Video 3	Falta de valor percibido en seguridad.	6	6
16	Video 4	ISO 9001 + IT Mark.	5	5

ID	Entrevista	Evidencia resumida	Cod_A	Cod_B
17	Video 4	Seguridad reduce retrabajo.	6	3
18	Video 4	Pruebas de seguridad por cliente.	4	4
19	Video 4	Cultura positiva hacia seguridad.	6	6
20	Video 4	Procesos definidos.	5	5
21	Video 5	Vulnerabilidades detectadas por cliente.	1	1
22	Video 5	Falta de monitoreo interno.	2	4
23	Video 5	Compartir credenciales.	4	4
24	Video 5	Seguridad en desarrollo.	4	4
25	Video 5	Nivel de madurez organizacional.	5	5
26	Video 6	Uso de herramientas DevSecOps.	3	3
27	Video 6	Integración de seguridad en CI/CD.	4	4
28	Video 6	Falta de monitoreo continuo.	2	4
29	Video 6	Necesidad de capacitación en seguridad.	6	6
30	Video 6	Evaluación de riesgos temprana.	3	3

Nota. Elaboración propia. La tabla presenta la codificación independiente de las evidencias cualitativas por dos investigadores, utilizada como base para el cálculo del coeficiente Kappa de Cohen en SPSS.

Figura 54.

Resultado coeficiente de Kappa de Cohen

Medidas simétricas

		Valor	Error estándar asintótico[a]	T aproximada[b]	Significación aproximada
Medida de acuerdo	Kappa	,825	,080	8,424	<,001
N de casos válidos		30			

a. No se presupone la hipótesis nula.

b. Utilización del error estándar asintótico que presupone la hipótesis nula.

Nota. Elaboración propia con base en el análisis de concordancia intercodificador mediante el coeficiente Kappa de Cohen, realizado en IBM SPSS Statistics (versión

27.0.1), a partir de la codificación de evidencias derivadas de las entrevistas semiestructuradas (n = 30 unidades de análisis).

El coeficiente Kappa de Cohen, calculado mediante el software IBM SPSS Statistics, arrojó un valor de $\kappa = 0{,}825$, con un nivel de significancia $p < 0{,}001$, lo que indica un nivel de acuerdo casi perfecto entre los codificadores, de acuerdo con los criterios de Landis y Koch (1977). Este resultado evidencia una alta consistencia en la asignación de categorías y respalda la confiabilidad del proceso de codificación cualitativa.

El valor alcanzado es resultado del proceso de revisión y ajuste de los criterios de codificación, lo que permitió reducir las discrepancias iniciales y consolidar una estructura categorial clara y coherente. En consecuencia, se garantiza la objetividad del análisis y la validez de las categorías utilizadas para la interpretación de los resultados cualitativos.

De acuerdo con lo anterior, el resultado de las seis entrevistas permitió identificar patrones consistentes, así como tensiones y vacíos en la forma en que la seguridad es concebida, implementada y gestionada dentro de la organización.

Nivel de madurez de gestión: De manera transversal, los entrevistados coinciden en la existencia de marcos formales como ISO 9001 e IT Mark, así como en la adopción de referentes como PMBOK e ITIL. La presencia de comités de seguridad, roles definidos y procesos documentados sugiere un nivel de madurez organizacional intermedio, caracterizado por la formalización de prácticas y estructuras. Sin embargo, este nivel de madurez presenta una limitación importante: la dependencia de factores externos, particularmente de los requerimientos de los clientes, para impulsar la adopción de estándares más avanzados como ISO 27001. Esto indica que la seguridad no se gestiona completamente como un eje estratégico interno, sino como una respuesta a exigencias del entorno.

Adicionalmente, se evidencian brechas a nivel individual, especialmente en perfiles operativos, donde la formación y certificación en seguridad no es prioritaria, lo que genera una desconexión entre la formalización organizacional y las capacidades del talento humano.

Controles de seguridad: Las entrevistas muestran la existencia de controles técnicos relevantes, tales como: uso de VPN para acceso seguro a repositorios**,** Herramientas de control de versiones (Git)**, a**nálisis de código con herramientas (SonarQube) y gestión de incidencias mediante plataformas colaborativas. No obstante, el análisis revela que estos controles tienden a ser parciales, heterogéneos y, en algunos casos, reactivos. Por ejemplo, se identificó que las pruebas de seguridad en algunos proyectos son realizadas por el cliente o terceros, donde no existe un monitoreo continuo interno de vulnerabilidades en producción y la detección de fallas depende, en ocasiones, de revisiones externas

Nivel organizacional de riesgo y exposición: Uno de los hallazgos más relevantes del análisis es la identificación de condiciones estructurales de riesgo, aun en ausencia de incidentes reportados. Entre las principales situaciones identificadas se encuentran:

- Dependencia del cliente para detectar vulnerabilidades (versiones desactualizadas de componentes como Apache Tomcat)
- Ausencia de monitoreo proactivo de seguridad en ambientes productivos
- Prácticas operativas riesgosas, como el intercambio de credenciales por medios no seguros
- Implementación parcial de controles debido a presión por tiempos de entrega

Estas condiciones reflejan un nivel de exposición organizacional significativo, que no necesariamente se traduce en incidentes visibles, pero sí en una vulnerabilidad latente. También, se evidencia que la ausencia de incidentes reportados no implica

necesariamente un entorno seguro, sino posiblemente un subregistro o falta de visibilidad del riesgo.

Impacto de la falta de integración de seguridad: De manera consistente en las seis entrevistas, no se reportan impactos concretos como retrasos, sobrecostos o incidentes de seguridad atribuibles directamente a la falta de integración de seguridad. El análisis sugiere varias posibles explicaciones:

- **Visibilidad limitada según el rol:** Los perfiles operativos (desarrolladores) no necesariamente tienen acceso a información sobre impactos a nivel de proyecto o negocio.
- **Externalización de la detección:** Como se evidenció en varios casos, los clientes o terceros identifican vulnerabilidades, lo que reduce la percepción interna de impacto.
- **Subregistro organizacional:** Es posible que los incidentes o efectos negativos no se documenten formalmente o no se comuniquen abiertamente.
- **Enfoque preventivo:** Varios entrevistados se centran en lo que la seguridad evita, más que en problemas experimentados.

En este sentido, el impacto de la falta de integración de seguridad se manifiesta más como riesgo potencial y dependencia externa, que como consecuencias explícitamente reconocidas.

Adopción de metodologías y mitigación de riesgos: La organización evidencia una adopción de metodologías híbridas, combinando enfoques tradicionales (PMI) con metodologías ágiles (Scrum). Esta combinación permite flexibilidad en la gestión de proyectos, pero presenta desafíos en la integración de la seguridad. Uno de los hallazgos más consistentes es que la seguridad no siempre se integra desde etapas tempranas,

puede ser reducida a controles básicos en contextos de presión por tiempos o no se encuentra completamente incorporada en los flujos de trabajo ágiles.

No obstante, emergen señales de mejora hacia enfoques más integrados a través de prácticas asociadas a DevSecOps, tales como automatización de controles de seguridad, integración de validaciones en pipelines de CI/CD y uso de herramientas para análisis continuo. Estas prácticas aún se encuentran en fases iniciales, pero representan un potencial camino de madurez para la organización.

Percepción y cultura de seguridad: El análisis de este eje revela una dualidad importante en la cultura organizacional. Se identificaron tanto elementos positivos como barreras. Por un lado, existe reconocimiento de la importancia de la seguridad, valoración de su rol en la calidad del producto y la existencia de lineamientos organizacionales; por otro lado, se evidencias resistencias del equipo ante controles, percepción de la seguridad como obstáculo, dificultades de comunicación y apropiación y brechas en formación y capacitación.

Esta tensión entre reconocimiento y resistencia evidencia que la seguridad aún no se encuentra completamente interiorizada como parte natural del proceso de desarrollo, sino que en algunos casos se percibe como un elemento externo o impuesto.

Revisión documental.

En relación con la revisión documental, se tomó como base el listado maestro de documentos de la organización *Q-DR-F-04-V1 LISTADO MAESTRO DOCUMENTOS,* y se seleccionaron aquellos asociados a los procesos de planeación estratégica, gestión de proyecto y calidad (incluye los subprocesos de control de documentos y registros, auditorías internas, gestión de producto no conforme, acciones correctivas y de mejora, monitoreo y seguimiento). Se consideró que dichos documentos podían contener información relevante como políticas, procedimientos, informes de auditoría en

tecnologías de la información y lecciones aprendidas de proyectos previos, entre otros elementos relacionados con la gestión de proyectos y la seguridad de la información.

Durante este proceso, se evidenció que la totalidad de los documentos no se encontraba disponible, debido a pérdidas de información dentro de la organización; no obstante, con los documentos accesibles se procedió a la construcción de la matriz de extracción de datos. En consecuencia, se presenta la matriz de revisión a partir de la información recopilada (ver Anexo 6).

Observación no participante.

En cuanto a la técnica de observación no participante, se desarrolló mediante una lista de verificación estructurada aplicada en reuniones de proyecto, con el propósito de identificar prácticas reales de integración de la seguridad de la información en las distintas fases de gestión, tanto en enfoques tradicionales como ágiles. La lista de verificación permitió evaluar aspectos como la incorporación de controles de seguridad, la gestión de riesgos, la documentación de decisiones y la consideración de la seguridad en la planificación, ejecución y seguimiento de los proyectos.

Este instrumento fue elaborado con base en referentes teóricos y normativos con el fin de garantizar su pertinencia frente a los objetivos del estudio (ver Anexo 7). La observación se realizó de manera no intrusiva, sin intervención del investigador en las dinámicas de las reuniones, con el fin de no alterar el comportamiento natural de los participantes y asegurar la validez de la información recolectada. El instrumento fue aplicado de manera acumulativa y progresiva a un conjunto de reuniones de proyecto seleccionadas de forma intencional, consideradas representativas de las diferentes fases del ciclo de vida y enfoques metodológicos utilizados en la organización. La valoración final de cada ítem corresponderá a la consistencia con la que se evidencie la práctica a lo largo del proceso de observación.

En consecuencia, se presentan los resultados obtenidos a partir de su aplicación:

Tabla 6.

Resultado de la técnica de observación no participante en las reuniones de ejecución de proyectos.

Ítem evaluado	Resultado	Observaciones
1. Inicio del proyecto / Planeación.	**Cumple parcialmente.**	Se evidenció que en la fase inicial del proyecto se consideran algunos elementos relacionados con la seguridad de la información, como la asignación de accesos y la definición general de responsabilidades. Sin embargo, la incorporación de la seguridad no se presenta como un componente estructurado ni estandarizado dentro de la planeación. No se identifican lineamientos formales que aseguren la inclusión sistemática de requisitos de seguridad, análisis de riesgos o definición explícita de controles desde el inicio. La práctica depende en gran medida del criterio del líder del proyecto, lo que genera variabilidad en su aplicación.
2. Ejecución del proyecto.	**Cumple parcialmente.**	Durante la ejecución se observaron prácticas operativas que reflejan cierto nivel de integración de la seguridad, como el control de accesos a repositorios, uso de herramientas de desarrollo y aplicación de medidas básicas de protección de la información. No obstante, estas prácticas no son homogéneas ni completamente integradas en la dinámica del proyecto. La seguridad suele abordarse de manera reactiva o condicionada por requerimientos externos, y no como un componente transversal del proceso de desarrollo. Se identifican debilidades en la implementación consistente de controles y en la integración de la seguridad dentro de los procesos ágiles.
3. Seguimiento y control.	**Cumple parcialmente.**	Se evidenció la existencia de actividades de seguimiento relacionadas con el avance del proyecto y la gestión de incidencias; sin embargo, el componente de seguridad no se encuentra formalmente integrado dentro de los mecanismos de control. No se observó el uso sistemático de indicadores o métricas específicas de seguridad, ni herramientas estructuradas para el monitoreo continuo de riesgos o vulnerabilidades. El seguimiento se centra principalmente en aspectos operativos y de cumplimiento de entregables, dejando la seguridad en un nivel secundario.
4. Cierre del proyecto.	**Cumple parcialmente.**	En la fase de cierre se identifican prácticas relacionadas con la documentación final, entrega de productos y

Ítem evaluado	Resultado	Observaciones
		validación de cumplimiento general del proyecto. No obstante, la evaluación específica de los controles de seguridad implementados no se presenta como un criterio formal de cierre. La verificación de cumplimiento en seguridad es limitada y no se evidencia un proceso sistemático de validación, auditoría o lecciones aprendidas centradas en este aspecto. Esto sugiere que la seguridad no está completamente integrada en los criterios de aceptación final del proyecto.
5. Gestión de servicios.	**Cumple parcialmente.**	Se observó un mayor nivel de estructuración en la gestión de servicios, evidenciado en la existencia de procedimientos para la gestión de incidentes, control de accesos, administración de cambios y documentación operativa. Sin embargo, estos elementos no se encuentran completamente formalizados ni estandarizados como procesos definidos. En particular, no se evidenció la existencia de procedimientos documentados específicos para la gestión de incidentes de seguridad, lo que limita la consistencia en su aplicación. Aunque se identifican esfuerzos operativos que contribuyen a la protección de la información, la integración de la seguridad en la operación del servicio es parcial y presenta oportunidades de mejora en aspectos como la trazabilidad, monitoreo y formalización de procesos.
6. Cultura y prácticas organizacionales.	**Cumple parcialmente.**	Se evidencia una percepción general positiva frente a la importancia de la seguridad de la información y disposición por parte de los equipos para su implementación. Sin embargo, esta conciencia no se traduce de manera consistente en prácticas formales y sostenidas. Se identifican comportamientos operativos que no están alineados con buenas prácticas de seguridad, así como una priorización de los tiempos de entrega sobre los controles de protección. La cultura organizacional muestra un nivel de desarrollo intermedio, con conocimiento presente, pero sin una apropiación integral ni estandarizada en todos los niveles.

Nota. Elaboración propia con base en los resultados de la aplicabilidad del formato Anexo 7. Lista de verificación observación no participante en reuniones de proyecto.

Bitácora de campo.

Durante el proceso de recolección de información cualitativa, se empleó una bitácora de campo como instrumento complementario de registro, en la cual se documentaron las

impresiones del investigador, incidencias presentadas durante la aplicación de las entrevistas y observaciones, así como reflexiones analíticas preliminares (ver Anexo 8).

Este registro incluyó aspectos como el contexto de interacción con los participantes, actitudes, énfasis en los discursos, elementos no verbales y situaciones relevantes que pudieran influir en la interpretación de la información recolectada. Asimismo, permitió identificar posibles sesgos, dificultades operativas y dinámicas organizacionales no evidentes en los datos explícitos.

La bitácora de campo fue utilizada como insumo para el proceso de análisis cualitativo, contribuyendo a la contextualización de las categorías emergentes y al fortalecimiento de la interpretación de los hallazgos, en coherencia con la estrategia de triangulación metodológica aplicada en el estudio.

Tabla 7.

Resultado de la bitácora de campo

Hallazgo observado	Descripción del patrón	Interpretación analítica	Implicación para el estudio
Predominio de respuestas organizacionales al inicio.	Al comenzar las entrevistas, es común que los participantes hablen primero de políticas, certificaciones o buenas prácticas, antes de mencionar dificultades concretas.	Sugiere que el discurso se construye inicialmente desde lo formal y lo esperado organizacionalmente, priorizando una imagen alineada con el “deber ser”.	Puede proyectar una percepción inicial de alta madurez en seguridad, que requiere ser contrastada con el desarrollo completo de la entrevista.
Aparición progresiva de limitaciones.	Las dificultades relacionadas con el tiempo, los roles o la dependencia del cliente suelen emerger más adelante o cuando se profundiza en las preguntas.	Las tensiones operativas no se expresan de manera inmediata, sino que aparecen gradualmente a medida que se genera mayor confianza o especificidad en la conversación.	Refuerza la necesidad de analizar el discurso en su totalidad, evitando conclusiones basadas únicamente en las primeras respuestas.

Uso de formulaciones idealizadas.	Se utilizan expresiones como “debería hacerse”, “lo ideal sería” o “se busca implementar”, sin detallar siempre acciones concretas.	Refleja una mezcla entre lo que realmente se hace y lo que se aspira a hacer, lo que puede dificultar diferenciar entre práctica e intención.	Invita a interpretar con cautela las afirmaciones normativas, sin asumir que representan ejecución efectiva.
Diferencias en el nivel de detalle.	Algunos entrevistados brindan explicaciones técnicas y específicas, mientras que otros se mantienen en generalidades.	El conocimiento sobre la seguridad no es homogéneo dentro de la organización, sino que depende del rol y la cercanía con la operación.	Evidencia que la comprensión del fenómeno varía entre actores, lo que debe considerarse en el análisis.
Contradicciones dentro de una misma entrevista.	En algunos casos, se destacan fortalezas en la gestión de seguridad, seguidas de reconocimientos de limitaciones.	Esto pone en evidencia una tensión entre el discurso formal de cumplimiento y la realidad operativa.	Permite identificar brechas entre lo que la organización declara y lo que realmente sucede en la práctica.
Conocimiento fragmentado de los procesos.	Cada participante describe solo una parte del proceso de seguridad, sin una visión completamente integrada.	El conocimiento organizacional aparece distribuido y segmentado, lo que sugiere una comprensión parcial del sistema.	Refuerza la idea de que la seguridad se vive de manera distinta según la función y experiencia de cada actor.
Baja mención espontánea de incidentes.	Rara vez se mencionan directamente eventos de seguridad o sus impactos negativos.	Esto no necesariamente indica que no existan incidentes, sino que pueden no estar plenamente visibilizados o formalizados.	Obliga a evitar interpretaciones simplistas que asocien la ausencia de mención con ausencia de problemas.
Dependencia de terceros para detectar fallas.	En varios casos, son los clientes quienes identifican vulnerabilidades o problemas.	Esto sugiere una gestión más reactiva que preventiva, con cierta dependencia de actores externos.	Indica posibles debilidades en los mecanismos internos de monitoreo y control.
Percepciones diversas sobre la madurez en seguridad.	Algunos participantes muestran confianza en la gestión, mientras otros son más críticos.	La percepción interna no es uniforme, sino que varía según experiencias, responsabilidades y niveles de involucramiento.	Ayuda a explicar por qué coexisten visiones positivas y críticas dentro de la misma organización.

Coexistencia de de controles formales y prácticas informales.	Se identifican controles estructurados junto con prácticas no estandarizadas en la operación.	La seguridad se apoya en una base formal, pero su aplicación en la práctica no siempre es consistente.	Permite entender la existencia de una “doble lógica”: lo que está definido y lo que realmente se hace.

Nota. Elaboración propia con base en los resultados de la aplicabilidad del formato Anexo 8. Bitácora de campo.

Triangulación metodológica

Con el propósito de conferir mayor validez, rigor y profundidad a los hallazgos de la presente investigación, se optó por una triangulación metodológica de tipo entre-métodos (inter-metódica). Este enfoque, definido por Denzin (2012) como el uso de múltiples estrategias para estudiar un mismo fenómeno, permite contrastar la información obtenida mediante instrumentos cuantitativos y cualitativos.

En este sentido, se articularon los resultados del análisis estadístico descriptivo e inferencial realizados en IBM SPSS Statistics (mediante el coeficiente de Spearman para la asociación de variables), con las categorías emergentes de las entrevistas semiestructuradas (validadas mediante el acuerdo entre codificadores bajo el índice Kappa de Cohen), la revisión documental del listado maestro, la observación no participante en reuniones de proyecto y la bitácora de campo del investigador.

Esta integración de perspectivas busca la convergencia de los datos y permite que la riqueza narrativa de los testimonios cualitativos complemente y explique las tendencias numéricas observadas, mitigando así los sesgos inherentes a un solo método de recolección (Hernández-Sampieri y Mendoza, 2018). Debido a la extensión y densidad técnica de este análisis cruzado, la matriz completa se presenta en el Anexo 9. No obstante, en la siguiente tabla se presenta una síntesis de los hallazgos integrados:

Tabla 8.

Resumen resultado matriz de triangulación metodológica del diagnóstico organizacionales.

Dimensión / Componente evaluado	Ejes asociados	Convergencia	Divergencia	Interpretación triangulada
1. Impacto y riesgos derivados de la falta de integración de seguridad.	Impacto de la falta de integración de seguridad- Nivel organizacional de riesgo y exposición- Nivel de madurez de gestión.	Existe una clara convergencia entre las percepciones cuantitativas, cualitativas y documentales que indican un impacto bajo, pero con un riesgo latente y dependencia externa para la detección y gestión de vulnerabilidades.	Se identifican divergencias en la percepción del impacto entre los diferentes niveles jerárquicos, así como entre el discurso formal institucional y la práctica operativa cotidiana.	El impacto negativo por falta de integración de seguridad es real, pero tiende a ser subestimado en los niveles operativos. La correlación estadística valida la relación entre riesgo e impacto, mientras que la evidencia cualitativa y documental explicita la dependencia externa y el subregistro de incidentes.
2. Adopción metodológica y efectividad en mitigación de riesgos.	Adopción de metodologías y mitigación de riesgos- Controles de seguridad en el ciclo de vida del proyecto- Nivel de madurez de gestión.	Existe convergencia en el uso de metodologías modernas, aunque con limitaciones evidentes en la efectividad real para mitigar riesgos, sustentada en múltiples fuentes.	Se observa divergencia entre la percepción positiva de los operativos y la visión más crítica de los directivos y la evidencia documental, lo que refleja tensiones en la interpretación de la efectividad.	La adopción metodológica es heterogénea y la efectividad parcial; los análisis inferenciales confirman relaciones significativas entre variables organizacionales, mientras que la evidencia cualitativa y documental muestra limitaciones prácticas que deben ser abordadas.

3. Cultura organizacional y controles para alineación estratégica.	Percepción y cultura de seguridad- Controles de seguridad en el ciclo de vida del proyecto- Marcos de gobernanza y herramientas.	Existe convergencia en la identificación de una brecha entre el discurso estratégico y la práctica operativa, con evidencia estadística que valida el impacto de la cultura en la reducción del riesgo.	Se detecta divergencia entre la percepción positiva reflejada en la encuesta y la evidencia observacional y documental que muestra prácticas insuficientes y desalineadas.	La cultura organizacional es un factor clave para la reducción del riesgo, pero su desarrollo es parcial y heterogéneo; los análisis inferenciales y la triangulación cualitativa-documental sustentan esta conclusión, evidenciando la necesidad de fortalecer la cultura para mejorar la seguridad.

Nota. Elaboración propia con base en los resultados de los instrumentos aplicados anteriormente.

En relación con los hallazgos presentados en la Tabla 8, se identificaron factores que podrían comprometer la validez de los datos, los cuales fueron mitigados mediante las siguientes estrategias:

- **Dimensión 1:** se reconoce un posible sesgo de deseabilidad social en las respuestas, mitigado mediante la triangulación con análisis estadístico y evidencia cualitativa. La limitación en la muestra cualitativa se compensa con la robustez del análisis inferencial.
- **Dimensión 2:** se mitiga el sesgo de reporte mediante análisis comparativo por roles y triangulación documental. Se reconoce la limitación en la muestra cualitativa, que se considera en la interpretación.
- **Dimensión 3:** Se mitiga el efecto Hawthorne mediante triangulación documental y análisis estadístico. Se considera la limitación en la muestra cualitativa para una interpretación equilibrada.

Análisis de los resultados.

El presente capítulo es el núcleo interpretativo de la investigación, donde se contrastan los hallazgos cuantitativos y cualitativos para dar respuesta a los objetivos planteados. Este análisis se estructura bajo lo desarrollado en el diagnóstico organizacional que permite identificar la situación actual de **OSP INTERNATIONAL CALA S.A.S.**, reconociendo sus fortalezas operativas y determinando las oportunidades de mejora críticas para la integración de la seguridad de la información. A través de la triangulación de datos, se exponen las brechas existentes y las estrategias necesarias para alinear la gestión de proyectos con los estándares de protección de activos digitales.

Análisis del impacto de la falta de integración de la seguridad de la información en la gestión de proyectos TI

1) Situación Actual: Análisis de impacto y contraste de evidencias

El diagnóstico evidencia una asimetría de información crítica entre la percepción interna de “bajo impacto” y la realidad operativa observada en la integración de seguridad. En la encuesta, el componente *Impacto de la falta de integración de seguridad* presenta un índice promedio bajo (2,24/5), con concentraciones altas en respuestas 1–2 para retrasos, vulnerabilidades tardías, sobrecostos, incidentes en sistemas recién implementados y retrabajos por incumplimiento. Esta lectura, se tensiona con los hallazgos cualitativos y de observación: no es que el riesgo no exista, sino que no se convierte en impacto visible y registrado, en gran medida por subregistro, dependencia de terceros para detectar fallas y una integración no estandarizada que varía por líder, cliente y contexto.

Desde la observación no participante, la integración de seguridad en el ciclo de vida del proyecto se clasifica como “cumple parcialmente” en *inicio/planeación, ejecución, seguimiento/control, cierre, gestión de servicios y cultura/prácticas*. Esto revela una

vulnerabilidad estructural por diseño: la seguridad aparece como un conjunto de prácticas operativas dispersas (por ejemplo, accesos, herramientas, controles básicos), pero no como un componente transversal, obligatorio y verificable desde planeación hasta cierre. En términos de impacto, esta condición incrementa la probabilidad de materialización de fallas por: (i) variabilidad metodológica (seguridad depende del criterio del líder), (ii) dilución del control en seguimiento y cierre (ausencia de métricas/validaciones sistemáticas), y (iii) puntos ciegos operativos (monitoreo continuo no consolidado; incidentes pueden no ser detectados ni formalizados).

Las entrevistas refuerzan el problema donde se reportan baja ocurrencia de impactos explícitos (no se mencionan de forma consistente retrasos, sobrecostos o incidentes atribuibles a seguridad), pero simultáneamente se describen condiciones que, metodológicamente, son precursores de impacto: presión por tiempos que reduce controles, prácticas operativas riesgosas (por ejemplo, compartir credenciales por medios no seguros), ausencia de monitoreo continuo interno y dependencia del cliente para identificar vulnerabilidades (por ejemplo, hallazgos externos como versiones desactualizadas). La bitácora de campo incluso advierte que los discursos tienden a iniciar desde lo “formal/esperado” y que las limitaciones emergen progresivamente, lo que sugiere una discrepancia entre cumplimiento declarado y ejecución efectiva.

En lo documental, la brecha se vuelve estructural dado que los procedimientos y formatos revisados del proceso de proyectos no incorporan explícitamente la seguridad de la información como criterio transversal u obligatorio. Aunque hay instrumentos donde “podría” documentarse (por ejemplo, requisitos no funcionales, gestión de riesgos en el plan del proyecto), el diagnóstico concluye que no se evidencia desarrollo detallado ni exigencia sistemática de seguridad como dimensión del ciclo de vida. En otras palabras,

aun cuando existan prácticas técnicas aisladas, la organización no garantiza por diseño que la seguridad sea trazable, verificable y auditable en cada proyecto.

El efecto principal no es un historial explícito de incidentes reportados, sino una exposición operativa latente con riesgo de fallas no detectadas. La organización opera con una seguridad “funcional” en ciertos equipos o proyectos, pero con fragilidad institucional. Si el control depende del líder, del cliente o del contexto, entonces el sistema es vulnerable a rotación de talento, presión comercial y heterogeneidad de prácticas. La ausencia de métricas sistemáticas de seguridad en seguimiento/control y la falta de validación formal en cierre implican que el impacto puede estar ocurriendo como riesgo acumulado, no necesariamente como eventos formalizados (lo cual es coherente con la “baja mención espontánea de incidentes” registrada en bitácora).

2) Fortalezas: Capacidades instaladas y activos estratégicos

Aunque la integración presenta fragilidades, el diagnóstico confirma capacidades instaladas que permiten reducir la exposición si se consolidan bajo gobernanza:

1. **Base de madurez y control técnico ya operativa.** En encuesta, *Controles en el ciclo de vida* (3,53) y *Madurez CMMI-DEV* (3,55) se ubican en niveles medio-altos. Ítems con valoraciones altas sugieren capacidades reales en controles como acceso/autenticación (P27 media 4,11), cifrado (P28 media 3,82) y gestión de secretos/configuración (P29 media 3,93), además de revisión de código con enfoque de seguridad (P26 media 3,53) e integración de pruebas de seguridad en pipeline (P19 media 3,62).
2. **Infraestructura y herramientas de trazabilidad y control** reportadas en entrevistas: uso de VPN, repositorios/control de versiones, herramientas de análisis (por ejemplo, SonarQube) e integración parcial CI/CD con prácticas

asociadas a DevSecOps. Estas capacidades son activos porque permiten pasar de controles “manuales” a controles “sistémicos” si se estandarizan.

3. **Marcos organizacionales formales existentes**. En entrevistas se menciona certificación ISO 9001 e IT Mark, y la existencia de un comité de seguridad. Aunque el diagnóstico también expone limitaciones (por ejemplo, dependencia de requerimientos externos y brechas de formación individual), la presencia de estos elementos constituye un activo organizacional que facilita y reduce las barreras para la institucionalización de prácticas de seguridad.
4. **Cultura en desarrollo con disposición declarada**. En encuesta, *Cultura y percepción* alcanzó un promedio de 3,49 con alta valoración en responsabilidad compartida (P43 media 3,91) y priorización directiva percibida (P40 media 3,78). Por su parte, la observación también evidenció una percepción general positiva frente a la seguridad, aunque esta no se refleja de manera consistente en las prácticas cotidianas.

En síntesis, la empresa tiene capacidades técnicas y de proceso suficientes para mitigar los riesgos operativos identificados; su limitación no es la ausencia de herramientas o conocimiento aislado, sino la fragmentación (heterogeneidad por proyecto) y la brecha entre formalidad y ejecución verificable.

3) Oportunidades de Mejora: Brechas de gestión y riesgos latentes

Las oportunidades de mejora no se centran en la incorporación aislada de nuevos controles, sino en el fortalecimiento de las capacidades ya existentes para asegurar un desempeño consistente. En este sentido, el reto principal radica en reducir la variabilidad en su aplicación, ya que esta es la que actualmente genera un riesgo latente en la organización.

1. **Cerrar la brecha de estandarización**

a. Riesgo actual: la observación evidencia que la seguridad depende del criterio del líder y es parcial en todas las fases.
b. Oportunidad: aprovechar la documentación ya existente (planes, definición de requisitos, pruebas, gestión de configuración y trazabilidad) para integrar la seguridad como un componente obligatorio, verificable y trazable en todas las fases del proyecto, especialmente en inicio/planeación, seguimiento/control y cierre, donde actualmente tiende a diluirse

2. **Reducir el subregistro y el punto ciego operativo**
    a. Riesgo actual: la baja mención de incidentes y la percepción de un impacto reducido coexisten con prácticas riesgosas y la ausencia de monitoreo continuo, lo que configura una vulnerabilidad de “impacto silencioso” difícil de detectar y gestionar.
    b. Oportunidad: apalancar herramientas ya utilizadas (pipeline, análisis de código y repositorios) para generar evidencia objetiva y trazabilidad que fortalezca los procesos de seguimiento y control. El diagnóstico señala explícitamente la ausencia de métricas sistemáticas de seguridad en esta fase, identificando allí un vacío crítico a intervenir.
3. **Disminuir la dependencia del cliente/terceros para detectar vulnerabilidades**
    a. Riesgo actual: las entrevistas evidencian que gran parte de los hallazgos de vulnerabilidades provienen de los clientes, en un contexto donde no se cuenta con un monitoreo interno continuo, lo que limita la capacidad de detección temprana.

b. Oportunidad: la organización ya dispone de controles técnicos y capacidades instaladas (herramientas especializadas y un enfoque incipiente de DevSecOps). El reto consiste en consolidar estos recursos como una práctica estándar y transversal, evitando que su aplicación dependa de las particularidades de cada proyecto.

4. **Mitigar la dualidad cultural de conciencia a cumplimiento.**

   a. Riesgo actual: aunque se declara una cultura organizacional positiva frente a la seguridad, en la práctica persiste la priorización de tiempos y cronogramas sobre los controles, junto con resistencias asociadas a limitaciones de tiempo, brechas de capacitación y dificultades en la integración de roles.

   b. Oportunidad: capitalizar la percepción favorable evidenciada (P40 y P43) para exigir coherencia en la operación. No implica únicamente reforzar la sensibilización, sino alinear lo que la organización valora con lo que efectivamente mide, verifica y exige en la práctica.

El diagnóstico permite sostener que la organización ya cuenta con: (i) herramientas técnicas, (ii) procesos de gestión de proyectos y (iii) una cultura organizacional en desarrollo. En este sentido, la transición hacia un escenario ideal no requiere la creación de capacidades desde cero, sino el cierre de la brecha metodológica entre la “existencia de controles” y su “cumplimiento sistemático”. Desde una perspectiva crítico-propositiva, puede plantearse que la empresa dispone de activos suficientes para gestionar adecuadamente la seguridad; sin embargo, su uso actual es heterogéneo. Esto da lugar a un sistema con “zonas seguras” y “zonas vulnerables”, que varían según el proyecto, el líder o el cliente, configurando así una forma de riesgo operativo que termina por institucionalizarse.

Evaluación del grado de adopción y efectividad de metodologías de gestión de proyectos (ágiles, híbridas y/o tradicionales) en la mitigación de riesgos de seguridad de la información

1) Situación Actual: Análisis de impacto y contraste de evidencias

La organización presenta un ecosistema metodológico híbrido y adaptativo, donde coexisten enfoques tradicionales (PMBOK/PMI - Cascada) con marcos ágiles (Scrum). Según la caracterización cuantitativa, el 46.7% de los participantes opera bajo metodologías híbridas y un 35.6% bajo enfoques ágiles (P3). Si bien el componente de *Adopción de metodologías y mitigación de riesgos* registra un índice de 3,51/5 (nivel de efectividad moderada-alta), el análisis crítico revela una fragmentación operativa. En particular, la seguridad no se encuentra integrada de manera intrínseca en el marco metodológico, sino que opera como un elemento complementario cuya aplicación depende del contexto y de las dinámicas de cada proyecto.

Existe una discrepancia metodológica significativa: mientras que los participantes perciben positivamente que las metodologías ágiles facilitan la integración continua (P15 media 3,98), la observación no participante califica el cumplimiento en todas las fases como "parcial". Esto indica que la "agilidad" se utiliza para la entrega funcional, pero no se traduce sistemáticamente en artefactos de seguridad (por ejemplo, Historias de Usuario de Seguridad o criterios de seguridad en el *Definition of Done*). En la práctica, la mitigación de riesgos es reactiva y desigual; los roles operativos y técnicos (66.7% de la muestra) perciben una alta efectividad metodológica (3,79 y 3,53 respectivamente), mientras que el nivel directivo es más crítico (3,33), sugiriendo que la metodología resulta efectiva para la ejecución del trabajo diario, pero falla en garantizar resultados de seguridad a nivel estratégico.

Finalmente, la efectividad en la mitigación de riesgos se ve limitada por una asimetría en la formación. La capacitación en seguridad se concentra principalmente en líderes y desarrolladores (DevOps), mientras que los roles administrativos y de apoyo quedan al margen. Al no establecerse como un requisito transversal dentro del marco metodológico, la seguridad pierde protagonismo a lo largo del proyecto y tiende a diluirse en las fases finales, especialmente en el cierre. La observación confirma que no existen criterios formales de aceptación en seguridad para la entrega final, lo que deja la protección de la información condicionada por la presión de los cronogramas.

2) Fortalezas: Capacidades instaladas y activos estratégicos

La principal fortaleza metodológica de la empresa radica en su capacidad de adaptación y resiliencia operativa. La adopción de modelos híbridos proporciona un nivel de flexibilidad que, si se gestiona adecuadamente, puede convertirse en un habilitador clave para la implementación de la seguridad desde el diseño. Así mismo, los líderes técnicos y de proyecto evidencian una disposición favorable para integrar controles de seguridad dentro de sus flujos de trabajo (pipelines), aprovechando la infraestructura ya existente.

La organización ha logrado implementar espacios de retroalimentación que actúan como barreras de defensa. Las autoevaluaciones postproyecto y las retrospectivas permiten identificar fallas previas y actualizar las matrices de riesgo para futuras iteraciones. Esta capacidad de incorporar “lecciones aprendidas” (P39, media de 3,64) es un activo estratégico, ya que evidencia que la metodología no es estática, sino que cuenta con mecanismos de mejora continua. La alta correlación entre cultura y madurez ($\rho = 0,821$) refuerza esta idea, sugiriendo que dichos mecanismos pueden orientarse eficazmente hacia una mitigación proactiva de los riesgos de seguridad.

Asimismo, la integración de pruebas en el pipeline (P19, media de 3,62), junto con el uso de herramientas como SonarQube, evidencia que la empresa ya dispone del “cómo” técnico dentro de su metodología de desarrollo. Además, al contar con roles definidos y un comité de seguridad activo, la estructura metodológica dispone de los mecanismos de supervisión necesarios para evolucionar de una mitigación accidental a una mitigación sistémica de los riesgos.

3) Oportunidades de Mejora: Brechas de gestión y riesgos latentes

La principal oportunidad radica en la estandarización y formalización de la seguridad dentro de la metodología, con el fin de reducir la variabilidad operativa. El escenario deseado es aquel en el que la seguridad no dependa de la “buena voluntad” ni del tiempo disponible de los líderes, sino que se establezca como un requisito obligatorio dentro del proceso de gestión.

Para capitalizar las fortalezas mencionadas, la empresa debe democratizar la responsabilidad de seguridad a través del marco metodológico. Esto implica expandir la capacitación (actualmente concentrada en perfiles técnicos) hacia todos los roles del proyecto, asegurando que los analistas y el personal administrativo comprendan su función en la mitigación de riesgos. El uso de las ceremonias ágiles es la oportunidad para que las retrospectivas y sesiones de planeación pueden transformarse en espacios donde los indicadores de seguridad (KPIs), derivados de herramientas como SonarQube o de auditorías, orienten la priorización del backlog. De esta manera, la seguridad puede competir en igualdad de condiciones con los tiempos de entrega dentro del proceso de desarrollo.

En conclusión, la empresa debe aprovechar su registro de lecciones aprendidas y su infraestructura de pipeline para avanzar hacia una gobernanza automatizada de la seguridad. El objetivo es transformar la mitigación de riesgos, actualmente percibida

como un evento ocasional (P13, media de 2,71), en un estándar obligatorio e innegociable. Para ello, es fundamental integrar los controles de seguridad en los manuales de procedimiento y en los criterios de aceptación final, de modo que ningún proyecto pueda cerrarse sin una validación formal en esta materia. Con esto, se reduciría significativamente el riesgo de que las vulnerabilidades sean detectadas por el cliente en etapas posteriores.

Identificación de marcos de gobernanza y herramientas de gestión que faciliten la alineación entre los objetivos estratégicos de la organización y la gestión operativa de TI asegurando la protección de la información.

1) Situación Actual: Análisis de impacto y contraste de evidencias

El diagnóstico muestra una desconexión entre lo que plantea la alta dirección y lo que realmente se ejecuta en seguridad. Aunque la gerencia afirma que este tema es una prioridad (P40, media de 3,78), esto no se refleja en una gestión integral. En la práctica, la seguridad se maneja como un tema exclusivo del área tecnológica y no como un compromiso de toda la organización. Una evidencia clara es la forma en que se distribuye la capacitación: mientras los equipos de I+D y DevOps reciben formación constante, el personal administrativo y operativo presenta vacíos importantes, lo que los convierte en el punto más débil en la protección de la información.

Desde la perspectiva de las herramientas de gestión, se evidencia una falta de integración en la información sobre riesgos. La organización no utiliza métricas tácticas (como hallazgos de *vulnerabilidades* o incidentes) para alimentar tableros de control estratégicos. Esto genera que la seguridad sea percibida por la base operativa como un **"obstáculo"** para el cumplimiento de los cronogramas, que siguen siendo el verdadero indicador de éxito priorizado por el negocio. La encuesta confirma esta vulnerabilidad: el ítem sobre presupuesto específico asignado (P41) tiene una valoración moderada-baja

(**3,27**), lo que sugiere que la gobernanza carece de un respaldo financiero autónomo y proporcional a los riesgos estratégicos identificados.

Asimismo, la integración de la seguridad en la gobernanza es principalmente reactiva y depende de factores externos. El diagnóstico cualitativo evidencia que la adopción de estándares como ISO 27001 responde más a exigencias de clientes o contratos específicos que a una política interna proactiva. Esta dependencia de terceros para detectar fallas (versiones desactualizadas o vulnerabilidades en producción) evidencia que las herramientas de gestión interna de riesgos no están alineadas con la protección proactiva de los activos digitales de la organización.

2) Fortalezas: Capacidades instaladas y activos estratégicos

A pesar de la desalineación operativa, OSP INTERNATIONAL CALA S.A.S. posee activos de gobernanza sólidos que representan una ventaja competitiva. La organización cuenta con marcos de referencia internacionales ya adoptados, como ISO 9001 e IT Mark, que proporcionan un lenguaje común de procesos y una estructura documental base. La existencia formal de un Comité de Seguridad y roles definidos (P37 media 3,71 en procesos documentados) son el activo más valioso para facilitar la alineación estratégica; este órgano tiene la capacidad instalada para actuar como puente entre la junta directiva y la realidad técnica.

Otra fortaleza reside en la infraestructura técnica que funciona como herramienta de gestión: el uso de SonarQube, Git, Jenkins y OWASP Dependency Check permite una trazabilidad técnica que es el insumo base para cualquier modelo de gobernanza basado en datos (*Data-Driven Governance*). La alta valoración en la cultura de responsabilidad compartida (P43 media 3,91) indica que el personal reconoce la importancia ética de su labor, lo que facilita la implementación de políticas de gobernanza sin enfrentar una resistencia cultural.

Finalmente, la capacidad de la organización para cumplir con requisitos regulatorios y de calidad exigidos por los clientes demuestra que ya existe una disciplina de cumplimiento consolidada. Esta "memoria institucional" de trabajar bajo estándares puede servir como base para avanzar hacia la adopción de la ISO 27001, permitiendo que la seguridad deje de ser un requisito contractual y se convierta en una ventaja estratégica interna.

3) Oportunidades de Mejora: Brechas de gestión y riesgos latentes

La principal oportunidad de mejora es la **democratización de la gobernanza** y la formalización de herramientas de monitoreo estratégico. La empresa necesita pasar de un modelo donde la seguridad es vista como un tema exclusivo de TI, a uno en el que sea una responsabilidad transversal en todo el negocio. Para ello, es clave cerrar la brecha de comunicación mediante la capacitación del personal administrativo, asegurando que la gestión de los datos no se limite únicamente al desarrollo de software, sino que abarque todo el ciclo organizacional.

Una oportunidad concreta es implementar tableros de riesgo estratégico que traduzcan los problemas técnicos (vulnerabilidades, incidentes, cumplimiento de controles) en indicadores de impacto de negocio (financieros y reputacionales). Esto permitiría a la alta gerencia tomar decisiones informadas sobre la asignación de presupuesto (P41) y la creación de incentivos reales (P44), permitiendo equilibrar la rapidez en las entregas con la necesidad de proteger los activos de la organización.

Finalmente, una de las acciones más urgentes es formalizar un rol de seguridad estable y con autonomía, como un CISO o un responsable de seguridad con presupuesto propio. Aprovechando la existencia de un Comité de Seguridad, la organización puede fortalecer la mejora continua (P39), asegurando que las lecciones aprendidas de cada proyecto no solo mejoren el código, sino también las políticas del Sistema de Gestión

(SG). El objetivo es que la seguridad deje de ser un requisito puntual y se convierta en una característica de calidad en todos los proyectos, reduciendo el riesgo de que los incidentes no se registren adecuadamente y garantizando una gestión más anticipada frente a nuevas amenazas.

Resultados de la Solución

En la presente consultoría, se desarrollaron como principales entregables un conjunto de instrumentos orientados a fortalecer la gestión de la seguridad de la información en los proyectos TI, con énfasis en el desarrollo de software seguro, en coherencia con las necesidades identificadas en el diagnóstico organizacional. Estos productos comprenden, por una parte, las estrategias para la incorporación de controles de seguridad de la información en cada fase del ciclo de vida de los proyectos, y por otra, el modelo de integración de la seguridad de la información en la gestión de proyectos TI.

Estrategias para la incorporación de controles de seguridad de la información en cada fase del ciclo de vida de los proyectos TI

A partir del diagnóstico organizacional, se evidenció que, aunque la empresa cuenta con lineamientos generales de tecnologías de la información y dispone de políticas relacionadas con el tratamiento de datos personales en cumplimiento de la normativa colombiana vigente, no cuenta con políticas específicas de seguridad de la información ni con mecanismos estandarizados que permitan su integración en el ciclo de vida de los proyectos TI.

Esta situación limita la incorporación sistemática de controles, genera vacíos en la trazabilidad y dificulta la verificación del cumplimiento normativo en las distintas fases del proyecto. Asimismo, se identificaron brechas asociadas a la aplicación inconsistente de prácticas de seguridad, la dependencia del criterio del líder del proyecto y la ausencia de lineamientos formales que orienten su gestión de manera transversal.

En coherencia con la intención estratégica de la organización de alinearse con estándares internacionales, se adopta la norma ISO/IEC 27001 como marco para la estructuración de un Sistema de Gestión de Seguridad de la Información (SGSI). Bajo

este enfoque, y tomando como referencia las directrices de la ISO/IEC 27002, se estableció una arquitectura documental basada en una jerarquía de políticas, lineamientos técnicos y procedimientos operativos, orientada a garantizar la adecuada gestión y control de la seguridad de la información. Las políticas establecen los principios y directrices generales, los lineamientos orientan la aplicación de controles, y los procedimientos permiten su implementación práctica.

En este contexto, se establecen políticas específicas que determinan los principios y directrices generales en materia de seguridad, complementadas por lineamientos técnicos que orientan la aplicación de controles en dominios como la gestión de accesos, la protección de la información, la seguridad de las comunicaciones y el uso adecuado de los recursos tecnológicos. A su vez, se desarrollan procedimientos operativos que permiten la implementación práctica de dichos controles con el propósito de asegurar su aplicación sistemática y verificable. Dentro de estos, se destaca el procedimiento de desarrollo seguro de software, el cual se articula directamente con la gestión de proyectos TI y se detalla como un elemento central para la mitigación de riesgos a lo largo del ciclo de vida del software (ver Anexo 10).

Adicionalmente, se incorpora la norma ISO 22301 como referente para la gestión de la continuidad del negocio, con el propósito de asegurar la disponibilidad de los servicios, la capacidad de recuperación ante incidentes y la resiliencia operativa de la organización frente a eventos que puedan afectar la ejecución de los proyectos TI. Esta integración permite complementar el enfoque de seguridad con una visión orientada a la continuidad y sostenibilidad de los procesos críticos.

De manera complementaria, se propone un procedimiento de desarrollo de software seguro, el cual define actividades, controles y responsabilidades alineadas con buenas prácticas internacionales como NIST SP 800-30, NIST SP 800-53, NIST SP 800-61, NIST

SP 800-218, OWASP SAMM, OWSAP Top 10, OWASP Testing Guide, ISO/IEC 27034 y el GDPR (UE 2016/679) (ver Anexo 11).

El criterio de selección y priorización de los marcos de referencia no se basa en su adopción simultánea, sino en su rol funcional dentro del modelo con el fin de evitar la sobreingeniería y la duplicidad de controles. En este sentido, se adopta un enfoque de complementariedad estructurada, donde cada estándar aporta valor en un nivel específico:

- **ISO/IEC 27001 y 27002** se establecen como el marco rector del Sistema de Gestión de Seguridad de la Información (SGSI), al proporcionar la estructura de gobernanza, control y mejora continua.
- **NIST (SP 800-30, 800-61, 800-218)** se utiliza de manera selectiva como guía metodológica para la gestión de riesgos, respuesta a incidentes y desarrollo seguro, complementando el “cómo” operativo que ISO define a nivel general.
- **OWASP (SAMM y Top 10)** se prioriza en el nivel técnico, especialmente en el desarrollo de software, por su enfoque práctico y específico en vulnerabilidades y buenas prácticas de codificación segura.
- **ISO/IEC 27034** se integra como marco de referencia conceptual para la seguridad en aplicaciones, permitiendo alinear el desarrollo seguro con el SGSI sin duplicar estructuras.
- **ISO/IEC 22301** se incorpora como el marco de referencia para la gestión de la continuidad del negocio, permitiendo estructurar capacidades de resiliencia organizacional, recuperación ante desastres y continuidad operativa frente a incidentes que afecten la disponibilidad de los servicios de información.
- **GDPR y normativa nacional** se incorporan como requisitos regulatorios opcionales, delimitando el tratamiento de datos personales dentro del modelo.

Bajo este enfoque, se evita la sobreingeniería mediante tres principios: (i) no duplicidad de controles, donde cada práctica se implementa una sola vez aunque esté referenciada en varios marcos; (ii) alineación por niveles, asignando cada estándar a una dimensión del modelo (estratégica, táctica u operativa); y (iii) adopción selectiva, priorizando únicamente aquellos controles y prácticas que responden a los riesgos y capacidades reales de la organización.

Sin embargo, para garantizar su efectividad, es necesario integrarlo de manera formal dentro del ciclo de vida de los proyectos TI. Para ello, se diseñan las estrategias orientadas a articular las políticas definidas y el procedimiento propuesto, con el fin de incorporar la seguridad de la información de manera estructurada en cada fase del proyecto.

Tabla 9.

Estrategias para la incorporación de controles de seguridad de la información en cada fase del ciclo de vida de los proyectos TI

Fase del proyecto	Estrategia	Controles de seguridad	Trazabilidad (evidencia)	Cumplimiento normativo
Inicio.	Incorporar la seguridad como criterio transversal desde la formulación del proyecto.	- Identificación y valoración inicial de riesgos. - Clasificación de activos de información. - Asociación de activos con riesgos identificados. - Definición de requisitos de seguridad alineados al negocio. - Designación del responsable de seguridad del proyecto. - Definición de roles y responsabilidades en seguridad basados en el modelo AAA	- Acta de inicio con criterios de seguridad. - Registro inicial de riesgos. - Inventario de activos. - Asignación de responsabilidades - Matriz de trazabilidad de requisitos (RTM). - Registro de capacitación - Matriz RACI del proyecto con roles AAA.	ISO 27001 (cláusula 6) / ISO 27002.

Fase del proyecto	Estrategia	Controles de seguridad	Trazabilidad (evidencia)	Cumplimiento normativo
		incorporados en la Matriz RACI. - Capacitación inicial en seguridad para el equipo.		
Planificación.	Integrar la gestión de seguridad mediante un enfoque basado en riesgos.	- Análisis de riesgos (NIST SP 800-30). - Definición de controles (ISO 27002 / NIST SP 800-53). - Plan de tratamiento de riesgos. - Evaluación de proveedores. - Identificación de datos personales. - Evaluación de impacto en privacidad. - Gestión de excepciones de seguridad con aprobación formal. - Aprobación formal del riesgo.	- Matriz de riesgos. - Plan de tratamiento. - Evaluación de terceros. - Registro de tratamiento de datos. - Acta de aceptación de riesgos. - Acta de aprobación gerencial del plan de seguridad.	ISO 27001 / ISO 27002 / NIST SP 800-30 / NIST SP 800-53 / Ley 1581 de 2012 / Decreto 1377 de 2013 / GDPR.
Desarrollo / Ejecución.	Implementar desarrollo seguro bajo enfoque preventivo (“shift-left”).	- Implementación de controles definidos en el plan de tratamiento de riesgos. - Aplicación de OWASP Top 10. - Implementación de OWASP SAMM. - Controles de desarrollo seguro (NIST SP 800-218). - Gestión de cambios (incluyendo control de versiones). - Análisis SAST/DAST. - Gestión de vulnerabilidades.	- Historial de versiones. - Registros de commits. - Reportes SAST/DAST. - SBOM. - Evidencia de accesos. - Registro de configuraciones - Reportes de vulnerabilidades en dependencias. - Actualización de RTM.	OWASP Top 10 / OWASP SAMM / NIST SP 800-218 / ISO 27034 / ISO 27002 / GDPR / Ley 1581 de 2012.

Fase del proyecto	Estrategia	Controles de seguridad	Trazabilidad (evidencia)	Cumplimiento normativo
		- Gestión de dependencias (librerías). - Gestión de configuración. - Principio de mínimo privilegio. - Gestión del ciclo de vida de accesos. - Segregación de funciones (SoD) - Privacy by design.		
Pruebas.	Validar la seguridad como criterio obligatorio de calidad del software.	- Pruebas de seguridad (SAST, DAST, pentesting controlado). - Validación en ambientes segregados. - Verificación contra OWASP Top 10. - Validación de requisitos de seguridad. - Revisión independiente de controles de seguridad. - Gestión de hallazgos. - Uso de datos anonimizados.	- Evidencias de pruebas. - Reportes de vulnerabilidades. - Actas de aprobación. - Registro de incidencias. - Evidencia de anonimización. - RTM validada.	ISO 27001 / ISO 27002 / OWASP Testing Guide / Ley 1581 de 2012 / GDPR.
Implementación / Despliegue.	Asegurar la seguridad en producción mediante controles formales.	- Gestión de cambios y versiones (ITIL). - Configuración segura (hardening). - Separación de ambientes (dev/test/prod). - Gestión de accesos (alta, baja, modificación). - Revisión de privilegios. - Aprobación de despliegue.	- Registros de despliegue. - Logs de acceso - Checklist de hardening. - Evidencia de cambios. - Planes de respaldo. - Registro de accesos.	ISO 27001 / ISO 27002 / ITIL / NIST SP 800-53 / ISO 22301.

Fase del proyecto	Estrategia	Controles de seguridad	Trazabilidad (evidencia)	Cumplimiento normativo
Seguimiento y control.	Monitoreo continuo y gestión activa de la seguridad.	- Planes de respaldo y recuperación. - Gestión de configuración. - Monitoreo de eventos e incidentes. - Gestión de incidentes (NIST SP 800-61). - Clasificación y priorización de incidentes. - Seguimiento de KPIs/KRIs. - Auditorías internas. - Monitoreo de disponibilidad. - Revisión periódica de logs. - Política de retención de registros. - Revisión periódica de activos. - Monitoreo de proveedores. - Evaluación del impacto de la seguridad en los objetivos del negocio. - Capacitación continua en seguridad.	- Reportes de incidentes. - Dashboards. - Informes de auditoría. - Logs y bitácoras. - Indicadores. - Evidencia de revisión de logs. - Reportes de proveedores. - Registro de capacitaciones. - Reporte de alineación seguridad y objetivos del negocio.	ISO 27001 / ISO 27002 / NIST SP 800-61 / ISO 22301.
Cierre.	Consolidar la seguridad como criterio de cierre y mejora continua.	- Auditoría final de controles. - Validación de cumplimiento técnico y legal. - Validación del tratamiento de riesgos. - Validación final de trazabilidad de requisitos de seguridad. - Lecciones aprendidas.	- Informe final de seguridad. - Checklist de cumplimiento. - Registro de lecciones aprendidas. - Informe de cierre. - Evaluación de indicadores. - Registro de actualización de activos.	ISO 27001 / ISO 27002.

Fase del proyecto	Estrategia	Controles de seguridad	Trazabilidad (evidencia)	Cumplimiento normativo
		- Evaluación de riesgos residuales. - Evaluación del desempeño de controles. - Actualización o baja de activos de información. - Definición de plan de mejora continua de controles de seguridad.	- Matriz RTM final consolidada. - Informe de validación del tratamiento de riesgos.	

Nota. Elaboración propia con base en la normatividad nacional vigente y en estándares internacionales de seguridad de la información, desarrollo seguro y continuidad del negocio, utilizados como marco de referencia para la estructuración de las estrategias propuestas.

De manera complementaria, se propuso la construcción de una Matriz RACI como instrumento de apoyo para la organización, integrada al modelo AAA (Arquitectura de Seguridad) planteado en el estudio, con el fin de facilitar la asignación clara de roles y responsabilidades en materia de seguridad de la información a lo largo del ciclo de vida de los proyectos TI (ver Anexo 12). Al categorizar los niveles de participación (Responsable, Accountable, Consultado e Informado), se optimiza la ejecución de actividades, se reducen los conflictos de rol y se garantiza una supervisión coherente con las políticas de seguridad organizacionales.

Modelo propuesto para la integración de Seguridad de la Información en la Gestión de Proyectos TI

Se evidenció que la principal limitación de **OSP INTERNATIONAL CALA S.A.S.** no radica en la ausencia de capacidades técnicas o herramientas de seguridad, sino en la falta de articulación, estandarización y gobernanza de dichas capacidades a lo largo del ciclo de vida de los proyectos TI. Esta situación genera una integración parcial,

heterogénea y dependiente del contexto, en donde la seguridad de la información no actúa como un componente transversal, verificable y obligatorio dentro de la gestión de proyectos.

En este sentido, las brechas identificadas asociadas a la variabilidad en la aplicación de controles, el subregistro de incidentes, la ausencia de métricas sistemáticas, la dependencia del cliente para la detección de vulnerabilidades y la desconexión entre el nivel estratégico y operativo, delimitan un escenario donde el riesgo se manifiesta de manera latente y acumulativa, afectando la capacidad de la organización para garantizar la protección efectiva de sus activos de información.

Bajo este contexto, se hace necesario trascender de un enfoque basado en la implementación aislada de controles hacia un modelo estructurado que permita integrar la seguridad de la información como un eje articulador de la gestión de proyectos TI. En respuesta a esta necesidad, se diseña el Modelo de Integración de Seguridad de la Información en la Gestión de Proyectos TI, concebido como un marco metodológico que alinea los componentes estratégicos, tácticos y operativos de la organización, con el fin de asegurar la incorporación sistemática, trazable y medible de la seguridad en cada fase del ciclo de vida del proyecto.

Este modelo se fundamenta en estándares internacionales como ISO/IEC 27001, ISO/IEC 27002, ISO 22301 y marcos de referencia enfocados en desarrollo seguro (OWASP, NIST). Para ello, se integran tres dimensiones: (i) la gobernanza de la seguridad de la información, orientada a la toma de decisiones estratégicas y la asignación de responsabilidades; (ii) la gestión metodológica de proyectos, donde se incorporan controles, criterios de aceptación y mecanismos de seguimiento en cada fase; y (iii) la operación técnica, soportada en herramientas, automatización y prácticas de DevSecOps.

A diferencia de los enfoques tradicionales, este modelo no propone la creación de nuevas capacidades desde cero, sino la consolidación y estandarización de las ya existentes en la organización. Se espera reducir la fragmentación operativa y fortalecer la coherencia entre lo que se define a nivel organizacional y lo que se ejecuta en los proyectos.

Desde la perspectiva de la consultoría, el modelo propuesto no resulta en un entregable conceptual, sino una intervención estructural sobre el proceso de gestión de proyectos TI, cuyos impactos se reflejan directamente en la forma en que la organización planifica, ejecuta, controla y cierra sus proyectos. En particular, su implementación permite transformar un esquema operativo caracterizado por la variabilidad y la dependencia del criterio individual, hacia un modelo estandarizado y gobernado, donde la seguridad se integra como criterio obligatorio de calidad.

En términos de valor agregado, los principales impactos para el área y el proceso se materializan en: (i) **la estandarización de la gestión de la seguridad**, al reducir la heterogeneidad entre proyectos y asegurar criterios homogéneos de aplicación de controles; (ii) **el fortalecimiento del seguimiento y control**, mediante la incorporación de métricas, indicadores y evidencia trazable que permiten una gestión basada en datos; (iii) **la disminución del riesgo operativo latente**, al promover una detección temprana de vulnerabilidades y reducir la dependencia de terceros para su identificación; (iv) **la mejora en la alineación estratégica**, al conectar los objetivos de seguridad con la toma de decisiones gerenciales y la priorización del negocio; y (v) **el fortalecimiento de la cultura organizacional**, al convertir la seguridad en una responsabilidad transversal y no exclusiva del área técnica.

A continuación, se presenta la estructura, componentes y funcionamiento del modelo propuesto, así como su articulación con los instrumentos desarrollados en el marco de la consultoría.

El modelo de integración de seguridad de la información en la gestión de proyectos TI se concibe como un marco sistémico y multinivel, orientado a garantizar que la seguridad deje de ser un componente operativo y se consolide como un criterio transversal, medible y gobernado a lo largo del ciclo de vida del software. El siguiente modelo responde directamente a las brechas identificadas en el diagnóstico organizacional, particularmente:

- La fragmentación en la aplicación de controles
- La dependencia del criterio del líder del proyecto
- El subregistro de incidentes y ausencia de métricas
- La desconexión entre el nivel estratégico y operativo

En este sentido, el modelo se estructura en tres dimensiones integradas que permiten alinear la organización de forma vertical (estratégico a operativo) y horizontal (a lo largo del ciclo de vida del proyecto):

1. Dimensión de Gobernanza de Seguridad de la Información (Nivel estratégico)

Esta dimensión establece el marco directivo, normativo y de control que orienta la gestión de la seguridad de la información en la organización, asegurando su alineación con los objetivos estratégicos del negocio y su integración dentro del sistema de gestión organizacional.

Propósito: Garantizar que la seguridad de la información sea gestionada como un activo estratégico, con respaldo institucional, asignación de recursos y capacidad de medición, control y mejora continua a nivel organizacional.

Alcance funcional dentro del modelo: Esta dimensión actúa como el nivel rector, definiendo las reglas, prioridades, niveles de riesgo aceptables y mecanismos de supervisión que deben ser adoptados por los proyectos y la operación técnica.

Componentes estructurales

- **Marco normativo y documental (SGSI)**: Definición de políticas, lineamientos técnicos y procedimientos operativos basados en ISO/IEC 27001 e ISO/IEC 27002, que establecen los criterios obligatorios de seguridad aplicables a todos los proyectos TI.
- **Estructura de gobierno y toma de decisiones**: Consolidación del Comité de Seguridad de la Información como instancia de direccionamiento, seguimiento y control, responsable de aprobar políticas, evaluar riesgos estratégicos y priorizar inversiones en seguridad.
- **Definición de roles y responsabilidades (accountability)**: Formalización de responsabilidades en seguridad a nivel organizacional y de proyecto (Responsable de Seguridad, Gerente de Proyecto, Tech Lead), asegurando segregación de funciones y trazabilidad en la toma de decisiones.
- **Gestión integral de riesgos de seguridad**: Implementación de un enfoque sistemático basado en ISO 27005 y NIST SP 800-30, que permita identificar riesgos estratégicos y operativos, definir niveles de riesgo aceptable y establecer planes de tratamiento alineados al negocio
- **Sistema de medición y monitoreo estratégico (KPIs/KRIs)**: Definición de indicadores que traduzcan la seguridad en métricas de negocio, tales como número de vulnerabilidades críticas, tiempo de remediación, incidentes de seguridad y nivel de cumplimiento de controles.

- **Integración con continuidad del negocio (ISO 22301)**: Articulación entre seguridad y resiliencia operativa, garantizando disponibilidad de servicios, capacidad de recuperación ante incidentes, protección de procesos críticos.
- **Gobernanza basada en datos (Data-Driven Governance):** Integración de información proveniente de herramientas técnicas (pipelines, escáneres, logs) hacia niveles directivos, reduciendo el subregistro y fortaleciendo la toma de decisiones basada en evidencia.
- **Función de aseguramiento y auditoría de seguridad:** Mecanismos de verificación independientes (auditorías internas, revisiones del SGSI, controles de segunda línea) que permitan validar el cumplimiento de políticas, la efectividad de controles y la madurez del proceso de desarrollo seguro.

Valor dentro del modelo: Esta dimensión aborda de manera directa la brecha entre los niveles estratégico y operativo, transforma la seguridad de un requisito reactivo, impulsado por terceros, en una prioridad organizacional. Al estar integrada en la gobernanza, la seguridad adquiere respaldo directivo y asignación presupuestal, permitiendo que sea gestionada como un riesgo de negocio medible y auditable. Asimismo, este enfoque mitiga el subregistro de incidentes mediante procesos formales de monitoreo y establece mecanismos de verificación independientes que garantizan la trazabilidad y coherencia entre la política definida y la operación ejecutada.

Indicadores de seguridad (KPIs y KRIs estratégicos)

Con el fin de fortalecer el sistema de medición y monitoreo estratégico de la seguridad de la información, se establecen indicadores clave de desempeño (KPIs) e indicadores clave de riesgo (KRIs) que permiten traducir los eventos técnicos de seguridad en métricas comprensibles para la toma de decisiones gerenciales. Estos indicadores

facilitan la visibilidad del riesgo, el control del desempeño y la anticipación de impactos sobre el negocio.

Tabla 10.

Matriz de indicadores de seguridad (SMART)

Indicador	Definición	Fórmula	Meta (SMART)	Frecuencia	Interpretación
Número de vulnerabilidades críticas abiertas.	Cantidad de vulnerabilidades críticas sin remediar en un periodo.	Conteo total.	≤ 5 vulnerabilidades críticas abiertas por mes en 6 meses.	Mensual.	Alto valor indica exposición crítica al riesgo.
Tiempo promedio de remediación de vulnerabilidades (MTTR).	Tiempo promedio en resolver vulnerabilidades identificadas.	Σ días de remediación / total vulnerabilidades.	≤ 5 días hábiles para vulnerabilidades críticas en 6 meses.	Mensual.	Mide capacidad de respuesta operativa.
Tasa de incidentes de seguridad.	Proporción de incidentes respecto a los activos o proyectos.	(Incidentes reportados / Total proyectos o activos) × 100.	≤ 10% trimestral.	Trimestral.	Permite medir estabilidad y exposición.
Nivel de cumplimiento de controles de seguridad.	Grado en que los controles definidos se implementan y verifican.	(Controles cumplidos / Controles definidos) × 100.	≥ 90% en 12 meses.	Trimestral.	Refleja madurez del sistema de control.
Vulnerabilidades detectadas en producción.	Proporción de fallas detectadas después del despliegue.	(Vulnerabilidades en producción / Total vulnerabilidades) × 100.	≤ 10% en 12 meses.	Trimestral.	Alto valor indica fallas en prevención.
Cobertura de análisis de seguridad.	Porcentaje de activos o proyectos evaluados con herramientas de seguridad.	(Activos analizados / Total activos) × 100.	≥ 85% en 6 meses.	Mensual.	Mide capacidad de detección preventiva.

Indicador	Definición	Fórmula	Meta (SMART)	Frecuencia	Interpretación
Índice de recurrencia de vulnerabilidades.	Frecuencia de repetición de vulnerabilidades previamente identificadas.	(Vulnerabilidades repetidas / Total vulnerabilidades) × 100.	≤ 15% en 9 meses.	Trimestral.	Evidencia fallas estructurales en controles.
Nivel de cumplimiento de tiempos de respuesta a incidentes.	Porcentaje de incidentes atendidos dentro del tiempo definido.	(Incidentes atendidos en SLA / Total incidentes) × 100.	≥ 90% en 6 meses.	Mensual.	Mide efectividad del proceso de respuesta.

Nota. Elaboración propia.

Los indicadores definidos permiten medir el estado actual de la seguridad. El enfoque predictivo y preventivo facilita la transición de una gestión reactiva hacia un modelo de seguridad basado en riesgo, alineado con los objetivos estratégicos del negocio.

2. Dimensión de Gestión Metodológica de Proyectos (Nivel táctico)

Esta dimensión operacionaliza la gobernanza, integra la seguridad de la información dentro del ciclo de vida de los proyectos TI, convirtiéndola en un criterio obligatorio de gestión, ejecución y calidad.

Propósito: Garantizar que la seguridad sea incorporada de manera sistemática, trazable y verificable en todas las fases del proyecto, independientemente del enfoque metodológico (ágil, tradicional o híbrido).

Alcance funcional dentro del modelo: Actúa como el mecanismo de traducción entre la estrategia (gobernanza) y la ejecución (operación técnica), asegurando que los lineamientos definidos se implementen de manera homogénea en todos los proyectos.

Componentes estructurales

- **Integración de seguridad por fases del ciclo de vida**: Incorporación de controles, actividades y criterios de validación en (Inicio, Planificación, Desarrollo, Pruebas, Despliegue, Seguimiento y control y cierre).

- **Gestión de requisitos de seguridad (Security by Design)**: Inclusión obligatoria de requisitos de seguridad en la matriz de trazabilidad (RTM) para asegurar su seguimiento desde la definición hasta la validación final.
- **Criterios formales de aceptación en seguridad**: Integración de la seguridad como condición de calidad mediante Definition of Done (en entornos ágiles) y Actas de aprobación y validación (en enfoques tradicionales).
- **Gestión de riesgos de seguridad en proyectos**: Incorporación del análisis, tratamiento y seguimiento de riesgos de seguridad dentro del plan del proyecto.
- **Integración con procesos transversales**: Articulación con Gestión de cambios, Gestión de vulnerabilidades, Gestión de configuración y Gestión de servicios.
- **Mecanismos de trazabilidad y evidencia**: Uso de artefactos como RTM, registros de pruebas, reportes de vulnerabilidades, actas de aprobación que permitan auditoría y control.
- **Incorporación de seguridad en marcos ágiles e híbridos**: Uso de ceremonias ágiles (planning, retrospectives) para priorizar riesgos de seguridad, integrar hallazgos en backlog y fortalecer mejora continua.
- **Puntos de control obligatorios de seguridad (Security Gates):** Definición de hitos dentro del ciclo de vida donde la continuidad del proyecto depende de la validación de seguridad (aprobación de requisitos, liberación a producción, cierre).

Relación con el diagnóstico: Esta dimensión aborda directamente la variabilidad en la aplicación de controles, la dependencia del criterio del líder, la ausencia de validaciones formales en el cierre y la falta de integración real en metodologías ágiles.

Valor dentro del modelo: Permite transformar la seguridad en los proyectos de opcional a obligatoria, de implícita a trazable, de reactiva a preventiva, dependiente del contexto a estandarizada organizacionalmente. La transición hacia una seguridad

preventiva y auditable se materializa mediante la integración de puntos de control obligatorios (*gates*). Estos mecanismos aseguran que el avance del proyecto esté supeditado a la verificación de controles técnicos y operativos, garantizando la coherencia entre las políticas institucionales y la ejecución real en los proyectos de TI.

3. Dimensión de Operación Técnica y DevSecOps (Nivel operativo)

Esta dimensión materializa la seguridad a través de la implementación de controles técnicos, automatización y herramientas, integrándola directamente en el desarrollo y operación del software.

Propósito: Asegurar la implementación efectiva, continua y automatizada de controles de seguridad, permitiendo una detección temprana de vulnerabilidades y una gestión proactiva del riesgo.

Alcance funcional dentro del modelo: Representa el nivel de ejecución, donde la seguridad se convierte en controles técnicos verificables y medibles.

Componentes estructurales

- **Integración de seguridad en pipelines CI/CD (DevSecOps)**: Automatización de controles de seguridad en el ciclo de integración y despliegue continuo.
- **Herramientas de análisis y detección de vulnerabilidades**
    - SAST (análisis estático)
    - DAST (análisis dinámico)
    - IAST (análisis interactivo)
    - SCA (gestión de dependencias - OWASP Dependency Check)
    - Análisis de código (SonarQube)
- **Gestión segura del código y versiones**: A través de repositorios controlados (Git), revisión de código (code review), control de ramas y releases

- **Gestión de configuraciones seguras**: Hardening de sistemas, gestión de secretos y separación de ambientes.
- **Monitoreo continuo y trazabilidad**: Logging centralizado, auditoría de eventos y detección de anomalías.
- **Gestión continua de vulnerabilidades**: Identificación, clasificación, remediación y validación.
- **Enfoque "shift-left security"**: Integración de la seguridad desde las fases tempranas del desarrollo para reducir costos y riesgos.
- **Generación de métricas operativas para la toma de decisiones:** Los resultados de herramientas (vulnerabilidades, cobertura de pruebas, tiempos de remediación, hallazgos recurrentes) deben estructurarse como insumo para KPIs/KRIs a nivel estratégico.

Relación con el diagnóstico: Esta dimensión permite integrar directamente las herramientas existentes (SonarQube, CI/CD, repositorios), las prácticas técnicas ya implementadas parcialmente y la capacidad instalada en equipos DevOps.

Valor dentro del modelo: Permite transformar la operación de seguridad de controles manuales a controles automatizados, de una detección tardía y limitada a una detección temprana con trazabilidad en tiempo real, de dependencia de clientes a autonomía interna de detección. Al integrar mecanismos de trazabilidad en tiempo real, se garantiza una visibilidad completa que reduce el riesgo latente revelado en el diagnóstico inicial. Además, la generación de datos objetivos permite alimentar los niveles de gobernanza, mitigar el subregistro de incidentes y asegurar que la toma de decisiones se sustente en una base de evidencia técnica sólida.

Figura 55.

Modelo de integración de seguridad de la información en proyectos TI

Nota. Elaboración propia.

Propuesta indicadores SMART para validación.

A continuación, se establecen indicadores bajo el enfoque SMART (Specific, Measurable, Achievable, Relevant, Time-bound) con el propósito de validar la implementación, desempeño y efectividad del modelo de integración de la seguridad de la información en la gestión de proyectos TI,

A continuación, los indicadores permiten evaluar de manera objetiva el grado de adopción del modelo, su impacto en la reducción de riesgos y su contribución a la alineación entre los niveles estratégico, táctico y operativo de la organización. Asimismo,

facilitan la toma de decisiones basada en datos, el fortalecimiento del control organizacional y la mejora continua del Sistema de Gestión de Seguridad de la Información.

Tabla 11.

Matriz de indicadores SMART para validación del modelo

Indicador	Definición	Fórmula	Meta (SMART)	Frecuencia	Responsable
		Gobernanza			
Cumplimiento de implementación del SGSI en proyectos.	Mide el porcentaje de proyectos que adoptan formalmente los lineamientos de seguridad definidos.	(Proyectos con SGSI aplicado / Total proyectos) × 100.	≥ 90% de proyectos con SGSI aplicado en un periodo de 12 meses.	Trimestral.	Responsable de Seguridad.
Nivel de reporte de riesgos e incidentes de seguridad.	Evalúa la formalización y visibilidad del riesgo mediante su registro y gestión.	(Riesgos/incidentes registrados / Riesgos/incidentes identificados) × 100.	≥ 85% de registro formal en 6 meses (reducción del subregistro).	Mensual.	Comité de Seguridad.
Cumplimiento de KPIs/KRIs de seguridad.	Mide el grado en que los indicadores definidos alcanzan sus metas establecidas.	(KPIs cumplidos / Total KPIs definidos) × 100.	≥ 80% de cumplimiento sostenido en 12 meses.	Trimestral.	Alta Dirección / Seguridad.
		Gestión de Proyectos			
Proyectos con requisitos de seguridad trazables.	Mide la integración de seguridad desde el diseño mediante RTM.	(Proyectos con RTM de seguridad / Total proyectos) × 100.	≥ 90% en 9 meses.	Trimestral.	PMO / Tech Lead.

Indicador	Definición	Fórmula	Meta (SMART)	Frecuencia	Responsable
Cumplimiento de Security Gates.	Evalúa si los proyectos cumplen puntos de control obligatorios de seguridad.	(Gates aprobados / Gates definidos) × 100.	100% de cumplimiento en cada proyecto (desde mes 6).	Por proyecto.	PMO / Seguridad.
Proyectos cerrados con validación de seguridad	Mide si la seguridad se valida formalmente como criterio de cierre.	(Proyectos con validación final / Total proyectos cerrados) × 100.	≥ 95% en 12 meses.	Trimestral.	PMO / Auditoría.
		Operación Técnica (DevSecOps)			
Cobertura de análisis de seguridad automatizados.	Mide el uso de herramientas de seguridad en el pipeline.	(Proyectos con SAST/DAST/SCA / Total proyectos) × 100.	≥ 85% en 6 meses.	Mensual.	DevOps / Seguridad de la Información.
Tiempo promedio de remediación de vulnerabilidades críticas.	Mide la capacidad de respuesta ante vulnerabilidades de alto impacto.	Promedio de días de remediación.	≤ 5 días hábiles en 6 meses.	Mensual.	Equipo técnico.
Tasa de vulnerabilidades detectadas en producción.	Mide la efectividad del enfoque preventivo (shift-left).	(Vulnerabilidades en producción / Total vulnerabilidades) × 100.	≤ 10% en 12 meses.	Trimestral.	Seguridad de la información / DevOps.

Nota. Elaboración propia con base en el modelo propuesto para la integración de la seguridad de la información en proyectos TI.

La matriz anterior tiene como propósito validar la implementación y efectividad del modelo propuesto, se establecen indicadores bajo el enfoque SMART, los cuales permiten medir el grado de adopción, desempeño y madurez de la seguridad de la información en los proyectos TI, alineados con las tres dimensiones del modelo: gobernanza, gestión metodológica y operación técnica.

Validación del modelo mediante técnica Delphi

Antes de realizar el prototipo del modelo, se implementó una validación cualitativa mediante la adaptación de la técnica Delphi, a través de la consulta a expertos en seguridad de la información con el propósito de fortalecer la validez conceptual y aplicabilidad del modelo propuesto. Según Reguant y Torrado (2016), esta técnica se define como un proceso sistemático y reflexivo de consulta a expertos que permite alcanzar un consenso sobre temas donde no existe una respuesta única o puramente estadística. En este proceso participaron dos profesionales con experiencia en roles de liderazgo en seguridad: un Chief Information Security Officer (CISO) y un especialista en seguridad de la información con enfoque en la gestión de proyectos TI.

La aplicación de esta técnica permitió someter el modelo a un proceso de revisión crítica, orientado a identificar su coherencia, pertinencia, viabilidad de implementación y alineación con las necesidades reales de la organización. La retroalimentación obtenida se centró en aspectos clave relacionados con la trazabilidad del modelo frente a los hallazgos del diagnóstico, su aplicabilidad mínima viable, su integración con marcos organizacionales existentes y su capacidad para generar valor sin incurrir en sobreingeniería.

Principales hallazgos de la validación experta

Los expertos coincidieron en la necesidad de fortalecer la correspondencia explícita entre los hallazgos críticos del diagnóstico y los componentes del modelo. En este sentido, se recomendó demostrar de manera estructurada cómo el modelo responde a problemáticas específicas identificadas en la organización. La retroalimentación obtenida se agrupó en categorías analíticas, permitiendo identificar los principales focos de ajuste y validación del modelo.

1. Correspondencia entre diagnóstico y modelo

Los expertos señalaron la necesidad de evidenciar de manera explícita la relación entre los hallazgos críticos del diagnóstico organizacional y los componentes del modelo propuesto. En particular, enfatizaron que el modelo debe demostrar cómo cada brecha identificada (como el subregistro de incidentes, la dependencia del cliente para la detección de vulnerabilidades, la ausencia de validaciones formales en el cierre de proyectos y la falta de métricas de seguridad) se encuentra directamente abordada mediante componentes específicos del modelo, así como los mecanismos de evidencia que soportan su gestión.

2. Priorización de brechas críticas

Se identificó como aspecto relevante la necesidad de priorizar las brechas más críticas para la organización, destacando especialmente la variabilidad en la aplicación de la seguridad entre proyectos. En este sentido, recomendaron que el modelo evidencie claramente cómo esta brecha es abordada de forma prioritaria.

3. Definición de un baseline mínimo del modelo

Los expertos recomendaron establecer un conjunto mínimo de elementos obligatorios que aseguren un nivel base de seguridad en todos los proyectos, independientemente de su tamaño o enfoque metodológico. Este baseline debe incluir tanto artefactos mínimos como puntos de control (gates), con el fin de garantizar aplicabilidad práctica sin generar sobrecarga operativa.

5. Definición de un enfoque de implementación progresiva (mínimo viable)

Los expertos destacaron la importancia de definir un alcance mínimo viable del modelo, que permita su implementación gradual dentro de la organización. Se enfatizó que no todos los componentes deben implementarse simultáneamente, sino que se requiere una priorización que facilite la adopción inicial y la evolución progresiva del modelo.

4. Integración efectiva de la seguridad en metodologías ágiles

Se evidenció la preocupación de que la seguridad, en entornos ágiles, pueda limitarse a espacios de discusión sin una implementación efectiva. En este sentido, los expertos sugirieron fortalecer los mecanismos que aseguren que la seguridad se traduzca en actividades concretas dentro del flujo de trabajo, particularmente en la priorización y gestión del backlog.

6. Integración con el sistema de gestión organizacional existente

Finalmente, se resaltó la necesidad de asegurar que el modelo se integre con el Sistema de Gestión existente, particularmente con marcos como ISO 9001 e IT Mark, evitando la duplicidad de procesos y documentación. Los expertos recomendaron que la seguridad se articule como un componente transversal dentro de los procesos ya establecidos, en lugar de configurarse como un sistema independiente.

Fortalecimiento del modelo para la integración de la seguridad de la información en la gestión de proyectos TI

A partir de los resultados obtenidos mediante la técnica Delphi, el modelo de integración de seguridad de la información fue ajustado con el fin de fortalecer su aplicabilidad, coherencia estructural y alineación con las necesidades reales de la organización. Estos ajustes no implican una modificación de su arquitectura base, sino una refinación funcional orientada a su implementación efectiva. Los principales ajustes incorporados se describen a continuación:

En primer lugar, se presenta la relación estructurada entre las principales brechas identificadas en el diagnóstico y los componentes del modelo que permiten su mitigación:

Tabla 12.

Matriz de trazabilidad diagnóstico - modelo

Brecha identificada (Diagnóstico)	Hallazgo	Componente del modelo	Mecanismo de mitigación	Evidencia / Trazabilidad
Subregistro de incidentes de seguridad.	Baja visibilidad de incidentes; percepción de bajo impacto pese a prácticas riesgosas y ausencia de monitoreo continuo.	Sistema de KPIs/KRIs; monitoreo continuo; gestión de incidentes (NIST SP 800-61).	Institucionalización del registro obligatorio de incidentes mediante flujos formales, integración de logs centralizados y automatización del monitoreo, reduciendo la dependencia de la percepción individual y habilitando la trazabilidad del evento desde su detección hasta su cierre.	Reportes de incidentes; dashboards de monitoreo; logs centralizados (SIEM o repositorios); indicadores de tasa de incidentes y tiempo de respuesta.
Dependencia del cliente para detección de vulnerabilidades.	Identificación reactiva de vulnerabilidades a partir de terceros.	Integración de seguridad en CI/CD (SAST, DAST, SCA); pruebas de seguridad en ciclo de testing.	Implementación de un enfoque preventivo “shift-left”, incorporando herramientas automatizadas de análisis de código, dependencias y comportamiento en el pipeline, permitiendo la detección temprana y reducción de vulnerabilidades en producción.	Reportes SAST/DAST/SCA; SBOM; reportes de vulnerabilidades; historial de remediación; evidencia de ejecución en pipeline.
Variabilidad en la aplicación de controles.	Aplicación heterogénea de la seguridad dependiendo del líder o contexto del proyecto.	Security Gates; estandarización de procesos; políticas del SGSI.	Definición de puntos de control obligatorios (gates) en cada fase del ciclo de vida, condicionando el avance del proyecto	Checklists de seguridad; actas de aprobación de gates; matriz de trazabilidad (RTM); informes de auditoría.

Brecha identificada (Diagnóstico)	Hallazgo	Componente del modelo	Mecanismo de mitigación	Evidencia / Trazabilidad
			a la validación de controles de seguridad y asegurando una aplicación homogénea organizacional.	
Ausencia de métricas sistemáticas de seguridad.	Falta de indicadores para medir desempeño, riesgo e impacto en seguridad.	Sistema de KPIs/KRIs; gobernanza basada en datos; métricas derivadas de herramientas técnicas.	Estructuración de un sistema de medición que transforme eventos técnicos (vulnerabilidades, incidentes, tiempos de respuesta) en indicadores estratégicos, facilitando la toma de decisiones basada en datos y el monitoreo continuo del desempeño.	Tableros de control; reportes periódicos; indicadores SMART; métricas de herramientas (SonarQube, CI/CD, logs).
Ausencia de validación formal en el cierre de proyectos.	Inexistencia de criterios obligatorios de seguridad como condición de entrega.	Validación de seguridad en cierre; evaluación de riesgos residuales; criterios de aceptación.	Integración de la seguridad como criterio obligatorio de calidad en el cierre del proyecto, mediante validaciones formales, verificación de cumplimiento de controles y evaluación de riesgos residuales antes de la liberación.	Informe final de seguridad; checklist de cierre; acta de aprobación; RTM validada; registro de lecciones aprendidas.
Desconexión entre nivel estratégico y operativo.	La seguridad es priorizada a nivel directivo, pero no se traduce en la operación.	Comité de seguridad; definición de roles; gobernanza basada en datos; integración con SGI.	Establecimiento de mecanismos de articulación entre niveles mediante flujos de información estructurados, donde los datos	Informes ejecutivos; dashboards estratégicos; reportes de cumplimiento;

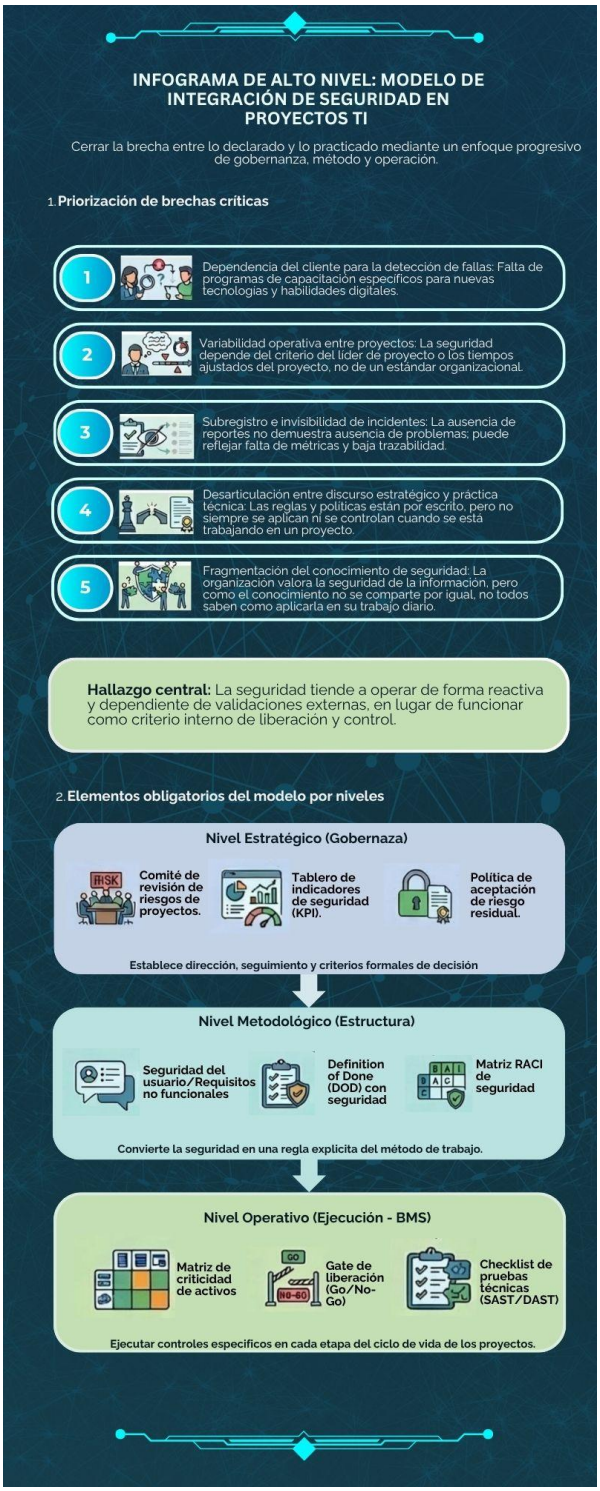
Brecha identificada (Diagnóstico)	Hallazgo	Componente del modelo	Mecanismo de mitigación	Evidencia / Trazabilidad
			operativos (vulnerabilidades, incidentes, cumplimiento) alimentan la toma de decisiones estratégicas y permiten el seguimiento organizacional.	actas de comité de seguridad.
Conocimiento fragmentado y desarticulación organizacional.	Cada rol describe parcialmente el proceso, evidenciando ausencia de una visión integral compartida sobre la seguridad en proyectos TI.	Marco de roles y responsabilidades de seguridad (Modelo AAA - Arquitectura de Seguridad); definición organizacional de responsabilidades	Definición e implementación de una matriz RACI de seguridad a lo largo del ciclo de vida del proyecto, asegurando claridad en responsabilidades, articulación entre roles y apropiación organizacional de la seguridad.	Matriz RACI de seguridad; manual de funciones actualizado; descripciones de cargo con responsabilidades de seguridad; evidencia de socialización.

Nota. Elaboración propia.

En segundo lugar, se presenta la siguiente infografía como ruta estratégica de despliegue para el modelo propuesto. La estructura inicia con la priorización estratégica de las brechas críticas; posteriormente, define el conjunto de artefactos obligatorios que deben integrarse en los niveles o dimensiones estratégico, metodológico y operativo de la organización; y finalmente, establece una ruta de implementación progresiva bajo la premisa de un Modelo Mínimo Viable (MMV).

Figura 56.

Ruta estratégica para la implementación del modelo de integración de seguridad en la gestión de proyectos TI.



Nota. Elaboración propia a partir de los resultados de la investigación.

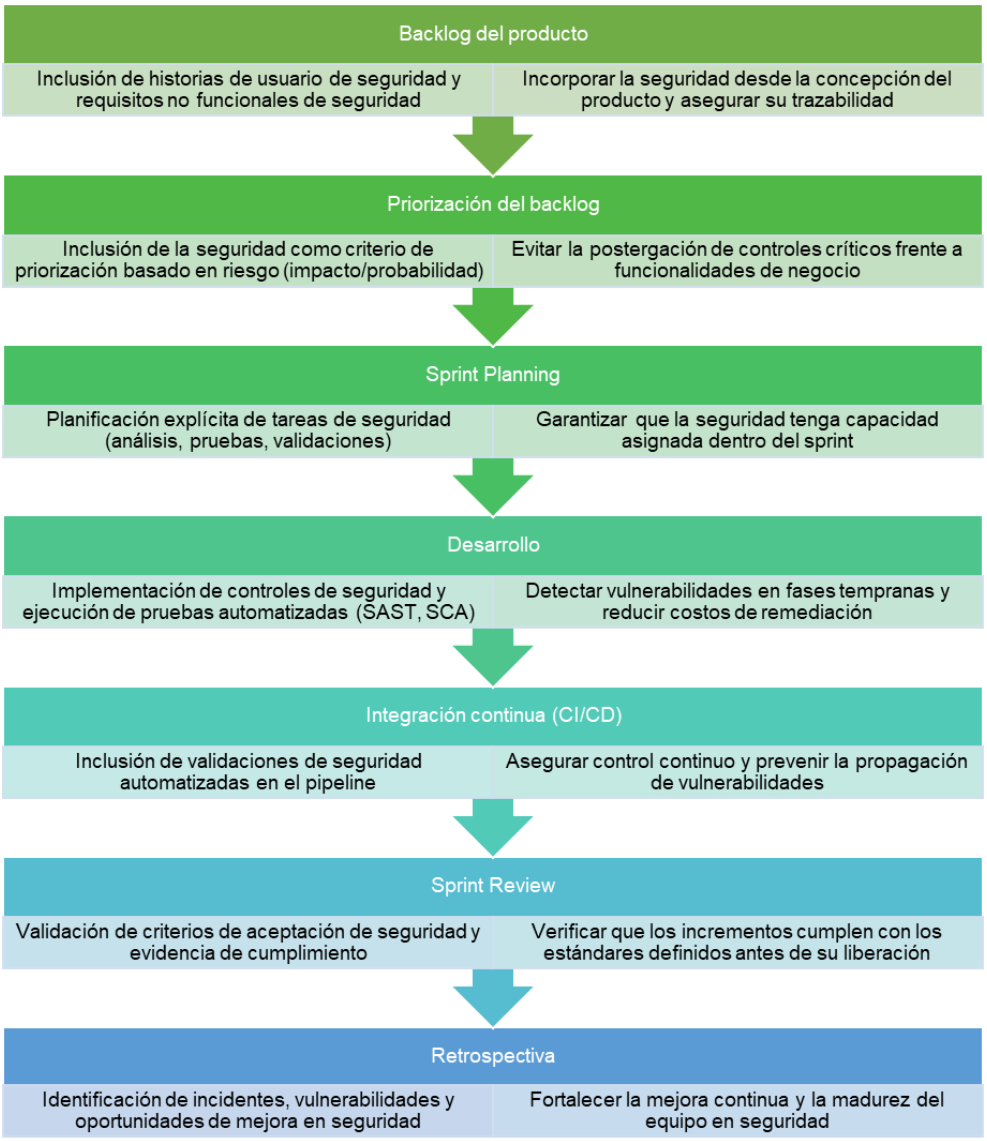
En tercer lugar, se establece la integración efectiva de la seguridad de la información en metodologías ágiles con el propósito de garantizar su materialización en actividades

concretas dentro del flujo de trabajo. Esta integración se operacionaliza mediante la incorporación de mecanismos propios de cada marco ágil, tales como requisitos funcionales y no funcionales de seguridad, criterios de validación y prácticas de aseguramiento continuo.

En el caso específico de Scrum, la seguridad se implementa mediante la inclusión de historias de usuario de seguridad, criterios de aceptación asociados y su incorporación dentro del Definition of Done, así como la gestión de vulnerabilidades como parte del backlog del producto.

Figura 57.

Mecanismos de integración de la seguridad de la información (enfoque DevSecOps) en el flujo de trabajo de metodologías ágiles.



Nota. Elaboración propia.

Por último, se establece la articulación del modelo con el Sistema de Gestión de la organización, evitando la generación de estructuras paralelas o la duplicidad de procesos. En este marco, la seguridad de la información se integra como un componente transversal dentro de los procesos existentes, alineándose con estándares organizacionales actuales como ISO 9001 e IT Mark, y aprovechando los mecanismos ya definidos en términos de gestión, control y mejora continua.

En este sentido, a continuación se presenta la arquitectura del modelo por capas, la cual evidencia cómo los diferentes marcos de referencia se encuentran organizados y convergen dentro de la organización, de acuerdo con su rol funcional. Esta arquitectura permite comprender la relación entre los niveles estratégico, metodológico y operativo, así como su articulación en la ejecución de los proyectos, garantizando una integración coherente, sin superposición de funciones y orientada a la aplicación efectiva de la seguridad de la información.

Tabla 13.

Arquitectura del modelo propuesto por capas

Nivel del modelo	Marcos / Referencias	Rol dentro del modelo	Cómo se integran	Resultado esperado
Gobernanza y Gestión (Estratégico).	ISO/IEC 27001 - 27002 ISO/IEC 9001 (Activa) IT Mark (Activa).	Definir lineamientos, control, cumplimiento y alineación estratégica de la seguridad con el negocio.	- ISO 27001 estructura el SGSI y los controles - ISO 9001 integra seguridad en procesos - IT Mark orienta el nivel de madurez organizacional.	Seguridad alineada con la estrategia organizacional, con gobierno, control y mejora continua.
Gobernanza y gestión (Estratégico transversal).	Ley 1581 de 2012 (Activa) GDPR ISO/IEC 22301.	Establecer lineamientos transversales de cumplimiento, protección de datos y continuidad del negocio aplicables a todos los niveles del modelo.	- Regulación define cumplimiento. - ISO 22301 gestiona continuidad.	Fortalece el cumplimiento normativo, protección de la información y continuidad operativa ante incidentes.
Metodológico (Gestión de proyectos).	PMI (Cascada) (Activa) Scrum (Ágil) (Activa) NIST (800-30, 800-61, 800-218) ISO 27034.	Traducir la seguridad en prácticas dentro del ciclo de vida del proyecto.	- NIST define el “cómo” (riesgos, incidentes, desarrollo seguro). - ISO 27034 estructura seguridad en aplicaciones.	Implementación estructurada, adaptable y consistente de la seguridad en proyectos.

Nivel del modelo	Marcos / Referencias	Rol dentro del modelo	Cómo se integran	Resultado esperado
Operativo (Técnico).	OWASP (SAMM, Top 10) DevSecOps CI/CD (Opcional: ITIL).	Implementar controles técnicos y asegurar ejecución continua de la seguridad.	- PMI integra seguridad en gestión formal. - Scrum la incorpora en backlog y sprints. - OWASP define vulnerabilidades y prácticas. - DevSecOps integra seguridad en desarrollo. - CI/CD automatiza controles. - ITIL gestiona servicios seguros (opcional).	Detección temprana de vulnerabilidades y control continuo en operación.
Ejecución (Proyectos TI).	Proyectos bajo enfoque Cascada o Ágil (Activa).	Materializar la seguridad en la ejecución real de los proyectos.	- Aplicación del baseline mínimo- Uso de Security Gates- Validación continua de seguridad.	Proyectos TI seguros, homogéneos y trazables.

Nota. Elaboración propia con base en el modelo propuesto para la integración de la seguridad de la información en proyectos TI.

La arquitectura presentada evidencia que los marcos de referencia se integran de forma estructurada dentro del modelo y permiten su complementariedad en los diferentes niveles organizacionales. De esta manera, la gobernanza define los lineamientos estratégicos, el nivel metodológico traduce estos lineamientos en prácticas aplicables en los proyectos, y el nivel operativo asegura su implementación técnica, materializándose finalmente en la ejecución de proyectos TI seguros.

Conclusiones y Recomendaciones

A continuación, se presentan las conclusiones de la consultoría académica desarrollada en la empresa, así como las recomendaciones de cierre del trabajo.

Conclusiones

Los resultados obtenidos a lo largo del diagnóstico, el diseño del modelo y su validación permiten establecer una visión integral sobre el estado actual de la seguridad de la información en la gestión de proyectos TI dentro de la organización. Dichos resultados evidencian tanto las principales brechas existentes como las oportunidades de mejora en términos de integración, gobernanza y operación.

En primer lugar, se concluye que la falta de integración formal de la seguridad de la información en la gestión de proyectos TI sí genera efectos relevantes sobre la operación organizacional, aunque estos no siempre se manifiestan de forma visible o sistemáticamente registrada. El diagnóstico evidenció brechas asociadas al subregistro de incidentes, la dependencia del cliente para la detección de vulnerabilidades, la ausencia de métricas sistemáticas, la variabilidad en la aplicación de controles y la desconexión entre el nivel estratégico y la ejecución operativa. Lo anterior permite afirmar que el principal problema no radica únicamente en la ocurrencia de eventos de seguridad, sino en la inexistencia de un marco organizacional que los prevenga, los haga trazables y los convierta en información útil para la toma de decisiones.

En segundo lugar, se identificó que la organización opera en un entorno metodológico predominantemente híbrido y ágil, lo cual representa una oportunidad importante para integrar la seguridad de manera continua dentro del ciclo de vida de los proyectos. Sin embargo, los hallazgos muestran que dicha integración no ocurre de manera homogénea ni estructurada, sino que depende del criterio del líder del proyecto, del nivel de

experiencia del equipo o de exigencias externas del cliente. En este sentido, si bien las metodologías ágiles y combinadas ofrecen condiciones favorables para incorporar prácticas de seguridad desde etapas tempranas, su efectividad depende de que existan mecanismos formales de priorización, criterios de aceptación, Definition of Done, validaciones técnicas y responsabilidades claramente definidas.

En tercer lugar, se concluye que la alineación entre los objetivos estratégicos de la organización y la gestión operativa de TI requiere fortalecerse a través de marcos de gobernanza que conviertan la seguridad de la información en un componente transversal. Aunque la empresa cuenta con referentes organizacionales valiosos, como ISO 9001 e IT Mark, el estudio evidenció que estos no han sido suficientes para traducir la seguridad en prácticas consistentes dentro de los proyectos. Por ello, la incorporación articulada de marcos como ISO/IEC 27001, NIST, ISO 27034 y principios de continuidad y cumplimiento normativo permite cerrar la brecha entre lo directivo y lo operativo, facilitando una visión más estructurada del riesgo, el control y la trazabilidad.

En cuarto lugar, se estableció que la incorporación de controles de seguridad en cada fase del ciclo de vida del proyecto no debe entenderse como la adición aislada de actividades técnicas, sino como el diseño de una estructura metodológica verificable que asegure consistencia organizacional. En este trabajo se evidenció que mecanismos como los Security Gates, los checklists de cierre, la matriz de trazabilidad, la formalización del riesgo residual, las historias de usuario de seguridad y la automatización de pruebas en entornos CI/CD son instrumentos clave para operacionalizar la seguridad de forma medible y sostenible. En consecuencia, la seguridad deja de ser una acción reactiva o dependiente del contexto y pasa a convertirse en un criterio de calidad y liberación del proyecto.

En quinto lugar, se concluye que el modelo propuesto representa una respuesta pertinente, viable y metodológicamente coherente frente al problema de investigación planteado. Su valor principal radica en que no propone una estructura paralela a los sistemas existentes, sino una arquitectura de integración por capas (estratégica, metodológica y operativa) que articula gobernanza, ejecución técnica y trazabilidad. La validación mediante técnica Delphi permitió confirmar su pertinencia conceptual y su aplicabilidad práctica, especialmente al enfatizar la necesidad de una implementación progresiva, un baseline mínimo obligatorio y una relación explícita entre cada brecha diagnosticada y los componentes de solución. De esta manera, el modelo aporta no solo una propuesta de mejora para la organización objeto de estudio, sino también una referencia adaptable para otras empresas del sector TI que enfrentan desafíos similares en seguridad y gestión de proyectos.

Recomendaciones

Con base en los resultados del diagnóstico y las conclusiones del estudio, se presentan las siguientes recomendaciones orientadas a mejorar la integración de la seguridad de la información en la gestión de proyectos TI. Estas acciones están diseñadas para ser implementadas de manera progresiva, considerando la capacidad operativa de la organización y su contexto actual.

Como primera recomendación, se debe integrar la seguridad de la información de forma obligatoria en todos los proyectos de TI, desde su inicio hasta su finalización. Esto implica dejar atrás la lógica reactiva basada en requerimientos del cliente y adoptar una postura preventiva, donde la identificación de riesgos, la definición de controles y la validación de cumplimiento sean parte natural del proyecto desde su concepción. Para ello, resulta indispensable que la alta dirección respalde formalmente esta integración mediante lineamientos, seguimiento y asignación de responsabilidades.

Como segunda recomendación, se propone implementar un Modelo Mínimo Viable (MMV) que permita una adopción progresiva del modelo sin generar sobrecarga operativa ni resistencia organizacional. Este despliegue debería iniciar con los elementos más críticos identificados en la validación experta y en la matriz de trazabilidad diagnóstico-modelo, particularmente el Gate de Liberación, el checklist de cierre seguro, la matriz RACI de seguridad, los criterios mínimos de aceptación y un conjunto básico de indicadores SMART. Una implementación escalonada facilitará la apropiación del modelo, permitirá generar resultados tempranos y creará condiciones favorables para su maduración posterior.

Como tercera recomendación, se considera necesario fortalecer la articulación entre seguridad, gestión de proyectos y equipos técnicos mediante mecanismos formales de coordinación y flujo de información. En este punto, la organización se beneficiaría de la creación o fortalecimiento de instancias como comités de seguridad, dashboards ejecutivos, reportes de cumplimiento y espacios periódicos de revisión de riesgos e incidentes. Esta articulación debe asegurar que la información operativa generada durante la ejecución de los proyectos alimente efectivamente la toma de decisiones estratégicas y contribuya a una gobernanza basada en evidencia.

Como cuarta recomendación, se sugiere consolidar un esquema de trazabilidad y medición que permita evaluar de forma continua el desempeño de la seguridad en los proyectos TI. La ausencia de métricas fue una de las brechas más relevantes del diagnóstico; por tanto, se recomienda priorizar indicadores relacionados con detección temprana de vulnerabilidades, tiempo de remediación, cumplimiento de controles, incidentes en producción y grado de adopción del modelo. Estos indicadores deben integrarse a herramientas y procesos ya existentes, con el fin de evitar duplicidades y facilitar su sostenibilidad dentro del sistema de gestión organizacional.

Finalmente, se recomienda fortalecer las capacidades organizacionales en cultura de seguridad, apropiación de roles y formación técnica aplicada. La integración efectiva de la seguridad no depende exclusivamente de marcos normativos o herramientas tecnológicas, sino también del nivel de comprensión y compromiso de las personas que participan en los proyectos. En consecuencia, se requiere avanzar en procesos de sensibilización, capacitación y socialización del modelo, especialmente en torno a responsabilidades por rol, prácticas seguras de desarrollo, gestión de riesgos y criterios de cumplimiento. Este componente cultural será determinante para que el modelo no se limite a una propuesta documental, sino que se consolide como una práctica organizacional sostenible.

Como recomendación adicional, se sugiere evaluar la adopción progresiva de marcos de gobernanza como COBIT, con el fin de fortalecer la alineación entre los objetivos estratégicos del negocio y la gestión de la seguridad de la información en proyectos TI. La incorporación de este tipo de marcos permitiría consolidar una visión integral de gobierno de TI, facilitando la definición de responsabilidades, la medición del desempeño, la gestión del riesgo y el control de los procesos, en coherencia con las necesidades organizacionales y el modelo propuesto.

En términos generales, la adopción de estas recomendaciones permitirá a la organización avanzar desde un enfoque reactivo hacia un modelo preventivo y estructurado de gestión de la seguridad de la información. Asimismo, abre la posibilidad de futuras líneas de trabajo orientadas a la maduración del modelo, su integración con otros sistemas de gestión y su adaptación a diferentes contextos organizacionales dentro del sector TI.

Referencias

Acuña Luna, J. A., Osuna-Millán, N., Flores Parra, J. M., & Rosales Cisneros, R. F. (2022). Hacia la selección de una metodología adecuada de gestión de proyectos de TI. Revista Ibérica de Sistemas e Tecnologias de Informação, (E54), 631-643. https://www.proquest.com/docview/2812104799/3FBB3D1E3D234EE6PQ/21?sourcetype=Scholarly%20Journals

Ali, M. S., & Zain, S. N. M. (2021). Cyber Threat Landscape and Vulnerabilities in Information Technology Systems: A Global Perspective. Journal of Cybersecurity, 12(1), 101-115.

Altamirano Di Luca, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances*, *21*(2). Recuperado de: https://www.redalyc.org/journal/6378/637869113010/html/

Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., ... & Thomas, D. (2001). Manifesto for Agile Software Development. Recuperado de https://agilemanifesto.org/

Buriticá, O., & López, M. (2018). Nivel de seguridad de los sistemas de información en las pymes del sector TIC de Santiago de Cali. Revista Entramado, 14(2), 214-228. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/6586847.pdf

Calder, A., & Watkins, S. (2017). ISO/IEC 27001:2013 – A Pocket

CCIT & Policía Nacional. (2024). Estudio anual de ciberseguridad en Colombia. Cámara Colombiana de Informática y Telecomunicaciones. Recuperado de: https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf

Centro Cibernético Policial. (2024). Informe de incidentes cibernéticos en Colombia 2024.

Chai, K. Y., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. Journal of ICT in Education, 8(2), 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021

CMMI Institute. (2018). CMMI for Development, Version 2.0. https://cmmiinstitute.com

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement, 20*(1), 37-46. https://doi.org/10.1177/001316446002000104

Congreso de la República de Colombia. (2009). Ley 1273 de 2009 – Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y de los datos. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=37808

Congreso de la República de Colombia. (2012). Ley 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587. Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República. (13 de mayo de 2014). Decreto 886 de 2014: Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012. Diario Oficial No. 49150.

Congreso de la República. (17 de octubre de 2012). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48587.

Congreso de la República. (2009). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”. Diario Oficial No. 47430.

Congreso de la República. (2013). Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48834.

Congreso de la República. (26 de mayo de 2015). Decreto 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Diario Oficial No. 49523.

Congreso de la República. (27 de junio de 2013). Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48834.

Coque Vásquez, J. y Kujundzic Riveros, M. D. (2018). *Uso de la seguridad de la información en la dirección de proyectos* [Tesis de maestría, Universidad Icesi]. Repositorio Institucional Universidad Icesi. Recuperado de: http://hdl.handle.net/10906/87790

Cronbach, L.J. Coefficient alpha and the internal structure of tests. *Psychometrika* 16, 297–334 (1951). https://doi.org/10.1007/BF02310555

De Haes, S., & Van Grembergen, W. (2015). Enterprise governance of information technology: Achieving strategic alignment and value (2nd ed.). Springer.

Denzin, N. K. (2012). Triangulation 2.0. Journal of Mixed Methods Research, 6(2), 80-88. https://doi.org/10.1177/1558689812437186

ESET. (2024). 30% de las organizaciones latinoamericanas sufrió al menos un incidente de ciberseguridad en 2023. ESET Latinoamérica. Recuperado de: https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/30-de-las-organizaciones-latinoamericanas-sufrio-al-menos-un-incidente-de-ciberseguridad-en-2023/

Fattah Ys, M. A., Parga Zen, B. y Wasitarini, D. E. (2023). Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. *Cybersecurity: Jurnal Riset Sains dan Teknologi Keamanan Siber*, *6*(2), 76–82. https://doi.org/10.14421/csecurity.2023.6.2.4190

Ferdiansyah, D., Isnanto, R. R., & Suseno, J. E. (2023). Strategy indicators for secure software development lifecycle in software startups based on information security governance. *Journal of Internet Services and Information Security (JISIS)*, *13*(4), 101-114. https://doi.org/10.56532/jisis.2023.13.4.101

Fiore, A. P. A., Facin, A. L. F. y Muniz Jr., J. (2023). Information security and quality management systems integration: Challenges and critical factors. *International Journal for Quality Research*, *17*(3), 635–650. https://doi.org/10.24874/IJQR17.03-01

Giordano, S. (2020). Cybersecurity and Privacy Law Handbook. Wiley.

Hair, J. F., Hult, G. T. M., Ringle, C. M., y Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage Publications.

Haro Sarango, A. F., Chisag Pallmay, E. R., Ruiz Sarzosa, J. P., & Caicedo Pozo, J. E. (2024). Tipos y clasificación de las investigaciones. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5(2), 956-966. https://doi.org/10.56712/latam.v5i2.1927

Hasan, E. F., Alzuod, M. A., Al Jasimee, K. H., Alshdaifat, S. M., Hijazin, A. F., & Khrais, L. T. (2025). The Role of Organizational Culture in Digital Transformation and Modern Accounting Practices Among Jordanian SMEs. Journal of Risk and Financial Management, 18(3), 147. Recuperado de: https://www.researchgate.net/publication/389726683_The_Role_of_Organizational_Culture_in_Digital_Transformation_and_Modern_Accounting_Practices_Among_Jordanian_SMEs

Heagney, J. (2022). Fundamentals of project management (6th ed.). HarperCollins Leadership. Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53128

Hernández-Sampieri, R., y Mendoza, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.

Huang, H.-L. (2024). The Strategic Alignment Maturity of Knowledge Management and Information Technology: Scale Development and Validation. Journal of the Knowledge Economy, 15, 10924-10955. https://doi.org/10.1007/s13132-023-01514-3

IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation. Recuperado de: https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

ICONTEC. (2013). NTC-ISO 21500 - Directrices para la dirección y gestión de proyectos. Instituto Colombiano de Normas Técnicas y Certificación.

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements.

International Organization for Standardization. (2024). *ISO/IEC 38500:2024 Information technology - Governance of IT for the organization*. ISO.

ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. ISACA.

ISACA. (2020). *COBIT 2019 framework: Governance and management objectives*. ISACA. Recuperado de: https://www.isaca.org/resources/cobit

ISO/IEC. (2018). ISO 31000:2018 Risk management - Guidelines. International Organization for Standardization.

ISO/IEC. (2018). ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management. International Organization for Standardization.

ISO/IEC. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. International Organization for Standardization.

ISO/IEC. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls. International Organization for Standardization

Janampa Patilla, H., Vilca Alviar, J. M., & Meneses Conislla, Y. (2023). Scrumban/XP: Propuesta para mejorar la eficiencia de la gestión de proyectos ágiles en el desarrollo de software. Revista Ibérica de Sistemas e Tecnologias de Informação, (E61), 14-32. Recuperado de: https://www.proquest.com/docview/2871351813/34DA939A699842EEPQ/7?sourcetype=Scholarly%20Journals

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. Revista Ibérica de Sistemas e Tecnologias de Informação, (E62), 16-31. https://doi.org/10.25043/2510-4148/revsegdef/2018v1n2/33

Kamil, Y., Lund, S. e Islam, M. S. (2023). Overview of ISO/IEC 27001 and output legitimacy: Stakeholder perspectives in Swedish private organizations. *Information Systems and e-Business Management*, *21*, 699–722. https://doi.org/10.1007/s10257-023-00646-y

Kerzner, H. (2017). Project Management: A Systems Approach to Planning, Scheduling, and Controlling (12th ed.). John Wiley & Sons.

Kitsios, F., Chatzidimitriou, E. y Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. *Sustainability*, *15*(7), 5828. https://doi.org/10.3390/su15075828

Landis, J. R., y Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*(1), 159-174. https://doi.org/10.2307/2529310

Lanz, J. (2024). The Updated NIST Cybersecurity Framework: Tools and Governance. The CPA Journal, May/June 2024, 70–72.

Lara, E., & Corella, F. (2018). Comparación de modelos tradicionales de seguridad de la información para centros de educación. Tierra Infinita, 4, 22–33.

Lee, M. T. S. M. (2018). The Hybrid Project Management Approach: A Review of the Literature. Project Management Journal, 49(6), 24-34.

López-Gómez, F., Marín-López, R., Canovas, O., López-Millán, G., & Pereniguez-García, F. (2025). SDN-AAA: Towards the standard management of AAA infrastructures. Journal of Network and Computer Applications, 236, 104114. https://doi.org/10.1016/j.jnca.2025.104114

Maimon, D. M., & Liao, M. W. S. (2020). The Increasing Complexity of Cyber Threats: An Analysis of Vulnerabilities in IT Systems. Journal of Cyber Threats, 11(1), 51-68.

McGraw, G. (2006). Software security: Building security in. Addison-Wesley Professional.

Mesquida, A. L., Mas, A., San Feliu, T., & Arcilla, M. (2014). Integración de estándares de gestión de TI mediante MIN-ITs. Revista Ibérica de Sistemas e Tecnologías de Información, (E1), 31-45. Recuperado de: https://www.proquest.com/docview/1515965751/73A902EB3BEB4F1FPQ/4?sourcetype=Scholarly%20Journals

Ministerio de Comercio, Industria y Turismo. (2013). Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48.834.

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2024). El sector TIC: Motor clave de la economía digital de Colombia. MinTIC. Recuperado de: https://www.mintic.gov.co/portal/715/w3-article-425878.html

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC] & Organización de Estados Americanos [OEA]. (2024). Estudio sobre el impacto económico de los incidentes, amenazas y ataques cibernéticos en Colombia. MinTIC. Recuperado de: https://gobiernodigital.mintic.gov.co/portal/Noticias/80507:Nuevo-estudio-del-MinTIC-y-la-OEA-busca-identificar-el-impacto-economico-de-los-incidentes-amenazas-y-ataques-ciberneticos-en-Colombia

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022, 9 de junio). Con el programa Un TICket para el Futuro, el Ministerio TIC financiará las maestrías en el exterior de 426 colombianos. Recuperado de: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/236950:Con-el-programa-Un-TICket-para-el-Futuro-el-Ministerio-TIC-financiara-las-maestrias-en-el-exterior-de-426-colombianos

Ministerio TIC (2023). Informe de Avance de Transformación Digital en Colombia.

Molina, A. & Chacón N. (2022). Análisis de riesgos de seguridad de la información en el área de Font Digital de la empresa Xorex de Colombia (Trabajo de grado). Universidad Católica de Colombia.

Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: A multivocal literature review. In Software Process Improvement and Capability Determination (pp. 17-29). Springer. https://doi.org/10.1007/978-3-319-67383-7_2

National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework 2.0. U.S. Department of Commerce. https://www.nist.gov/cyberframework

Netser Group. (2024). Demanda vs escasez de talento TI en América Latina. Netser Group Blog. Recuperado de: https://www.netsergroup.com/blog/demanda-vs-escasez-de-talento-ti/

Nicholas, J. M., & Steyn, H. (2020). Project Management for Engineering, Business and Technology (6th ed.). Routledge.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology. https://nvlpubs.nist.gov

NIST. (2018). Special Publication 800-160 Vol. 1: Systems security engineering. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v1

NIST. (2018). *Special Publication 800-37 Rev. 2: Risk Management Framework for information systems and organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

NIST. (2020). Special Publication 800-53B: Control baselines for information systems and organizations. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53B

OSP INTERNATIONAL CALA S.A.S. (s.f.). Soluciones tecnológicas y consultoría en TI. OSP INTERNATIONAL CALA S.A.S. Recuperado de: https://ospinternational.com/

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, L 119.

Policía Nacional de Colombia. (2022). Centro Cibernético Policial. Recuperado de: https://caivirtual.policia.gov.co/

Porter, M. E. (2008). The five competitive forces that shape strategy. *Harvard Business Review*, *86*(1), 78-93.

Project Management Institute (PMI). (2013). The Standard for Program Management (3rd ed.). PMI.

Project Management Institute (PMI). (2021). A guide to the Project Management Body of Knowledge (PMBOK® Guide) (7th ed.). Project Management Institute.

Putra, D., Nugraheni, D. M. K., & Suseno, J. E. (2025). *Desain arsitektur enterprise berbasis risiko teknologi informasi untuk sistem pelatihan: Integrasi COBIT 2019 dan TOGAF ADM*. Jurnal Sains dan Teknologi, 14(1), 35-46. https://doi.org/10.23887/jstundiksha.v14i1.93498

Rahman, M. M., Williams, L., & Kazman, R. (2022). Security in Agile Software Development: A Systematic Mapping Study. ACM Computing Surveys, 55(2), 1-38.

Ramaj, X., Sánchez-Gordón, M., Gkioulos, V., & Colomo-Palacios, R. (2024). *On DevSecOps and risk management in critical infrastructures: Practitioners' insights on needs and goals*. En Proceedings of the 2024 ACM/IEEE 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) and 2024 IEEE/ACM Second International Workshop on Software Vulnerability (pp. 45–52). Association for Computing Machinery. https://doi.org/10.1145/3643662.3643954

Reguant-Álvarez, M., y Torrado-Fonseca, M. (2016). El método Delphi. *REIRE. Revista d'Innovació i Recerca en Educació*, *9*(1), 87-102. https://doi.org/10.1344/reire2016.9.1916

Riaño Nossa, N. D. (2021). Estudio comparativo de metodologías tradicionales y ágiles aplicadas en la gestión de proyectos [Trabajo de grado, Universidad Pontificia Bolivariana].

Rindell, K., Ruohonen, J., Holvitie, J., Hyrynsalmi, S., & Leppänen, V. (2021). *Security in agile software development: A practitioner survey*. Information and Software Technology, 131, 106488. https://doi.org/10.1016/j.infsof.2020.106488

Robayo Bautista, E. C. (2020). Guía de principios y buenas prácticas para pruebas de seguridad de software en aplicaciones web para una empresa del sector privado [Trabajo de grado, Universidad Católica de Colombia].

Rogers, D. L. (2016). The Digital Transformation Playbook: Rethink Your Business for the Digital Age. Columbia University Press.

Ruiz Garzón, M. P., & Aguirre Olmos, D. P. (2020). Seguridad informática: Relación e impacto frente a la Ley de Protección de Datos Personales (Ley 1581 de 2012) [Trabajo de grado, Universidad Nacional Abierta y a Distancia].

Salinas Guzmán, J. (2021). Optimización de la gestión de proyectos TI. [Trabajo de grado, Tecnológico de Estudios Superiores de Cuautitlán Izcalli].

Samaniego, E. A., & Ponce, J. A. (2021). Fundamentos de seguridad informática. Editorial Grupo Compás.

Schwaber, K. (2004). Agile Project Management with Scrum. Microsoft Press.

Siebel, T. M. (2020). Digital Transformation: Survive and Thrive in an Era of Mass Extinction. RosettaBooks.

Superintendencia de Industria y Comercio. (2017, junio 8). Por violaciones de datos personales, Superindustria ha impuesto sanciones por más de $21 mil millones de pesos. https://www.sic.gov.co/noticias/por-violaciones-de-datos-personales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de-pesos

Uzunova, N., Pavlič, L., & Beranič, T. (2024). Quality gates in software development: Concepts, definition and tools. En Proceedings of the SQAMIA 2024: Workshop on Software Quality, Analysis, Monitoring, Improvement, and Applications (pp. s. p.). CEUR Workshop Proceedings. Recuperado de: https://ceur-ws.org/Vol-3845/paper06.pdf

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista Ibérica de Sistemas e Tecnologias de Informação, (22), 73-88. Recuperado de: https://www.proquest.com/docview/1915308773/73A902EB3BEB4F1FPQ/6?sourcetype=Scholarly%20Journals

Velásquez Restrepo, S. M., Vahos-Montoya, J. D., Gómez-Adasme, M. E., Pino-Martínez, A. A., Restrepo-Zapata, E. J., & Londoño-Marín, S. (2019). Una revisión comparativa de la literatura acerca de metodologías tradicionales y modernas de desarrollo de software. Revista CINTEX, 24(2), 13–23.

Viveros Meneses, D. E., Pardo-Calvache, C. J., Chilito-Gómez, P. R., & Pino, F. J. (2019). Scrum+: Un Scrum escalado para la gestión ágil de proyectos de desarrollo de software global con múltiples modelos. Revista Facultad de Ingeniería, Universidad de Antioquia, (93), 105–116. Recuperado de: https://www.proquest.com/docview/2287347031/1374394972D24FBCPQ/3?sourcetype=Scholarly%20Journals

WeLiveSecurity. (2024). Incidentes de ciberseguridad en 2024 en América Latina. Recuperado de: https://www.welivesecurity.com/es/cibercrimen/incidentes-ciberseguridad-2024-america-latina/

Anexos

Anexo 1. Proceso Metodológico Consultoría OSP INTERNATIONAL CALA SAS

Anexo 2. Consentimiento informado y autorización para la recolección de información en investigación académica.

Anexo 3. Taller de sensibilización de seguridad de la información

Anexo 4. Cuestionario Likert adaptado de CMMI-DEV & ISO 27001.

Anexo 4.1. Cuestionario Integración de Seguridad en Gestión de Proyectos TI - Formularios de Google.

Anexo 5. Guion de entrevista semiestructurada aplicada.

Anexo 6. Matriz de extracción y revisión de los documentos del SGI de la organización.

Anexo 7. Lista de verificación observación no participante en reuniones de proyecto

Anexo 8. Bitácora de campo

Anexo 9. Matriz de triangulación metodológica

Anexo 10. Políticas y lineamientos de seguridad de la información ISO/IEC 27001 e ISO/IEC 27002

Anexo 11. Procedimiento de gestión y desarrollo de software

Anexo 12. Matriz RACI propuesta