Integrating ISO/IEC 27001 and ISO 9001 for Cybersecurity Governance in a Software Company

Eira Micaela Martinez[1] y María Luciana Roldán[1,2][0000-0002-4786-5592]

[1] Universidad Tecnológica Nacional, Facultad Regional Santa Fe, Argentina
[2] Instituto de Desarrollo y Diseño (CONICET/UTN), Santa Fe, Argentina
emmartinez@frsf.utn.edu.ar, lroldan@santafe-conicet.gov.ar

Abstract. This paper presents a systematic experience report on the practical implementation of an integrated management system combining ISO/IEC 27001:2022 and ISO 9001:2015 as a cybersecurity governance mechanism in an Argentine software company. The organization already had a certified quality management system and needed to incorporate an information security management system without creating a parallel bureaucracy. The article reconstructs the implementation through traceable evidence: a detailed project plan, monthly dashboards, asset and risk spreadsheets, treatment plans, and internal and external audit records. Its contribution is threefold: it documents how an existing ISO 9001 backbone was extended to absorb ISO/IEC 27001 requirements; it systematizes an operational model that connects assets, threats, vulnerabilities, and Annex A controls with risk treatment decisions; and it reports verifiable outcomes and lessons from the certification process. Results include 81 completed project activities, including a 68-action 2024 risk treatment plan; analysis of 154 assets with all residual risks reduced to the acceptable threshold; formalization of 36 monitored security controls; closure of three major internal-audit nonconformities in secure development; and external audit results recommending the award of ISO/IEC 27001 certification while maintaining ISO 9001 certification.

Keywords: cybersecurity governance, integrated management systems, ISMS, ISO/IEC 27001, software development.

Integración de ISO/IEC 27001 e ISO 9001 para la gobernanza de la ciberseguridad en una empresa de software

Resumen. Este artículo se presenta como un reporte sistemático de experiencia sobre la implementación práctica de un sistema de gestión integrado que combina ISO/IEC 27001:2022 e ISO 9001:2015 como mecanismo de gobernanza de la ciberseguridad en una empresa argentina de software. La organización ya contaba con un sistema de gestión de la calidad certificado y necesitaba incorporar un

sistema de gestión de la seguridad de la información sin crear una burocracia paralela. El trabajo reconstruye la implementación mediante evidencia trazable: plan detallado del proyecto, reportes mensuales, planillas de activos y riesgos, planes de tratamiento y registros de auditoría interna y externa. Su aporte se ve en tres puntas: documenta cómo una base ISO 9001 preexistente fue extendida para absorber los requisitos de ISO/IEC 27001; sistematiza un modelo operativo que vincula activos, amenazas, vulnerabilidades y controles del Anexo A con decisiones de tratamiento; y reporta resultados verificables y lecciones del proceso de certificación. Entre los resultados se destacan 81 actividades completadas, incluido un PTR 2024 de 68 acciones; el análisis de 154 activos con reducción de todos los riesgos residuales al umbral aceptable; la formalización de 36 controles de seguridad monitorizados; el cierre de tres no conformidades mayores de auditoría interna en desarrollo seguro; y la recomendación de certificación externa ISO/IEC 27001 con mantenimiento de ISO 9001.

Palabras clave: gobernanza de la ciberseguridad, sistemas integrados de gestión, SGSI, ISO/IEC 27001, desarrollo de software.

1 Introducción

La creciente exposición de las organizaciones a incidentes de seguridad y a exigencias de clientes y reguladores ha desplazado la ciberseguridad desde el plano exclusivamente técnico hacia el de la gobernanza organizacional. En ese contexto, ISO/IEC 27001 ofrece un marco de gestión basado en contexto, riesgos, controles y mejora continua, mientras que ISO 9001 aporta disciplina de procesos, seguimiento y revisión sistemática del desempeño (Humphreys, 2008; Tarí et al., 2012; Culot et al., 2021).

La literatura sobre sistemas integrados de gestión sostiene que la integración de normas puede reducir duplicaciones, mejorar la coherencia documental y fortalecer la toma de decisiones, aunque también introduce dificultades vinculadas con la complejidad del cambio, la demanda de recursos y la resistencia interna (Simon et al., 2012; Bernardo et al., 2015; Nunhes et al., 2017). Para las empresas de desarrollo de software, el desafío es mayor: los controles de seguridad conviven con equipos distribuidos, servicios cloud, ciclos rápidos de entrega y tensiones entre control y autonomía técnica.

Este trabajo se formula como un reporte sistemático de experiencia sobre la integración entre un sistema de gestión de la calidad ya certificado según ISO 9001:2015 y un sistema de gestión de la seguridad de la información conforme a ISO/IEC 27001:2022. Su propósito no es probar causalidad ni generalizar estadísticamente, sino reconstruir con trazabilidad documental las decisiones, artefactos, evidencias y resultados de una implementación aplicada.

En lugar de presentar contribuciones en términos de validación de hipótesis, el artículo aporta como reporte sistemático de experiencia tres elementos. Primero, ordena y hace trazable una experiencia de implementación mediante evidencia verificable: plan detallado del proyecto, bitácora, reportes mensuales, inventario de activos, matrices de riesgos y registros de auditoría. Segundo, describe cómo se integraron en un único

sistema de gestión componentes ya maduros de ISO 9001 con elementos nuevos o adaptados de ISO/IEC 27001, evitando sistemas paralelos. Tercero, documenta resultados observables y lecciones de ejecución (cierre del PTR 2024, reducción de riesgos residuales, cierre de hallazgos y avance del proceso de certificación) que pueden reutilizarse como referencia práctica en organizaciones con características similares.

2 Marco conceptual y trabajos relacionados

2.1 Sistemas integrados de gestión

Un sistema integrado de gestión busca administrar bajo una misma arquitectura procesos, responsabilidades, documentos y mecanismos de mejora que son comunes a diferentes normas. En lugar de operar con subsistemas aislados, la integración procura compartir políticas, objetivos, control documental, auditorías internas, revisión por la dirección y tratamiento de no conformidades. La evidencia empírica muestra que los beneficios de la integración suelen concentrarse en eficiencia operativa, mejor comunicación interna, mayor consistencia metodológica y visión más amplia de la gestión (Simon et al., 2012; Bernardo et al., 2015).

Al mismo tiempo, la integración no se produce automáticamente por compartir una estructura normativa similar. Requiere madurez organizacional, capacidad de coordinación interáreas y decisiones explícitas sobre qué elementos se unifican y cuáles deben conservar especificidad. Nunhes et al. (2017) identifican como elementos particularmente integrables la responsabilidad de la alta dirección, las instrucciones de trabajo, el control de documentos y registros, la comunicación interna y la asignación de responsabilidades. Estos hallazgos resultan especialmente útiles cuando la integración involucra normas de naturaleza diferente, como calidad y seguridad de la información.

2.2 ISO 9001, ISO/IEC 27001 y enfoque basado en riesgos

ISO 9001:2015 establece requisitos para gestionar la calidad con enfoque a procesos, seguimiento del desempeño y mejora continua. La literatura reporta que sus beneficios son principalmente operativos y organizacionales: sistematización, claridad de responsabilidades, mejora en la relación con clientes y mayor estabilidad en la ejecución de procesos, aunque la evidencia sobre impacto financiero directo es menos concluyente (Tarí et al., 2012; ISO, 2015).

ISO/IEC 27001:2022, por su parte, define los requisitos para establecer, implementar, mantener y mejorar un SGSI orientado a proteger la confidencialidad, integridad y disponibilidad de la información. Su aporte distintivo es vincular la selección de controles con un proceso explícito de evaluación y tratamiento de riesgos, incorporando gobierno, roles, monitoreo y mejora continua, no solo medidas técnicas aisladas (Humphreys, 2008; ISO/IEC, 2022). La revisión de Culot et al. (2021) muestra que la investigación sobre ISO/IEC 27001 se concentra en motivaciones de adopción, problemas de implementación, resultados y relación con otras normas, lo que refuerza la pertinencia de estudiar su integración con sistemas de gestión ya existentes.

Ambas normas comparten la estructura de alto nivel adoptada por los sistemas de

gestión ISO, lo que habilita una integración basada en el ciclo Planificar-Hacer-Verificar-Actuar. Sin embargo, esa compatibilidad formal solo produce resultados cuando se traduce en prácticas operativas consistentes y sostenibles. En este caso, además, el análisis de riesgos se apoyó en MAGERIT versión 3.0 para clasificar activos, amenazas y dimensiones de valoración, mientras que el Anexo A de ISO/IEC 27001 funcionó como catálogo de controles de referencia.

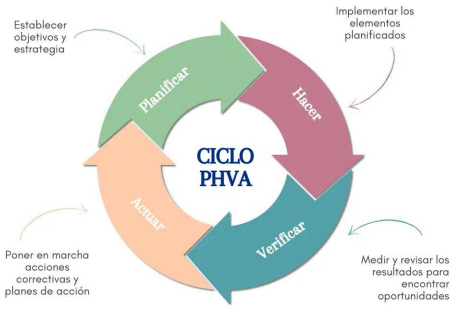

Fig. 1. Ciclo PHVA utilizado como soporte conceptual de la estrategia de implementación del sistema integrado.

3 Metodología

El artículo se construye como reporte sistemático de experiencia profesional a partir de una implementación real desarrollada durante 2025. El objetivo es describir de manera ordenada el diseño, la ejecución, los desvíos y la verificación de la implementación, identificando la evidencia que respalda cada resultado relevante.

Empresa Crombie es una firma argentina de desarrollo de software a medida, con operación remota e híbrida y una trayectoria previa de certificación ISO 9001. Durante 2025 definió como objetivo estratégico incorporar un SGSI acorde a ISO/IEC 27001:2022 para fortalecer su posicionamiento en sectores con mayores exigencias de seguridad. El alcance certificado comprendió presupuesto, planificación de recursos de producción y ciclo de vida de desarrollo de software para soluciones verticalizadas en fintech y retail, con foco en los mercados estadounidense, argentino y español.

El equipo núcleo del proyecto estuvo conformado por una responsable interna con dedicación completa, un perfil de apoyo operativo del área de mejora continua y dos consultores externos especializados. También participaron referentes de Tecnología, Proyectos, People, Administración y Dirección, ya que la mayoría de las definiciones requerían información, validación o ejecución distribuida.

3.1 Estrategia de implementación y criterios de evaluación

Las fuentes de evidencia utilizadas fueron: plan general del proyecto, bitácora de trabajo, plan detallado con 81 actividades cerradas, inventario de 154 activos, matrices de amenazas y vulnerabilidades, plan de tratamiento de riesgos 2024, documentos y registros del SGI, reportes mensuales de seguimiento, actas de revisión por la dirección, informe de auditoría interna y reportes de auditoría externa de fases 1 y 2.

El criterio de sistematización consistió en triangular decisiones, ejecución operativa y resultados de auditoría, de modo de sostener el artículo sobre evidencia verificable y no solo sobre relato retrospectivo. El criterio de éxito definido al inicio del trabajo combinó cinco condiciones: cierre del PTR 2024, integración documental del sistema, evidencia operativa de controles, realización de auditoría interna y recomendación favorable del organismo certificador.

La estrategia de ejecución se estructuró en ciclos mensuales de planificación y revisión. Al comienzo de cada mes se fijaban objetivos y tareas prioritarias; al cierre se contrastaban avances, desvíos y necesidades de reprogramación. Los reportes mensuales siguieron por separado el avance del PTR y del SGI mediante indicadores de cumplimiento de sprint y grado de avance acumulado, lo que facilitó la reprogramación temprana. Este esquema permitió mantener alineación con el enfoque PHVA y, al mismo tiempo, absorber cambios de contexto sin perder el objetivo de certificación.

Tabla 1. Fases de la implementación, actividades principales y fuentes de evidencia.

Fase	Actividades principales	Fuentes de evidencia
Diagnóstico y alcance	Revisión del SGC existente, definición del alcance, análisis de partes interesadas y compromiso directivo.	Análisis de contexto, reuniones, mapa de procesos y manual del SGI.
Diseño del modelo de riesgos	Inventario de activos, valoración CID, amenazas, umbral aceptable, SOA y PTR.	Inventario, matrices de amenazas y vulnerabilidades, análisis de riesgos y PTR 2024.
Integración documental	Adecuación de procesos compartidos y formalización de políticas, procedimientos e indicadores.	Manual, interacción de procesos, responsabilidades y protocolos.
Despliegue operativo	Implementación progresiva de controles, concientización, seguimiento y pruebas externas.	Registros de control, evidencias técnicas, tableros de seguimiento y capacitaciones.
Evaluación y cierre	Auditoría interna, resolución de 3 NCM y 2 OM, cierre del PTR y auditorías externas fase 1 y fase 2.	Informe ejecutivo de auditoría interna, reportes de certificadora TÜV, actas de revisión y actualización del riesgo residual.

4 Diseño e implementación del sistema integrado

4.1 Diagnóstico inicial y definición del alcance

El diagnóstico inicial mostró que el sistema de calidad existente ofrecía una base valiosa, pero no estaba preparado para absorber de forma inmediata todos los requisitos del SGSI. Existían componentes reutilizables (análisis de contexto, control documental, revisión por la dirección, gestión de no conformidades y lógica de procesos), aunque con distintos niveles de conocimiento y apropiación por parte de los gerentes.

A partir de ese diagnóstico se descartó crear dos sistemas paralelos. La decisión fue conservar un único SGI y avanzar por etapas: primero madurar las prácticas de seguridad y luego consolidar la unificación formal. Esta decisión resultó clave para evitar duplicaciones y para alinear el sistema con la capacidad real de adopción de la organización.

El alcance de la certificación incluyó presupuesto, planificación de recursos de producción y ciclo de vida de desarrollo de software para soluciones a medida. Asimismo, se excluyó el control A.8.30 del Anexo A de la norma ISO/IEC 27001;2022, dado que la organización no terceriza desarrollo.

4.2 Modelo de análisis y tratamiento de riesgos

El núcleo técnico del proyecto fue la operacionalización del análisis y tratamiento de riesgos. Se partió de un inventario de activos de información donde cada activo se clasificó por tipo, dueño, custodio y nivel de criticidad en confidencialidad, integridad y disponibilidad. Sobre esa base se construyó un catálogo de amenazas apoyado en MAGERIT 3 y se valoró la vulnerabilidad de los controles asociados al Anexo A de ISO/IEC 27001.

El modelo de priorización combinó tres niveles de análisis. Primero, la valoración de amenazas según tipos y subtipos de activos. Segundo, la valoración de vulnerabilidad de los controles según su grado de documentación, implementación, auditabilidad e incidentes asociados. Tercero, la estimación de impacto considerando criterios operativos, económicos, legales y reputacionales. De manera simplificada, la probabilidad de ocurrencia se obtuvo a partir de la combinación entre amenaza y vulnerabilidad, y el riesgo total integró esa probabilidad con la criticidad CID y el impacto. En la Fig.2 se pueden observar ejemplos de esta implementación.

Activo				Valoración CID			Valoración Amenazas y Vulnerabilidades		Riesgo (previo al PTR)					Gestión	
ID	Nombre Activo	Tipo Activo	Subtipo	Confidencialidad	Integridad	Disponibilidad	Max A	Max V/C	Probabilidad	Impacto	Risk C	Risk I	Risk D	Estrategia	Va
SW - 127	Jira Estandard (Nube)	Software-Aplicaciones informáticas	Atlassian	Alta	Alta	Alta	3	4	12	Severo	180	180	180	Tratar/Mitigar	
SW - 128	Bitbucket Standard (Nube)	Software-Aplicaciones informáticas	Atlassian	Alta	Alta	Alta	3	4	12	Alto	108	108	108	Tratar/Mitigar	
SW - 129	People Force (Nube)	Software-Aplicaciones informáticas	Otros Aplicativos	Baja	Baja	Alta	2	4	8	Alto	24	24	72	Aceptar	
SW - 130	Hubspot (Nube)	Software-Aplicaciones informáticas	Hubspot	Alta	Alta	Alta	2	4	8	Menor	24	24	24	Aceptar	
SW - 131	Airtable (Nube)	Software-Aplicaciones informáticas	Airtable	Alta	Alta	Alta	2	4	8	Severo	120	120	120	Tratar/Mitigar	
SW - 132	Panel Administracion Nic.ar	Software-Aplicaciones informáticas	Sitio Web	Alta	Alta	Alta	2	4	8	Medio	48	48	48	Aceptar	
SW - 133	Panel Administracion AWS	Software-Aplicaciones informáticas	Sitio Web	Alta	Alta	Alta	2	4	8	Severo	120	120	120	Tratar/Mitigar	

Fig. 2. Ejemplo de análisis de riesgos de algunos activos.

La dirección definió un umbral de riesgo aceptable de 90 y, a partir de él, se seleccionaron los activos y controles que requerían tratamiento. El análisis cubrió 154 activos; 20 quedaron inicialmente por encima del umbral y requirieron tratamiento específico. La Fig. 3 resume la matriz de aceptabilidad utilizada y el efecto agregado

del PTR 2024 sobre los riesgos inicialmente no aceptables.

Nivel de Riesgo Aceptable
90

NIVELES DE RIESGOS																
		Impacto por Dimensión CID														
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Probabilidad (Amenaza x Vulnerabilidad)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
	3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45
	4	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
	5	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75
	6	0	6	12	18	24	30	36	42	48	54	60	66	72	78	84	90
	7	0	7	14	21	28	35	42	49	56	63	70	77	84	91	98	105
	8	0	8	16	24	32	40	48	56	64	72	80	88	96	104	112	120
	9	0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135
	10	0	10	20	30	40	50	60	70	80	90	100	110	120	130	140	150
	11	0	11	22	33	44	55	66	77	88	99	110	121	132	143	154	165
	12	0	12	24	36	48	60	72	84	96	108	120	132	144	156	168	180
	13	0	13	26	39	52	65	78	91	104	117	130	143	156	169	182	195
	14	0	14	28	42	56	70	84	98	112	126	140	154	168	182	196	210
	15	0	15	30	45	60	75	90	105	120	135	150	165	180	195	210	225

Nivel de Riesgo		Descripción
<45	Bajo	No es necesario adoptar ninguna medida. El nivel de riesgo es suficientemente bajo y no justifica la implantación de controles adicionales.
entre 45 y 134	Medio	La Dirección de la empresa y/o el Comité de Seguridad de la empresa, determinará el nivel de los riesgos aceptables o no a su juicio. El Responsable de Seguridad de la Información determinará los controles que deberán aplicarse para mitigar razonablemente los riesgos.
>=135	Alto	El nivel de riesgos no es aceptable, y sólo se podrán excluir controles que los mitiguen justificando dicha exclusión por parte de la Dirección de la empresa y/o el Comité de Seguridad. El Responsable de Seguridad de la Información determinará los controles que deberán aplicarse para mitigar razonablemente los riesgos.

Fig. 3. Matriz de aceptabilidad del riesgo utilizada en el proyecto.

4.3 Integración documental y adecuación de procesos

La integración documental buscó incorporar la seguridad de la información dentro de la arquitectura ya existente del SGI. En lugar de duplicar manuales o revisiones, se adaptaron componentes comunes y se añadieron documentos específicos allí donde la norma lo exigía. Entre los artefactos actualizados o creados se destacan el análisis de contexto, la determinación del alcance del SGI, el mapa e interacción de procesos, las responsabilidades de seguridad, el protocolo de comunicación, los objetivos e indicadores de calidad y seguridad y la Declaración de Aplicabilidad.

En el plano operativo se revisaron o formalizaron procedimientos vinculados con incidentes, activos, gestión de usuarios, gestión de vulnerabilidades, backups, actualizaciones, control de accesos, cifrado, teletrabajo, continuidad del negocio y uso de infraestructura propia y cloud. También se reforzó la trazabilidad entre procesos de compras, gestión de proveedores, incorporación y desvinculación de personas y desarrollo de software.

Esta capa documental no se trató como un fin en sí mismo, sino como mecanismo de coherencia entre lo declarado y lo ejecutado. Un aspecto crítico de la implementación fue abandonar la lógica de 'anexar seguridad' a un sistema existente y pasar a incorporarla dentro del mismo circuito de seguimiento, control documental y

auditoría. La Fig. 4 sintetiza la lógica de integración adoptada, distinguiendo los componentes heredados de ISO 9001, el núcleo común de gobierno y los elementos incorporados o reforzados por ISO/IEC 27001.

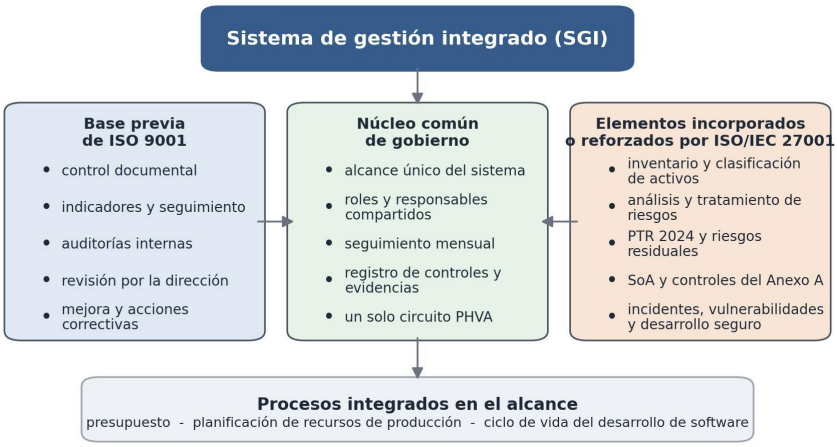

Fig. 4. Esquema de integración del SGI: componentes reutilizados de ISO 9001, núcleo común de gobierno y capacidades incorporadas o reforzadas por ISO/IEC 27001.

4.4 Despliegue operativo y auditorías

El despliegue se organizó en ciclos mensuales con reuniones semanales de seguimiento junto con los consultores y encuentros específicos con las áreas involucradas. La implementación fue progresiva porque varias acciones dependían de decisiones interáreas y de cambios tecnológicos en curso. En particular, la articulación con Tecnología fue central, dado que allí se concentraban las definiciones sobre infraestructura, accesos, endpoints, entornos cloud y prácticas de desarrollo.

La auditoría interna operó como instancia de validación independiente previa a la certificación y funcionó como acelerador de madurez. Identificó tres no conformidades mayores ligadas al desarrollo seguro (A.8.25, A.8.26 y A.8.27) y dos oportunidades de mejora en gestión de incidentes y usuarios privilegiados. Su resolución obligó a formalizar un checklist de seguridad para los proyectos de desarrollo de software, la clasificación y tratamiento de vulnerabilidades en desarrollo y la validación técnica previa al pasaje a producción. Luego de esa revisión se completó el cierre formal del PTR 2024 y se actualizó el riesgo residual de los activos tratados.

El proceso de certificación externa se realizó en dos fases. La fase 1 verificó la preparación documental y organizacional y declaró a la organización lista para la fase 2. La fase 2 se centró en la operación efectiva del sistema y concluyó con la recomendación de emitir el certificado ISO/IEC 27001:2022 y mantener la certificación ISO 9001:2015. Entre ambas instancias se ajustaron prácticas, evidencias y definiciones metodológicas, lo que confirmó que el sistema no solo estaba documentado, sino funcionando en condiciones reales.

5 Resultados

Los resultados del trabajo pueden analizarse en cinco planos complementarios: gobierno, gestión de riesgos, operación, aseguramiento e impacto organizacional. El primero corresponde a la consolidación de un SGI único, con alcance definido, revisión por la dirección, objetivos compartidos y criterios homogéneos de mejora. El segundo refiere al cierre del PTR 2024, a la actualización del análisis sobre 154 activos y a la reducción de todos los riesgos residuales al nivel aceptable definido por la organización. El tercero se observa en la existencia de procedimientos operativos y 36 controles de seguridad monitoreados de forma periódica. El cuarto surge de las auditorías interna y externa. El quinto, menos visible pero más relevante a mediano plazo, consiste en la incorporación de la seguridad como variable de decisión en procesos técnicos y gerenciales.

Tabla 2. Resultados observados y evidencia principal del trabajo.

Dimensión	Resultado observado	Evidencia principal
Gobierno y alcance	SGI único con alcance certificado, contexto, partes interesadas, objetivos e indicadores compartidos.	Manual del SGI, análisis de contexto, definición de alcance y actas de revisión por la dirección.
Gestión de riesgos	Inventario de 154 activos; 20 activos tratados por superar el nivel de riesgo aceptable; todos los riesgos residuales quedaron en el umbral aceptable o por debajo de él.	Matrices de riesgos, SOA, PTR, registros de cierre y actualización del riesgo residual.
Operación y monitoreo	81 actividades completadas, 68 correspondientes al PTR 2024, y 36 controles de seguridad con seguimiento periódico.	Plan detallado del proyecto, registros de control, evidencias técnicas y procedimientos operativos.
Aseguramiento	Auditoría interna con 3 NCM y 2 OM; fase 1 declaró preparación para fase 2; fase 2 recomendó emitir ISO/IEC 27001 y mantener ISO 9001.	Informe de auditoría interna, reporte de fase 1 y reporte de fase 2 del organismo certificador.
Impacto organizacional	Mayor involucramiento directivo y seguridad integrada a decisiones de tecnología, people, proveedores y desarrollo seguro.	Reuniones gerenciales, cambios de proceso, redefinición de roles y reportes mensuales de seguimiento.

En relación con los objetivos iniciales, el trabajo alcanzó los resultados esperados.

Se cerró el plan de tratamiento de riesgos, se integraron las dos normas dentro de una misma estructura de gestión, se formalizaron métricas y objetivos de seguridad, se coordinó la auditoría interna y se completó exitosamente el proceso de certificación externa. Más allá del cumplimiento formal, el valor principal fue la transición desde una seguridad reactiva hacia una seguridad gestionada, medible y respaldada por evidencias.

Otro resultado relevante fue el cambio en la relación entre áreas. La seguridad dejó de descansar exclusivamente en decisiones puntuales del equipo técnico o en exigencias del consultor externo y pasó a discutirse en espacios de dirección, finanzas, people, proyectos y mejora continua. Esa transversalidad incrementó la trazabilidad de responsabilidades y mejoró la capacidad de sostener el sistema más allá del proyecto inicial.

6 Discusión

Los hallazgos coinciden con la literatura sobre integración de sistemas de gestión. Igual que en Simon et al. (2012) y Nunhes et al. (2017), los principales beneficios no fueron solamente documentales, sino también de coordinación, eficiencia y visibilidad gerencial. Asimismo, la implementación documentada confirma lo señalado por Bernardo et al. (2015): la integración genera más valor cuando reutiliza procesos comunes y amplía el alcance de la gestión, en lugar de superponer estructuras independientes.

También se verificaron las dificultades reportadas por estudios previos: complejidad de implementación, alta demanda de tiempo y recursos, y necesidad de traducir requerimientos normativos generales a prácticas organizacionales situadas (Simon et al., 2012; Culot et al., 2021). En una empresa de software, estas tensiones se manifestaron especialmente en el equilibrio entre imponer restricciones y preservar la agilidad de desarrollo. Además, la experiencia mostró dificultades concretas: compresión del cronograma, reestructuración de roles de seguridad, inconsistencias del inventario de activos y necesidad de incorporar horas adicionales de trabajo para revisiones documentales y ajustes de alcance. La decisión de priorizar controles mínimos obligatorios, monitoreo y corrección por encima de prohibiciones indiscriminadas resultó más viable para la cultura de la organización.

La experiencia de Crombie muestra que la integración de ISO/IEC 27001:2022 sobre un sistema ISO 9001:2015 preexistente no avanzó de manera lineal ni homogénea, sino mediante dos trayectorias parcialmente desacopladas. Por un lado, el Plan de Tratamiento de Riesgos (PTR) exhibió una curva de maduración relativamente sostenida: su grado de avance pasó de 48,8% en mayo a 58,5% en junio, 69,5% en julio, 75,6% en agosto y 87,8% en septiembre. Por otro lado, el sistema de gestión integrado avanzó más lentamente al comienzo, pero aceleró en el segundo semestre: 8% en mayo, 40% en junio, 48% en julio, 76% en agosto y 96% en septiembre. Esta diferencia resulta consistente con la naturaleza de ambas líneas de trabajo: mientras muchas acciones del PTR se resuelven como controles puntuales o decisiones operativas concretas, la integración del sistema exige armonización documental, redefinición de responsabilidades, acuerdos interáreas y producción de evidencia verificable.

Las métricas mensuales también muestran que el avance no debe leerse solo en

términos de volumen de tareas cerradas. El PTR registró cumplimientos mensuales de 85,7% en mayo, 88,9% en junio, 100% en julio, 71,4% en agosto y 91% en septiembre, mientras que el sistema integrado osciló entre 100%, 88,9%, 40%, 100% y 83% en esos mismos meses. En particular, julio expuso con claridad la asimetría del proyecto: el PTR alcanzó 100% de cumplimiento mensual y 69,5% de avance acumulado, pero el sistema integrado solo logró 40% de cumplimiento mensual y quedó en 48% de avance frente a 60% planificado. En términos de discusión, esto sugiere que la gestión del cronograma fue útil para orientar prioridades, pero no bastó por sí sola para asegurar una madurez homogénea entre controles, procesos y documentación. En línea con la literatura previa citada en este trabajo, los beneficios de la integración no fueron meramente documentales, sino de coordinación y visibilidad gerencial; al mismo tiempo, la principal dificultad estuvo en traducir requisitos normativos generales a prácticas sostenibles en una empresa de software. En la Fig. 5 se muestran estas observaciones sobre la evolución de los indicadores en el tiempo.

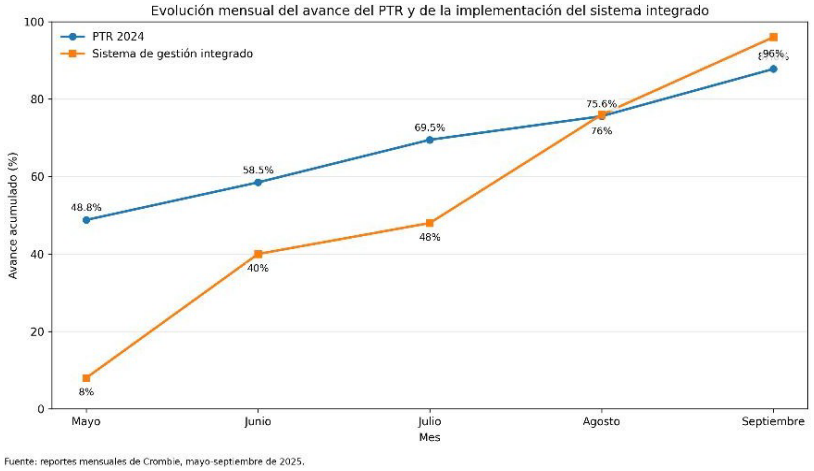

Fig. 5. Gráfico de avance del PRT y de la implementación del SGI de mayo a septiembre.

Un aspecto clave es que los indicadores de seguimiento solo adquirieron valor cuando se contrastaron con evidencia de auditoría. La auditoría interna de octubre identificó tres no conformidades mayores y dos oportunidades de mejora; las tres no conformidades mayores se concentraron en seguridad en el desarrollo de software, protección de entornos de desarrollo y pruebas de seguridad (A.8.25, A.8.27 y A.8.26). Por lo tanto, el proyecto mostró una tensión importante entre "ejecutar tareas" y "demostrar operación efectiva". En Crombie, la brecha no estuvo principalmente en la ausencia absoluta de controles, sino en la consistencia de su aplicación, la formalización del checklist de seguridad, la separación de entornos y la trazabilidad del tratamiento de vulnerabilidades. Este punto es relevante porque matiza la lectura de las métricas: un porcentaje alto de avance puede coexistir con debilidades sustantivas cuando la organización todavía no consolidó evidencia técnica robusta.

La evolución posterior indica, sin embargo, que el dispositivo de seguimiento

mensual sí fue eficaz como mecanismo de corrección y aprendizaje. La auditoría de Fase 1 del 13 de noviembre de 2025 concluyó que Crombie estaba plenamente preparada para la Fase 2. Más tarde, la auditoría externa realizada entre el 17 y el 19 de diciembre de 2025 recomendó la emisión del nuevo certificado ISO/IEC 27001:2022 y el mantenimiento de la certificación ISO 9001:2015. Ese recorrido, que va desde hallazgos mayores en la auditoría interna hasta la recomendación formal de certificación, permite sostener que el valor del enfoque adoptado no residió únicamente en medir avance, sino en habilitar ciclos cortos de priorización, cierre de brechas y consolidación de evidencia. En ese sentido, la discusión no debería plantearse en términos de éxito lineal, sino de maduración iterativa verificable.

También resulta relevante el quiebre observado sobre el final del proyecto. El informe final consigna que Crombie decidió comprimir los plazos para concluir durante 2025 e intensificar aún más el cierre hacia noviembre; sin embargo, la falta de disponibilidad del área de Tecnología para actualizar el inventario de activos dejó pendiente el análisis de riesgos 2025 y obligó a extender el acompañamiento hasta diciembre. Esa tensión aparece reflejada en el reporte mensual de noviembre, donde el PTR mostró 20% de cumplimiento mensual y cuatro de cinco tareas quedaron en curso. Lejos de invalidar el proceso, ese descenso final ilustra un patrón frecuente en implementaciones reales: cuando la certificación se acerca, el cuello de botella deja de ser la planificación general y pasa a ser la calidad del inventario, la disponibilidad de responsables técnicos y la resolución fina de hallazgos. Por eso, el principal aporte del artículo como reporte sistemático de experiencia no es describir una implementación idealizada, sino mostrar, con evidencia verificable, cómo una organización real como Crombie transformó métricas operativas, hallazgos de auditoría y retrabajo técnico en un sistema integrado finalmente certificable.

Desde la perspectiva de la ciberseguridad, el principal aporte del artículo como reporte sistemático de experiencia es mostrar que la madurez de un SGSI depende tanto de la arquitectura de gobernanza como de la calidad de las evidencias con las que se demuestra su operación. La experiencia documentada no solo describe qué decisiones se tomaron sino también qué artefactos permitieron verificarlas: matrices de riesgos, controles monitorizados, reportes mensuales y auditorías.

Como línea futura, sería valioso comparar este tipo de integración en varias empresas de software con distintos grados de madurez previa, así como seguir longitudinalmente la evolución de controles, incidentes y métricas después de la certificación. También resulta pertinente profundizar la relación entre SGSI, desarrollo seguro y gobernanza de proveedores cloud.

7 Conclusiones

La integración entre ISO 9001:2015 e ISO/IEC 27001:2022 realizada en la empresa Crombie demostró que un SGSI puede incorporarse de forma efectiva a un sistema de gestión preexistente si la organización trabaja con una lógica de etapas, priorización por riesgo y fuerte compromiso directivo.

El resultado tangible fue la recomendación formal del organismo certificador para emitir ISO/IEC 27001:2022 y mantener la certificación ISO 9001:2015. No obstante, el aporte más significativo del trabajo como paper es dejar un reporte sistemático de

experiencia, sustentado en evidencia trazable, sobre cómo integrar seguridad de la información en un sistema de gestión preexistente sin duplicar estructuras ni perder operatividad.

En términos aplicados, el artículo propone una referencia útil para organizaciones de desarrollo de software que ya cuentan con un sistema de calidad y necesitan fortalecer su gobernanza de ciberseguridad. Su valor reside menos en la generalización estadística que en la explicitación verificable de decisiones, evidencias, resultados y lecciones transferibles.

El sistema resultante no agota la agenda de mejora, pero deja una base sólida para profundizar prácticas de desarrollo seguro, gestión de terceros y métricas de madurez. Esa combinación entre certificación y capacidad de aprendizaje continuo es, precisamente, el principal valor del enfoque integrado.

Referencias

Bernardo, M., Simon, A., Tarí, J. J., & Molina-Azorín, J. F. (2015). Benefits of management systems integration: A literature review. Journal of Cleaner Production, 94, 260-267. https://www.sciencedirect.com/science/article/abs/pii/S0959652615000803?via%3Di hub

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76-105. https://www.emerald.com/tqm/article/33/7/76/459175/The-ISO-IEC-27001-information-security-management

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information Security Technical Report, 13(4), 247-255. https://www.sciencedirect.com/science/article/abs/pii/S1363412708000514?via%3Di hub

ISO. (2015). Quality management systems - Requirements (ISO 9001:2015). International Organization for Standardization.

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

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I: Método. Gobierno de España.

Nunhes, T. V., Motta Barbosa, L. C. F., & de Oliveira, O. J. (2017). Identification and analysis of the elements and functions integrable in integrated management systems. Journal of Cleaner Production, 142, 3225-3235. https://www.sciencedirect.com/science/article/abs/pii/S0959652616317784?via%3Di hub

Simon, A., Karapetrovic, S., & Casadesús, M. (2012). Difficulties and benefits of integrated management systems. Industrial Management & Data Systems, 112(5), 828-846. https://www.emerald.com/imds/article-abstract/112/5/828/183893/Difficulties-and-benefits-of-integrated-management?redirectedFrom=fulltext

Tarí, J. J., Molina-Azorín, J. F., & Heras, I. (2012). Benefits of the ISO 9001 and ISO 14001 standards: A literature review. Journal of Industrial Engineering and Management, 5(2), 297-322. https://www.jiem.org/index.php/jiem/article/view/488