DISEÑO E IMPLEMENTACIÓN DE UN MARCO DE GESTIÓN DE RIESGOS Y RESPALDO PARA AUTOMATIZACIONES EN FW INGENIERÍA

STEPHANY RIVEROS SALAMANCA

Director:
Ing. GERALD BREEK FUENMAYOR RIVADENEIRA, M.Sc.

(Trabajo de grado para optar por el título de Ingeniero de Telecomunicaciones)

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERIAS TIC
BOGOTÁ D. C.
2025

DEDICATORIA

Dedico este trabajo de grado, en primer lugar, a Dios, por permitirme llegar hasta este momento y darme la fortaleza necesaria para superar cada reto del camino.

A mis padres por su amor incondicional, sus consejos, sus sacrificios silenciosos y por creer en mí incluso cuando yo misma dudaba. Gracias por enseñarme con su ejemplo el valor del esfuerzo, la responsabilidad y la perseverancia. Este logro es el reflejo de todo lo que han sembrado en mí.

Finalmente, a todas las personas que de una u otra forma hicieron parte de este proceso y que, con sus palabras, gestos y compañía, me ayudaron a llegar hasta aquí.

AGRADECIMIENTOS

Agradezco, en primer lugar, a Dios, por brindarme la vida, la salud, la sabiduría y la fortaleza necesarias para culminar esta etapa tan importante de mi formación profesional.

A mi familia, por su apoyo constante, sus palabras de ánimo y su confianza en mí cada consejo, cada gesto de cariño y cada muestra de apoyo fueron fundamentales para avanzar incluso en los momentos más difíciles.

A mi compañero y amigo Daniel Pedraza, quien estuvo a mi lado durante toda la carrera, su compañía, apoyo y amistad hicieron de este camino un proceso mucho más llevadero y significativo.

A mi tutor, por su orientación, dedicación y paciencia durante el desarrollo de este trabajo de grado, así como por sus observaciones y sugerencias, que permitieron mejorar el proyecto y darle una estructura adecuada.

A los profesores de la facultad, por compartir sus conocimientos, experiencias y exigencia académica, los cuales contribuyeron de manera decisiva a mi formación personal y profesional.

Finalmente, a todas las personas que, de una u otra manera, aportaron a este proceso con su apoyo, sus palabras y su compañía. A cada uno, muchas gracias.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Este trabajo de grado presenta el diseño e implementación de un marco de gestión de riesgos y respaldo para las automatizaciones del área SOC de la empresa FW Ingeniería, con el objetivo de mejorar la confiabilidad, trazabilidad y seguridad de los procesos automatizados. En una primera etapa, se realizó un diagnóstico del proceso actual de automatización, identificando falencias como la ausencia de respaldos formales, la falta de validación estructurada y la limitada documentación de cambios. Posteriormente, se llevó a cabo la identificación y clasificación de riesgos técnicos y operativos, utilizando una matriz cuantitativa basada en probabilidad e impacto, priorizando aquellos catalogados como altos y críticos. Con base en estos resultados, se diseñó un marco metodológico compuesto por fases de análisis de riesgos, respaldo inicial, pruebas en entorno controlado, despliegue en producción, validación y mejora continua, integrando buenas prácticas de ITIL, la norma ISO/IEC 27005:2018 y la metodología ágil Scrum. Finalmente, su implementación piloto evidenció una reducción significativa de errores en reportes, fallos sin respaldo y reprocesos operativos en el SOC.

Palabras clave: gestión de riesgos, automatización, respaldo, SOC, ITIL 4, ISO/IEC 27005:2018, Scrum.

ABSTRACT

This thesis presents the design and implementation of a Risk and Backup Management Framework for automations in the Security Operations Center (SOC) of the company FW Ingeniería, with the objective of improving the reliability, traceability and security of automated processes. First, a diagnosis of the current automation process was carried out, identifying weaknesses such as the absence of formal backups, lack of structured validation and limited documentation of changes. Subsequently, technical and operational risks were identified and classified using a quantitative matrix based on probability and impact, prioritizing those categorized as high and critical. Based on these results, a methodological framework was designed, structured in phases of risk analysis, initial backup, testing in a controlled environment, deployment in production, validation and continuous improvement, integrating good practices from ITIL, the ISO/IEC 27005:2018 standard and the Scrum agile

methodology. Finally, the pilot implementation showed a significant reduction in report errors, failures without backup and operational rework within the SOC.

Keywords: gestión de riesgos, automatización, respaldo, SOC, ITIL 4, ISO/IEC 27005:2018, Scrum.

INTRODUCCIÓN

FW Ingeniería es una empresa dedicada a la prestación de servicios de soporte, implementación y monitoreo tecnológico para diversas organizaciones a nivel nacional. En la actualidad, el área de Seguridad Operacional (SOC) de la compañía ha venido realizando procesos de automatización mediante una plataforma de orquestación, automatización y respuesta de seguridad. Sin embargo, dichas automatizaciones se desarrollan de manera independiente y sin procedimientos estandarizados de respaldo ni gestión de riesgos, lo cual ha ocasionado incidentes operativos que afectan la continuidad y disponibilidad de los servicios, como el baneo de canales de comunicación empresariales.

El presente proyecto propuso el diseño de un marco de gestión de riesgos y respaldo para la implementación de automatizaciones en FW Ingeniería, basado en las metodologías ITIL y Scrum. La metodología ITIL permitió estructurar las prácticas de gestión del cambio, continuidad y mejora continua, mientras que Scrum facilitó una ejecución ágil e iterativa del marco, promoviendo la validación y retroalimentación constante durante su desarrollo.

Como resultado, se estableció un procedimiento formal que garantiza que toda automatización desarrollada en la empresa cuente con respaldo previo, análisis de riesgos, pruebas controladas y mecanismos de recuperación ante posibles fallos, con el fin de fortalecer la confiabilidad de los procesos automatizados, reducir los incidentes derivados de errores en la implementación y fomentar la cultura de documentación y mejora continua dentro del área SOC.

El documento se organiza de la siguiente manera: en el Capítulo 1 se presenta el planteamiento del problema, la justificación y los objetivos del proyecto; en el Capítulo 2 se describe el marco de referencia institucional; en el Capítulo 3 se expone el marco metodológico; en el Capítulo 4 se desarrolla el marco teórico relacionado con automatizaciones, gestión de riesgos, respaldos y metodologías ITIL y Scrum; en el Capítulo 5 se presenta el desarrollo del proyecto, donde se incluyen el diagnóstico del SOC, la identificación y análisis de riesgos, el diseño del marco propuesto y su implementación piloto; finalmente, en el Capítulo 6 se exponen las conclusiones y recomendaciones derivadas del trabajo realizado.

1 MARCO GENERAL DEL PROYECTO

En esta sección se presenta una visión general del proyecto, en la que se describen los objetivos, el alcance y la metodología empleada para su desarrollo. Se busca ofrecer al lector un contexto claro sobre el problema abordado, la forma en que se estructuró la investigación y las principales etapas seguidas para diseñar el marco de gestión de riesgos y respaldo aplicado a las automatizaciones del área SOC de la empresa FW Ingeniería. De esta manera, se facilita la comprensión del contenido posterior del documento y la valoración del grado de cumplimiento de los objetivos planteados.

1.1 PLANTEAMIENTO DEL PROBLEMA

FW Ingeniería es una empresa colombiana dedicada a la prestación de servicios de soporte técnico, implementación de soluciones y monitoreo de infraestructura tecnológica para diferentes organizaciones del país. En este contexto, el área de Seguridad Operacional (SOC) ha incrementado el uso de una plataforma de orquestación, automatización y respuesta de seguridad para reducir tareas manuales y optimizar tiempos de atención. No obstante, este avance tecnológico no ha sido acompañado por una gestión formal de riesgos ni por procedimientos estructurados de respaldo.

En la práctica, las automatizaciones son diseñadas y modificadas de manera individual por un analista, sin lineamientos claros sobre validación previa, control de cambios o documentación de las versiones. Esta forma de trabajo ha derivado en incidentes operativos que afectan tanto a FW Ingeniería como a sus clientes, entre ellos interrupciones en la continuidad del servicio, errores en reportes y bloqueos en canales de comunicación corporativa, lo que evidencia una alta dependencia del conocimiento tácito y la ausencia de controles preventivos.

La observación realizada en el área SOC permitió identificar que, antes de ejecutar una automatización, no se evalúan de manera sistemática los riesgos técnicos y operativos asociados, ni se garantiza la existencia de un respaldo confiable que permita revertir cambios en caso de falla. Esta carencia incrementa la probabilidad de pérdida de datos,

configuraciones o servicios, y dificulta la recuperación oportuna ante errores, generando reprocesos, sobrecarga operativa y posibles afectaciones en la percepción de calidad por parte de los clientes.

De acuerdo con las buenas prácticas de ITIL, la gestión del cambio y la continuidad del servicio son fundamentales para reducir riesgos y asegurar la recuperación ante incidentes en entornos tecnológicos (1), mientras que marcos ágiles como Scrum enfatizan la mejora continua y la revisión frecuente de los procesos (2). En contraste con estas recomendaciones, la situación actual del SOC de FW Ingeniería evidencia la necesidad de contar con un marco estructurado que integre gestión de riesgos, respaldos y validación sistemática en las automatizaciones.

En este sentido, el problema central que orienta este trabajo se plantea en la siguiente pregunta:

¿De qué manera se puede contribuir a mejorar la confiabilidad y trazabilidad de las automatizaciones en FW Ingeniería?

1.2 OBJETIVOS

1.2.1 Objetivo general

Diseñar e implementar un marco de gestión de riesgos y respaldo para las automatizaciones en el área SOC de la empresa FW Ingeniería, basado en las metodologías ITIL y la norma ISO/IEC 27005:2018, con el fin de mejorar la confiabilidad, trazabilidad y seguridad de los procesos automatizados.

1.2.2 Objetivos específicos

- Analizar el proceso de automatización de FW Ingeniería y los marcos de gestión de referencia con el fin de establecer las bases de diseño del marco propuesto.
- Identificar los riesgos técnicos y operativos presentes en las automatizaciones con el fin incluirlos en la arquitectura del marco de gestión propuesto.
- Implementar el marco de gestión de riesgos propuesto con enfoque ágil para determinar su nivel de eficacia.

1.3 ALCANCE

El alcance de este trabajo de grado se centra en el análisis y mejora de las automatizaciones implementadas en el área de operaciones de seguridad (SOC) de la empresa FW Ingeniería. En particular, el proyecto se enfoca en las automatizaciones relacionadas con la generación y envío de reportes, desarrolladas sobre la plataforma de orquestación, automatización y respuesta de seguridad utilizada por la organización.

El trabajo no pretende intervenir toda la infraestructura tecnológica de la empresa ni rediseñar sus servicios de TI, sino delimitarse al proceso de automatización dentro del SOC, tomando como base principios de gestión de servicios de TI y de mejora continua sugeridos en marcos como ITIL4, que proponen la gestión de cambios y el control de riesgos como elementos clave para la estabilidad del servicio (1).
En este contexto, el alcance del proyecto comprende:

Analizar el proceso actual de automatización de reportes, identificando fallas y debilidades en la gestión de riesgos.

Diseñar un marco de gestión de riesgos y respaldo aplicable a las automatizaciones del SOC.

Implementar dicho marco en una automatización piloto de reportes.

Evaluar la efectividad del marco a partir de indicadores de confiabilidad, tiempos de recuperación y reducción de incidentes asociados a automatizaciones fallidas.

No se aborda la certificación formal de la empresa en marcos de referencia como ITIL o Scrum ni el rediseño organizacional completo de la gestión de TI. El proyecto se limita a adaptar buenas prácticas de estos marcos al contexto específico del SOC de FW Ingeniería, siguiendo el enfoque de gestión de riesgos recomendado por la norma ISO/IEC 27005:2018 (3) y lineamientos de trabajo ágil basados en Scrum (4).

1.4 JUSTIFICACIÓN

En el contexto actual de la transformación digital, las organizaciones dependen cada vez más de procesos automatizados para optimizar su operación, reducir errores humanos y responder con rapidez a los requerimientos del negocio. No obstante, la ausencia de una gestión estructurada de riesgos y respaldos en las automatizaciones del área SOC ha evidenciado vulnerabilidades que comprometen la continuidad de los servicios y la integridad de la información.

Este proyecto adquiere importancia debido a la necesidad de fortalecer la gestión operativa de la organización mediante la implementación de prácticas estandarizadas que permitan reducir los riesgos asociados a las automatizaciones, garantizar la estabilidad de los servicios tecnológicos y asegurar la recuperación ante fallos. Además, su desarrollo aporta beneficios relevantes al promover la cultura de documentación, trazabilidad y mejora continua dentro del equipo técnico, elementos esenciales para incrementar la confiabilidad y eficiencia de los procesos del área SOC.

Desde el punto de vista metodológico, la adopción de ITIL proporciona una estructura sólida para la gestión del cambio, la continuidad y la mejora del servicio, asegurando que cada automatización se ejecute bajo criterios de seguridad y control (3). De manera complementaria, Scrum facilita la ejecución ágil e incremental de las mejoras, fomentando la colaboración entre los analistas SOC y la retroalimentación constante durante el ciclo de desarrollo (4).

Los aportes de este trabajo se reflejan en diferentes ámbitos:

Académico: contribuye al fortalecimiento del conocimiento sobre la integración de metodologías ITIL y Scrum en la gestión de riesgos y respaldos, sirviendo como referencia para futuras investigaciones o proyectos académicos en el campo de las tecnologías de la información.

Económico: optimiza el uso de recursos tecnológicos al disminuir los errores operativos y tiempos de inactividad, generando un impacto positivo en la productividad y reduciendo costos asociados a fallos en las automatizaciones.
Social: fomenta la cultura de responsabilidad y mejora continua dentro de los equipos técnicos, promoviendo prácticas seguras y colaborativas que fortalecen la confianza entre empleados y clientes.

Ambiental: al mejorar la eficiencia de los procesos automatizados y reducir retrabajos o ejecuciones fallidas, se contribuye al menor consumo de energía y optimización del uso de infraestructura tecnológica.

En conjunto, la implementación de este proyecto representa una contribución integral al desarrollo tecnológico y organizacional, alineada con los principios de sostenibilidad, innovación y mejora continua.

2 MARCO REFERENCIAL

El presente capítulo desarrolla los fundamentos conceptuales que soportan este trabajo de grado y permiten comprender el contexto técnico y metodológico en el que se propone el marco de gestión de riesgos y respaldo para las automatizaciones del área SOC de FW Ingeniería. Para ello, se abordan, en primer lugar, las bases de la automatización en entornos empresariales y su relación con la eficiencia operativa. Posteriormente, se profundiza en la gestión de riesgos en TI y en los conceptos de respaldo y recuperación como elementos clave para la continuidad del servicio. Finalmente, se presentan los marcos de referencia ITIL y ISO/IEC 27005:2018, cuya integración sirve como soporte metodológico para el diseño e implementación del marco propuesto. Estos apartados permiten articular la problemática identificada con las mejores prácticas reconocidas a nivel internacional, ofreciendo un sustento sólido para las decisiones y propuestas planteadas en los capítulos posteriores.

2.1 AUTOMATIZACIONES EN ENTORNOS EMPRESARIALES

La automatización de procesos empresariales se define como la utilización de herramientas tecnológicas para ejecutar tareas repetitivas, reducir la intervención humana y optimizar la eficiencia operativa dentro de una organización. Su objetivo principal es mejorar la productividad, garantizar la precisión de los procesos y disminuir los errores derivados de la gestión manual (5).

En el contexto de las operaciones tecnológicas y de ciberseguridad, la automatización cumple un papel esencial, ya que permite a los equipos reducir los tiempos de respuesta, estandarizar procedimientos y mantener un control más preciso sobre los flujos de trabajo. Según Gartner (2021), más del 70 % de las organizaciones a nivel mundial están implementando estrategias de automatización para fortalecer la eficiencia y la seguridad de sus procesos críticos (6).

En el caso de FW Ingeniería, la automatización se aplica principalmente en el área de Seguridad Operacional (SOC), donde se utilizan plataformas de orquestación, automatización y respuesta para generar reportes, ejecutar acciones automáticas ante

alertas de seguridad y optimizar la operación diaria. No obstante, cuando las automatizaciones se realizan sin una planeación estructurada, sin mecanismos de respaldo o sin gestión de riesgos, pueden originarse fallos que afecten la disponibilidad de servicios o incluso provoquen interrupciones operativas.

Autores como Hammer y Champy (7) destacan que la automatización no debe considerarse sólo como un cambio tecnológico, sino como una transformación organizacional que requiere planificación, control y evaluación continua para evitar impactos negativos. En este sentido, la falta de gestión en los procesos automatizados puede aumentar los riesgos operativos y de seguridad, comprometiendo la confiabilidad de la infraestructura tecnológica.

Por tanto, la automatización debe implementarse bajo un enfoque metodológico que contemple la evaluación previa de riesgos, la creación de respaldos, las pruebas controladas y la documentación de cada cambio. Solo de esta forma es posible garantizar la continuidad del negocio, la trazabilidad de las acciones y la reducción de errores en los entornos empresariales.

2.2 GESTIÓN DE RIESGOS EN TI

La gestión de riesgos en Tecnologías de la Información (TI) consiste en un proceso sistemático orientado a identificar, analizar, evaluar y tratar los riesgos que pueden afectar la disponibilidad, integridad y confidencialidad de los sistemas, datos y servicios tecnológicos de una organización. Su propósito principal es reducir la probabilidad de incidentes y mitigar sus impactos sobre los objetivos del negocio (8).

Según la ISO/IEC 27005:2018, la gestión del riesgo es una parte integral de todos los procesos organizacionales y debe incorporarse en la toma de decisiones, pues su aplicación permite anticipar amenazas y fortalecer la resiliencia operativa (9). En el ámbito de TI, esto implica reconocer las vulnerabilidades presentes en los sistemas, las posibles amenazas que puedan explotarlas y los efectos que dichas amenazas tendrían sobre los servicios críticos.

En entornos donde se realizan automatizaciones de procesos, la gestión de riesgos adquiere especial relevancia, ya que una automatización mal diseñada o implementada sin controles adecuados puede generar fallos masivos, pérdidas de información o interrupciones en la operación. Estos riesgos no solo se relacionan con aspectos técnicos, sino también con errores humanos, configuraciones inadecuadas y ausencia de mecanismos de respaldo o rollback.

De acuerdo con Cárdenas y Bernal (10), la gestión del riesgo en TI debe enfocarse en la evaluación preventiva, donde cada cambio o implementación tecnológica sea precedida por una revisión de impacto y la existencia de planes de recuperación. Este principio se alinea directamente con las prácticas del marco ITIL, que promueve la planificación y control de los riesgos asociados a los servicios tecnológicos antes de realizar cualquier modificación en la infraestructura.

En el contexto de FW Ingeniería, la ausencia de un proceso formal de gestión de riesgos antes de ejecutar automatizaciones ha provocado incidentes operativos que afectan la continuidad de los servicios. Implementar un marco que contemple la evaluación sistemática de riesgos, la definición de planes de mitigación y la creación de respaldos permitirá fortalecer la seguridad y confiabilidad de los procesos automatizados del área SOC.

2.3 RESPALDO Y RECUPERACIÓN

El respaldo y la recuperación son componentes esenciales dentro de la gestión de continuidad del servicio en el ámbito de las Tecnologías de la Información. Su propósito es garantizar la disponibilidad e integridad de los datos y configuraciones ante fallos, errores humanos, incidentes de ciberseguridad o desastres operativos. El respaldo consiste en la copia y almacenamiento seguro de la información crítica, mientras que la recuperación implica el proceso de restaurarla en caso de pérdida o daño (11).

Según la norma ISO/IEC 27031:2011, los mecanismos de respaldo y recuperación deben formar parte del plan de continuidad del negocio y ser probados periódicamente para asegurar su efectividad. Estos procedimientos permiten restablecer la operación de los

servicios tecnológicos en un tiempo aceptable, minimizando los impactos financieros y operativos que puedan derivarse de una interrupción (12).

Existen diferentes tipos de respaldo, entre los cuales se destacan el respaldo completo, que realiza una copia total de los datos; el respaldo incremental, que copia únicamente la información modificada desde el último respaldo; y el respaldo diferencial, que almacena los cambios efectuados desde la última copia completa (13). La elección del tipo de respaldo depende de los requerimientos del servicio, los tiempos de recuperación esperados y los recursos de almacenamiento disponibles.

En el contexto de las automatizaciones del área SOC de FW Ingeniería, la ausencia de procedimientos formales de respaldo ha generado vulnerabilidades operativas. Algunas automatizaciones, al ejecutarse sin una copia previa del entorno o de la configuración, han ocasionado interrupciones en servicios de comunicación y fallos en reportes. Por tanto, se hace necesario incorporar un protocolo obl.00igatorio de respaldo previo y validación posterior para cada automatización desarrollada, de manera que se garantice la posibilidad de reversión ante cualquier error.

Implementar políticas de respaldo y recuperación permite no solo salvaguardar la información, sino también aumentar la confianza y la trazabilidad de los procesos automatizados. Adicionalmente, estas medidas se alinean con las prácticas de ITIL, que establecen la gestión de continuidad como un proceso fundamental dentro del ciclo de vida del servicio (1).

En conclusión, contar con estrategias de respaldo y recuperación en las automatizaciones del área SOC contribuye directamente a la resiliencia tecnológica de FW Ingeniería, reduciendo la probabilidad de pérdida de datos, minimizando los tiempos de inactividad y fortaleciendo la capacidad de respuesta ante incidentes operativos o de seguridad.

2.4 METODOLOGÍA ITIL

La metodología ITIL (Information Technology Infrastructure Library) es un marco de buenas prácticas internacionalmente reconocido para la gestión de servicios de TI, cuyo propósito

es alinear los servicios tecnológicos con las necesidades del negocio, garantizando calidad, continuidad y mejora continua. ITIL proporciona lineamientos estructurados que permiten gestionar de manera eficiente los procesos, incidentes, cambios, problemas y la seguridad de la información dentro de una organización (14).

El marco ITIL se compone de cinco fases principales dentro del ciclo de vida del servicio: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua (15). Cada fase integra procesos específicos que contribuyen al control y gestión de los servicios tecnológicos. Entre ellos destacan la gestión del cambio, la gestión de la continuidad del servicio y la gestión de riesgos, los cuales resultan esenciales para el desarrollo de automatizaciones seguras y controladas.

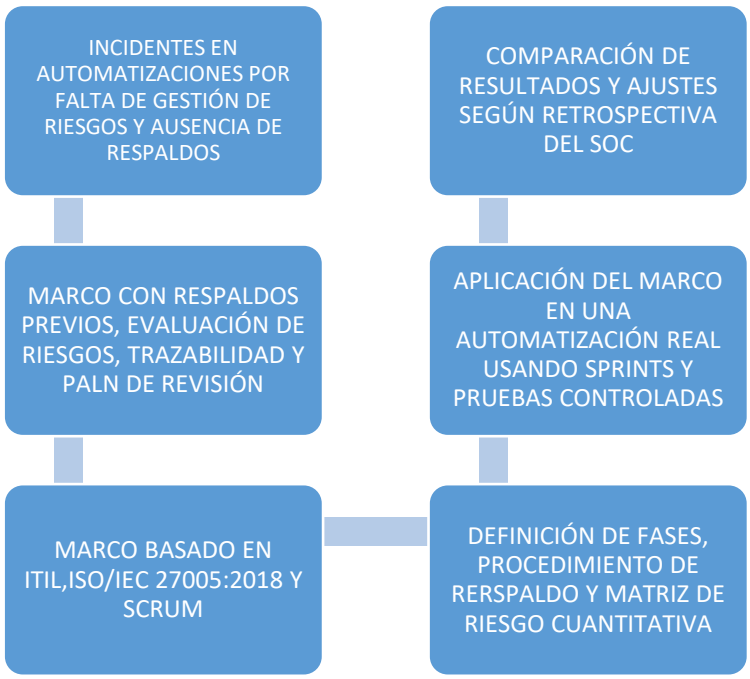
De acuerdo con AXELOS (1), la gestión del cambio tiene como finalidad garantizar que todas las modificaciones en la infraestructura tecnológica —incluyendo scripts, configuraciones o automatizaciones— se planifiquen, evalúen y aprueben antes de su implementación, reduciendo así los riesgos de interrupciones no deseadas. Este proceso incluye la revisión del impacto, el plan de respaldo, las pruebas controladas y la documentación posterior a la ejecución.

La gestión de la continuidad del servicio, por su parte, busca asegurar que la organización pueda mantener sus operaciones críticas ante fallos o desastres tecnológicos. Para ello, ITIL recomienda establecer planes de respaldo y recuperación, así como realizar pruebas periódicas de efectividad. Estas prácticas son especialmente relevantes en el contexto de FW Ingeniería, donde la ausencia de respaldos en automatizaciones ha generado incidentes que afectaron la disponibilidad de los servicios corporativos.

Asimismo, ITIL incorpora la mejora continua del servicio (CSI, Continual Service Improvement), cuyo objetivo es analizar los resultados obtenidos, identificar lecciones aprendidas y optimizar los procesos implementados. Esta filosofía de mejora continua coincide con la naturaleza iterativa de la metodología Scrum, permitiendo una integración armónica entre ambas metodologías dentro del marco propuesto para FW Ingeniería.

Desde la perspectiva de la ingeniería, el diseño se entiende como un proceso sistemático en el que, a partir de un problema identificado, se formulan requisitos, se proponen alternativas de solución y se estructura un modelo técnico que pueda ser implementado y evaluado. En este trabajo, dicho concepto se materializa en el diseño de un marco de gestión de riesgos y respaldo aplicado a las automatizaciones del SOC: se definieron requerimientos (confiabilidad, trazabilidad, respaldo previo, capacidad de reversión), se seleccionaron como referencias ITIL e ISO/IEC 27005:2018 y se estructuraron fases, procedimientos y controles específicos. De este modo, el proyecto no solo describe la situación existente, sino que aplica el diseño en ingeniería para construir una solución formal, verificable y alineada con las buenas prácticas de gestión de servicios de TI.

Figura 1. Proceso de diseño en ingeniería aplicado al marco de gestión de riesgos y respaldo



Fuente: Elaboración propia

2.5 METODOLOGÍA SCRUM

Figura 2. Esquema gráfico de la metodología Scrum

Elaborado por: VLADGRIN. Metodología ágil para el diagrama de ciclo de vida de desarrollo de software

La metodología Scrum es un marco de trabajo ágil utilizado para la gestión y desarrollo de proyectos complejos, cuyo enfoque se basa en la entrega incremental y continua de valor mediante sprints, permitiendo adaptarse rápidamente a los cambios y garantizar resultados funcionales en periodos cortos (16); se fundamenta en tres pilares esenciales: transparencia, inspección y adaptación, de modo que la transparencia asegura que todos los miembros del equipo comprendan el estado del proyecto y los objetivos, la inspección permite evaluar periódicamente el progreso y detectar desviaciones, y la adaptación posibilita ajustar el trabajo ante cambios o descubrimientos durante el proceso (17). El marco define tres roles principales —Product Owner, Scrum Master y Equipo de desarrollo— y una serie de eventos clave como la planificación del sprint, las reuniones diarias, la revisión y la retrospectiva, los cuales se representan de forma esquemática en la Figura X, donde se observa el flujo desde el Product Backlog y el Sprint Backlog hasta la ejecución del sprint y sus actividades de revisión y mejora continua (18).

En el contexto específico de FW Ingeniería, Scrum se adapta a las necesidades del área SOC para gestionar de forma ordenada las automatizaciones que se desarrollan sobre la plataforma de orquestación y respuesta de seguridad: el Product Owner puede ser asumido por la persona encargada en el SOC, quien prioriza las automatizaciones según el impacto en los servicios de los clientes; el Equipo de desarrollo está conformado por los analistas SOC encargados de diseñar, configurar y probar los flujos de automatización; y el Scrum

Master actúa como facilitador del proceso, ayudando a eliminar impedimentos y garantizando que cada sprint incluya actividades de identificación de riesgos, definición de respaldos y validación de resultados.

De esta forma, cada sprint puede enfocarse en una automatización concreta, por ejemplo, la generación y envío de reportes, incorporando tareas específicas como el análisis de riesgos asociados, la implementación de respaldos previos, la ejecución en entorno controlado y la revisión de incidentes ocurridos en automatizaciones anteriores del SOC.
Así, el ciclo iterativo que muestra la Figura 2 se utiliza en FW Ingeniería para mejorar progresivamente la calidad de las automatizaciones, reducir fallos como bloqueos de canales de comunicación o errores en reportes y reforzar la trazabilidad de los cambios realizados; en ese sentido, Scrum se integra con las buenas prácticas de ITIL para la gestión del cambio, la continuidad del servicio y la gestión de riesgos, mientras aporta una estructura ágil para la entrega incremental, la documentación permanente y la retroalimentación constante (19). De esta manera, Scrum se consolida como la metodología adecuada para la fase de implementación y validación del marco de gestión de riesgos y respaldo en el área SOC de FW Ingeniería, garantizando que el desarrollo de automatizaciones se realice de manera controlada, alineada con las necesidades operativas de la empresa y orientada a la mejora continua de sus servicios de seguridad.

2.6 ANTECEDENTES

2.6.1 Nacionales

En el trabajo “Propuesta desde la gestión de proyectos para la implementación de la metodología ágil SCRUM para el desarrollo web”, desarrollado en una universidad colombiana, se presenta una propuesta para introducir Scrum en proyectos de desarrollo web, destacando la necesidad de definir roles, artefactos y ceremonias para lograr una adopción efectiva de la metodología (25). Este antecedente es pertinente porque evidencia que en el contexto local se está promoviendo formalizar el uso de Scrum en proyectos tecnológicos, lo cual se alinea con el enfoque ágil del marco propuesto en este trabajo.

De igual manera, el desarrollo “Software para la Gestión de Proyectos ágiles de TI tipo SCRUM”, referenciado en sistemas de información científicos nacionales, propone una herramienta para apoyar la planificación y seguimiento de proyectos que utilizan Scrum

(26). Este trabajo refuerza la relevancia de disponer de mecanismos que permitan estructurar y documentar las actividades de un equipo ágil, aspecto que también se busca en el marco de gestión de riesgos y respaldo planteado para las automatizaciones del SOC.

El estudio “Análisis correlacional de la gestión de riesgos según marcos de trabajo ágiles (Scrum) y marcos de trabajo predictivo (PMBOK)”, desarrollado en una institución colombiana, compara la gestión de riesgos en proyectos gestionados bajo enfoques ágiles y tradicionales, concluyendo que los marcos ágiles pueden gestionar riesgos de forma efectiva siempre que se integren prácticas explícitas de identificación, análisis y seguimiento de los mismos (27). Este antecedente aporta un sustento teórico importante al objetivo del proyecto, que busca integrar la gestión de riesgos en un contexto donde se pretende utilizar Scrum como enfoque de trabajo.

Por otra parte, el informe “Digital Trust Insights 2025” elaborado por PwC Colombia presenta un panorama de los principales riesgos en ciberseguridad y adopción tecnológica en organizaciones del país, destacando que la automatización y el uso de herramientas basadas en inteligencia artificial incrementan la necesidad de contar con controles robustos de seguridad y gestión de riesgos (28). Este documento contextualiza la problemática de FW Ingeniería dentro de una tendencia más amplia, en la cual la automatización trae beneficios, pero también incrementa la superficie de riesgo.

Finalmente, la “Encuesta Agentes de IA PwC 2025: resultados clave”, también en el contexto colombiano, resalta que muchas organizaciones están implementando automatizaciones y agentes inteligentes sin contar con marcos adecuados de gobierno y gestión de riesgos, lo que puede derivar en incidentes operativos y de seguridad (29). Este antecedente refuerza la relevancia y actualidad del problema abordado por este trabajo, ya que evidencia que la falta de gestión de riesgos en automatizaciones no es un caso aislado, sino una situación recurrente en el entorno empresarial.

2.6.2 Internacionales

En el trabajo titulado “Propuesta de un modelo de gestión de riesgos para proyectos de desarrollo de software bajo una metodología ágil”, se plantea un modelo que integra la gestión de riesgos dentro de proyectos que utilizan metodologías ágiles, mostrando cómo

la identificación temprana de riesgos y su tratamiento sistemático mejoran la calidad del producto y reducen la probabilidad de fallos en las entregas (19). Este antecedente resulta relevante para el presente proyecto, dado que también busca integrar la gestión de riesgos en un contexto donde se utilizan enfoques ágiles para la automatización de procesos.

Por su parte, el artículo “Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT” propone un modelo específico para la gestión de riesgos de tecnologías de la información en pequeñas y medianas empresas, resaltando la importancia de adaptar los marcos de referencia a la realidad y capacidad de las organizaciones (20). Esta idea de adaptación contextual es clave para el diseño de un marco de gestión de riesgos y respaldos aplicable al área SOC de FW Ingeniería, que no es una gran corporación, pero sí requiere prácticas formales de gestión de riesgos.

El trabajo “Metodologías ágiles: Scrum para la innovación en los procesos crediticios” analiza la aplicación de Scrum en el sector financiero, mostrando cómo la metodología permite gestionar mejor la incertidumbre, mejorar la comunicación entre los equipos y reducir tiempos de entrega (21). Aunque se desarrolla en otro sector, evidencia que Scrum puede emplearse no solo en desarrollo de software, sino también en procesos operativos, lo cual respalda su uso como enfoque para estructurar las iteraciones del marco propuesto en este proyecto.

Adicionalmente, el documento “Gestión de riesgos en el proceso ITIL de gestión de cambios” profundiza en cómo la gestión de riesgos puede integrarse de manera explícita dentro del proceso de gestión de cambios de ITIL, planteando que cada cambio debe ser evaluado en términos de probabilidad de fallo e impacto en el servicio (23). Este antecedente se relaciona directamente con la necesidad de evaluar los riesgos antes de implementar automatizaciones que, en la práctica, constituyen cambios sobre la operación habitual del SOC.

Finalmente, el recurso “ITIL 4 y la Gestión de Riesgos: ¿Cómo se relacionan?” ofrece una visión práctica sobre cómo ITIL 4 incorpora la gestión de riesgos dentro de la gestión de servicios, destacando la importancia de considerar el riesgo como un elemento transversal a todo el ciclo de vida del servicio (24). Este enfoque refuerza la pertinencia de utilizar

principios de ITIL como base para estructurar el marco de gestión de riesgos y respaldo en las automatizaciones de FW Ingeniería.

En conclusión, Scrum representa la metodología ideal para la fase de implementación y validación del marco de gestión en FW Ingeniería, ya que combina agilidad, colaboración y mejora continua. Esto asegura que el desarrollo de automatizaciones se realice de manera controlada, con respaldo documentado y con retroalimentación constante, garantizando un ciclo de mejora sostenible en el tiempo.

2.7 METODOLOGÍA

La metodología de este proyecto se enmarca en una investigación aplicada y de tipo descriptivo, orientada a resolver la problemática específica del área SOC de FW Ingeniería relacionada con la ausencia de una gestión formal de riesgos y respaldos en las automatizaciones. Se adoptó un enfoque mixto, combinando información cualitativa (descripción de procesos, observación directa e intercambio informal con el equipo SOC) con datos cuantitativos (registro de incidentes, frecuencia de errores y tiempos de recuperación), en concordancia con lo planteado por Hernández, Fernández y Baptista sobre el uso de diseños descriptivos y mixtos para comprender y mejorar fenómenos en contextos reales (31).

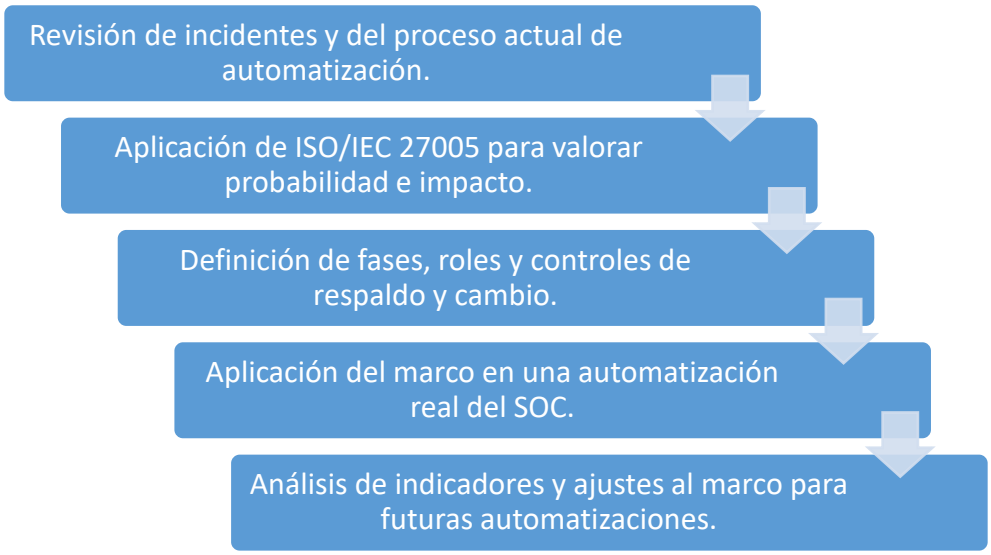
En una primera fase se realizó el diagnóstico del proceso actual de automatización, a partir de la revisión de correos asociados a fallos, registros de incidentes y observación de cómo se diseñaban y ejecutaban las automatizaciones. Posteriormente, se desarrolló la identificación y análisis de riesgos tomando como referencia la norma ISO/IEC 27005:2018, que orienta la gestión de riesgos de seguridad de la información mediante las etapas de identificación, análisis, evaluación y tratamiento (3); con base en este marco se construyó una matriz de riesgos que valoró probabilidad e impacto y permitió priorizar los riesgos más críticos para la continuidad del servicio.

En una fase posterior se diseñó el marco de gestión de riesgos y respaldo integrando principios de ITIL 4, especialmente en gestión de cambios, incidentes y mejora continua (1), junto con un enfoque ágil basado en Scrum, utilizando iteraciones cortas (sprints) para el diseño, prueba y ajuste del marco, tal como lo propone la guía de Scrum para lograr

incrementos graduales y verificables (4). Finalmente, se implementó una prueba piloto sobre una automatización real de reportes y se evaluó su efectividad mediante la comparación de indicadores antes y después de la aplicación del marco.

Las fuentes de información provinieron principalmente de la experiencia directa de la autora en el SOC de FW Ingeniería, de los registros internos de incidentes y de las reuniones del equipo donde se socializaban los errores en automatizaciones. La población de referencia estuvo conformada por los 14 integrantes del área SOC, empleándose una muestra no probabilística por conveniencia basada en la interacción con este equipo, lo cual es coherente con estudios aplicados en contextos organizacionales donde se prioriza el acceso a los actores directamente involucrados en el proceso analizado (31).

Figura 3. Fases metodológicas del proyecto en el área SOC de FW Ingeniería



Fuente: Elaboración propia

En primera instancia, se desarrolló una fase de diagnóstico del proceso actual de automatización en el SOC. Para ello se recurrió a la revisión de registros de incidentes, análisis de correos asociados a fallos en automatizaciones y observación de la forma en que se diseñan, prueban y despliegan los flujos de automatización. Este tipo de análisis descriptivo es consistente con enfoques metodológicos orientados a comprender el funcionamiento real de los procesos antes de proponer mejoras (2).

En segundo lugar, se llevó a cabo la identificación y análisis de riesgos asociados a las automatizaciones, tomando como referencia la norma ISO/IEC 27005:2018, la cual establece un proceso sistemático para la gestión de riesgos de seguridad de la información, incluyendo las etapas de identificación, análisis, evaluación y tratamiento de riesgos (3).

Con base en este marco, se construyó una matriz de riesgos en la que se valoraron probabilidad e impacto en una escala numérica y se categorizó cada riesgo en niveles bajo, medio, alto o crítico, permitiendo priorizar aquellos con mayor relevancia para la continuidad del servicio en el SOC.

En tercer lugar, en la fase de diseño del marco de gestión de riesgos y respaldo, se integraron principios de gestión de servicios de TI inspirados en ITIL4, particularmente en lo relacionado con la gestión de cambios, la mejora continua y la gestión de incidentes, buscando asegurar que las automatizaciones se implementen de manera controlada, documentada y con mecanismos de recuperación ante fallos (1).

Paralelamente, se adoptó un enfoque ágil de trabajo basado en Scrum, utilizando iteraciones cortas para el diseño, prueba y ajuste del marco. Este enfoque se sustenta en la guía de Scrum, que propone ciclos de planificación, revisión y retrospectiva para lograr incrementos de valor y mejora continua en productos y procesos (4).

En cuarto lugar, se llevó a cabo la implementación del marco mediante una prueba piloto aplicada a una automatización real de reportes en el SOC. Para ello se organizó el trabajo en un sprint, en el que se definieron claramente el objetivo del incremento, las tareas a realizar, los criterios de aceptación y los artefactos a registrar (documentación de riesgos, evidencias de respaldos, resultados de pruebas y ajustes). Durante esta fase se recopiló información cuantitativa sobre la frecuencia de errores en reportes, duplicidad de envíos y tiempos de recuperación ante fallos antes y después de la aplicación del marco.

Finalmente, se realizó una evaluación de la efectividad del marco propuesto a partir de los indicadores definidos. Los resultados obtenidos se analizaron comparativamente, identificando mejoras en la estabilidad y confiabilidad de las automatizaciones. Este proceso de evaluación y retroalimentación permitió ajustar el marco, en coherencia con el

principio de mejora continua tanto de ITIL 4 como de los marcos ágiles, y derivar recomendaciones para su futura ampliación a otras automatizaciones del área SOC.

2.7.1 Etapas

El desarrollo metodológico del proyecto se estructuró en cuatro etapas principales, que permitieron cumplir los objetivos específicos establecidos. Cada etapa contempla las actividades, el propósito y las herramientas utilizadas durante el proceso investigativo.

Tabla 1. Fases del marco de gestión de riesgos y respaldo

Etapa	Objetivo asociado	Actividades principales	Resultado esperado	Herramientas utilizadas
1. Diagnóstico inicial del SOC	Analizar el proceso actual de automatización para determinar las debilidades relacionadas con la ausencia de gestión de riesgos y respaldos.	- Revisión de procedimientos de automatización. - Observación directa de flujos de trabajo. - Entrevistas con analistas SOC. - Identificación de incidentes registrados.	Contar con un panorama detallado del estado actual de las automatizaciones y un listado claro de las falencias operativas detectadas.	Observación directa, entrevistas, registros de incidentes, hojas de control en Excel.

2. Análisis de riesgos	Identificar y clasificar los riesgos técnicos y operativos presentes en las automatizaciones.	- Aplicación de matriz de probabilidad e impacto. - Evaluación del nivel de criticidad. - Definición de medidas preventivas.	Disponer de una matriz de riesgos cuantificada y priorizada, con los riesgos clasificados por nivel de criticidad y sus medidas de mitigación preliminares.	Matriz de riesgos, ISO/IEC 27005:2018, Excel.
3. Diseño del marco metodológico	Diseñar un marco de gestión de riesgos y respaldo alineado con ITIL y Scrum.	- Definición de roles y responsabilidades. - Elaboración de flujos de trabajo y procedimientos. - Integración de prácticas ITIL y Scrum.	Tener documentado un marco formal que establezca roles, procedimientos, flujos y controles para garantizar trazabilidad, respaldo y mejora continua en las automatizaciones.	Diagramas de flujo, documentación ITIL 4, Scrum Guide (2020), Microsoft Visio, documentos técnicos.

4. Implementación piloto y evaluación	Evaluar la efectividad del marco mediante indicadores de confiabilidad, tiempo de recuperación y reducción de incidentes.	- Aplicación del marco en una automatización real. - Monitoreo de ejecución y registro de resultados. - Medición de indicadores antes y después. - Análisis comparativo de desempeño.	Evidenciar, a partir de indicadores medibles, la mejora en la confiabilidad, tiempos de recuperación y disminución de incidentes tras la implementación del marco.	Plataforma de automatización SOC, Excel para indicadores, reportes operativos, observación directa.

Elaborado por la autora

2.7.2 Herramientas

Durante el desarrollo del proyecto se emplearon diversas herramientas tecnológicas y de gestión, entre las cuales se destacan:

Almacenamiento local: dispositivo de almacenamiento en red utilizado para alojar los respaldos generados desde los servidores de automatización y monitoreo.

Almacenamiento cloud empresarial: servicio en la nube sincronizado con el almacenamiento local, empleado para mantener copias redundantes y facilitar la recuperación ante fallos.

Plataforma de orquestación y automatización de seguridad: herramienta utilizada por el área SOC para ejecutar automatizaciones y flujos de trabajo.

Microsoft Excel: para la elaboración de la matriz de riesgos y los registros de control.

Metodologías ITIL y Scrum: empleadas como base conceptual para la gestión de riesgos, control de cambios y mejora continua mediante iteraciones ágiles.

3 DESARROLLO DEL PROYECTO

3.1 ANÁLISIS DEL PROCESO DE AUTOMATIZACIÓN DE FW INGENIERÍA Y LOS MARCOS DE GESTIÓN DE RIESGO Y RESPALDO.

El área de Seguridad Operacional (SOC) de FW Ingeniería tiene como función principal la supervisión, automatización y respuesta ante eventos tecnológicos dentro de las infraestructuras administradas por la empresa. Para ello, el equipo SOC utiliza una plataforma de orquestación y automatización de seguridad, la cual permite ejecutar tareas automáticas orientadas de la generación de algunos reportes.

Flujo actual de automatizaciones

El flujo operativo actual inicia con la recepción de datos desde las plataformas de monitoreo, que recolecta información proveniente de los distintos dispositivos conectados a la red Posteriormente, las automatizaciones programadas en la herramienta de automatizaciones procesan esta información y generan resultados en forma de reportes automáticas.

En términos generales, el proceso actual cumple la función de recolección y entrega de datos automatizada; sin embargo, carece de procedimientos formales que garanticen el control de calidad, la verificación previa o la validación posterior de los resultados generados.

Falencias detectadas:

Durante el diagnóstico técnico y operativo se identificaron varias debilidades en el proceso de automatización, que afectan la confiabilidad y estabilidad del servicio.

Falta de documentación ya que no existe un registro centralizado que describa las automatizaciones implementadas, sus flujos, resultados o versiones anteriores, lo cual dificulta el seguimiento y la trazabilidad.

Ausencia de validación estructurada ya que las automatizaciones pasan directamente a entornos productivos sin pruebas controladas, lo que incrementa la probabilidad de errores operativos.

Se logra evidenciar incidentes de denegación de servicio (por ejemplo, la suspensión de cuentas corporativas de WhatsApp tras una automatización fallida) y errores en reportes, que en ocasiones presentan datos erróneos o repetidos debido a configuraciones duplicadas o fallas en la integración, sin embargo, antes de ser enviados a los clientes hay una persona la cual deba revisar el documento antes de enviarlo para validar la información.

Estas falencias reflejan la necesidad de establecer un marco metodológico formal de gestión de riesgos y respaldo que permita controlar las automatizaciones, asegurar la existencia de respaldos válidos y minimizar los impactos ante fallos.

3.1.1 Análisis del proceso actual

El primer paso del proyecto consistió en analizar el proceso actual de automatización llevado a cabo por el área SOC de FW Ingeniería. Este análisis permitió comprender cómo se están construyendo y ejecutando las automatizaciones, así como identificar las principales debilidades derivadas de la ausencia de una gestión formal de riesgos y de un esquema de respaldos estructurado.

3.1.1.1 Descripción general del proceso actual

El área SOC de FW Ingeniería es responsable del monitoreo, soporte e implementación de soluciones de seguridad para diferentes clientes a nivel nacional. En los últimos años, con el fin de optimizar tiempos y reducir actividades repetitivas, el equipo ha comenzado a utilizar una plataforma de orquestación, automatización y respuesta de seguridad para automatizar tareas, principalmente relacionadas con la generación y envío de reportes periódicos.

De manera general, el proceso de automatización inicia cuando el analista SOC identifica una tarea recurrente que puede ser automatizada, como la generación diaria o semanal de

reportes de monitoreo. A partir de esta necesidad, el analista diseña un flujo o playbook dentro de la plataforma de automatizaciones, el cual se conecta a distintas fuentes de información y repositorios de datos internos. El flujo se prueba de forma manual en algunos casos puntuales y, si los resultados parecen correctos, se configura la ejecución automática en un horario determinado. Una vez configurada la automatización, el playbook queda programado y su funcionamiento se asume como estable, salvo que se presenten incidentes visibles.

Aunque este procedimiento ha permitido reducir la carga manual del SOC, el análisis evidenció que no existe una metodología formal que integre la gestión de riesgos ni contemple actividades obligatorias de respaldo previo, pruebas sistemáticas, validación posterior ni documentación estructurada de los cambios realizados. La dependencia del conocimiento tácito del analista, la falta de formatos de registro y la ausencia de un flujo de aprobación son elementos que se repiten en la mayoría de las automatizaciones revisadas.

3.1.1.2 Falencias operativas detectadas

Durante el diagnóstico se utilizaron la observación directa, la revisión de correos y registros de incidentes, así como entrevistas informales con el analista responsable de las automatizaciones. A partir de estas actividades fue posible identificar varios problemas recurrentes. En primer lugar, se confirmó que antes de desplegar una automatización no se realiza un respaldo sistemático de los scripts, configuraciones o parámetros implicados. Si una automatización modifica un flujo que antes funcionaba correctamente y el resultado es fallido, no siempre es posible restaurar de forma rápida la versión anterior, porque no se cuenta con un respaldo registrado ni con un control de versiones claro.

En segundo lugar, las pruebas de funcionamiento se realizan de manera limitada, generalmente se ejecuta el flujo una o dos veces en condiciones controladas, pero no se siguen criterios formales de validación, ni se documentan los resultados o los criterios de aceptación. Esto incrementa la probabilidad de que errores de integración, problemas de dependencias o comportamientos inesperados solo se identifiquen cuando la automatización ya está en producción y afecta a usuarios reales.

Adicionalmente, se evidenció una falta de trazabilidad en los cambios realizados sobre las automatizaciones, no se cuenta con un registro histórico estructurado que permita conocer qué modificaciones se hicieron, quién las autorizó, qué riesgos se evaluaron o qué pruebas se llevaron a cabo. En algunos casos, la única evidencia son correos o mensajes aislados, lo cual dificulta el análisis post incidente y la mejora continua, de igual forma, la documentación disponible sobre cada automatización es limitada: en ocasiones no se explicita con precisión su propósito, los sistemas involucrados, las condiciones de ejecución ni los posibles impactos.

Estas falencias se sintetizaron en una tabla de diagnóstico interno (no incluida aquí por extensión) donde se cruzaron los procesos analizados con los tipos de debilidades encontradas: ausencia de respaldos, pruebas no estandarizadas, documentación incompleta y falta de evaluación de riesgos.

3.1.1.3 Impactos en la continuidad del servicio

Las debilidades identificadas no se limitan a un plano teórico, sino que han generado impactos concretos en la operación del SOC. Uno de los casos más relevantes fue la automatización diseñada para el envío de notificaciones a través de cuentas corporativas de WhatsApp. Debido a que no se establecieron límites de frecuencia y volumen en los mensajes enviados, la plataforma externa interpretó el comportamiento como potencialmente abusivo o no deseado, lo que derivó en la suspensión temporal de dichas cuentas. Este incidente no solo afectó la comunicación con los clientes, sino que obligó al equipo a gestionar de forma reactiva la recuperación del servicio, sin contar con un plan de contingencia claro.

De manera similar, se han reportado situaciones en las que los reportes generados de manera automatizada contenían información incompleta o errónea. En algunos casos, las consultas a las fuentes de datos no tomaban los intervalos de tiempo correctos; en otros, las integraciones con Grafana o con los dispositivos FGT presentaban fallos que no fueron detectados a tiempo. Estos errores en el contenido de los reportes pueden conducir a interpretaciones equivocadas por parte de los destinatarios y, en consecuencia, a decisiones operativas o estratégicas basadas en información incorrecta.

También se identificaron episodios en los cuales una automatización produjo envíos duplicados de correos con el mismo reporte en un corto periodo de tiempo, generando saturación en las bandejas de entrada e incluso confusión sobre qué versión del reporte debía considerarse válida. Estos incidentes se traducen en reprocesos, consultas adicionales de los clientes y una percepción de poca estabilidad en las automatizaciones.

En conjunto, los hallazgos del diagnóstico muestran que, si bien las automatizaciones han aportado eficiencia, la ausencia de una gestión estructurada de riesgos y respaldos ha incrementado la exposición a incidentes que afectan la continuidad del servicio, la confiabilidad de la información y la carga operativa del analista SOC.

3.1.2 Identificación y clasificación de riesgos

A partir del diagnóstico del proceso actual, se procedió a identificar y evaluar los riesgos asociados a las automatizaciones en el área SOC de FW Ingeniería. El propósito de esta etapa fue clasificar dichos riesgos y establecer una base objetiva para priorizar las acciones de mitigación que serían incorporadas al marco propuesto.

3.1.2.1 Metodología de análisis de riesgos

Para la identificación y análisis de riesgos se siguió un enfoque alineado con la norma ISO/IEC 27005:2018, adaptándolo al contexto particular del SOC. En primer lugar, se elaboró un listado inicial de riesgos potenciales a partir de los incidentes ocurridos, las observaciones realizadas y las entrevistas con el personal. Este listado incluyó riesgos técnicos (fallos de integración, pérdida de datos, errores en scripts) y operativos (envío duplicado de reportes, bloqueo de servicios externos, falta de trazabilidad, entre otros).

Posteriormente, se definieron dos criterios de evaluación: probabilidad e impacto. La probabilidad se valoró en una escala de 1 a 10, donde 1 indica una ocurrencia poco probable y 10 una ocurrencia muy frecuente o casi segura. El impacto también se valoró en una escala de 1 a 10, considerando el efecto del riesgo sobre la continuidad del servicio, la calidad de la información entregada, la relación con los clientes y la carga operativa generada. Con estas dos variables se calculó el nivel de riesgo mediante la fórmula:

Nivel de riesgo (NR) = Probabilidad (P) × Impacto (I)

Finalmente, se establecieron rangos para clasificar el nivel de riesgo de cada ítem: valores entre 1 y 20 se consideraron riesgos bajos, entre 21 y 40 riesgos medios, entre 41 y 70 riesgos altos y entre 71 y 100 riesgos críticos. Esta clasificación sirvió para identificar aquellos riesgos que debían ser atendidos prioritariamente dentro del marco de gestión.

3.2 IDENTIFACIÓN DE LOS RIESGOS TÉCNICOS Y OPERATIVOS PRESENTES EN LAS AUTOMATIZACIONES

Con base en la metodología descrita, se consolidó una matriz de riesgos que resume los riesgos más relevantes identificados en las automatizaciones del SOC de FW Ingeniería. En la tabla 2 se presentan los resultados de esta evaluación.

Tabla 2. Matriz de riesgos en automatizaciones del SOC de FW Ingeniería

N.º	Riesgo identificado	Probabilidad (1–10)	Impacto (1–10)	Nivel de riesgo (P×I)	Clasificación	Tipo de riesgo
1	Pérdida de datos o configuraciones por ausencia de respaldo previo	9	9	81	Crítico	Técnico
2	Bloqueo o suspensión de servicios externos (ej. WhatsApp corporativo)	7	8	56	Alto	Técnico / Operativo
3	Fallos de integración entre sistemas (plataformas)	8	7	56	Alto	Técnico

4	Generación de reportes erróneos o incompletos	7	6	42	Alto	Técnico / Operativo
5	Envío duplicado o masivo de correos automatizados	8	6	48	Alto	Operativo
6	Falta de trazabilidad y documentación de automatizaciones	7	6	42	Alto	Operativo

Fuente: Elaboración propia

La matriz evidencia que el riesgo de pérdida de datos o configuraciones por ausencia de respaldos previos alcanza un nivel de riesgo crítico, mientras que los restantes riesgos se ubican en el rango alto. Esto indica que, sin intervención, las automatizaciones continuarán expuestas a incidentes con potencial de causar afectaciones significativas.

3.2.1 Principales riesgos identificados

Entre los riesgos analizados, el de mayor criticidad corresponde a la pérdida de datos o configuraciones debido a la falta de respaldos. La alta probabilidad asignada se justifica por el hecho de que, en el proceso actual, el respaldo no es una actividad obligatoria ni estandarizada, por lo que cualquier modificación sobre un flujo automatizado se realiza sin contar con una copia confiable del estado anterior. El impacto, a su vez, se considera muy alto porque una falla en la automatización puede dejar inoperante un proceso clave y requerir reconstrucciones manuales que consumen tiempo y recursos.

El bloqueo de servicios externos, como las cuentas de WhatsApp corporativas, se clasifica como un riesgo alto debido a que depende de políticas de terceros proveedores que pueden reaccionar de forma automática ante comportamientos anómalos. La probabilidad es

significativa teniendo en cuenta antecedentes en los que una automatización generó un volumen de mensajes que activó mecanismos de protección de la plataforma externa. El impacto incluye la interrupción de canales de comunicación críticos con los clientes y la necesidad de realizar gestiones adicionales para restaurar el servicio.

Los fallos de integración entre la plataforma SOAR, Grafana, dispositivos FGT, la NAS y OneDrive representan otro riesgo alto. Pequeños cambios en credenciales, rutas de acceso, APIs o estructuras de datos pueden provocar que una automatización aparentemente se ejecute, pero produzca resultados incompletos o vacíos, sin que el error sea detectado inmediatamente. De forma similar, la generación de reportes erróneos o incompletos y el envío duplicado de correos automatizados afectan directamente la percepción de calidad del servicio y pueden generar confusión en los usuarios finales.

Finalmente, la falta de trazabilidad y documentación de las automatizaciones agrava todos los riesgos anteriores, ya que dificulta entender qué se cambió, por qué se cambió y cómo volver a un estado estable. Este riesgo, aunque no se traduce directamente en un incidente técnico, incrementa el tiempo de respuesta ante fallos y limita la capacidad de aprendizaje del equipo.

Estos resultados justifican la necesidad de un marco que incorpore controles específicos para los riesgos identificados, especialmente aquellos clasificados como altos y críticos.

3.3 PROCESO DE INTEGRACIÓN

El Marco de Gestión de Riesgos y Respaldo para la implementación de automatizaciones fue diseñado con base en los principios de la norma ISO/IEC 27005:2018, que establece las directrices para gestionar riesgos de seguridad en entornos tecnológicos (1), y en las buenas prácticas de ITIL 4 y Scrum, que permiten mantener control, trazabilidad y mejora continua en los procesos del área SOC.

El propósito del marco es minimizar los riesgos operativos derivados de automatizaciones incorrectas o no validadas, garantizar la existencia de respaldos confiables y promover un ciclo de mejora continua mediante retroalimentación constante.

3.3.1 Marco de gestión de riesgos para automatizaciones

Una vez identificados y clasificados los riesgos, se procedió a diseñar un marco de gestión de riesgos y respaldo que pudiera integrarse de manera práctica al proceso de automatización del SOC. Este marco se construyó tomando como referencia las buenas prácticas de ITIL, especialmente en lo relacionado con la gestión de cambios y la continuidad del servicio, y el enfoque iterativo de Scrum para estructurar el trabajo en ciclos de mejora continua.

Tabla 3. Marco de gestión de riesgos para automatizaciones

Código del riesgo	Riesgo identificado	Medida de control principal	Tipo de medida de control	Tipo de acción frente al riesgo	Prioridad	Responsable principal	Alcance
R1	Pérdida de datos o configuraciones por ausencia de respaldo previo	Implementar respaldos obligatorios antes de cualquier cambio en automatizaciones (NAS + OneDrive + verificación).	Tecnológica / Administrativa	Mitiga / Evita	Crítica	Analista SOC / Líder SOC	Todas las automatizaciones que modifiquen scripts, configuraciones o flujos en producción.
R2	Bloqueo o suspensión de servicios externos (ej. WhatsApp corporativo)	Definir límites de frecuencia y volumen de envío; uso de ambientes de prueba y listas de destinatarios controladas.	Tecnológica / Administrativa	Mitiga	Alta	Analista SOC	Automatizaciones que interactúan con plataformas externas de mensajería o notificación.
R3	Fallos de integración entre sistemas (plataformas)	Validar credenciales, rutas, APIs y conexiones en entorno de pruebas; monitoreo de logs y alertas ante errores.	Tecnológica	Mitiga	Alta	Analista SOC	Integraciones entre SOAR, Grafana, FGT, NAS, OneDrive y otras plataformas relacionadas.
R4	Generación de reportes erróneos o incompletos	Definir criterios de aceptación; revisión de consultas y filtros de tiempo; validación de reportes por un segundo revisor.	Administrativa / Tecnológica	Mitiga	Alta	Analista SOC / Líder SOC	Automatizaciones de generación y envío de reportes operativos o de monitoreo.
R5	Envío duplicado o masivo de correos automatizados	Configuración correcta de tareas programadas; pruebas con destinatarios de prueba; monitoreo inicial tras despliegue.	Tecnológica	Mitiga	Alta	Analista SOC	Automatizaciones que utilizan correo electrónico como canal de notificación.
R6	Falta de trazabilidad y documentación de automatizaciones	Implementar registro centralizado de automatizaciones, control de versiones y formatos de documentación obligatoria.	Administrativa	Mitiga / Evita	Alta	Líder SOC	Todas las automatizaciones creadas o modificadas en el SOC.

Fuente: Elaboración propia

3.3.1.1 Estructura del marco propuesto

El marco de gestión de riesgos y respaldo se estructura en fases que acompañan el ciclo de vida de cada automatización. En la fase inicial se define el propósito de la

automatización, su alcance, los sistemas involucrados y los resultados esperados. A continuación, se realiza una identificación de riesgos, en la cual se listan los posibles eventos que pueden afectar negativamente el funcionamiento de la automatización o la calidad de los resultados.

Una vez identificados los riesgos, se procede a su análisis utilizando la matriz presentada en la sección anterior. Los riesgos con clasificación alta o crítica deben estar asociados a acciones de mitigación concretas, que serán integradas obligatoriamente en el diseño de la automatización. Posteriormente, se desarrolla el flujo automatizado en la plataforma SOAR, pero su despliegue no se realiza de manera inmediata, sino que está condicionado a la ejecución de respaldos previos y pruebas controladas.

El marco también incluye una fase de monitoreo y validación posterior a la puesta en producción. En esta fase se revisan los primeros resultados de la automatización, se verifica que los reportes generados sean correctos y se confirma que no se estén generando incidentes derivados del cambio. Finalmente, se reserva un espacio para la documentación de lo realizado y para la reflexión sobre oportunidades de mejora, lo cual se articula con las retrospectivas propias de Scrum.

Aunque el marco puede representarse gráficamente mediante un diagrama de flujo, en el documento se sugiere incluirlo como una figura donde se muestren de forma secuencial las fases: definición, análisis de riesgos, respaldo, pruebas, despliegue, monitoreo y mejora continua. Esta figura ayuda a visualizar que el marco no es un conjunto aislado de actividades, sino un proceso cíclico e integrado.

3.3.1.2 Procedimiento de respaldo y validación

Uno de los componentes centrales del marco es el procedimiento de respaldo y validación previo al despliegue de automatizaciones. En este procedimiento se establece como requisito indispensable realizar un respaldo completo de los elementos implicados en la automatización. Dicho respaldo incluye los scripts o flujos configurados en la plataforma, las configuraciones específicas (parámetros, rutas, filtros de tiempo) y, cuando aplique, las plantillas de reportes generadas.

Estos respaldos se almacenan en dos espacios complementarios: la NAS corporativa, que actúa como repositorio interno centralizado, y el OneDrive empresarial, que mantiene una copia sincronizada en la nube. La combinación de ambos medios permite disponer de al menos dos ubicaciones para cada respaldo, reduciendo el riesgo de pérdida de información por fallos puntuales en uno de los repositorios.

Para asegurar que los respaldos no han sido alterados o corrompidos, se definió el uso de sumas de verificación (checksums) mediante el algoritmo SHA-256. Durante la creación del respaldo se calcula el checksum del archivo, se registra el valor en un formato de control y se asocia con la fecha, el nombre de la automatización y el responsable. En caso de que sea necesario restaurar un respaldo, se vuelve a calcular el checksum y se compara con el valor registrado originalmente. Si coinciden, se tiene la certeza de que el archivo no ha sufrido modificaciones.

Además de los respaldos, el procedimiento exige la realización de pruebas controladas. Estas pruebas consisten en ejecutar la automatización en un entorno de alcance reducido, ya sea con un subconjunto de datos o con destinatarios de prueba, verificando el contenido de los reportes, las frecuencias de envío y el comportamiento frente a posibles errores de integración. Solo después de superar estas pruebas y de documentar los resultados se autoriza el despliegue en producción.

3.3.1.3 Integración ITIL–Scrum

El diseño del marco se apoyó en la convergencia de ITIL y Scrum. Desde la perspectiva de ITIL, se adoptan principios de la gestión de cambios, la gestión de incidentes y la continuidad del servicio. Cada automatización o modificación significativa debe ser tratada como un cambio que requiere evaluación previa, aprobación y planificación de reversión. El marco incorpora esta lógica al exigir respaldos, documentos de registro y revisiones formales antes de la puesta en producción.

Por su parte, Scrum aporta la organización del trabajo en sprints y la realización de ceremonias que facilitan la comunicación y la mejora continua. La planificación de sprints permite definir qué automatizaciones serán intervenidas o creadas en un periodo determinado, qué tareas están asociadas al análisis de riesgos y respaldos y quién será

responsable de cada actividad. La reunión de revisión al final del sprint ofrece un espacio para evaluar el comportamiento de las automatizaciones en producción, mientras que la retrospectiva permite identificar lecciones aprendidas y ajustar el marco según la experiencia.

De esta forma, la integración ITIL–Scrum no se limita a una combinación teórica, sino que se traduce en un conjunto de prácticas concretas que ordenan el trabajo del equipo SOC y fortalecen la confiabilidad de las automatizaciones.

3.3.2 Fases del marco propuesto

Tabla 4. Etapas metodológicas del proyecto

Fase	Nombre de la fase	Descripción resumida	Actividades clave	Resultado esperado
1	Identificación y análisis de riesgos	Se analiza la necesidad de la automatización y se evalúan los riesgos asociados, considerando su probabilidad e impacto sobre los servicios, la información y los recursos del SOC.	• Identificación de la automatización y su objetivo. • Evaluación de riesgos con matriz cuantitativa (P × I) .• Asignación del nivel de criticidad (bajo, medio, alto, crítico).	Registro de riesgos documentado, con nivel de criticidad definido.
2	Respaldo inicial	Antes de ejecutar la automatización, se realiza un respaldo completo de archivos, configuraciones y elementos críticos, almacenándolos en el repositorio	• Identificación de scripts y configuraciones a respaldar. • Generación de copia en almacenamiento cloud/NAS • Registro del respaldo en formato de control	Respaldo validado y disponible para reversión ante fallos.

		definido (cloud/NAS) y dejando evidencia formal.	(fecha, responsable, ubicación).	
3	Pruebas en entorno controlado	La automatización se ejecuta en un entorno controlado o con datos simulados, observando comportamiento, logs y errores. Se trabaja en iteraciones tipo sprint Scrum para ajustar y mejorar antes del despliegue en producción.	• Ejecución de pruebas en entorno aislado. • Revisión de logs y resultados. •Ajustes iterativos mediante reuniones cortas de seguimiento .•Definición y verificación de criterios de aceptación.	Automatización ajustada y validada funcionalmente antes de su paso a producción.
4	Despliegue en entorno productivo	La automatización se ejecuta en el ambiente productivo bajo supervisión. Se monitorean los registros en tiempo real y, en caso de fallos, se activa el plan de reversión utilizando los respaldos realizados en la fase anterior.	• Ejecución de la automatización en producción. • Monitoreo en tiempo real de logs y comportamiento. • Activación del plan de reversión en caso de incidentes. • Registro de incidencias presentadas durante el despliegue.	Automatización desplegada en producción con capacidad de reversión ante incidentes.

5	Ejecución completa y validación final	Tras un período de monitoreo sin incidencias relevantes y el cumplimiento de todos los criterios de aceptación, se considera que la automatización ha sido implementada con éxito y se documenta su estado final.	• Verificación del funcionamiento estable durante el período definido. • Confirmación del cumplimiento de criterios de aceptación. • Actualización del inventario de automatizaciones .• Registro del estado final en el formato.	Automatización aprobada y documentada como versión vigente en el entorno productivo.
6	Evaluación y mejora continua	Se realiza una retrospectiva con el equipo SOC para analizar los resultados, incidentes, oportunidades de mejora y lecciones aprendidas, ajustando el marco y los procedimientos según sea necesario.	• Revisión de resultados e indicadores. • Análisis de incidentes y causas raíz. • Identificación de mejoras al proceso y al marco. • Actualización de procedimientos y formatos.	Marco y procedimientos ajustados, alimentando un ciclo de mejora continua en el SOC.

Fuente: Elaboración propia

3.3.3 PROCEDIMIENTO TÉCNICO DE RESPALDO

El componente de respaldo constituye el eje del marco, al ser el principal control de mitigación de riesgo ante fallos en las automatizaciones. El procedimiento se define así:

Identificación de elementos a respaldar:

Archivos de configuración, scripts y módulos involucrados.

Logs del sistema y parámetros previos a la ejecución.

Reportes históricos y bases temporales de datos.

Ejecución del respaldo:

Se realiza una copia local en el servidor donde se ejecutará la automatización.

Luego se envía automáticamente una copia al repositorio.

Finalmente, se sincroniza donde se encuentran todas las copias de seguridad.

Validación de integridad:

El analista verifica que el tamaño y fecha de modificación coincidan con la fuente.

Registro del respaldo:

En un formato estandarizado, el analista deja evidencia de la fecha, tipo de automatización y responsable del respaldo.

3.4 IMPLEMENTACIÓN PILOTO Y EVALUACIÓN DEL MARCO DE GESTIÓN DE RIESGO PARA AUTOMATIZACIONES

La implementación del Marco de Gestión de Riesgos y Respaldo se llevó a cabo en el área del SOC de la empresa FW Ingeniería, con el fin de validar su efectividad en entornos reales de automatización. Este proceso se ejecutó durante el 1 de octubre y el 24 de octubre del 2025 y se desarrolló siguiendo los principios de la metodología Scrum, que permitió organizar las actividades en sprints cortos y medibles, garantizando iteraciones de mejora continua.

El piloto se aplicó sobre una automatización existente relacionada con la generación y envío automático de reportes de monitoreo, integrados a través de la plataforma de orquestación. Antes de la implementación del marco, esta automatización presentaba incidentes frecuentes, como el envío duplicado de reportes, errores en los datos extraídos de las fuentes, y falta de respaldo previo a las modificaciones, lo que generaba pérdida de información en caso de fallas.

3.4.1 Planeación del sprint

Durante la fase de planeación, el equipo del SOC definió el alcance y los objetivos del sprint piloto, estableciendo un conjunto de tareas concretas que debían completarse en un plazo de 6 días hábiles, el propósito principal era aplicar el marco de gestión propuesto en una

automatización, documentar los resultados obtenidos y analizar los beneficios frente al proceso anterior.

Las tareas planificadas incluyeron:

Identificar los riesgos técnicos y operativos asociados a la automatización del reporte como pérdida de datos y fallos en la ejecución.

Realizar respaldos previos de los scripts, configuraciones y bases de datos involucradas, utilizando el almacenamiento local corporativa como almacenamiento principal y el almacenamiento cloud empresarial como respaldo sincronizado.

Ejecutar la automatización en un entorno de validación controlado, registrando los resultados y eventos del sistema.

Documentar los hallazgos y presentar los resultados al final del sprint para su revisión.

Durante la planeación se asignaron los roles dentro del marco:

Analista SOC ejecutor el cual es el encargado de validar riesgos, comprobar la creación del respaldo y ejecución de la automatización.

Líder SOC supervisor del cumplimiento del marco, encargado de consolidar la documentación y verificar los resultados finales.

3.4.2 EJECUCIÓN CONTROLADA

Durante esta fase se aplicó el marco paso a paso según lo planificado, inicialmente, el analista ejecutor realizó los respaldos de las configuraciones de la plataforma, los scripts, los respaldos fueron almacenados en almacenamiento local y en el almacenamiento cloud.

Los valores de los checksums coincidieron, validando la integridad de los respaldos antes de continuar con la automatización.

Posteriormente, se ejecutó la automatización en un entorno de pruebas independiente, configurado con las mismas características que el entorno productivo, pero sin conexión directa a clientes o servicios externos.

Durante las pruebas iniciales se identificaron los siguientes hallazgos:

Error en la secuencia de consulta SQL: algunos campos no se estaban actualizando correctamente, generando reportes con información incompleta.

Duplicidad de tareas programadas ya que el flujo de envío automático se ejecutaba dos veces cada 4 horas debido a un error en la configuración del cron interno.

Después de aplicar correcciones, se ejecutó nuevamente el flujo, obteniendo un funcionamiento estable sin duplicaciones ni pérdida de datos, los resultados fueron revisados y validados por el líder, quien autorizó el despliegue en el entorno productivo.

3.4.3 Despliegue en entorno productivo

El despliegue final se realizó el 24 de octubre de 2025, bajo supervisión directa del líder SOC, se monitoreó la automatización durante un periodo de una semana, verificando su desempeño y el correcto envío de reportes. Durante esta fase, el marco demostró su efectividad en la prevención de incidentes y en la recuperación ante errores menores gracias a la existencia de respaldos verificados.

Los resultados obtenidos fueron los siguientes:

Estos resultados se relacionan directamente con los beneficios planteados en la justificación del proyecto, ya que demuestran que el marco propuesto contribuye a mejorar la confiabilidad de las automatizaciones, reducir la ocurrencia de incidentes operativos y fortalecer la trazabilidad de los procesos en el área SOC. La disminución de errores y fallos sin respaldo confirma que la implementación de procedimientos formales de gestión de riesgos, respaldos previos y validación controlada genera un impacto real en la continuidad del servicio y en la calidad de la información entregada a los clientes. De esta manera, se

evidencia que el proyecto no solo responde a una necesidad identificada en FW Ingeniería, sino que además aporta una solución concreta y medible, alineada con los objetivos de estabilidad operativa y mejora continua definidos por la organización.

Tabla 5. Comparación de indicadores antes y después de la implementación del marco

Indicador	**Antes del marco**	**Después del marco**	**Variación (%)**
Reportes duplicados	23 por semana	4 por semana	-83%
Errores de extracción de datos	12 por semana	1 por semana	-92%
Automatizaciones fallidas sin respaldo	100%	0%	-100%

Fuente: Elaboración propia

En conclusión, la aplicación del marco permitió pasar de un esquema reactivo, sin respaldos formales ni criterios claros de validación, a un proceso estructurado que integra gestión de riesgos, respaldo previo, pruebas en entorno controlado y monitoreo posterior. Esto se refleja en mejoras cuantificables en la operación diaria del SOC y respalda el cumplimiento del objetivo general del proyecto.

3.4.4 Retrospectiva del sprint

En la reunión el equipo SOC analizó el rendimiento del marco y los aprendizajes obtenidos durante la implementación piloto, se destacó la importancia de los respaldos verificados como elemento clave de recuperación.

Asimismo, se acordó, incorporar un registro centralizado de automatizaciones, donde cada proceso incluya su historial de ejecución, respaldos y responsables, establecer un control de versiones de los scripts, para mantener trazabilidad de los cambios realizados,

programar sprints trimestrales de revisión del marco para actualizar la matriz de riesgos y los procedimientos de respaldo.

Estas mejoras permitirán mantener la vigencia y eficacia del marco en el tiempo, alineando el proceso con la mejora continúa promovida por ITIL y Scrum.

4 CUMPLIMIENTO DE OBJETIVOS

El desarrollo del proyecto permitió alcanzar de manera progresiva los objetivos específicos planteados y, con ello, el cumplimiento del objetivo general.

En relación con el primer objetivo específico, consistente en analizar el proceso actual de automatización de FW Ingeniería con el fin de establecer las bases para el diseño de un marco de mejora en las automatizaciones del área SOC, este se cumplió a través del diagnóstico descrito en el capítulo 8. Allí se documentó el funcionamiento del área SOC, el flujo actual de generación de reportes automatizados y las principales falencias operativas, tales como la ausencia de respaldos formales, la falta de pruebas controladas y la carencia de trazabilidad en los cambios realizados. Este análisis permitió comprender el contexto real de operación y definir claramente el problema a intervenir, proporcionando los insumos necesarios para estructurar el marco propuesto.

El segundo objetivo específico, orientado a identificar los riesgos técnicos y operativos presentes en las automatizaciones realizadas por el área SOC, se alcanzó mediante la aplicación de un enfoque de gestión de riesgos basado en la norma ISO/IEC 27005:2018. A partir de los incidentes observados, la revisión de registros y las entrevistas realizadas, se elaboró una matriz de riesgos en la que se evaluaron probabilidad e impacto, clasificando los riesgos como bajos, medios, altos o críticos. Entre los riesgos más relevantes se identificaron la pérdida de datos por ausencia de respaldos, el bloqueo de servicios externos, los fallos de integración entre plataformas y la falta de trazabilidad de los cambios. Estos resultados permitieron priorizar las acciones de control que debían ser integradas en el marco de gestión.

El tercer objetivo específico, relacionado con implementar el marco propuesto bajo un enfoque ágil basado en la metodología Scrum, utilizando iteraciones de prueba y revisión, se cumplió a través del diseño, aplicación piloto y evaluación del marco de gestión de riesgos y respaldo. El marco fue estructurado en fases (identificación y análisis de riesgos, respaldo inicial, pruebas en entorno controlado, despliegue en producción, validación final y mejora continua) e integrado con prácticas de ITIL para la gestión del cambio y la

continuidad del servicio. Posteriormente, se ejecutó un sprint piloto sobre una automatización real de reportes, aplicando respaldos verificados, pruebas controladas y monitoreo posterior. Los indicadores obtenidos (reducción de reportes duplicados, disminución de errores de datos y eliminación de automatizaciones sin respaldo) evidenciaron la efectividad del marco y permitieron su ajuste mediante una retrospectiva del equipo SOC.

En conjunto, el cumplimiento de los tres objetivos específicos condujo al logro del objetivo general del proyecto: implementar un marco de gestión de riesgos y respaldo para las automatizaciones en el área SOC de FW Ingeniería, basado en las metodologías ITIL y la norma ISO/IEC 27005:2018, que mejora la confiabilidad, trazabilidad y seguridad de los procesos automatizados. El marco diseñado y validado no solo responde a la problemática inicial identificada, sino que se constituye en una herramienta práctica que puede ser extendida a futuras automatizaciones dentro del área SOC.

5 CONCLUSIONES

1. La propuesta y aplicación de un marco de gestión de riesgos y respaldo para las automatizaciones del área SOC de FW Ingeniería permitió transformar un proceso inicialmente basado en prácticas informales en un esquema ordenado, documentado y controlado. El marco integró de manera coherente lineamientos de ITIL, ISO/IEC 27005:2018 y Scrum, logrando que las automatizaciones se gestionen ahora como activos críticos del servicio y no solo como tareas técnicas aisladas.

2. El análisis detallado del proceso actual de automatización evidenció que la principal debilidad no era únicamente técnica, sino de gestión: la ausencia de políticas claras de respaldo, la limitada trazabilidad de cambios y la falta de criterios formales de validación incrementaban la exposición a incidentes operativos. Este diagnóstico permitió delimitar con precisión las causas raíz de los problemas y orientar el diseño del marco hacia la mejora de la confiabilidad y la continuidad del servicio.

3. La identificación y clasificación de riesgos, apoyada en la metodología de la norma ISO/IEC 27005:2018, hizo visible el impacto que pueden generar las automatizaciones mal gestionadas sobre la operación del SOC y sobre los servicios prestados a los clientes. La priorización de riesgos críticos, como la pérdida de datos y la suspensión de servicios externos, permitió enfocar los controles del marco en aquellos puntos donde el efecto potencial sobre el negocio era más alto.

4. La estructuración del marco en fases —que incluyen identificación de riesgos, respaldo previo, pruebas controladas, despliegue supervisado, monitoreo y mejora continua— demostró que es posible integrar prácticas de gestión de cambios de ITIL con el trabajo iterativo de Scrum sin generar sobrecarga operativa. Por el contrario, el uso de sprints, revisiones y retrospectivas favoreció la comunicación dentro del equipo SOC y facilitó la incorporación progresiva del marco en la rutina de trabajo.
5. La implementación piloto sobre una automatización real evidenció una mejora notable en el comportamiento del proceso automatizado, reflejada en la disminución de incidentes, en la disponibilidad de respaldos verificables y en la capacidad de

recuperación ante fallos. Más allá de los valores numéricos de los indicadores, el principal aporte del marco es haber dejado una base metodológica que puede ser replicada, ajustada y ampliada a futuras automatizaciones, contribuyendo a una cultura de gestión de riesgos, documentación y mejora continua en FW Ingeniería.

6 RECOMENDACIONES

Las principales recomendaciones derivadas de este trabajo apuntan a formalizar el Marco de Gestión de Riesgos y Respaldo como procedimiento obligatorio para toda automatización del área SOC, asegurando su documentación, socialización y aplicación consistente. Asimismo, se sugiere mantener un inventario centralizado de automatizaciones con sus responsables, respaldos y riesgos asociados, capacitar periódicamente al personal del SOC en gestión de riesgos y respaldos, y revisar de manera periódica la matriz de riesgos para ajustarla según nuevos incidentes, cambios tecnológicos y lecciones aprendidas.

En cuanto al trabajo futuro, se propone extender gradualmente la aplicación del marco a otros procesos y áreas de FW Ingeniería que empleen automatizaciones, de manera que el modelo se convierta en un estándar organizacional. Además, se recomienda evaluar el desarrollo de un panel o dashboard que consolide información sobre automatizaciones, respaldos, indicadores de desempeño y riesgos, así como ampliar el análisis hacia otros tipos de riesgos, incluyendo aspectos legales, contractuales y de reputación asociados a fallos en automatizaciones críticas.

7 REFERENCIAS

1. AXELOS. ITIL® Foundation: ITIL 4 Edition. United Kingdom: The Stationery Office; 2019.
2. Schwaber, K., Sutherland, J. The Scrum Guide: The Definitive Guide to Scrum, The Rules of the Game. 2020.
3. Rincon Dallos, A. P., Córdoba Chivata, L. E., & Campo Londoño, M. A. (2019). Implementación de metodología ágil Scrum y marco de referencia ITIL V 3.0 como plan de mejora dirigido al proceso de desarrollo de software en la empresa Hitss Colombia SAS en la ciudad de Bogotá (Tesis de grado). Universidad Cooperativa de Colombia, Bogotá.
4. Zea Jiménez, J. M. (2021). Análisis correlacional de la gestión de riesgos según marcos de trabajo ágiles (Scrum) y marcos de trabajo predictivo (PMBOK) (Trabajo de grado). Universidad Militar Nueva Granada, Bogotá.
5. Reijers, H. A., & Mansar, S. L. Best practices in business process redesign: an overview and qualitative evaluation of successful redesign heuristics. Omega, 2005; 33(4):283–306.
6. Gartner. Top Strategic Technology Trends 2021: Hyperautomation. Stamford, Connecticut: Gartner Inc.; 2021.
7. Hammer, M., & Champy, J. Reengineering the Corporation: A Manifesto for Business Revolution. New York: Harper Business; 1993.
8. Stoneburner, G., Goguen, A., & Feringa, A. Risk Management Guide for Information Technology Systems (NIST SP 800-30). Gaithersburg, MD: National Institute of Standards and Technology; 2002.
9. International Organization for Standardization. ISO 31000:2018 Risk Management — Guidelines. Geneva: ISO; 2018.
10. Cárdenas, L., & Bernal, J. Gestión del riesgo en tecnologías de información y comunicación: fundamentos y aplicación práctica. Bogotá: Universidad Distrital Francisco José de Caldas; 2019.
11. Laudon, K., & Laudon, J. Sistemas de información gerencial. 16ª ed. México: Pearson Educación; 2021.

12. International Organization for Standardization. ISO/IEC 27031:2011 — Guidelines for information and communication technology readiness for business continuity. Geneva: ISO; 2011.
13. Stallings, W. Operating Systems: Internals and Design Principles. 9ª ed. Boston: Pearson; 2018.
14. Galup, S., Dattero, R., Quan, J., & Conger, S. An overview of IT service management. Communications of the ACM. 2009; 52(5):124–127.
15. Office of Government Commerce. ITIL Service Lifecycle Publication Suite. London: The Stationery Office; 2011.
16. Pressman, R. Ingeniería del software: un enfoque práctico. 8ª ed. México: McGraw-Hill; 2015.
17. Highsmith, J. Agile Project Management: Creating Innovative Products. 2ª ed. Boston: Addison-Wesley; 2010.
18. Rising, L., & Janoff, N. The Scrum Software Development Process for Small Teams. IEEE Software. 2000; 17(4):26–32.
19. Schwaber, K., & Sutherland, J. The Scrum Guide: The Definitive Guide to Scrum, The Rules of the Game. 2020.
20. International Organization for Standardization. *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.* Geneva: ISO; 2018.}
21. Stoneburner, G., Goguen, A., & Feringa, A. *Risk Management Guide for Information Technology Systems (NIST SP 800-30).* Gaithersburg, MD: National Institute of Standards and Technology; 2002. International Organization for Standardization. *ISO 31000:2018 Risk Management — Guidelines.* Geneva: ISO; 2018.
22. GARZÓN QUITO, Ernesto Mauricio; AYALA SALGUERO, César Xavier. Propuesta de un modelo de gestión de riesgos para proyectos de desarrollo de software bajo una metodología ágil [trabajo de maestría]. Cuenca: Universidad Politécnica Salesiana, 2021.
23. Propuesta desde la gestión de proyectos para la implementación de la metodología ágil SCRUM para el desarrollo web [trabajo de grado]. Bogotá: Corporación Universitaria Minuto de Dios – UNIMINUTO, 2020.

24. LAGARES ARRAZOLA, Juan David; SARABIA CERVANTES, Josue David; ARIAS BORJA, Andy. *Software para la Gestión de Proyectos ágiles de TI tipo SCRUM* [trabajo de grado]. Barranquilla: Universidad del Norte, 2020.
25. ULLOA-ULLOA, Daniel; BAQUERO-VALLADARES, María Gracia. Metodologías ágiles: Scrum para la innovación en los procesos crediticios. *593 Digital Publisher CEIT*. 2025, vol. 10, n.° 3, p. 1612-1627. DOI: 10.33386/593dp.2025.3.3289.
26. VANEGAS DEVIA, Gonzalo Andrés; PARDO, César Jesús. Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. *Revista Sistemas & Telemática*. 2014, vol. 12, n.° 30, p. 35-48.
27. INVGATE. ITIL 4 y la Gestión de Riesgos: ¿Cómo se relacionan? [en línea]. 2023. Disponible en: InvGate Blog. Consulta: día mes año.
28. *Análisis correlacional de la gestión de riesgos según marcos de trabajo ágiles (Scrum) y marcos de trabajo predictivo (PMBOK)* [trabajo de grado]. Bogotá: Universidad Militar Nueva Granada, 2020.
29. PRICEWATERHOUSECOOPERS (PwC) COLOMBIA. *Digital Trust Insights 2025* [en línea]. Bogotá: PwC Colombia, 2025.
30. VLADGRIN. Metodología ágil para el diagrama de ciclo de vida de desarrollo de software [ilustración en línea]. s. l.: iStockphoto, 2021. Disponible en: https://www.istockphoto.com/es/vector/metodolog%C3%ADa-%C3%A1gil-para-el-diagrama-de-ciclo-de-vida-de-desarrollo-de-software-gm1336228211-417563528
31. HERNÁNDEZ, Roberto; FERNÁNDEZ, Carlos; BAPTISTA, Pilar. *Metodología de la investigación*. 6. ed. México D. F.: McGraw-Hill, 2014. 600 p.