Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), Noviembre-Diciembre 2025,
Volumen 9, Número 6.

https://doi.org/10.37811/cl_rcm.v9i6

GESTIÓN DEL RIESGO TECNOLÓGICO EN LA MODERNIZACIÓN DE SISTEMAS LEGACY: ESTRATEGIAS PARA UNA TRANSICIÓN EFICIENTE

TECHNOLOGY RISK MANAGEMENT IN LEGACY SYSTEM MODERNIZATION: STRATEGIES FOR AN EFFICIENT TRANSITION

Samuel Elías Díaz Alvarado
Universidad Mariano Gálvez, Guatemala

DOI: https://doi.org/10.37811/cl_rcm.v9i6.21454

Gestión del Riesgo Tecnológico en la Modernización de Sistemas Legacy: Estrategias Para una Transición Eficiente

Samuel Elías Díaz Alvarado[1]
samm.diaz.alvarado@gmail.com
https://orcid.org/0009-0005-1462-2497
Universidad Mariano Gálvez
Guatemala

RESUMEN

La modernización de sistemas legacy representa un desafío significativo para las organizaciones, especialmente en términos de gestión de riesgos tecnológicos. La transición hacia nuevas arquitecturas y tecnologías expone a las organizaciones a diversos riesgos, que incluyen problemas de interoperabilidad, continuidad operativa y seguridad de la información. A pesar de la existencia de modelos tradicionales de gestión de riesgos, muchos de ellos no logran adaptarse a la naturaleza dinámica y compleja de los entornos híbridos en la transformación digital. En respuesta a estas limitaciones, se ha propuesto un modelo flexible y modular, diseñado para gestionar de manera efectiva los riesgos en procesos de modernización tecnológica, este modelo integra metodologías ágiles y arquitecturas resilientes, con un enfoque cíclico que permite una evaluación continua del riesgo y su adaptación a cambios imprevistos. Un aspecto fundamental de este enfoque es la inclusión de un proceso de evaluación contextual, que permite la validación y ajuste dinámico de las decisiones estratégicas a medida que la organización avanza en su transición; su diseño conceptual permite facilitar una transición eficiente y segura hacia nuevas infraestructuras tecnológicas. Este enfoque busca alinearse con los objetivos organizacionales y garantizar una gestión de riesgos que evoluciona junto con el entorno

Palabras clave: sistemas heredados, devops, resiliencia computacional, cumplimiento

[1] Autor principal
Correspondencia: samm.diaz.alvarado@gmail.com

Technology Risk Management in Legacy System Modernization: Strategies for an Efficient Transition

ABSTRACT

The modernization of legacy systems represents a significant challenge for organizations, especially in terms of managing technological risks. The transition to new architectures and technologies exposes organizations to various risks, including issues of interoperability, operational continuity, and information security. Despite the existence of traditional risk management models, many of them fail to adapt to the dynamic and complex nature of hybrid environments in the digital transformation. In response to these limitations, a flexible and modular model has been proposed, designed to effectively manage risks in technology modernization processes. This model integrates agile methodologies and resilient architectures, with a cyclical approach that allows for continuous risk evaluation and adaptation to unforeseen changes. A fundamental aspect of this approach is the inclusion of a contextual assessment process, which enables the dynamic validation and adjustment of strategic decisions as the organization progresses in its transition. Its conceptual design facilitates an efficient and secure transition toward new technological infrastructures. This approach seeks to align with organizational objectives and ensure a risk management process that evolves along with the environment

Keywords: legacy, devops, computational resilience, compliance

INTRODUCCIÓN

La modernización de sistemas legacy se ha convertido en una necesidad estratégica para las organizaciones que buscan responder a entornos tecnológicos cada vez más cambiantes. Aunque estos sistemas han sostenido durante años la operación institucional por su estabilidad y fiabilidad, hoy enfrentan limitaciones importantes en escalabilidad, interoperabilidad y capacidad de adaptación. Esta brecha genera un problema relevante, ya que la transición hacia plataformas modernas implica riesgos que pueden afectar la continuidad operativa, la seguridad de la información y el cumplimiento normativo. En este escenario, comprender el fenómeno desde una perspectiva amplia permite dimensionar tanto la complejidad técnica del proceso como la necesidad de contar con esquemas de gestión del riesgo que se ajusten a estas transformaciones.

Los marcos tradicionales como COBIT, ISO 31000, NIST o ITIL ofrecen lineamientos consolidados, pero suelen mostrar rigidez cuando se aplican a entornos híbridos donde conviven sistemas heredados y tecnologías emergentes. Sus dificultades para integrarse con metodologías ágiles o reevaluar amenazas en tiempo real han dejado vacíos evidentes en prácticas de transformación digital. Estas limitaciones resaltan la importancia de plantear alternativas más flexibles, capaces de responder a escenarios donde el cambio tecnológico y las necesidades del negocio avanzan con rapidez.

Los riesgos asociados a este proceso no se limitan a lo técnico; también incluyen impactos operativos, financieros y reputacionales. Interrupciones de servicio, fallas de interoperabilidad o incumplimientos regulatorios pueden afectar directamente la estabilidad institucional. Ante ello, se vuelve necesario un enfoque que permita anticipar y mitigar riesgos sin frenar el avance tecnológico. En respuesta a esta necesidad surge el modelo de Gestión Avanzada de Riesgos Tecnológicos (GARTEC), diseñado con una estructura modular y cíclica que integra cinco macroprocesos y un enfoque AAA (Ágil, Adaptativo y Avanzado) para ajustar continuamente la evaluación de riesgos según el contexto.

La propuesta se basa en una revisión crítica de los marcos tradicionales y en la identificación de fallos frecuentes en procesos reales de transformación digital, especialmente en la integración ágil, la evaluación contextual y la alineación con la gobernanza tecnológica. Aunque el modelo aún no ha sido validado empíricamente, su diseño apunta a facilitar una implementación progresiva en organizaciones con distintos niveles de madurez, promoviendo transiciones más seguras y sostenibles.

Este artículo se desarrolla en el marco de los procesos contemporáneos de modernización tecnológica y tiene como propósito presentar el modelo GARTEC como una alternativa innovadora para gestionar riesgos tecnológicos en la transición de sistemas legacy hacia arquitecturas más modernas. Su aporte radica en ofrecer un enfoque más dinámico y contextualizado para apoyar decisiones críticas durante la transformación digital.

METODOLOGÍA

El estudio se desarrolló con un enfoque cualitativo, basado exclusivamente en fuentes secundarias, utilizando artículos científicos, tesis, informes técnicos y otras publicaciones académicas relacionadas con la gestión del riesgo tecnológico y la modernización de sistemas legacy. No se emplearon encuestas ni experimentos, lo que permitió centrarse en el análisis conceptual y comparativo de modelos documentados.

El proceso metodológico consistió en identificar y depurar diversos modelos de gestión de riesgo tecnológico hasta seleccionar un conjunto final de cuatro, que fueron analizados para reconocer sus enfoques y determinar los elementos más útiles para la propuesta del modelo propio. Para ello se realizó una búsqueda sistemática en bases de datos académicas y repositorios abiertos, utilizando palabras clave definidas en el estudio y combinando búsquedas directas con búsquedas relacionales. Se aplicaron criterios de inclusión que exigieron textos completos, un tratamiento central del riesgo tecnológico y una fecha de publicación igual o posterior a 2020, lo que permitió integrar información reciente y coherente con las tendencias de los últimos años.

RESULTADOS Y DISCUSIÓN

Desafíos Técnicos y Operativos en Entornos Legacy

Los desafíos técnicos en un entorno de sistemas heredados (legacy) son complejos de determinar, por la costumbre que los propios técnicos tienen a ellos; es una tarea compleja ver fuera de la caja para detectarlos y es aún más complejo administrativamente coordinar los cambios que se requieren. El nivel de adopción de tecnologías que integre la entidad determinará realmente la complejidad que puede llegar a generar un cambio de entorno y así poder superar realmente esas deudas técnicas para contar con un ambiente tecnológico sostenible en la organización.

La modernización de software es una actividad fundamental en la actualidad, por la variedad de requerimientos que surgen y el dinamismo que requieren los nuevos requerimientos de usuarios. Los avances tecnológicos con los nuevos modelos de negocio también generan esta necesidad y cada vez es más evidente el problema que pueden generar mantener sistemas legacy en las organizaciones (Assunção et al., 2024).

Cuando se habla de la implementación de nuevas tecnologías no es suficiente con la utilización de una variedad de tecnologías digitales adecuadas, es necesario integrarlas en los empleados, los procesos operativos y rutinas de la organización para lograr una ventaja competitiva real en un mercado tan dinámico como en la actualidad (González Varona, 2021).

Riesgos de Continuidad Operativa y Soporte Técnico

La modernización de sistemas legacy conlleva riesgos inherentes que pueden traducirse en periodos de inactividad no planificados, potenciales pérdidas de información y alteraciones en los procesos operativos. Estos eventos adversos, de materializarse, amenazan la continuidad de las operaciones y pueden erosionar la confianza de los clientes. Con el fin de contener y atenuar dichas contingencias, resulta esencial implementar una estrategia basada en ciclos iterativos e incrementales, de modo que cada fase de la transformación se someta a validaciones y ajustes antes de avanzar a la siguiente.

La ejecución de proyectos piloto en entornos controlados permite identificar y corregir desvíos sin exponer el ambiente productivo a riesgos significativos. La elaboración de planes de contingencia detallados, que incluyan procedimientos de respaldo y recuperación de datos, asegura una respuesta ágil ante eventualidades. Paralelamente, la instalación de sistemas de monitoreo continuo, capaces de alertar de forma temprana sobre anomalías en el rendimiento o en la integridad de la información, contribuye a minimizar el impacto de interrupciones imprevistas. Este conjunto de prácticas, articulado de manera coherente, favorece una modernización ordenada y con menor exposición a impactos negativos en la operación diaria (Charles James & Meyer, 2024).

Es imprescindible diseñar y poner en práctica mecanismos y protocolos que permitan una respuesta ágil y eficiente ante incidentes, garantizando la recuperación rápida de procesos críticos. De este modo, no solo se protege la reputación organizacional, sino que también se fortalece la posición competitiva, al

demostrar a clientes y socios la solidez de la gestión integral de riesgos y la capacidad de mantener la operatividad en escenarios adversos (Montalban Ordoñez, 2022).

Riesgos Tecnológicos y Organizacionales en Procesos de Modernización

Las organizaciones disponen de cuatro enfoques fundamentales para gestionar los riesgos: evitarlos, mitigarlos, transferirlos o aceptarlos. La selección de la estrategia adecuada depende tanto de la naturaleza y criticidad del riesgo como de la capacidad de la entidad para enfrentar sus posibles efectos. Adoptar un método estructurado de clasificación y respuesta garantiza que los esfuerzos de control de riesgos se alineen con los objetivos estratégicos y operativos, optimizando la asignación de recursos y salvaguardando la continuidad del negocio.

La estrategia de evitación se basa en suprimir cualquier iniciativa que pueda incrementar la probabilidad de que un riesgo identificado llegue a materializarse. En la práctica, esto implica renunciar o modificar proyectos, procesos o características específicas cuya ejecución conlleve peligros inaceptables. La mitigación persigue disminuir tanto la probabilidad como el impacto de un riesgo a niveles tolerables. Esto se logra mediante la implementación de controles técnicos y organizativos como pruebas de penetración continuas, segmentación de la red o revisiones periódicas de código y el seguimiento sistemático de indicadores clave de riesgo. La transferencia del riesgo consiste en desplazar las consecuencias económicas o legales de un evento adverso a un tercero, generalmente mediante contratos de seguro o acuerdos de servicio gestionados por proveedores externos. Al hacerlo, la organización conserva la operación del proceso en cuestión, pero delega la responsabilidad financiera o la restitución de servicios en otra parte. Finalmente, la aceptación del riesgo implica reconocer su existencia y continuar con la actividad sin medidas de contención específicas; se suele aplicar cuando el coste de mitigación supera a las posibles pérdidas derivadas del propio riesgo, o cuando su probabilidad e impacto son considerados marginales para la operación global (Salazar-Coto, 2022).

Vulnerabilidades en Seguridad de la Información y Ciberataques

Para abordar este desafío de forma efectiva, es indispensable desglosar y caracterizar cada componente del sistema: desde el inventario de activos críticos y las configuraciones de red hasta los procesos, acciones de los usuarios y eventos clave que puedan abrir brechas de seguridad.

También es fundamental trazar la secuencia de sucesos e hitos en los que una amenaza podría aprovechar una vulnerabilidad, lo que permite priorizar los controles más adecuados y diseñar contramedidas específicas. Al realizar este mapeo detallado de escenarios potenciales de ciberataque, las organizaciones están en posición de anticipar y neutralizar proactivamente los puntos débiles, reduciendo a su vez la superficie de exposición y fortaleciendo la resiliencia de sus entornos frente a incidentes de seguridad (Chuqui Quille & Orellana González, 2023).

Un componente fundamental en esta defensa es la gestión de vulnerabilidades. Este es un proceso sistemático y constante que involucra la identificación proactiva de debilidades o fallos de seguridad en los sistemas y aplicaciones de una organización. Una vez identificadas, estas vulnerabilidades se evalúan en términos de su potencial impacto y se abordan mediante la implementación de medidas correctivas. El objetivo primordial de la gestión de vulnerabilidades es minimizar el riesgo de que actores malintencionados puedan explotar estas debilidades para llevar a cabo ciberataques, asegurando así que las amenazas se neutralicen antes de que puedan ser utilizadas para comprometer la seguridad de la información (Santillan et al., 2025).

Para resaltar la trascendencia de salvaguardar datos sensibles, resulta imprescindible reforzar las medidas de control en el marco de la gestión de riesgos de la información, de modo que se prevengan filtraciones que pongan en peligro la integridad de los sistemas. Como lo mencionan los expertos:

“Cuando la información es de carácter privado, es necesario considerar medidas de prevención para evitar el robo de información con fines desconocidos que pueden generar pérdidas a la organización y perjudicar la reputación” (Ortiz et al., 2023).

Compliance y Riesgo Reputacional

La efectividad del compliance tecnológico radica en su integración estratégica dentro de la infraestructura de TI y en el apoyo de una cultura organizacional que valore la transparencia y la mejora continua. Al fusionar innovación digital y prácticas de cumplimiento, las organizaciones pueden fortalecer su integridad operativa, asegurar la confiabilidad de sus sistemas y mantener un grado alto de conformidad sin sacrificar agilidad ni eficiencia (Galicia, 2025). La tecnología ha transformado por completo el modo en que las empresas gestionan el cumplimiento normativo, con la automatización del procesamiento avanzado de datos y las plataformas de gestión de riesgos, las organizaciones pueden

operar dentro del marco legal con mayor rapidez y precisión. Conforme estas soluciones tecnológicas sigan evolucionando, el compliance será todavía más eficiente y se ajustará mejor a las necesidades de un entorno empresarial dinámico. Es importante contar con un equipo jurídico que se mantenga constantemente informado sobre las últimas novedades en materia de regulación (Fraguas García, 2023).

Estrategias para Mitigar los Riesgos Tecnológicos

Muchas organizaciones han integrado la tecnología de manera intuitiva en sus operaciones diarias, sin apoyarse en un marco estructurado de gestión de riesgos. Al carecer de un modelo específico que permita anticipar y responder de forma inmediata a eventos como la pérdida de datos o el daño a los activos tecnológicos, se deja expuesto todo proceso que dependa de TI. Esta vulnerabilidad inherente pone en peligro la continuidad operativa y la seguridad de la información, por lo que resulta imprescindible diseñar e implementar un sistema de gestión de riesgos de TI que identifique amenazas, evalúe impactos y defina protocolos de reacción ágil ante incidentes (Milian Saavedra, 2024).

Metodologías de Migración Gradual: DevOps y Arquitecturas Escalables

Las metodologías ágiles favorecen la incorporación paulatina de los microservicios y permiten validar de manera constante los avances en la migración. Finalmente, se destaca la necesidad de realizar pruebas rigurosas y continuas tanto en etapas previas como durante la propia migración. Este enfoque garantiza que cada nuevo componente introducido cumpla con los estándares de calidad establecidos y minimiza la probabilidad de errores en producción (Muraca, 2023).

Las prácticas de Integración Continua (CI) y Entrega Continua (CD) constituyen pilares fundamentales de DevOps que aportan gran valor en proyectos de modernización. Estas metodologías permiten integrar cambios de forma frecuente y controlada, así como desplegarlos con mayor agilidad, lo que resulta especialmente útil cuando se trabaja con arquitecturas complejas o poco documentadas, como suele ser el caso de los sistemas legacy (Islavath, 2022).

Diseño de Arquitecturas Resilientes y Tolerantes a Fallos

El diseño de arquitecturas resilientes y tolerantes a fallos ha emergido como una respuesta clave, especialmente en entornos distribuidos de creciente complejidad.

Estas arquitecturas no buscan necesariamente evitar todos los errores, sino asegurar que el sistema continúe operando de forma aceptable incluso ante fallos parciales, degradación del rendimiento o resultados aproximados.

A medida que los sistemas distribuidos continúan creciendo en escala y complejidad, se vuelve indispensable consolidar estos principios como pilares en la construcción de infraestructuras tecnológicas confiables. La resiliencia, entendida no solo como resistencia al fallo, sino como la capacidad del sistema para adaptarse y continuar operando, se convierte en una característica crítica para enfrentar los retos actuales y futuros (Aponte Moreno, 2023; Chandra, 2025)

Esta tensión ha motivado el desarrollo de arquitecturas resilientes y tolerantes a fallos, capaces de mantener su funcionamiento incluso ante condiciones imperfectas. Este enfoque resulta especialmente valioso en entornos donde la continuidad operativa es prioritaria, y donde los sistemas deben ser capaces de seguir funcionando de forma aceptable incluso ante errores internos, fallos de componentes o degradación del rendimiento. Así, el diseño de arquitecturas resilientes no solo apunta a evitar fallos, sino a convivir con ellos sin perder la capacidad de respuesta ni comprometer la experiencia del usuario (Aponte Moreno, 2023).

Propuesta de un Modelo Personalizado para la Gestión del Riesgo Tecnológico

En un entorno cada vez más dinámico y dependiente de la tecnología, la gestión del riesgo tecnológico se ha convertido en un componente estratégico para garantizar la continuidad operativa, la seguridad de la información y la sostenibilidad del negocio. Diversas metodologías han sido desarrolladas con el objetivo de evitar, mitigar, transferir o aceptar los riesgos asociados al uso de tecnologías de la información, cada una con enfoques, niveles de formalismo y contextos de aplicación particulares. Al analizar su aplicabilidad en organizaciones específicas, especialmente en aquellas con estructuras tecnológicas híbridas o en transición como las que migran de sistemas legacy hacia arquitecturas distribuidas surgen limitaciones prácticas que exigen enfoques más flexibles y adaptables.

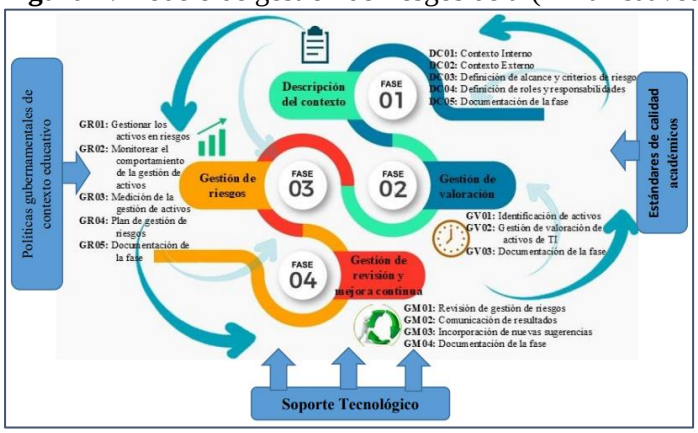
A partir del análisis comparativo de cuatro modelos reconocidos en la literatura, se identificaron tanto fortalezas como vacíos metodológicos que motivaron el desarrollo de una propuesta personalizada. Esta propuesta busca integrar buenas prácticas consolidadas con elementos que respondan a las necesidades particulares de contextos organizacionales en los que la gestión del riesgo debe alinearse con procesos

ágiles, entornos de alta disponibilidad, y arquitecturas resilientes. El modelo personalizado planteado en este apartado no pretende sustituir marcos existentes, sino complementarlos, adaptando su aplicación a realidades técnicas y operativas concretas.

El primer modelo tomado como referencia para el desarrollo de la propuesta personalizada es el presentado en la Figura 1 (Milian Saavedra, 2024), el cual estructura la gestión de riesgos tecnológicos en un ciclo de cuatro fases claramente definidas: descripción del contexto, gestión de valoración, gestión de riesgos y gestión de revisión y mejora continua.

En la segunda fase, la gestión de valoración, se profundiza en la identificación de activos, vulnerabilidades y amenazas, sentando así las bases para la tercera fase, orientada a la definición de acciones para mitigar o controlar los riesgos detectados. Finalmente, la fase de revisión y mejora continua permite retroalimentar el ciclo mediante auditorías, lecciones aprendidas y ajustes metodológicos.

Figura 1: modelo de gestión de riesgos de ti (milian saavedra, 2024)

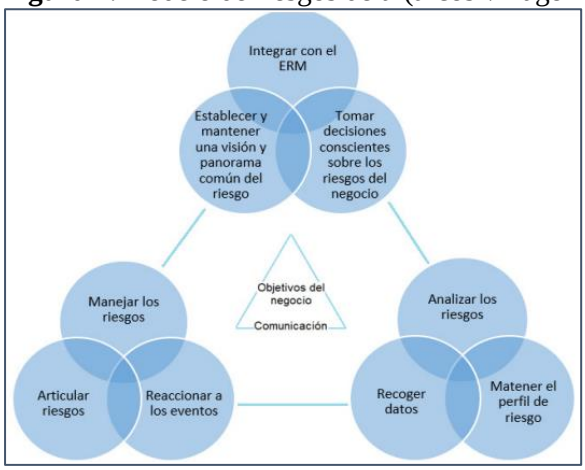


El segundo marco conceptual utilizado como base para la propuesta personalizada es el modelo ilustrado en la Figura 2 (Arcos Villagómez et al., 2022), el cual se organiza a partir de la articulación entre los objetivos del negocio, la comunicación efectiva y la gestión estratégica del riesgo. Este enfoque plantea una estructura triangular compuesta por tres pilares: integración con el Enterprise Risk Management (ERM), establecimiento de una visión común del riesgo, y toma de decisiones informadas sobre riesgos tecnológicos.

A diferencia de enfoques operativos más estructurados, este modelo prioriza la alineación entre la gestión del riesgo y la estrategia organizacional, destacando la importancia de integrar la visión de riesgos tecnológicos con los objetivos globales del negocio.

La comunicación fluida entre actores clave es vista como un facilitador transversal, que permite articular acciones coherentes y sostenidas. Dentro del modelo, se definen dos grandes procesos interrelacionados: por un lado, el análisis del riesgo, que incluye actividades como recoger datos relevantes y mantener un perfil actualizado del riesgo; y por otro, el manejo del riesgo, que abarca acciones para articular riesgos, reaccionar a eventos y diseñar respuestas adaptativas.

Figura 2: modelo de riesgos de ti (arcos villagómez et al., 2022)

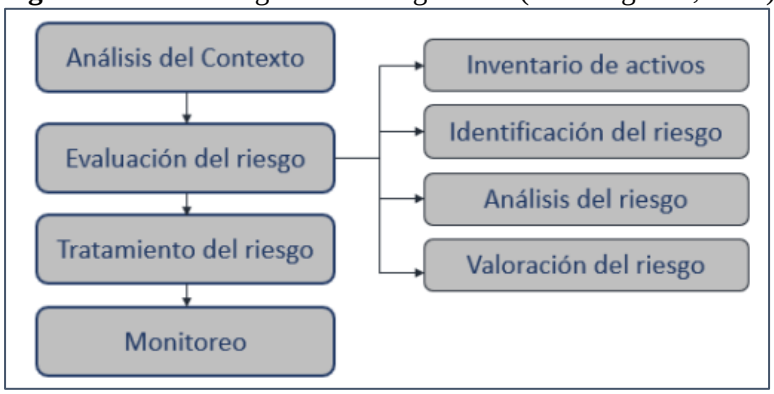


El tercer modelo corresponde a la Figura 3 (Romero Garcia, 2023), el cual propone un enfoque secuencial para la gestión integral del riesgo tecnológico, dividido en cuatro etapas principales: análisis del contexto, evaluación del riesgo, tratamiento del riesgo y monitoreo. Este enfoque se centra en una aplicación práctica y sistemática, con un nivel de granularidad que facilita su implementación en entornos organizativos con procesos definidos.

Durante la fase de análisis del contexto, se contempla la elaboración de un inventario de activos, lo cual permite identificar los elementos críticos de la infraestructura tecnológica y sirve como punto de partida para evaluar vulnerabilidades. Posteriormente, en la evaluación del riesgo, se desglosan tres subprocesos esenciales: identificación, análisis y valoración del riesgo, que en conjunto permiten priorizar las amenazas en función de su probabilidad e impacto.

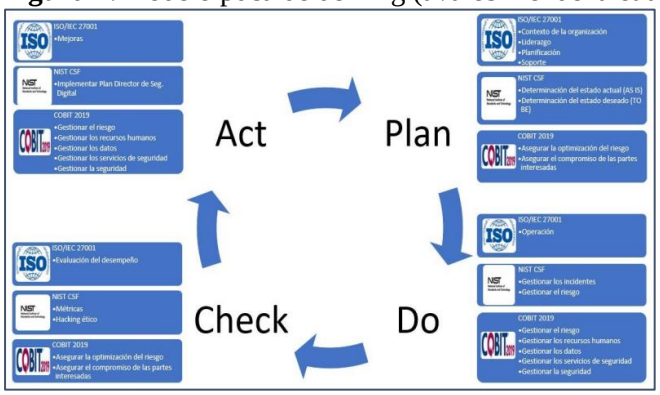
La fase de tratamiento del riesgo contempla la definición de estrategias de mitigación, transferencia, aceptación o eliminación, dependiendo de la naturaleza del riesgo y los recursos disponibles. Finalmente, el modelo incorpora una fase de monitoreo continuo, que permite validar la efectividad de las medidas adoptadas y ajustar las acciones en función de los cambios en el entorno o en los activos tecnológicos.

Figura 3: modelo de gestión de riegos de ti (romero garcia, 2023)



El cuarto modelo seleccionado es el PDCA (Plan-Do-Check-Act) de Deming, tal como se presenta en la Figura 4 (Avalos Mendoza et al., 2023), ofrece un enfoque cíclico y de mejora continua para la gestión del riesgo tecnológico. A diferencia de los modelos anteriores, que presentaban fases o pilares más específicos para la identificación, evaluación y tratamiento del riesgo. El Modelo PDCA de Deming aporta una perspectiva de mejora continua que puede complementar y enriquecer los modelos de gestión de riesgos más específicos. Su naturaleza cíclica enfatiza la importancia de la retroalimentación y la adaptación en la gestión del riesgo tecnológico, asegurando que las estrategias implementadas se mantengan relevantes y efectivas a lo largo del tiempo.

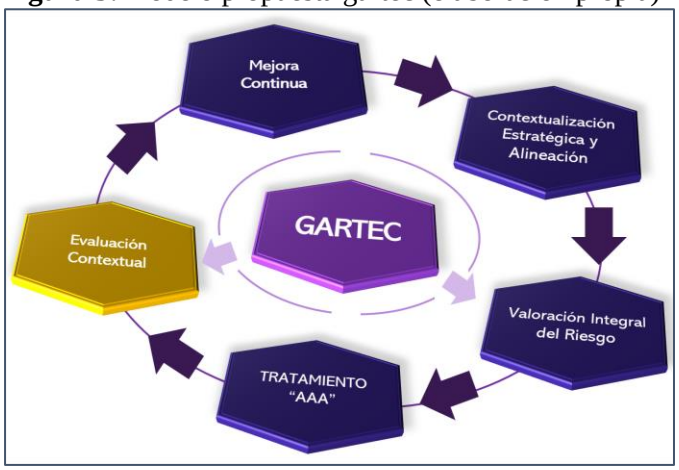
Figura 4: modelo pdca de deming (avalos mendoza et al., 2023)



Después de analizar y considerar cada aspecto de los modelos mencionados se generó la propuesta denominada GARTEC “Gestión Avanzada de Riesgos Tecnológicos” se estructura en cinco macroprocesos cíclicos y flexibles, diseñados para gestionar el riesgo tecnológico en entornos complejos, híbridos o en transformación digital. Su enfoque modular permite adaptarlo tanto a organizaciones consolidadas como a contextos en investigación, prototipado o innovación disruptiva.

Como innovación clave se introduce un macroproceso orientado a la Evaluación Contextual, el cual permite cuestionar y validar los supuestos del análisis original tras aplicar medidas de control, fomentando un pensamiento crítico orientado a la adaptación profunda.

Figura 5: modelo propuesta gartec (elaboración propia)



A continuación, se describen los cinco procesos y su respectivo desglose de actividades con sus objetivos:

Macroproceso 1: Contextualización Estratégica y Alineación

- Análisis del entorno interno y externo (tecnológico, normativo, operativo).
- Identificación de objetivos estratégicos y procesos críticos.
- Alineación con políticas de gestión de riesgos empresariales (ERM).
- Comunicación temprana y activa con stakeholders clave.
- Definición de apetito y tolerancia al riesgo.

Aquí se establece la brújula estratégica: qué se protege, por qué, y bajo qué criterios. Objetivo: Asegurar que la gestión del riesgo esté alineada con la estrategia organizacional y cuente con apoyo directivo.

Macroproceso 2: Valoración Integral del Riesgo

- Inventario de activos clave.
- Identificación de vulnerabilidades, amenazas y escenarios de impacto.
- Evaluación cualitativa y cuantitativa del riesgo.
- Priorización basada en impacto y probabilidad.
- Construcción y mantenimiento del perfil dinámico de riesgo tecnológico.

No solo se detectan los riesgos, se comprende su peso real en el negocio. Objetivo: Lograr una comprensión clara y priorizada de los riesgos tecnológicos presentes y emergentes.

Macroproceso 3: Tratamiento AAA (Ágil, Adaptativo y Avanzado)

- Definición de estrategias: mitigación, transferencia, aceptación o eliminación.
- Evaluación costo-beneficio de acciones según velocidad y criticidad.
- Implementación de planes de acción ajustados a marcos ágiles y contextuales.
- Coordinación técnica, operativa y legal para respuestas integradas.

La respuesta al riesgo no es rígida: es una jugada inteligente, rápida y evolutiva. Objetivo: Diseñar e implementar acciones adaptativas que puedan integrarse en flujos de trabajo flexibles.

Macroproceso 4: Evaluación Contextual

- Reevaluación crítica del entorno tras aplicar tratamientos.
- Análisis de cambios colaterales, nuevos riesgos emergentes y desplazamientos sistémicos.
- Validación de supuestos previos: ¿aún es válido el modelo mental original?
- Ajustes estratégicos y operativos basados en el “efecto retroactivo” de las decisiones.

Aquí se hace la pausa inteligente: ¿lo que entendimos antes aún aplica hoy? este proceso detiene el piloto automático: valida si seguimos entendiendo bien el contexto o si este ha mutado como consecuencia de nuestras acciones. Objetivo: Reexaminar si el entorno y los supuestos del análisis de riesgo siguen siendo vigentes tras aplicar medidas, ajustando la comprensión del riesgo ante posibles cambios o efectos colaterales.

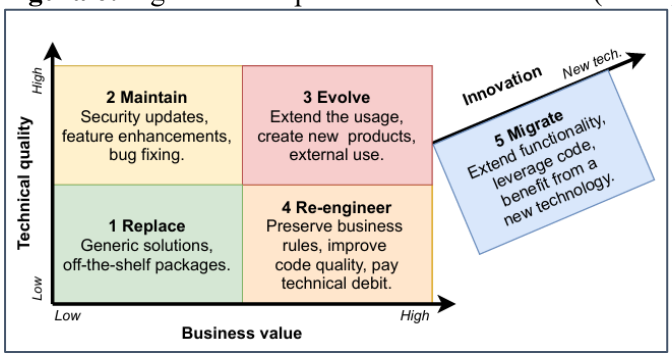
Macroproceso 5: Mejora Continua

- Monitoreo de controles implementados y nuevas amenazas.
- Auditorías, KPIs, métricas y retroalimentación estructurada.
- Ciclo PDCA aplicado a la gestión del riesgo.
- Documentación de lecciones aprendidas y aprendizaje institucionalizado.

El modelo no termina: se afina, se adapta y se prepara para enfrentar mejor los riesgos del mañana. Objetivo: Fortalecer la gestión del riesgo mediante el aprendizaje continuo, el monitoreo sistemático y la adaptación progresiva, asegurando que el modelo evolucione junto con el entorno.

La modernización de sistemas legacy implica desafíos complejos en términos de interoperabilidad, continuidad operativa y exposición a riesgos tecnológicos. El análisis realizado evidencia que los modelos tradicionales de gestión de riesgo, aunque conceptualmente sólidos, presentan limitaciones en su aplicación a entornos híbridos, especialmente en contextos de transformación digital acelerada. La toma de decisiones sobre qué partes del sistema modernizar y cómo hacerlo se vuelve crucial y está influenciada por diversas perspectivas, tal como se ilustra en la siguiente imagen.

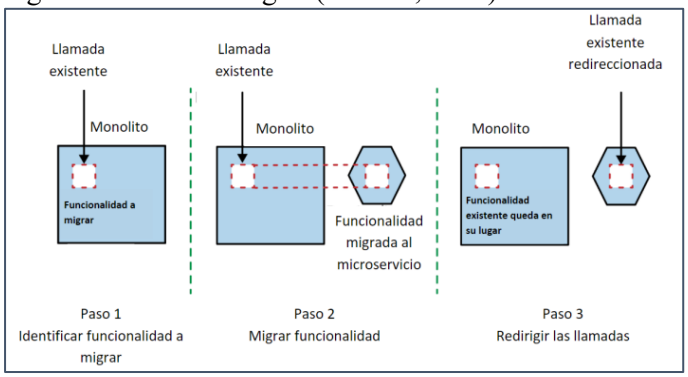
Figura 6: segmentación por necesidad de cambio (assunção et al., 2024)



Este gráfico muestra cómo la segmentación según la necesidad de cambio en un sistema de información puede estar orientada directamente al estado de la organización en relación con su área de Tecnologías de la Información, considerando tanto el valor de negocio como la calidad técnica del sistema existente. Esta visión subraya la importancia de una evaluación que trasciende la mera identificación de riesgos y se alinea con los objetivos estratégicos y la realidad tecnológica de la organización. (Assunção et al., 2024)

La propuesta del modelo GARTEC se posiciona como una alternativa innovadora y contextualizada, al integrar enfoques ágiles, resiliencia operativa y una evaluación crítica del entorno posterior al tratamiento del riesgo. Su estructura modular permite adaptarse a diferentes niveles de madurez tecnológica, facilitando una gestión dinámica y estratégica del riesgo. Para abordar los desafíos de interoperabilidad y la transición gradual hacia nuevas arquitecturas, se pueden considerar patrones como el patrón Strangler.

Figura 7: Patrón Strangler (Muraca, 2023)



Como se visualiza en esta imagen, el patrón Strangler consta de tres pasos fundamentales: identificar la funcionalidad a migrar, migrar esa funcionalidad a un nuevo microservicio y, finalmente, redirigir las llamadas desde el monolito hacia el nuevo microservicio. Este enfoque permite una modernización paulatina, minimizando las interrupciones y facilitando la coexistencia de sistemas heredados y modernos durante la transición. (Muraca, 2023)

La incorporación del macroproceso de Evaluación Contextual y el enfoque AAA (Ágil, Adaptativo y Avanzado) representan aportes clave para garantizar la pertinencia y efectividad de las acciones en entornos cambiantes. La Evaluación Contextual permite una comprensión profunda del entorno organizacional y tecnológico, tal como lo sugiere la necesidad de alinear las decisiones de modernización con la perspectiva de TI y el estado de la organización.

El modelo propuesto GARTEC aporta un marco práctico y escalable para gestionar riesgos tecnológicos en procesos de modernización, contribuyendo a una transición más eficiente, segura y alineada con las necesidades reales de las organizaciones. Al considerar la segmentación de sistemas según su necesidad de cambio y adoptar estrategias de migración gradual como el patrón Strangler, las organizaciones pueden mitigar los riesgos inherentes a la modernización y asegurar una evolución tecnológica más fluida y exitosa.

CONCLUSIONES

La modernización de sistemas legacy implica una serie de retos complejos relacionados con la integración de nuevas tecnologías, la continuidad operativa y la gestión de riesgos tecnológicos. Este estudio evidencia que, aunque los modelos tradicionales de gestión de riesgos aportan lineamientos útiles, su aplicación en entornos híbridos y sometidos a transformaciones digitales aceleradas presenta limitaciones importantes.

Estas limitaciones se manifiestan principalmente en su falta de flexibilidad y en su capacidad reducida para adaptarse a los cambios constantes que caracterizan a las arquitecturas tecnológicas contemporáneas.

El modelo GARTEC se posiciona como un marco conceptual que permite analizar de forma estructurada los desafíos inherentes a la modernización de sistemas heredados. Su enfoque modular y cíclico integra elementos vinculados a la gobernanza, la arquitectura tecnológica, la racionalización de aplicaciones y la gestión del cambio, proporcionando una visión que facilita la comprensión de los factores técnicos y organizacionales que inciden en los procesos de transformación. A través de este enfoque, se contribuye a una lectura más clara de los riesgos y tensiones que surgen durante la transición hacia plataformas más modernas.

Asimismo, la inclusión de un macroproceso orientado a la evaluación contextual permite plantear la importancia de validar continuamente las decisiones vinculadas a la modernización tecnológica. Esta perspectiva resalta la necesidad de alinear la gestión del riesgo con los objetivos estratégicos institucionales, especialmente en organizaciones donde la estabilidad, la regulación y la integridad operativa son elementos críticos. Al destacar este componente, el estudio subraya la relevancia de adoptar metodologías que reconozcan la naturaleza dinámica del entorno tecnológico.

Los hallazgos del estudio permiten identificar una tendencia clara: la gestión del riesgo en procesos de modernización requiere enfoques adaptativos que consideren tanto la complejidad técnica como los factores de resistencia organizacional. Explorar estas líneas podría fortalecer la comprensión de los mecanismos que facilitan o dificultan la transición hacia arquitecturas modernas en instituciones bancarias supervisadas. Si otros investigadores amplían esta discusión, será posible profundizar en modelos que respondan con mayor precisión a las necesidades del sector.

LISTA DE REFERENCIAS

González Varona, J. M. (2021). Retos para la transformación digital de las PYMES: Competencia organizacional para la transformación digital (Tesis doctoral). Universidad de Valladolid. Obtenido de: https://uvadoc.uva.es/bitstream/handle/10324/47767/Tesis1874-210729.pdf

Assunção et al. (2024). Contemporary Software Modernization: Perspectives and Challenges to Deal with Legacy Systems. Obtenido de: https://arxiv.org/pdf/2407.04017

Charles James & Wayne Meyer (2024). Challenges and Solutions in Legacy System Modernization for Cloud Readiness. Obtenido de: https://www.researchgate.net/publication/387750421_Challenges_and_Solutions_in_Legacy_System_Modernization_for_Cloud_Readiness

Montalban Ordoñez, W. E. (2022). Diseño de un plan de continuidad operativa de los servicios críticos del área de Sistemas y Tecnologías de la Información de la empresa Boticas y Salud, con base en la norma ISO/IEC 27031:2011 [Tesis de licenciatura, Universidad Peruana de Ciencias Aplicadas]. Repositorio Académico UPC. Obtenido de: http://hdl.handle.net/10757/660227

Salazar-Coto, D. (2022, agosto). Propuesta de desarrollo de una herramienta para la visualización de riesgos tecnológicos para el Banco Central de Costa Rica [Tesis de licenciatura, Instituto Tecnológico de Costa Rica]. Repositorio TEC. Obtenido de: https://repositoriotec.tec.ac.cr/bitstream/handle/2238/14970/TF9707_BIB311841_Daniel_Salazar-Coto.pdf

Ortiz, A., Guerrero, C., Simba, W., & Acosta, J. (2023). Análisis de vulnerabilidades de Seguridad Informática en la Escuela Superior Militar "Eloy Alfaro". [Tesis de maestría, UIDE]. Repositorio UIDE. Obtenido de: https://repositorio.uide.edu.ec/handle/37000/6104

Chuqui Quille, J. F., & Orellana González, D. A. (2023). Análisis de las vulnerabilidades del sistema de información académica: caso de estudio Instituto Superior Tecnológico del Azuay [Tesis de licenciatura, Universidad Politécnica Salesiana]. Repositorio Digital UPS. Obtenido de: http://dspace.ups.edu.ec/handle/123456789/25183

Santillan, H., Arévalo Satán, J. A., & Wong, P. (2025). Un análisis integral de la infraestructura de ciberseguridad en ambientes académicos. RI, 35(1). Obtenido de: https://doi.org/10.15517/ri.v35i1.60075

Galicia, M. A. (2025, 2 de enero). Compliance y tecnología: el futuro de la integridad corporativa. Revista Abogacía. Obtenido de: https://www.revistaabogacia.com/compliance-y-tecnologia-el-futuro-de-la-integridad-corporativa/

Fraguas García, A. (2023, 25 de septiembre). El papel de la tecnología en el Cumplimiento

Normativo. Belzuz Abogados. Obtenido de: https://www.belzuz.net/es/publicaciones/en-espanol/item/11880-el-papel-de-la-tecnologia-en-el-cumplimiento-normativo.html

Milian Saavedra, J. J. (2024). Modelo de gestión de riesgos de tecnología de información para garantizar la continuidad del servicio en los procesos organizacionales en los institutos de educación superior tecnológicos públicos (Tesis de maestría, Universidad Católica Santo Toribio de Mogrovejo). Obtenido de: https://tesis.usat.edu.pe/bitstream/20.500.12423/7177/1/TM_MilianSaavedraJefferson.pdf

Muraca, F. (2023, noviembre). De monolitos a microservicios: tendencias y oportunidades en la transición de arquitecturas de software (Tesis de Especialización, Universidad Tecnológica Nacional). https://ria.utn.edu.ar/server/api/core/bitstreams/f329afb4-1e75-4dd7-9b7f-a3acaaaffd4f/content

Islavath, N. (2022). Bridging the Gap: A DevOps Strategy for Modernizing Legacy Systems. Journal of Scientific and Engineering Research, 9(12), 196-201. Obtenido de: https://jsaer.com/download/vol-9-iss-12-2022/JSAER2022-9-12-196-201.pdf

Aponte Moreno, J. A. (2023). Design of Fault Tolerant Embedded Systems using Approximate Computing Techniques (Tesis de maestría, Universidad Nacional de Colombia). Obtenido de: https://repositorio.unal.edu.co/bitstream/handle/unal/85008/80017086.2023.pdf

Chandra, P. (2025). Building Fault-Tolerant Systems with Redundancy and Recovery Mechanisms in Distributed Environments. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(1), 2616-2625. Obtenido de: https://doi.org/10.32628/CSEIT251112251

Arcos Villagómez, S. F., Tapia León, F. M., Chafla Altamirano, G. X., & Nicolalde Rodríguez, D. A. (2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. Sathiri, (17), 26-46. Obtenido de: https://doi.org/10.32645/13906925.1129

Romero Garcia, D. A. (2023). Modelo de gestión de riesgos de TI que contribuye a la operación de procesos core en empresas de telecomunicaciones (Tesis de maestría, Universidad Católica Santo Toribio de Mogrovejo). Obtenido de: https://tesis.usat.edu.pe/bitstream/20.500.12423/6566/1/TM_RomeroGarciaDaniel.pdf

Avalos Mendoza, M. R., Castilla Tasaico, J. L., & Gordillo López, C. P. (2023). Diseño de un modelo de Gestión en Seguridad Digital para la aplicación en entidades peruanas del Sector Público (Tesis de maestría, Universidad ESAN). Obtenido de: https://core.ac.uk/download/578161448.pdf