CIBERSEGURIDAD
PARA LA
TRANSFORMACIÓN DIGITAL

Gobierno de TI, Arquitecturas Empresariales e Innovación para la Empresa Inteligente

Carlos Leopoldo Guerrero Valarezo
Enrique Alfredo Guerrero Ferreccio

EDITORIAL
SAGA

Ciberseguridad para la Transformación Digital

Gobierno de TI, Arquitecturas Empresariales e Innovación para la Empresa Inteligente

Autor:
Carlos Leopoldo Guerrero Valarezo
Enrique Alfredo Guerrero Ferreccio

EDITORIAL SAGA

Datos bibliográficos

ISBN:	**978-9907-803-62-4**
Título del libro:	Ciberseguridad para la Transformación Digital Gobierno de TI, Arquitecturas Empresariales e Innovación para la Empresa Inteligente
Autores:	Guerrero Valarezo, Carlos Leopoldo Guerrero Ferreccio, Enrique Alfredo
Editorial:	SAGA
Materia:	600 - Tecnologías de la Información y la Comunicación
Público objetivo:	Profesional / académico
Publicado:	2026-08-09
Número de edición:	1
Tamaño:	5Mb
Soporte:	Libro digital descargable
Formato:	Pdf (.pdf)
Idioma:	Español
DOI:	https://doi.org/10.63415/saga.2026.116

Hecho en Ecuador / Made in Ecuador

Autores

Carlos Leopoldo Guerrero Valarezo
Investigador Independiente
carlos@guerrero.ec
https://orcid.org/0009-0001-7608-9713
Guayaquil, Ecuador

Carlos Leopoldo Guerrero Valarezo es profesional de Tecnologías de la Información con más de veinte años de experiencia en consultoría, infraestructura tecnológica, telecomunicaciones, ciberseguridad y gestión de proyectos. Su trayectoria combina el ejercicio profesional, la dirección de iniciativas de transformación digital y la docencia universitaria, con especial interés en la seguridad de la información, las redes de comunicaciones y la administración de sistemas.

Posee maestrías en Gestión de Proyectos por la Universidad Estatal de Milagro, Ciberseguridad por la Universidad Internacional del Ecuador y Redes de Comunicaciones por la Pontificia Universidad Católica del Ecuador, además de una Licenciatura en Redes y Sistemas Operativos por la Escuela Superior Politécnica del Litoral.

Su experiencia comprende la administración y optimización de entornos empresariales, SAP S/4HANA RISE, SAP BASIS, Microsoft Dynamics AX, sistemas Linux y Windows, así como redes FTTH, WAN, LAN, WiFi y VPN. Ha liderado equipos multidisciplinarios en proyectos de modernización, migración tecnológica y mejora de procesos. Complementa su perfil con experiencia en gestión presupuestaria, negociación con proveedores y docencia en redes, ciberseguridad, administración de sistemas y competencias digitales, integrando conocimiento técnico, gestión estratégica y formación académica.

Enrique Alfredo Guerrero Ferreccio
Investigador Independiente
eaguerrerof@gmail.com
https://orcid.org/0009-0009-2876-0152
Guayaquil, Ecuador

Enrique Alfredo Guerrero Ferreccio es un profesional del ámbito de la ingeniería y la gestión de proyectos, cuya formación académica integra conocimientos técnicos especializados con competencias orientadas a la planificación, dirección y ejecución de iniciativas de carácter tecnológico y organizacional.

Es Magíster en Gestión de Proyectos por la Universidad Estatal de Milagro e Ingeniero en Electricidad, especialización Electrónica, por la Escuela Superior Politécnica del Litoral (ESPOL). Esta combinación académica le proporciona una perspectiva integral para abordar proyectos que requieren análisis técnico, planificación estratégica, administración eficiente de recursos y toma de decisiones.

Su formación en ingeniería eléctrica y electrónica constituye la base para comprender y gestionar sistemas tecnológicos, infraestructura y procesos asociados al ámbito de la ingeniería, mientras que sus estudios de posgrado fortalecen sus capacidades para la formulación, planificación, seguimiento y evaluación de proyectos.

Su perfil profesional se caracteriza por la integración de la ingeniería con la gestión, orientada al desarrollo de soluciones eficientes y al cumplimiento de objetivos institucionales y empresariales. Esta perspectiva multidisciplinaria favorece su participación en proyectos de innovación, modernización y mejora de procesos, articulando conocimientos técnicos con metodologías de gestión y una visión enfocada en resultados.

EDITORIAL
SAGA

Sinopsis

Ciberseguridad para la Transformación Digital: Gobierno de TI, Arquitecturas Empresariales e Innovación para la Empresa Inteligente presenta una visión académica e integradora de la seguridad digital como componente transversal de la dirección organizacional, vinculando gobierno de tecnologías de información, gestión de riesgos, arquitectura empresarial e innovación con los procesos que sustentan la evolución de las organizaciones contemporáneas. La obra examina principios, modelos y prácticas destinados a proteger activos, datos, servicios e infraestructuras frente a amenazas crecientes, mientras relaciona la toma de decisiones tecnológicas con objetivos estratégicos, cumplimiento normativo, continuidad operativa y generación de valor. Su enfoque articula personas, procesos y tecnología. Mediante una perspectiva orientada a la empresa inteligente, el libro aborda la incorporación responsable de automatización, analítica, inteligencia artificial, servicios digitales y ecosistemas interconectados, destacando la necesidad de diseñar capacidades resilientes, mecanismos de control y estructuras de gobernanza que favorezcan confianza y adaptabilidad. También analiza la arquitectura empresarial como instrumento para alinear estrategia, información, aplicaciones e infraestructura, facilitando decisiones coherentes ante cambios tecnológicos acelerados. Dirigida a profesionales, directivos, investigadores y estudiantes, la obra ofrece fundamentos para comprender la ciberseguridad como disciplina estratégica capaz de fortalecer innovación, competitividad, sostenibilidad y madurez digital en entornos organizacionales complejos, dinámicos y conectados globalmente.

Palabras clave: ciberseguridad; transformación digital; gobierno de TI; arquitectura empresarial; gestión de riesgos

Synopsis

Cybersecurity for Digital Transformation: IT Governance, Enterprise Architectures, and Innovation for the Intelligent Enterprise presents an academic and integrative view of digital security as a cross-cutting component of organizational management, linking information technology governance, risk management, enterprise architecture, and innovation with the processes that support the evolution of contemporary organizations. The book examines principles, models, and practices aimed at protecting assets, data, services, and infrastructures against growing threats, while connecting technology decision-making with strategic objectives, regulatory compliance, business continuity, and value creation. Its approach integrates people, processes, and technology. From an intelligent-enterprise perspective, the book addresses the responsible adoption of automation, analytics, artificial intelligence, digital services, and interconnected ecosystems, emphasizing the need to design resilient capabilities, control mechanisms, and governance structures that foster trust and adaptability. It also analyzes enterprise architecture as an instrument for aligning strategy, information, applications, and infrastructure, facilitating coherent decisions amid accelerated technological change. Intended for professionals, executives, researchers, and students, the book provides foundations for understanding cybersecurity as a strategic discipline capable of strengthening innovation, competitiveness, sustainability, and digital maturity within complex, dynamic, and globally connected organizational environments.

Keywords: cybersecurity; digital transformation; IT governance; enterprise architecture; risk management

Índice General

Introducción

La transformación digital ha modificado de manera profunda la relación entre estrategia, tecnología y continuidad organizacional. La expansión de servicios digitales, plataformas interconectadas, inteligencia artificial y modelos operativos basados en datos amplía las posibilidades de innovación, pero también incrementa la exposición frente al riesgo cibernético. Saeed et al. (2023) vinculan esta transformación con la resiliencia empresarial y advierten que la ciberseguridad debe incorporarse a las decisiones organizacionales. Desde esta perspectiva, proteger y transformar constituyen responsabilidades estratégicas estrechamente relacionadas.

Esta realidad adquiere especial relevancia en organizaciones que avanzan hacia modelos de Empresa Inteligente, entendida en esta obra como aquella capaz de integrar personas, procesos, información y tecnología para aprender, decidir y adaptarse mediante capacidades digitales confiables. La seguridad deja entonces de ocupar una posición periférica. Gale, Bongiovanni y Slapničar (2022) muestran que su gobierno alcanza directamente a juntas directivas y estructuras ejecutivas, mientras Saveljeva y Volkova (2025) relacionan confianza digital, gobernanza, cumplimiento, trazabilidad y sostenibilidad.

El punto de partida reside en reconocer que la exposición digital constituye un problema empresarial antes que una cuestión exclusivamente técnica. Los activos de información, aplicaciones, infraestructuras, identidades y cadenas de suministro participan en procesos cuya interrupción puede afectar reputación, operaciones, cumplimiento y resultados económicos. Aghazadeh Ardebili, Lezzi y Pourmadadkar (2024) destacan la articulación entre evaluación del riesgo, gobernanza y resiliencia. Seid et al. (2024), por su parte,

evidencian el valor de cuantificar económicamente el ciberriesgo para respaldar decisiones fundamentadas.

La pertinencia académica del libro procede de la necesidad de estudiar estas dimensiones mediante una visión articulada. Analizar riesgos sin gobierno limita la capacidad de decisión; establecer controles sin arquitectura puede fragmentar las respuestas; incorporar inteligencia artificial sin criterios de gobernanza introduce nuevas exposiciones. McIntosh et al. (2024) examinan precisamente la complementariedad entre marcos de ciberseguridad, gestión y regulación frente al desarrollo de grandes modelos de lenguaje. Esta convergencia demanda enfoques capaces de relacionar dirección, ingeniería, cumplimiento e innovación responsable.

En correspondencia con esta problemática, el objetivo general de la obra es analizar la ciberseguridad como capacidad estratégica habilitadora de la transformación digital y de la evolución hacia la Empresa Inteligente. De este propósito se derivan objetivos orientados a relacionar gestión del riesgo, gobierno de TI, arquitectura empresarial, protección de activos, resiliencia operativa, inteligencia artificial e innovación. Hardi y Legowo (2023) respaldan la función de la arquitectura empresarial como mecanismo de articulación entre transformación y procesos operacionales, dimensión indispensable dentro de este recorrido.

Las preguntas que orientan el desarrollo responden a esa misma lógica integradora: ¿de qué manera puede gestionarse el riesgo digital desde las prioridades del negocio?, ¿qué estructuras de gobierno permiten convertir la ciberseguridad en responsabilidad ejecutiva?, ¿de qué forma la arquitectura empresarial puede incorporar seguridad y resiliencia desde el diseño? También interesa establecer qué aportes ofrecen la inteligencia artificial y la automatización a las operaciones de seguridad y qué riesgos acompañan su adopción. Vourganas y

Michala (2024) documentan la creciente aplicación del aprendizaje automático en este ámbito.

El primer capítulo desarrolla la gestión integral del riesgo digital como fundamento para las decisiones posteriores, desde su identificación y valoración hasta su cuantificación, tratamiento y monitoreo continuo. El segundo traslada ese análisis al gobierno digital, la supervisión ejecutiva, las métricas, la privacidad y la gobernanza de la inteligencia artificial. Levstek, Pucihar y Hovelja (2022) destacan la necesidad de modelos adaptativos de gobierno de TI, mientras Aksoy (2024) incorpora la cultura organizacional como componente de la resiliencia frente a ataques cibernéticos.

El tercer capítulo aborda las arquitecturas empresariales, Zero Trust, DevSecOps y los entornos de nube como espacios donde las decisiones estratégicas adquieren expresión técnica. La seguridad por diseño ocupa aquí una posición central. Rajapakse et al. (2022) examinan las dificultades y respuestas asociadas con la adopción de DevSecOps, mientras Matias et al. (2024) relacionan efectividad y seguridad en arquitecturas de microservicios. El cuarto capítulo continúa esta trayectoria mediante protección de identidades, datos, infraestructuras, respuesta a incidentes y resiliencia operativa.

El quinto capítulo estudia la inteligencia artificial, la analítica avanzada y la automatización aplicadas a la ciberseguridad, considerando detección de anomalías, UEBA, SOAR, inteligencia de amenazas y respuesta automatizada. La capacidad defensiva convive, sin embargo, con nuevas superficies de exposición. Ferrag et al. (2025) analizan aplicaciones y vulnerabilidades asociadas con la IA generativa, incluidos ataques adversarios, envenenamiento de datos y riesgos de privacidad. Esta dualidad obliga a vincular innovación tecnológica con evaluación permanente, trazabilidad y mecanismos de gobierno.

El sexto capítulo proyecta la discusión hacia confianza digital, criptografía postcuántica, gemelos digitales, sistemas autónomos, sostenibilidad y edge intelligence. Liu y Moody (2024) sitúan la criptografía postcuántica dentro de la preparación necesaria ante el avance de la computación cuántica, mientras Homaei et al. (2024) examinan la relación entre gemelos digitales, inteligencia artificial y ciberseguridad. La secuencia Riesgos → Gobierno → Arquitectura → Protección y Operación → IA e Innovación organiza, por tanto, una trayectoria académica destinada a comprender la Empresa Inteligente desde la seguridad, la resiliencia, la confianza y la creación sostenible de valor.

Por qué la ciberseguridad debe habilitar la transformación digital, no frenarla

La transformación digital amplía las capacidades de las organizaciones mediante servicios digitales, automatización, analítica, inteligencia artificial y ecosistemas interconectados. Sin embargo, cada avance incorpora nuevas superficies de exposición que requieren decisiones de seguridad coherentes con los objetivos empresariales. Saeed et al. (2023) relacionan transformación digital, ciberseguridad y resiliencia organizacional, evidenciando que gestionar el riesgo forma parte del proceso de evolución empresarial y de la capacidad para sostener operaciones confiables.

Desde esta perspectiva, la ciberseguridad debe actuar como habilitadora de innovación, continuidad y confianza, en lugar de convertirse en una barrera para adoptar nuevas tecnologías. Su incorporación desde las primeras etapas permite que controles, arquitecturas y decisiones de riesgo acompañen el cambio organizacional. Aflakhah y Soewito (2023) muestran la importancia de traducir riesgos y hallazgos de seguridad en controles y planes de mitigación, fortaleciendo una transformación digital gobernada, resiliente y alineada con las prioridades institucionales.

Qué es una "Empresa Inteligente"

En el marco conceptual de este libro, la Empresa Inteligente se concibe como una organización capaz de integrar personas, procesos, datos y tecnologías para aprender, decidir y adaptarse mediante capacidades digitales confiables. No se define únicamente por incorporar inteligencia artificial o automatización. Su madurez depende de la articulación entre estrategia, gobierno, arquitectura empresarial, gestión del riesgo, seguridad e innovación, de manera que las capacidades tecnológicas contribuyan efectivamente a la generación sostenible de valor.

Esta concepción reconoce además que la inteligencia organizacional requiere confianza en los sistemas que procesan información y sustentan decisiones. Saveljeva y Volkova (2025) vinculan la confianza digital con seguridad, gobernanza, cumplimiento, transparencia y trazabilidad. En paralelo, Wang et al. (2025) relacionan la inteligencia distribuida con seguridad, confiabilidad y sostenibilidad. La Empresa Inteligente representa, por ello, una organización tecnológicamente avanzada que también desarrolla capacidades para gobernar y proteger su evolución digital.

A quién va dirigido este libro y cómo usarlo

La obra está dirigida a directivos, profesionales de tecnologías de información y ciberseguridad, responsables de riesgos y cumplimiento, arquitectos empresariales, investigadores, docentes y estudiantes interesados en comprender la seguridad digital desde una perspectiva organizacional. Su orientación integradora permite aproximarse a la ciberseguridad más allá de los controles técnicos, vinculándola con gobierno corporativo, decisiones ejecutivas y generación de valor. Gale, Bongiovanni y Slapničar (2022) respaldan esta perspectiva al situar la supervisión de la ciberseguridad en el ámbito directivo.

El libro puede utilizarse mediante una lectura secuencial o como obra de consulta temática. La primera modalidad permite avanzar desde los fundamentos del riesgo hasta las tecnologías que configuran el futuro de la Empresa Inteligente; la segunda facilita abordar capítulos específicos según necesidades académicas o profesionales. Los anexos complementan ambos recorridos mediante un glosario, plantillas prácticas y referencias normativas vinculadas con gestión de riesgos, gobierno de TI, Zero Trust, respuesta a cibercrisis y protección de datos.

La secuencia moderna: Riesgos → Gobierno → Arquitectura → Protección y Operación → IA e Innovación

La organización temática responde a una secuencia deliberada: Riesgos → Gobierno → Arquitectura → Protección y Operación → IA e Innovación. El riesgo establece aquello que debe protegerse y orienta las prioridades; el gobierno transforma dichas prioridades en responsabilidades, políticas y decisiones; la arquitectura las incorpora al diseño organizacional y tecnológico; mientras la protección y la operación materializan controles, capacidades de detección, respuesta, continuidad y resiliencia. Cada componente prepara las condiciones necesarias para el siguiente.

La inteligencia artificial y la innovación ocupan la etapa de mayor evolución de este recorrido porque requieren fundamentos previos de riesgo, gobierno y seguridad. McIntosh et al. (2024) relacionan precisamente los marcos de ciberseguridad y gobernanza con los riesgos derivados de los grandes modelos de lenguaje, mientras Ferrag et al. (2025) estudian tanto las aplicaciones defensivas de la IA generativa como sus vulnerabilidades. La secuencia propuesta permite comprender la innovación como una capacidad gobernada, protegida y orientada hacia la creación de valor.

Capítulo 1:

Gestión Integral del Riesgo Digital como Punto de Partida

La transformación digital ha convertido el riesgo en una conversación que atraviesa estrategia, operaciones, tecnología y gobierno corporativo. Cada servicio conectado amplía posibilidades de crecimiento, pero también introduce dependencias capaces de afectar continuidad, confianza y valor empresarial. Por eso, la ciberseguridad comienza mucho antes de seleccionar herramientas. Saeed et al. (2023) plantean que transformación digital, exposición cibernética y resiliencia organizacional mantienen una relación estrecha, especialmente cuando las empresas dependen crecientemente de infraestructuras y procesos digitalizados.

Mirar el riesgo desde la empresa modifica el orden habitual de las preguntas. Primero importa reconocer qué debe preservarse, qué pérdidas resultarían relevantes y qué nivel de exposición puede aceptarse; después corresponde decidir qué capacidades tecnológicas serán necesarias. McIntosh et al. (2024) muestran que los marcos contemporáneos de ciberseguridad y gobierno ofrecen perspectivas complementarias para gestionar riesgos, oportunidades y exigencias regulatorias. Esa complementariedad permite conectar estrategia, responsabilidad directiva, arquitectura y controles bajo una lógica común de decisión.

Los marcos aportan disciplina, pero gestionar riesgo exige interpretar una realidad empresarial que cambia continuamente. Identificar activos, amenazas, vulnerabilidades y dependencias constituye apenas el comienzo. Luego aparecen preguntas sobre probabilidad, impacto, escenarios y criterios de valoración. Aghazadeh Ardebili et al. (2024) vinculan estos procesos de evaluación con la resiliencia cibernética, destacando el papel de métodos, estándares y estructuras de gobernanza. Evaluar bien significa convertir incertidumbre técnica en conocimiento capaz de orientar decisiones organizacionales responsables.

No toda exposición merece idéntica respuesta. Algunas organizaciones aceptarán determinados riesgos para favorecer

innovación, mientras otras establecerán límites estrictos debido a obligaciones regulatorias, financieras u operativas. El apetito y la tolerancia proporcionan referencias para resolver esa tensión. Chong et al. (2025) relacionan la evaluación del riesgo cibernético con decisiones de capital, mostrando que las pérdidas potenciales pueden analizarse mediante criterios económicos. El riesgo digital entra entonces en conversaciones ejecutivas sobre recursos, estabilidad y capacidad institucional de absorción.

La dependencia empresarial tampoco termina en los límites jurídicos de una compañía. Proveedores tecnológicos, plataformas, servicios administrados y cadenas de suministro participan diariamente en procesos sensibles. Una vulnerabilidad distante puede propagarse hasta interrumpir una operación esencial. Cyber Supply Chain Resilience (2025) analiza los marcos ISO, NIST y NIS2 frente al riesgo de terceros y destaca la necesidad de fortalecer resiliencia mediante evaluación, gobernanza y mitigación coordinadas. La confianza contractual necesita acompañarse de visibilidad y supervisión permanente.

Comprender la exposición carecería de propósito si ese conocimiento no condujera hacia decisiones de tratamiento. El riesgo debe traducirse en responsabilidades, prioridades arquitectónicas, controles y tecnologías proporcionadas a las consecuencias que pretenden reducir. Aflakhah y Soewito (2023) muestran que la evaluación apoyada en COBIT 2019 e ISO 27001 permite identificar brechas y convertir hallazgos en planes de mitigación. Allí aparece una relación fundamental: los controles adquieren sentido cuando responden a riesgos previamente comprendidos y valorados.

La conversación alcanza otra profundidad cuando el riesgo puede expresarse mediante consecuencias económicas. Las categorías cualitativas facilitan clasificaciones, aunque muchas decisiones ejecutivas requieren estimaciones comparables con inversiones, reservas o pérdidas operativas. Seid et al. (2024)

presentan FAIR como una aproximación para cuantificar ciberriesgos mediante frecuencia y magnitud de pérdida. Esta perspectiva permite traducir escenarios técnicos hacia métricas financieras, haciendo visible la incertidumbre y proporcionando mejores fundamentos para priorizar tratamientos, justificar inversiones y comparar alternativas empresariales.

Pero ninguna valoración permanece vigente indefinidamente. Los entornos digitales cambian mientras la organización opera: aparecen vulnerabilidades, dispositivos modifican su postura, usuarios alteran patrones y nuevas dependencias transforman la exposición. Goshikonda y Pulipati (2024) relacionan zero trust, telemetría continua y aprendizaje automático con mecanismos dinámicos de evaluación del riesgo. Esta visión desplaza la gestión desde fotografías periódicas hacia observación persistente, donde nuevas evidencias pueden modificar puntuaciones, decisiones de acceso y prioridades de protección empresarial.

Vistas en conjunto, estas dimensiones revelan que la gestión integral del riesgo digital funciona como una disciplina articuladora. Une estrategia y tecnología, conecta directorios con especialistas, relaciona arquitectura con continuidad y convierte señales técnicas en decisiones sobre valor. McIntosh et al. (2024) destacan la complementariedad existente entre marcos contemporáneos, mientras Saeed et al. (2023) vinculan ciberseguridad y resiliencia con transformación digital. Ambas perspectivas convergen en una premisa: proteger tecnología carece de sentido cuando se desconoce aquello que sostiene.

Este capítulo parte, por tanto, del riesgo para construir una visión integrada de la empresa digital. Desde su identificación y valoración hasta la cuantificación, tratamiento y vigilancia continua, cada etapa alimenta decisiones posteriores y obliga a revisar las anteriores. Aghazadeh Ardebili et al. (2024) vinculan evaluación y resiliencia, mientras Seid et al. (2024) muestran el

valor de traducir exposición cibernética a magnitudes económicas. Gobernar el riesgo significa aprender a decidir responsablemente bajo incertidumbre permanente.

Figura 1
Gestión integral del riesgo digital

1.1. Por qué todo empieza por el riesgo de negocio, no por la tecnología

La gestión integral del riesgo digital comienza antes de elegir plataformas, controles o arquitecturas. Su punto de partida es el negocio: aquello que genera valor, sostiene operaciones y preserva la confianza de clientes y reguladores. La tecnología adquiere sentido cuando protege esos intereses frente a eventos capaces de alterar objetivos estratégicos. Saeed et al. (2023) vinculan la transformación digital con una exposición creciente a amenazas que pueden comprometer la resiliencia empresarial y su continuidad operativa.

Cuando una organización inicia la conversación desde herramientas, corre el riesgo de confundir medios con propósitos. Un firewall, una plataforma de identidad o un servicio de monitoreo poseen valor en la medida en que reducen exposiciones relevantes para la empresa. La pregunta inicial debe orientarse hacia pérdidas posibles, procesos sensibles y dependencias críticas. Desde esta perspectiva, Saeed et al. (2023) señalan que la digitalización amplía superficies de ataque y exige respuestas vinculadas con prioridades organizacionales.

El riesgo de negocio permite traducir la ciberseguridad al lenguaje de quienes toman decisiones sobre inversión, crecimiento y continuidad. Hablar de vulnerabilidades técnicas puede resultar distante para un directorio; hablar de interrupciones, pérdidas, sanciones o deterioro reputacional modifica la conversación. Esta traducción favorece decisiones responsables porque relaciona amenazas digitales con consecuencias económicas. Saeed et al. (2023) destacan que la resiliencia empresarial depende de integrar la protección digital mediante prácticas organizacionales capaces de responder ante incidentes.

La transformación digital incrementa oportunidades, pero también modifica la naturaleza de las dependencias empresariales. Procesos antes manuales pasan a plataformas conectadas, los datos circulan entre actores y las decisiones descansan cada vez más en servicios digitales. Cada avance introduce relaciones de riesgo que deben comprenderse desde el valor empresarial comprometido. Para Saeed et al. (2023), la adopción tecnológica requiere considerar amenazas de ciberseguridad que pueden afectar operaciones, información y capacidad de recuperación de las organizaciones.

Partir del riesgo empresarial también evita inversiones defensivas innecesarias. No todos los activos merecen idéntico nivel de protección, ni todas las amenazas producen consecuencias equivalentes. Una gestión madura distingue aquello que puede detener operaciones, afectar obligaciones legales o erosionar

ventajas competitivas. Esa priorización permite asignar recursos con criterio y justificar decisiones ante la dirección. Saeed et al. (2023) relacionan la resiliencia con medidas de seguridad ajustadas a las necesidades empresariales derivadas de la transformación digital.

Este enfoque exige conocer el negocio con profundidad: procesos, productos, información, terceros, obligaciones y expectativas de servicio. Sin esa comprensión, los equipos de seguridad pueden proteger componentes técnicamente visibles mientras permanecen expuestas dependencias decisivas para la organización. La conversación cambia cuando se pregunta qué acontecimiento impediría cumplir una promesa al cliente o sostener una operación esencial. Saeed et al. (2023) advierten que las amenazas digitales pueden generar efectos amplios sobre continuidad, desempeño y confianza empresarial.

La tecnología cambia rápidamente; los objetivos empresariales ofrecen una referencia más estable para gobernar el riesgo. Hoy una organización puede operar en nube, mañana incorporar inteligencia artificial y después automatizar cadenas completas de decisión. Las herramientas variarán, pero seguirá siendo necesario proteger ingresos, información, reputación y capacidad operativa. En esta línea, Saeed et al. (2023) plantean que la transformación digital demanda estrategias de ciberseguridad vinculadas con resiliencia, preparación organizacional y respuesta frente a amenazas persistentes.

Ubicar el riesgo de negocio en el origen también mejora la relación entre seguridad, arquitectura empresarial y gobierno de TI. Ambas disciplinas dejan de funcionar como dominios aislados y pasan a compartir una pregunta: qué capacidades deben preservarse para alcanzar los objetivos. La arquitectura identifica dependencias, el gobierno establece responsabilidades y la ciberseguridad trata exposiciones prioritarias. Saeed et al. (2023)

resaltan la necesidad de enfoques integrados para fortalecer la resistencia organizacional frente a riesgos digitales.

Existe además una dimensión humana que rara vez aparece en los diagramas técnicos. Las decisiones sobre riesgo expresan tolerancias, prioridades y compromisos asumidos por personas que deben responder ante consecuencias. Un incidente afecta cifras, pero también relaciones, credibilidad y confianza acumulada durante años. Por ello, gobernar el riesgo digital requiere liderazgo y criterio, no únicamente controles. Saeed et al. (2023) reconocen que la resiliencia frente a amenazas cibernéticas demanda capacidades organizacionales, concienciación y prácticas coordinadas.

En consecuencia, comenzar por el riesgo de negocio establece una disciplina de pensamiento: primero se identifica aquello que la organización necesita preservar; después se valoran amenazas, impactos y tolerancias; entonces se seleccionan respuestas tecnológicas coherentes. El orden importa porque evita convertir la ciberseguridad en una colección de herramientas desconectadas de la estrategia. Saeed et al. (2023) vinculan la protección digital con la continuidad y resiliencia empresarial, recordando que la tecnología debe servir a prioridades organizacionales.

1.2. Marcos de gestión de riesgo actualizados (ISO 31000, ISO 27005, NIST RMF, NIST CSF 2.0, COSO ERM)

La gestión contemporánea del riesgo digital requiere marcos capaces de conectar incertidumbre, estrategia, gobierno y decisiones tecnológicas. ISO 31000, ISO 27005, NIST RMF, NIST CSF 2.0 y COSO ERM responden a esa necesidad desde perspectivas distintas, aunque compatibles. Ninguno resuelve por sí mismo toda la complejidad empresarial. McIntosh et al. (2024) destacan que los marcos actuales pueden complementarse para atender riesgos,

oportunidades y exigencias regulatorias vinculadas con tecnologías digitales en permanente transformación organizacional.

ISO 31000 aporta una visión transversal del riesgo, aplicable a decisiones estratégicas, operativas y corporativas sin quedar restringida al ámbito tecnológico. Su valor reside en integrar la incertidumbre dentro de la gestión y relacionarla con objetivos organizacionales. Esta amplitud permite que la ciberseguridad dialogue con otras categorías de exposición empresarial. La comparación desarrollada por McIntosh et al. (2024) evidencia que los marcos de gobierno y riesgo adquieren mayor utilidad cuando articulan perspectivas empresariales, tecnológicas y regulatorias.

ISO 27005 lleva esa conversación al terreno específico de la seguridad de la información. Su orientación facilita identificar, analizar, evaluar y tratar riesgos asociados con activos informacionales, amenazas, vulnerabilidades y consecuencias para la organización. Más que una metodología aislada, funciona estrechamente vinculada con sistemas de gestión de seguridad. McIntosh et al. (2024) observan que los estándares especializados adquieren relevancia cuando permiten relacionar controles técnicos con responsabilidades organizacionales, cumplimiento normativo y decisiones de gobierno empresarial contemporáneo.

NIST RMF ofrece una aproximación estructurada para administrar riesgos vinculados con sistemas y organizaciones mediante actividades que acompañan su ciclo de vida. La selección, implementación, evaluación y seguimiento de controles forman parte de una disciplina continua, no de una revisión ocasional. Esta característica resulta especialmente pertinente en entornos tecnológicos cambiantes. Según McIntosh et al. (2024), los marcos contemporáneos deben responder a riesgos dinámicos mediante mecanismos capaces de integrar seguridad, gobernanza, evaluación y obligaciones regulatorias crecientes.

NIST CSF 2.0 amplió significativamente la conversación sobre ciberseguridad al incorporar Govern como función central junto con Identify, Protect, Detect, Respond y Recover. El cambio refuerza una idea relevante: administrar riesgos digitales pertenece a la dirección empresarial y no exclusivamente a departamentos técnicos. McIntosh et al. (2024) sostienen que la evolución de los marcos refleja una atención creciente hacia gobernanza, responsabilidad y cumplimiento, especialmente frente a tecnologías cuya adopción modifica rápidamente perfiles de riesgo corporativo.

COSO ERM aporta otra pieza del mapa al vincular riesgo con estrategia y desempeño empresarial. Desde esta mirada, gestionar incertidumbre significa comprender aquello que puede afectar la creación, preservación o deterioro del valor. La ciberseguridad entra entonces en conversaciones sobre objetivos, apetito de riesgo y decisiones ejecutivas. McIntosh et al. (2024) muestran que los marcos orientados al gobierno ofrecen mecanismos valiosos para conectar riesgos tecnológicos con responsabilidades directivas, controles organizacionales y requerimientos de cumplimiento regulatorio empresarial.

Comparar estos marcos como alternativas excluyentes conduce a una lectura limitada. ISO 31000 proporciona principios generales; ISO 27005 profundiza en seguridad de la información; NIST RMF estructura procesos de administración del riesgo; NIST CSF 2.0 organiza capacidades de ciberseguridad; COSO ERM conecta incertidumbre, estrategia y desempeño. McIntosh et al. (2024) resaltan precisamente el valor de examinar diferentes marcos atendiendo sus fortalezas, limitaciones y complementariedades frente a escenarios tecnológicos y regulatorios cada vez más complejos.

La complementariedad adquiere especial importancia cuando una empresa opera bajo múltiples regulaciones, tecnologías y modelos de servicio. Un marco puede orientar el gobierno

corporativo mientras otro ofrece mayor precisión para evaluar riesgos técnicos o seleccionar controles. La arquitectura resultante debe evitar duplicidades y conservar trazabilidad entre decisiones. McIntosh et al. (2024) señalan que evaluar marcos desde oportunidades, riesgos y cumplimiento permite reconocer diferencias funcionales y construir aproximaciones mejor alineadas con necesidades empresariales y tecnológicas contemporáneas.

Figura 2

Marcos contemporáneos de gestión del riesgo

La actualización de los marcos también responde a cambios profundos en el panorama digital. Inteligencia artificial, servicios distribuidos, automatización y modelos basados en grandes volúmenes de datos alteran las fronteras tradicionales de control. Ya no basta con revisar riesgos mediante ciclos demasiado espaciados. McIntosh et al. (2024) analizan esta evolución al estudiar marcos aplicables a modelos de lenguaje, destacando la necesidad de gobernanza, gestión de riesgos y cumplimiento frente a innovaciones tecnológicas aceleradas.

Una gestión integral madura, por tanto, no adopta marcos por prestigio institucional ni acumula certificaciones como evidencia automática de seguridad. Los selecciona, adapta y articula según objetivos, exposición, obligaciones y capacidades internas. ISO 31000, ISO 27005, NIST RMF, NIST CSF 2.0 y COSO ERM ofrecen lentes diferentes para una misma responsabilidad empresarial. McIntosh et al. (2024) permiten entender que su verdadero valor aparece cuando gobernanza, riesgo, tecnología y cumplimiento permanecen conectados.

1.3. Identificación, análisis y valoración de riesgos digitales y cibernéticos

Identificar riesgos digitales exige mirar la organización más allá del inventario tecnológico. El análisis comienza reconociendo activos, procesos, datos, servicios y dependencias cuya alteración podría afectar objetivos empresariales. También requiere comprender amenazas, vulnerabilidades y posibles consecuencias, pues una debilidad carece de significado suficiente sin relacionarla con aquello que puede comprometer. Aghazadeh Ardebili et al. (2024) destacan que la evaluación del riesgo constituye un componente relevante para fortalecer la resiliencia cibernética en infraestructuras críticas contemporáneas.

La identificación gana profundidad cuando incorpora relaciones entre componentes técnicos, personas, proveedores y procesos operativos. Un servicio aparentemente secundario puede sostener funciones esenciales mediante dependencias poco visibles, mientras una aplicación destacada quizá tenga mecanismos adecuados de redundancia. Conviene, por tanto, evitar conclusiones derivadas únicamente de criticidad técnica. Aghazadeh Ardebili et al. (2024) examinan métodos de evaluación orientados a reconocer amenazas y vulnerabilidades dentro de sistemas complejos, vinculando estos elementos con resiliencia, gobernanza y continuidad operativa institucional.

El análisis transforma los riesgos identificados en escenarios comprensibles para quienes deben decidir. No basta registrar que existe una amenaza; resulta necesario estimar la posibilidad de ocurrencia, las condiciones que facilitarían su materialización y las consecuencias derivadas. Un ataque puede afectar disponibilidad, confidencialidad, integridad o varias dimensiones simultáneamente. Según Aghazadeh Ardebili et al. (2024), los métodos de evaluación cibernética requieren considerar múltiples factores para representar adecuadamente exposiciones que afectan infraestructuras críticas y capacidades de recuperación organizacional.

La valoración incorpora un juicio organizacional sobre la importancia de cada riesgo analizado. Probabilidad e impacto ofrecen referencias útiles, pero adquieren verdadero significado cuando se contrastan con criterios previamente definidos, tolerancias y objetivos empresariales. Dos organizaciones expuestas a una amenaza semejante pueden valorarla de manera diferente debido a sus operaciones y responsabilidades. Aghazadeh Ardebili et al. (2024) vinculan la evaluación del riesgo con estructuras de gobernanza capaces de orientar decisiones destinadas a fortalecer la resiliencia cibernética institucional.

Las matrices de riesgo continúan siendo instrumentos frecuentes porque facilitan conversaciones entre perfiles técnicos y ejecutivos. Sin embargo, sus categorías pueden producir una apariencia de precisión que merece cautela. Clasificar un riesgo como alto, medio o bajo no elimina incertidumbres ni reemplaza el análisis de escenarios. Aghazadeh Ardebili et al. (2024) revisan diversos métodos empleados en evaluación de riesgos cibernéticos, mostrando que cada aproximación presenta características particulares frente a sistemas complejos y requerimientos de resiliencia.

La cuantificación añade otra perspectiva cuando permite expresar consecuencias mediante pérdidas económicas, tiempos de

interrupción u otras magnitudes relevantes. Su utilidad depende de la calidad de los datos y de las premisas empleadas, porque una cifra aparentemente exacta puede ocultar incertidumbre considerable. Los modelos cuantitativos deben apoyar el juicio profesional, no reemplazarlo. Aghazadeh Ardebili et al. (2024) señalan la diversidad metodológica existente para evaluar riesgos y fortalecer decisiones relacionadas con resiliencia de infraestructuras críticas digitalizadas actuales.

Los escenarios cibernéticos permiten conectar amenaza, activo, vulnerabilidad y consecuencia dentro de una narrativa comprensible. Pensar en escenarios obliga a preguntar qué puede ocurrir, mediante qué condiciones y con qué efectos sobre operaciones esenciales. Esa formulación aproxima el análisis técnico a decisiones empresariales concretas. Aghazadeh Ardebili et al. (2024) relacionan los métodos de evaluación con la capacidad de anticipar y gestionar eventos adversos, destacando su aporte al fortalecimiento de la resiliencia en infraestructuras críticas contemporáneas.

La evaluación tampoco debería limitarse al riesgo inherente. Una vez considerados controles existentes, capacidades de detección, respuesta y recuperación, aparece el riesgo residual, cuya aceptación requiere responsabilidad explícita. Esta distinción permite conocer cuánto cambia realmente la exposición después de aplicar medidas de seguridad. En el estudio de Aghazadeh Ardebili et al. (2024), gobernanza, estándares y metodologías de evaluación mantienen una relación estrecha con las capacidades destinadas a sostener resiliencia frente a incidentes cibernéticos graves.

Otro aspecto relevante es la temporalidad. Los riesgos digitales cambian conforme aparecen nuevas vulnerabilidades, proveedores, tecnologías, amenazas y dependencias operativas. Una evaluación realizada meses atrás puede perder vigencia después de una migración tecnológica o modificación significativa del servicio. Por ello, valorar riesgos demanda revisión periódica y

aprendizaje institucional. Aghazadeh Ardebili et al. (2024) presentan la evaluación como parte de una perspectiva amplia de resiliencia, donde métodos, gobernanza y estándares contribuyen a enfrentar entornos cambiantes.

Identificar, analizar y valorar riesgos constituye, en esencia, un proceso de construcción de conocimiento para decidir bajo incertidumbre. Su calidad depende tanto de métodos rigurosos como de conversaciones capaces de conectar tecnología, operación, gobierno y consecuencias empresariales. La organización madura no busca eliminar toda exposición, sino comprenderla y mantenerla dentro de niveles aceptables. Aghazadeh Ardebili et al. (2024) vinculan esta disciplina evaluativa con una resiliencia cibernética orientada a anticipar, resistir y recuperarse ante perturbaciones.

1.4. Apetito de riesgo, tolerancia y umbrales de decisión ejecutiva

El apetito de riesgo expresa la disposición de una organización para asumir incertidumbre mientras persigue objetivos estratégicos y económicos. En materia cibernética, esta definición convierte una discusión aparentemente técnica en una decisión ejecutiva sobre exposición, continuidad y capital. No todas las pérdidas potenciales reciben igual tratamiento. Chong et al. (2025) relacionan la evaluación del riesgo cibernético con decisiones de gestión de capital, ofreciendo una perspectiva cuantitativa para comprender consecuencias financieras derivadas de incidentes digitales relevantes.

Definir el apetito requiere reconocer que asumir riesgo forma parte de la actividad empresarial. Una organización excesivamente conservadora puede limitar innovación, mientras una exposición desmedida amenaza continuidad y estabilidad financiera. Entre ambos extremos existe un espacio deliberado de decisión. Chong et al. (2025) estudian el riesgo cibernético desde la perspectiva del capital necesario para absorber pérdidas, aportando

elementos que permiten vincular incertidumbre tecnológica con recursos financieros destinados a preservar capacidad operativa ante eventos adversos de magnitud.

La tolerancia traduce declaraciones generales de apetito en márgenes observables para gestionar exposiciones concretas. Puede expresarse mediante pérdidas económicas aceptables, duración máxima de interrupciones, cantidad de registros comprometidos o variaciones admisibles respecto de objetivos establecidos. Su utilidad reside en convertir preferencias ejecutivas en referencias para decidir. Chong et al. (2025) muestran que la estimación de pérdidas cibernéticas puede contribuir a determinar necesidades de capital y evaluar niveles de exposición desde una perspectiva financiera empresarial más disciplinada.

Apetito y tolerancia no representan conceptos intercambiables. El primero orienta la disposición general hacia determinada categoría de riesgo; la segunda establece variaciones aceptables alrededor de objetivos específicos. Esta diferencia cobra importancia cuando los equipos deben decidir entre mitigar, transferir, aceptar o evitar exposiciones. Desde una perspectiva económica, Chong et al. (2025) vinculan la medición del riesgo cibernético con decisiones sobre capital, permitiendo interpretar eventos tecnológicos mediante consecuencias financieras relevantes para quienes gobiernan la organización.

Los umbrales de decisión cumplen una función práctica: determinan cuándo una exposición deja de pertenecer al ámbito operativo y requiere atención de niveles superiores. Un incidente potencial cuya pérdida estimada excede determinada cifra puede necesitar aprobación ejecutiva, mientras exposiciones menores permanecen bajo responsabilidad delegada. Chong et al. (2025) aportan métodos para evaluar pérdidas cibernéticas y sus implicaciones de capital, relación que favorece decisiones basadas en magnitud económica y capacidad institucional para absorber eventos adversos sin comprometer estabilidad.

Establecer umbrales también ayuda a evitar decisiones dominadas por percepciones individuales. El riesgo cibernético suele despertar respuestas intensas debido a la incertidumbre, la presión regulatoria y la posible exposición pública. Criterios previamente acordados permiten responder con mayor consistencia cuando ocurre un evento. Chong et al. (2025) analizan distribuciones de pérdidas y requerimientos de capital asociados con riesgo cibernético, aportando fundamentos para evaluar exposiciones mediante métricas económicas que favorecen comparaciones y decisiones ejecutivas mejor informadas institucionalmente.

Figura 3
Apetito, tolerancia y decisión ejecutiva

La relación entre riesgo cibernético y capital adquiere especial relevancia cuando las pérdidas presentan comportamientos difíciles de anticipar mediante promedios históricos. Eventos infrecuentes pueden ocasionar impactos severos, obligando a considerar escenarios extremos dentro de la planificación financiera. Chong et al. (2025) desarrollan una

aproximación orientada a valorar el capital requerido frente a exposiciones cibernéticas, reforzando la necesidad de relacionar métricas técnicas con pérdidas potenciales, capacidad de absorción y decisiones empresariales sobre recursos disponibles para contingencias.

El apetito tampoco permanece invariable. Cambia cuando la empresa modifica su estrategia, entra en nuevos mercados, adopta tecnologías diferentes o enfrenta mayores obligaciones regulatorias. También puede reducirse después de incidentes significativos o aumentar cuando mejoran capacidades de protección y recuperación. Esta naturaleza dinámica demanda revisiones periódicas. Chong et al. (2025) permiten observar que la valoración financiera del riesgo cibernético depende de características de exposición y pérdidas, elementos relevantes para ajustar decisiones de capital a condiciones empresariales cambiantes.

Una declaración de apetito adquiere valor cuando influye realmente en inversiones, excepciones, proyectos y prioridades. Si permanece como documento corporativo apartado de las decisiones cotidianas, su efecto es escaso. Debe orientar conversaciones entre directorio, finanzas, riesgo, tecnología y seguridad. Chong et al. (2025) ofrecen una conexión especialmente útil entre evaluación cibernética y administración de capital, permitiendo que las decisiones sobre exposición digital se expresen mediante variables económicas comprensibles para la alta dirección y órganos de gobierno.

Apetito, tolerancia y umbrales conforman una arquitectura de decisión que transforma incertidumbre digital en responsabilidad ejecutiva. El apetito marca orientación; la tolerancia delimita márgenes; los umbrales establecen momentos de intervención y escalamiento. Juntos permiten decidir qué riesgos aceptar, cuáles reducir y cuánto capital respaldará esas elecciones. Chong et al. (2025) demuestran que evaluar financieramente la

exposición cibernética contribuye a vincular pérdidas potenciales con capital, fortaleciendo decisiones empresariales frente a eventos digitales de elevada severidad.

1.5. Riesgo tecnológico, riesgo operacional y gestión de riesgo de terceros (TPRM/SCRM)

El riesgo tecnológico adquiere significado empresarial cuando una falla, vulnerabilidad o dependencia digital puede alterar servicios, información y objetivos estratégicos. No reside únicamente en servidores, aplicaciones o redes; también aparece en decisiones de arquitectura, obsolescencia, integraciones y concentración de proveedores. La investigación sobre resiliencia de cadenas cibernéticas (Cyber Supply Chain Resilience, 2025) plantea que las dependencias externas amplían la superficie de exposición y requieren enfoques coordinados de gestión apoyados en marcos reconocidos internacionalmente para empresas.

El riesgo operacional mantiene una relación estrecha con el tecnológico porque numerosos procesos empresariales dependen actualmente de plataformas digitales. Una interrupción técnica puede convertirse rápidamente en retrasos, pérdidas económicas, incumplimientos contractuales o deterioro del servicio. La frontera entre ambos riesgos resulta cada vez menos evidente. Cyber Supply Chain Resilience (2025) analiza esta interdependencia al señalar que vulnerabilidades presentes en proveedores y cadenas digitales pueden propagarse hacia organizaciones vinculadas, comprometiendo continuidad, seguridad y capacidad de respuesta operativa.

La gestión de riesgos de terceros, conocida como TPRM, responde a una realidad sencilla: contratar un servicio no transfiere automáticamente la responsabilidad por sus consecuencias. Proveedores tecnológicos, operadores de nube, desarrolladores y prestadores especializados participan en procesos empresariales sensibles. Cada relación introduce dependencias que deben

evaluarse durante su ciclo contractual. Cyber Supply Chain Resilience (2025) destaca que los marcos ISO, NIST y NIS2 aportan orientaciones destinadas a identificar y reducir exposiciones provenientes de terceros digitales relevantes.

SCRM amplía la mirada hacia la cadena de suministro y considera relaciones que pueden extenderse varios niveles más allá del proveedor contratado directamente. Un prestador confiable puede depender, a su vez, de componentes, bibliotecas, infraestructuras o servicios externos cuya vulnerabilidad termine afectando al cliente principal. Cyber Supply Chain Resilience (2025) examina esta dimensión mediante el concepto de resiliencia cibernética de la cadena, destacando que gestionar terceros demanda visibilidad sobre dependencias y mecanismos coordinados de mitigación del riesgo.

TPRM y SCRM comparten objetivos, aunque observan dimensiones parcialmente diferentes. TPRM suele concentrarse en evaluar relaciones individuales con proveedores, mientras SCRM presta mayor atención a dependencias encadenadas, componentes y flujos que atraviesan ecosistemas completos. Ambas perspectivas resultan necesarias en empresas digitalizadas. De acuerdo con Cyber Supply Chain Resilience (2025), la convergencia entre marcos ISO, NIST y disposiciones NIS2 proporciona referencias complementarias para fortalecer controles, gobernanza y resiliencia frente a riesgos procedentes de terceros externos.

Evaluar un proveedor exige ir más allá del cuestionario de seguridad cumplimentado durante la contratación. Importan su arquitectura, prácticas de desarrollo, gestión de vulnerabilidades, continuidad, respuesta ante incidentes y relaciones con otros proveedores. También importa verificar esas capacidades periódicamente. Cyber Supply Chain Resilience (2025) destaca que la gestión efectiva de riesgos en cadenas digitales requiere mecanismos continuos de evaluación y mitigación, pues las condiciones de exposición pueden cambiar durante la relación

entre organizaciones, proveedores y servicios tecnológicos contratados.

La concentración constituye otro riesgo frecuentemente subestimado. Varias unidades empresariales pueden depender del mismo proveedor, plataforma o componente sin que esa exposición agregada resulte evidente para quienes autorizan contratos individuales. Cuando una dependencia compartida falla, el impacto atraviesa procesos que parecían independientes. Cyber Supply Chain Resilience (2025) aborda la necesidad de fortalecer resiliencia frente a riesgos de terceros mediante marcos que favorecen identificación, evaluación y tratamiento coordinado de vulnerabilidades presentes en cadenas de suministro digitales complejas actuales.

Los contratos representan una herramienta importante, aunque insuficiente por sí misma. Cláusulas sobre notificación de incidentes, auditoría, continuidad, protección de datos y subcontratación establecen responsabilidades, pero necesitan acompañarse de supervisión efectiva. Una obligación contractual desconocida durante una crisis aporta escasa protección operativa. Cyber Supply Chain Resilience (2025) muestra que los enfoques regulatorios y normativos contemporáneos conceden importancia creciente a gobernanza, controles y responsabilidades dentro de relaciones con terceros y cadenas digitales sometidas a amenazas cibernéticas persistentes.

La resiliencia exige asumir que algún proveedor puede fallar pese a evaluaciones rigurosas. Por ello, gestionar terceros también significa preparar alternativas, redundancias, mecanismos de recuperación y estrategias de salida. La pregunta relevante no termina en determinar si un proveedor es seguro; debe considerar qué ocurrirá cuando deje de prestar el servicio esperado. Cyber Supply Chain Resilience (2025) relaciona la mitigación del riesgo con capacidades de resiliencia destinadas a mantener operaciones

frente a disrupciones provenientes de cadenas tecnológicas externas.

Integrar riesgo tecnológico, operacional y de terceros permite abandonar visiones fragmentadas de la exposición digital. Una vulnerabilidad técnica puede originarse en un proveedor, propagarse mediante una dependencia y convertirse en interrupción empresarial con consecuencias financieras o regulatorias. Esa cadena causal debe permanecer visible para quienes gobiernan el riesgo. Cyber Supply Chain Resilience (2025) concluye que ISO, NIST y NIS2 ofrecen aproximaciones complementarias para gestionar riesgos cibernéticos de terceros y fortalecer la resiliencia de cadenas digitales interconectadas contemporáneas.

1.6. Del riesgo al control: cómo el riesgo determina el gobierno, la arquitectura y la tecnología

El tránsito del riesgo al control comienza cuando la organización convierte una exposición identificada en una decisión concreta de tratamiento. Conocer vulnerabilidades carece de valor práctico si los hallazgos no modifican prioridades, responsabilidades o inversiones. El control aparece, entonces, como respuesta deliberada frente a una condición de riesgo previamente comprendida. Aflakhah y Soewito (2023) relacionan la evaluación de seguridad de la información con el desarrollo de planes de mitigación, vinculando hallazgos con acciones organizacionales orientadas al tratamiento.

La selección de controles debe responder a la naturaleza y magnitud de la exposición, no a preferencias tecnológicas circunstanciales. Un riesgo elevado sobre información sensible puede requerir medidas preventivas, detectivas y correctivas combinadas, mientras otro escenario admite aceptación documentada. Esta proporcionalidad evita arquitecturas defensivas costosas y desconectadas de necesidades reales. Aflakhah y Soewito

(2023) muestran que COBIT 2019 e ISO 27001 permiten evaluar condiciones de seguridad y estructurar acciones de mejora vinculadas con deficiencias identificadas previamente.

El gobierno interviene cuando determina quién decide, quién responde y bajo qué criterios se acepta una exposición residual. Desde esta perspectiva, el riesgo precede a la estructura de autoridad: establece qué decisiones requieren escalamiento, qué responsabilidades corresponden a cada nivel y qué evidencias deben presentarse. Aflakhah y Soewito (2023) emplean COBIT 2019 para valorar prácticas de seguridad, mostrando la utilidad de marcos de gobierno al identificar brechas y orientar planes destinados a mejorar capacidades institucionales existentes.

La arquitectura empresarial traduce esas decisiones de gobierno en estructuras coherentes de procesos, información, aplicaciones e infraestructura. Cuando el riesgo orienta el diseño, las decisiones arquitectónicas dejan de responder únicamente a eficiencia o rendimiento y consideran también resiliencia, segmentación, redundancia y protección. Una dependencia crítica puede justificar cambios profundos. Aflakhah y Soewito (2023) relacionan los resultados de evaluación con recomendaciones de mitigación, evidenciando que las brechas detectadas pueden transformarse en acciones destinadas a fortalecer seguridad organizacional.

La arquitectura de seguridad ocupa un lugar intermedio entre intención y ejecución. Recibe prioridades derivadas del riesgo y las convierte en patrones, principios y capacidades que posteriormente serán materializados mediante tecnologías. Este orden evita adquirir herramientas antes de comprender qué exposición deben reducir. En el estudio de Aflakhah y Soewito (2023), la evaluación basada en COBIT 2019 e ISO 27001 permite reconocer diferencias entre condiciones existentes y objetivos esperados, proporcionando fundamentos para formular medidas de mitigación pertinentes.

La tecnología aparece después de comprender el riesgo, definir responsabilidades y establecer criterios arquitectónicos. Este orden puede parecer incómodo en organizaciones acostumbradas a iniciar proyectos mediante productos, pero evita que la herramienta determine la estrategia. Autenticación, cifrado, monitoreo o segmentación tienen sentido cuando responden a escenarios definidos. Aflakhah y Soewito (2023) evidencian que la mejora de seguridad requiere partir de evaluaciones estructuradas para determinar brechas y posteriormente desarrollar recomendaciones destinadas a reducir exposiciones identificadas en la organización.

No todo riesgo requiere incorporar un nuevo control. En ocasiones, los controles existentes necesitan mayor madurez, mejor configuración, responsables claros o evidencias confiables de funcionamiento. Esta distinción resulta importante porque evita confundir acumulación tecnológica con reducción efectiva de exposición. Aflakhah y Soewito (2023) analizan niveles de capacidad mediante COBIT 2019 y los relacionan con requisitos de ISO 27001, permitiendo identificar áreas donde las prácticas existentes requieren fortalecimiento antes que una expansión indiscriminada de herramientas defensivas adicionales.

El control tampoco debe evaluarse por su mera existencia documental. Una política aprobada, un procedimiento publicado o una herramienta instalada pueden ofrecer una sensación engañosa de protección si su eficacia no se verifica. La pregunta relevante es cuánto reduce la exposición y qué riesgo permanece después de operar. Aflakhah y Soewito (2023) utilizan evaluación de capacidades y análisis de brechas para desarrollar un plan de mitigación, vinculando el estado observado con mejoras orientadas hacia niveles esperados de seguridad.

La trazabilidad entre riesgo y control fortalece las decisiones ejecutivas porque permite explicar por qué existe cada inversión defensiva y qué consecuencia empresarial pretende

reducir. También facilita revisar controles cuando cambia la exposición, evitando conservar medidas que perdieron pertinencia. Aflakhah y Soewito (2023) demuestran que comparar condiciones actuales con niveles deseados permite formular recomendaciones específicas de mitigación. Esta lógica convierte la evaluación en un mecanismo para priorizar mejoras y asignar esfuerzos según necesidades de seguridad previamente reconocidas.

Figura 4
Del riesgo a los controles empresariales

Cuando el riesgo gobierna la elección del control, gobierno, arquitectura y tecnología dejan de operar como capas separadas. El gobierno establece responsabilidades y criterios; la arquitectura organiza capacidades; la tecnología materializa medidas; la evaluación verifica resultados. Entre estas dimensiones existe una relación continua de retroalimentación. Aflakhah y Soewito (2023) muestran que combinar COBIT 2019 con ISO 27001 facilita pasar de la evaluación de seguridad hacia planes de mitigación, conectando brechas observadas con acciones de mejora organizacional.

1.7. Cuantificación del riesgo (FAIR) y su traducción a métricas de impacto financiero y de negocio

Cuantificar el riesgo cibernético responde a una necesidad empresarial concreta: expresar incertidumbre mediante magnitudes que permitan comparar decisiones, inversiones y pérdidas potenciales. FAIR aporta una estructura para representar el riesgo en términos económicos, alejándose de categorías cualitativas excesivamente amplias. La conversación cambia cuando una exposición deja de describirse mediante colores y comienza a estimarse monetariamente. Seid et al. (2024) presentan FAIR como un enfoque aplicable a la cuantificación del riesgo de ciberseguridad en organizaciones del sector logístico.

El modelo FAIR descompone el riesgo mediante factores que permiten comprender con mayor precisión la frecuencia probable de eventos de pérdida y la magnitud de sus consecuencias. Esta separación ayuda a evitar juicios generales donde probabilidad e impacto terminan mezclados bajo una categoría común. Seid et al. (2024) aplican esta lógica de cuantificación al ámbito logístico, mostrando que el análisis estructurado puede transformar información sobre amenazas y pérdidas en estimaciones útiles para decisiones relacionadas con ciberseguridad empresarial.

La frecuencia de eventos de pérdida permite examinar cuántas veces podría materializarse un escenario dentro de determinado periodo. No equivale simplemente a contar ataques, pues muchos intentos nunca generan consecuencias económicas relevantes. FAIR distingue factores relacionados con amenazas, contacto, acción y vulnerabilidad para construir estimaciones mejor fundamentadas. En su investigación, Seid et al. (2024) emplean el modelo para cuantificar escenarios cibernéticos, demostrando su utilidad al representar incertidumbre mediante variables susceptibles de análisis económico y probabilístico sistemático.

La magnitud de pérdida constituye la segunda gran dimensión del análisis. Un incidente puede generar costos de respuesta, interrupción operativa, recuperación tecnológica, obligaciones legales, afectación reputacional y pérdidas derivadas de menor productividad. Traducir estas consecuencias a valores económicos permite observar impactos que las escalas cualitativas frecuentemente comprimen. Seid et al. (2024) destacan que FAIR facilita estimaciones monetarias del riesgo, ofreciendo información con mayor capacidad para respaldar decisiones empresariales relacionadas con exposición y tratamiento del ciberriesgo.

Una ventaja relevante de FAIR reside en trabajar explícitamente con incertidumbre. Las estimaciones cibernéticas rara vez disponen de datos perfectos, especialmente ante eventos poco frecuentes o tecnologías recientes. En lugar de ocultar esa limitación, pueden utilizarse rangos y distribuciones para representar diferentes resultados posibles. Seid et al. (2024) muestran mediante su aplicación de FAIR que la cuantificación puede estructurar información disponible y convertirla en estimaciones económicas, aun cuando el análisis dependa de variables sujetas a incertidumbre considerable.

Las simulaciones probabilísticas fortalecen este enfoque al permitir observar múltiples combinaciones posibles entre frecuencia y magnitud de pérdida. El resultado no necesita reducirse a una cifra aparentemente exacta; puede presentarse como distribución, percentiles o intervalos relevantes para decidir. Esta lectura ofrece una visión más rica de la exposición. Seid et al. (2024) utilizan FAIR para analizar cuantitativamente riesgos cibernéticos, mostrando el potencial de métodos probabilísticos para respaldar valoraciones económicas en entornos empresariales vinculados con operaciones logísticas digitales.

La traducción financiera modifica también la conversación con la alta dirección. Expresar que una vulnerabilidad posee severidad elevada aporta información técnica; estimar pérdidas

anuales probables permite compararla con inversiones, seguros, reservas y otras exposiciones empresariales. El riesgo entra entonces en un lenguaje compartido con finanzas. Seid et al. (2024) señalan que la cuantificación mediante FAIR puede apoyar decisiones al proporcionar estimaciones monetarias que facilitan comprender la relevancia económica de escenarios de ciberseguridad dentro de organizaciones logísticas modernas.

La cuantificación resulta especialmente útil al evaluar controles. Si una medida requiere determinada inversión, FAIR permite estimar la reducción esperada de frecuencia, magnitud o ambas, facilitando comparar el costo del tratamiento con la exposición evitada. No convierte automáticamente la decisión en una ecuación financiera, pero aporta disciplina. Seid et al. (2024) evidencian que el enfoque cuantitativo ayuda a representar económicamente escenarios de riesgo, creando una base más informada para valorar alternativas de mitigación y asignación de recursos organizacionales.

FAIR tampoco elimina la necesidad de criterio profesional. Los resultados dependen de escenarios bien formulados, datos razonables y estimaciones defendibles. Una cuantificación construida sobre premisas débiles puede producir cifras elegantes con escaso valor decisional. Por ello, la transparencia metodológica resulta tan importante como el resultado numérico. Seid et al. (2024) muestran que aplicar FAIR requiere identificar componentes del riesgo y analizarlos sistemáticamente, favoreciendo una comprensión estructurada de las pérdidas potenciales derivadas de eventos cibernéticos relevantes.

La contribución más significativa de la cuantificación consiste en conectar ciberseguridad con decisiones de negocio mediante una unidad comprensible: el impacto económico. FAIR permite comparar escenarios, priorizar tratamientos, evaluar inversiones y comunicar incertidumbre sin reducir el riesgo a etiquetas generales. Seid et al. (2024) demuestran su aplicabilidad

para cuantificar exposiciones cibernéticas en el sector logístico, ofreciendo una vía para convertir escenarios técnicos en información financiera capaz de respaldar decisiones sobre protección, resiliencia y recursos empresariales.

1.8. Monitoreo continuo, evaluación de postura y actualización dinámica del perfil de riesgo

El riesgo digital cambia con una velocidad que vuelve insuficiente cualquier evaluación concebida como fotografía permanente. Nuevos dispositivos, identidades, vulnerabilidades y patrones de acceso modifican diariamente la exposición empresarial. El monitoreo continuo responde a esta realidad mediante observación frecuente de señales relevantes para la seguridad. Goshikonda y Pulipati (2024) plantean una evaluación continua apoyada en arquitectura zero trust y aprendizaje automático, donde la información procedente de dispositivos y comportamientos alimenta valoraciones dinámicas del riesgo cibernético organizacional.

La telemetría constituye una fuente esencial para mantener vigente el perfil de riesgo. Registros de autenticación, actividad de red, configuraciones, eventos de seguridad y comportamiento de usuarios proporcionan señales que permiten detectar variaciones significativas. Su verdadero valor aparece cuando los datos dejan de permanecer dispersos y participan en procesos de evaluación. Goshikonda y Pulipati (2024) relacionan la recopilación continua de información con mecanismos inteligentes capaces de evaluar condiciones cambiantes y ajustar puntuaciones de riesgo durante la operación tecnológica.

La postura de un dispositivo tampoco permanece estable durante toda su vida operativa. Un equipo inicialmente confiable puede acumular vulnerabilidades, perder actualizaciones, modificar configuraciones o presentar comportamientos anómalos. Evaluarlo únicamente durante su incorporación deja una brecha

temporal relevante. Goshikonda y Pulipati (2024) consideran la postura de los dispositivos dentro de un modelo de evaluación continua, permitiendo que las decisiones de acceso respondan a condiciones observadas y no exclusivamente a autorizaciones establecidas con anterioridad por sistemas corporativos.

La analítica de comportamiento aporta otra dimensión porque permite observar variaciones respecto de patrones habituales. Una identidad legítima puede realizar acciones atípicas debido a credenciales comprometidas, abuso interno o automatizaciones inesperadas. El análisis continuo ayuda a distinguir esas desviaciones y convertirlas en señales de riesgo. Goshikonda y Pulipati (2024) incorporan inteligencia basada en aprendizaje automático para analizar comportamientos, fortaleciendo mecanismos capaces de modificar valoraciones conforme aparecen nuevas evidencias durante la interacción con recursos digitales empresariales.

Zero trust ofrece una base arquitectónica compatible con esta visión dinámica. La confianza deja de concederse de manera permanente por ubicación, pertenencia o autenticación previa y pasa a verificarse durante las interacciones. Cada solicitud puede considerar identidad, dispositivo, comportamiento y nivel de riesgo observado. Goshikonda y Pulipati (2024) articulan principios zero trust con evaluación continua y aprendizaje automático, proponiendo decisiones de seguridad adaptativas que responden a cambios detectados mediante información operativa generada en tiempo real.

La puntuación dinámica permite convertir señales dispersas en una representación actualizada de exposición. Su propósito no consiste en producir un número incuestionable, sino facilitar decisiones consistentes ante variaciones observadas. Una puntuación creciente puede activar autenticación adicional, restringir privilegios o elevar un evento para revisión. Goshikonda y Pulipati (2024) proponen mecanismos de valoración continua

donde diferentes indicadores alimentan cálculos de riesgo capaces de modificar decisiones de acceso y protección según condiciones presentes del entorno digital corporativo.

Actualizar dinámicamente el perfil de riesgo exige conectar observaciones técnicas con escenarios empresariales. Miles de alertas carecen de utilidad ejecutiva cuando no permiten distinguir qué activos, servicios o procesos enfrentan mayor exposición. El monitoreo debe ayudar a priorizar, no incrementar ruido. Goshikonda y Pulipati (2024) muestran que combinar telemetría, evaluación de postura y analítica inteligente permite construir valoraciones adaptativas, proporcionando información para responder con mayor rapidez ante cambios que alteran las condiciones de seguridad organizacional existentes.

La automatización resulta necesaria cuando el volumen y velocidad de señales superan la capacidad de revisión humana. Sin embargo, automatizar decisiones de riesgo requiere reglas, supervisión y mecanismos para revisar resultados inesperados. Los modelos pueden identificar patrones, pero necesitan gobernanza para conservar trazabilidad y responsabilidad. Goshikonda y Pulipati (2024) emplean aprendizaje automático como componente de evaluación continua, destacando su capacidad para procesar información conductual y apoyar respuestas dinámicas ante variaciones detectadas en ambientes digitales complejos y distribuidos.

El monitoreo continuo modifica también la función de las evaluaciones periódicas. Estas conservan valor para revisiones estratégicas, auditorías y decisiones de gobierno, pero dejan de ser la única fuente para comprender exposición. La evidencia operativa permite actualizar apreciaciones entre ciclos formales. Goshikonda y Pulipati (2024) presentan un modelo donde la evaluación permanece activa mediante observación constante, facilitando que el nivel de riesgo refleje cambios recientes en dispositivos,

comportamientos y condiciones de acceso a recursos empresariales sensibles.

Una organización madura trata su perfil de riesgo como un instrumento vivo. Cada vulnerabilidad relevante, cambio arquitectónico, comportamiento anómalo o modificación de postura puede alterar prioridades y decisiones de protección. La evaluación continua convierte esas variaciones en conocimiento accionable antes de la siguiente revisión formal. Goshikonda y Pulipati (2024) vinculan zero trust, telemetría y aprendizaje automático para construir valoraciones dinámicas, ofreciendo una perspectiva donde la gestión del riesgo acompaña permanentemente la operación digital y sus transformaciones cotidianas.

Tabla 1

Componentes de la gestión integral del riesgo digital y su aplicación empresarial

Componente de gestión	**Aplicación en la gestión empresarial del riesgo digital**
Riesgo de negocio como punto de partida	Vincula las exposiciones digitales con objetivos estratégicos, continuidad operativa, reputación, obligaciones regulatorias y creación de valor, antes de determinar controles o soluciones tecnológicas.
Marcos de gestión de riesgo	ISO 31000, ISO 27005, NIST RMF, NIST CSF 2.0 y COSO ERM proporcionan perspectivas complementarias para gobernar, identificar, evaluar, tratar y supervisar riesgos empresariales y cibernéticos.
Identificación, análisis y valoración	Reconoce activos, amenazas, vulnerabilidades, dependencias y escenarios de pérdida; posteriormente estima probabilidad, impacto y nivel de exposición para establecer prioridades de tratamiento.

Componente de gestión	Aplicación en la gestión empresarial del riesgo digital
Apetito, tolerancia y umbrales	Determina la exposición que la organización está dispuesta a asumir, los márgenes aceptables y los niveles que requieren escalamiento, intervención o decisión ejecutiva.
Riesgo tecnológico y operacional	Relaciona fallas tecnológicas, vulnerabilidades y dependencias digitales con interrupciones operativas, pérdidas económicas, incumplimientos y afectaciones sobre servicios empresariales.
TPRM y SCRM	Gestiona exposiciones derivadas de proveedores, servicios externos, componentes tecnológicos y cadenas de suministro, considerando dependencias directas e indirectas durante todo el ciclo de relación.
Riesgo, gobierno y arquitectura	Convierte exposiciones priorizadas en responsabilidades de gobierno, principios arquitectónicos, capacidades de seguridad y controles proporcionales al riesgo empresarial identificado.
Cuantificación mediante FAIR	Expresa escenarios cibernéticos mediante frecuencia y magnitud de pérdida, facilitando estimaciones económicas y comparaciones entre exposición, costo de controles y decisiones de inversión.
Monitoreo continuo	Utiliza telemetría, postura de dispositivos, comportamiento y señales operativas para detectar variaciones relevantes en la exposición durante la operación digital.
Perfil dinámico de riesgo	Actualiza prioridades y niveles de exposición ante cambios tecnológicos, nuevas amenazas, vulnerabilidades, incidentes, modificaciones operativas y variaciones en dependencias empresariales.

Nota. TPRM = Third-Party Risk Management; SCRM = Supply Chain Risk Management; FAIR = Factor Analysis of Information Risk; RMF = Risk Management Framework; CSF = Cybersecurity

Framework; ERM = Enterprise Risk Management. Elaboración basada en Saeed et al. (2023), Aflakhah y Soewito (2023), Goshikonda y Pulipati (2024), McIntosh et al. (2024), Seid et al. (2024), Aghazadeh Ardebili et al. (2024), Chong et al. (2025) y Cyber Supply Chain Resilience (2025).

Capítulo 2:

Gobierno Digital, Gobernanza de la IA y Ciberseguridad Estratégica

La transformación digital ha modificado la relación entre tecnología, autoridad y responsabilidad empresarial. Ya no resulta suficiente administrar infraestructura, aprobar inversiones o verificar controles mediante ciclos rígidos. Las organizaciones operan entre datos, plataformas, inteligencia artificial y dependencias digitales que alteran continuamente sus perfiles de riesgo. Levstek et al. (2022) plantean que el gobierno estratégico de TI necesita capacidad adaptativa, pues los mecanismos empleados adquieren distinta relevancia según necesidades, capacidades y etapas organizacionales. Gobernar exige, entonces, criterio y aprendizaje permanente.

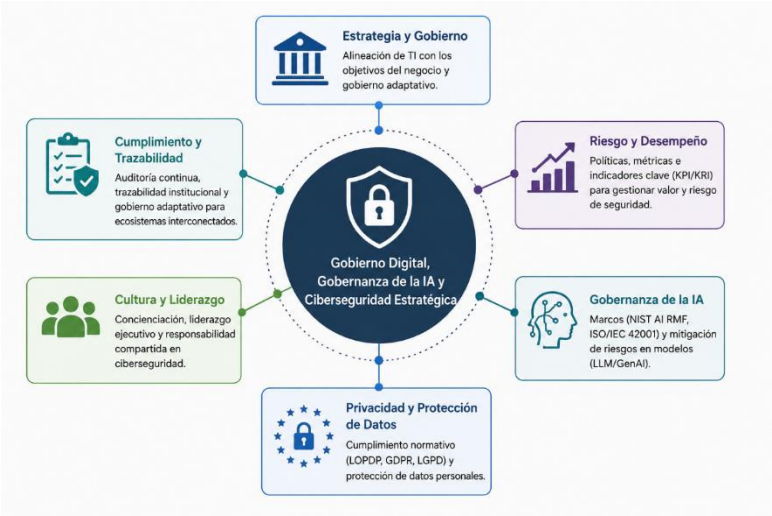
Esta evolución también modifica el sentido práctico de los marcos de referencia. COBIT 2019, ISO/IEC 27001:2022 y las propuestas del NIST aportan lenguajes complementarios para organizar responsabilidades, riesgos, controles y capacidades institucionales. Arellano et al. (2023), mediante la aplicación de COBIT 2019, muestran que evaluar procesos permite identificar brechas y orientar acciones de mejora. El valor del marco no reside en acumular requisitos, sino en convertir principios estructurados en decisiones pertinentes, verificables y vinculadas con prioridades empresariales.

Sin embargo, ningún esquema de gobierno alcanza verdadera influencia cuando la ciberseguridad permanece confinada al departamento tecnológico. La exposición digital atraviesa operaciones, reputación, continuidad, regulación e inversiones; por ello, necesita formar parte de las conversaciones donde se decide el rumbo empresarial. Gale et al. (2022) destacan que la supervisión desde la Junta Directiva requiere información apropiada, responsabilidades claras y capacidades suficientes para interpretar el riesgo cibernético. El lenguaje técnico debe transformarse, entonces, en lenguaje de decisión ejecutiva.

Esa conversación directiva necesita evidencia. Políticas, métricas, indicadores de desempeño y señales de riesgo permiten

observar si los recursos destinados a seguridad producen resultados y si la exposición permanece dentro de niveles aceptables. Bhol et al. (2023) desarrollan una taxonomía destinada a ordenar métricas de ciberseguridad y valorar su fortaleza desde diferentes dimensiones. Medir, sin embargo, no equivale a gobernar. Una cifra adquiere significado cuando orienta decisiones, revela tendencias y permite relacionar seguridad con valor empresarial.

Figura 5
Gobierno digital y ciberseguridad estratégica



La expansión de la inteligencia artificial generativa agrega otra dimensión al gobierno digital. Los modelos lingüísticos pueden acelerar procesos, ampliar capacidades analíticas y transformar servicios, pero también introducen riesgos vinculados con datos, sesgos, respuestas incorrectas, seguridad y dependencia tecnológica. McIntosh et al. (2024) examinan diversos marcos aplicables a la comercialización de grandes modelos lingüísticos y encuentran coberturas diferenciadas frente al riesgo y cumplimiento. NIST AI RMF e ISO/IEC 42001 ofrecen referentes para institucionalizar responsabilidades y controles.

A medida que datos y algoritmos adquieren mayor presencia en las decisiones organizacionales, la privacidad deja de ser una cuestión jurídica separada de la estrategia tecnológica. En Ecuador, la LOPDP configura derechos, obligaciones y principios que demandan incorporar protección de datos dentro de procesos y sistemas. Molina-Natib y Pachano-Zurita (2025) advierten que la eficacia normativa depende también de transparencia, fiscalización y cultura jurídica. La comparación con GDPR y LGPD permite comprender una convergencia internacional orientada hacia responsabilidad verificable.

Pero las políticas mejor redactadas pierden eficacia cuando las conductas cotidianas contradicen aquello que la organización declara proteger. La cultura de ciberseguridad se construye mediante decisiones repetidas, ejemplos directivos, aprendizaje y responsabilidades distribuidas. Aksoy (2024) vincula el desarrollo de una cultura orientada a seguridad con organizaciones capaces de resistir mejor los ataques cibernéticos. El liderazgo ejecutivo adquiere aquí especial relevancia: aquello que los dirigentes preguntan, financian, practican y reconocen termina modelando las prioridades colectivas.

La responsabilidad compartida tampoco elimina la necesidad de trazabilidad. En ecosistemas formados por proveedores, plataformas, servicios en nube y múltiples actores, resulta indispensable reconstruir decisiones, verificar controles y conservar evidencia confiable. Saveljeva y Volkova (2025) relacionan la confianza digital con dimensiones como gobernanza, seguridad, transparencia, cumplimiento y auditabilidad. Desde esta perspectiva, la auditoría continua adquiere una función más amplia que verificar requisitos: permite aprender de desviaciones, ajustar mecanismos y sostener rendición de cuentas ante relaciones digitales crecientemente interdependientes.

Vistas en conjunto, estas dimensiones revelan una transformación profunda del gobierno corporativo.

Adaptabilidad, marcos de referencia, supervisión ejecutiva, indicadores, inteligencia artificial, privacidad, cultura y auditabilidad ya no pueden administrarse mediante iniciativas desconectadas. Levstek et al. (2022) resaltan el carácter situacional de diversos mecanismos de gobierno, mientras Gale et al. (2022) enfatizan la necesidad de fortalecer capacidades directivas para supervisar riesgos cibernéticos. Ambas perspectivas convergen en una idea: gobernar tecnología requiere coordinación institucional y juicio estratégico.

Este capítulo aborda, por tanto, el gobierno digital como una capacidad organizacional que conecta estrategia, responsabilidad, seguridad, inteligencia artificial y confianza. McIntosh et al. (2024) evidencian que los marcos disponibles presentan fortalezas diferentes frente a tecnologías generativas, mientras Saveljeva y Volkova (2025) muestran que la confianza digital depende de múltiples dimensiones interrelacionadas. La empresa inteligente necesita gobernar esa complejidad con evidencia, aprendizaje y responsabilidad compartida, preservando capacidad de adaptación sin renunciar a principios institucionales verificables.

2.1. Evolución del gobierno de TI hacia modelos organizacionales inteligentes y adaptativos

La evolución del gobierno de TI refleja un cambio profundo en la manera de entender la relación entre tecnología, estrategia y dirección empresarial. Durante años, muchas organizaciones privilegiaron estructuras normativas concebidas para mantener control, uniformidad y previsibilidad. Sin embargo, la digitalización ha vuelto insuficiente esa lógica cuando las decisiones tecnológicas modifican productos, procesos y relaciones competitivas. Levstek, Pucihar y Hovelja (2022) plantean que la gobernanza requiere enfoques adaptativos capaces de responder a necesidades empresariales cambiantes.

Este desplazamiento hacia modelos adaptativos parte de reconocer que los mecanismos de gobierno no poseen idéntico valor en todas las organizaciones ni durante todas sus etapas. La pertinencia de estructuras, procesos y relaciones depende de condiciones específicas, capacidades disponibles y prioridades estratégicas. Levstek et al. (2022) encontraron que una proporción relevante de los mecanismos analizados presentaba carácter situacional. Tal hallazgo cuestiona la aplicación rígida de marcos universales y favorece configuraciones sensibles a necesidades reales empresariales.

La organización inteligente requiere que el gobierno de TI abandone una visión centrada exclusivamente en supervisar recursos tecnológicos. Su función adquiere una dimensión estratégica cuando articula inversiones, capacidades digitales, riesgos y objetivos de negocio dentro de decisiones compartidas. En esta transición, gobernar significa aprender institucionalmente. Levstek et al. (2022) señalan que la tecnología puede influir directa e indirectamente sobre el desempeño, razón por la cual su gobierno debe vincularse con la creación de valor empresarial.

La adaptabilidad organizacional tampoco equivale a improvisación. Requiere criterios que permitan determinar qué mecanismos conviene activar, fortalecer o reducir según la situación de la empresa. Esta perspectiva introduce una disciplina distinta: observar necesidades, evaluar capacidades y ajustar prácticas sin convertir el marco de gobierno en una carga administrativa. Para Levstek et al. (2022), los modelos tradicionales pueden resultar complejos y costosos para empresas medianas y pequeñas, especialmente cuando demandan recursos que exceden sus posibilidades operativas.

Un rasgo de los modelos inteligentes reside en la integración entre estructuras formales y mecanismos relacionales. Comités, responsabilidades y políticas conservan importancia, pero su eficacia depende de vínculos que faciliten entendimiento de

dirección, negocio y tecnología. La investigación de Levstek et al. (2022) destaca el valor de la comunicación informal, el liderazgo de TI y la comprensión compartida de objetivos. En práctica, decisiones sensibles maduran primero mediante conversaciones que después adquieren forma institucional y trazabilidad.

La inteligencia organizacional descansa en la capacidad directiva para interpretar la tecnología más allá de su dimensión técnica. Cuando la alta dirección comprende implicaciones estratégicas, riesgos y posibilidades digitales, el gobierno deja de operar como instancia periférica. Levstek et al. (2022) advierten que las competencias de TI en niveles superiores resultan relevantes durante determinadas fases de construcción de la gobernanza. Esa competencia favorece decisiones informadas y una relación equilibrada entre autoridad corporativa y conocimiento especializado.

Desde esta perspectiva, la madurez del gobierno de TI no debería medirse por la cantidad de mecanismos implantados, sino por su pertinencia y capacidad para producir decisiones coherentes. La organización puede acumular controles, comités y procedimientos sin mejorar su dirección tecnológica. El planteamiento adaptativo cambia la pregunta: interesa saber qué mecanismo aporta valor en situación determinada. Levstek et al. (2022) sostienen que mecanismos estratégicos varían en importancia durante implementación y uso dentro de la empresa.

La transición hacia organizaciones adaptativas exige reconocer que el gobierno de TI se desarrolla en el tiempo. Ciertas estructuras son decisivas al iniciar la construcción institucional, mientras otras adquieren relevancia cuando la relación entre negocio y tecnología alcanza mayor madurez. Levstek et al. (2022) observaron que la integración de la gobernanza y estructuras organizativas de TI tienen importancia situacional. Esta temporalidad convierte el gobierno en una arquitectura dinámica,

susceptible de revisión conforme cambian prioridades empresariales.

Esta concepción cobra especial relevancia ante la expansión de inteligencia artificial, automatización y servicios digitales, pues las decisiones tecnológicas penetran áreas separadas. El gobierno de TI necesita entonces funcionar como sistema de coordinación estratégica, capaz de distribuir responsabilidades y mantener coherencia entre innovación, riesgo y desempeño. Aunque Levstek et al. (2022) estudian empresas medianas y pequeñas, su enfoque contingente aporta una idea transferible: la gobernanza efectiva debe guardar correspondencia con necesidades y capacidades organizacionales concretas.

Avanzar hacia modelos inteligentes implica concebir el gobierno de TI como una capacidad adaptativa de dirección y aprendizaje. La organización madura no replica mecánicamente marcos externos; selecciona mecanismos, evalúa resultados y reajusta su arquitectura de gobierno con criterio estratégico propio. Levstek et al. (2022) ofrecen evidencia que respalda esta orientación contingente y cuestiona la universalidad de mecanismos. Bajo esta mirada, gobernar tecnología significa preservar dirección, responsabilidad y valor mientras la empresa transforma sus capacidades digitales.

2.2. Marcos de referencia de gobierno de TI (COBIT 2019, ISO/IEC 27001:2022, NIST) en la práctica

La aplicación práctica de marcos de gobierno de TI exige traducir principios, controles y objetivos en decisiones comprensibles para la dirección. COBIT 2019 ofrece una arquitectura orientada al gobierno y la gestión, mientras ISO/IEC 27001:2022 estructura la seguridad mediante un sistema de gestión y NIST aporta guías para administrar riesgos cibernéticos. Arellano et al. (2023) evidencian que COBIT puede apoyar diagnósticos institucionales, identificar brechas y orientar mejoras vinculadas

con necesidades organizacionales concretas, medibles y sostenibles.

En la práctica, COBIT 2019 adquiere valor cuando deja de percibirse como un catálogo distante y se convierte en instrumento para ordenar responsabilidades, procesos y prioridades. Su aplicación permite observar la organización desde objetivos de gobierno y gestión, estableciendo relaciones entre tecnología y desempeño institucional. Arellano et al. (2023) muestran que evaluar procesos mediante este marco facilita reconocer niveles de capacidad y áreas que requieren intervención, aportando criterios verificables para orientar decisiones de mejora tecnológica.

ISO/IEC 27001:2022 introduce una perspectiva complementaria al concentrarse en la gestión sistemática de la seguridad de la información. Su utilidad práctica reside en organizar políticas, responsabilidades, evaluación de riesgos, tratamiento y mejora continua dentro de una estructura auditable. Frente a COBIT 2019, que ofrece una visión amplia del gobierno tecnológico, esta norma profundiza la disciplina de seguridad. La experiencia documentada por Arellano et al. (2023) permite apreciar la importancia de institucionalizar prácticas mediante criterios evaluables.

NIST aporta otra capa de utilidad al gobierno tecnológico mediante orientaciones centradas en identificación, protección, detección, respuesta y recuperación frente al riesgo cibernético. Su lenguaje favorece conversaciones entre especialistas, responsables operativos y directivos, algo valioso cuando la seguridad necesita incorporarse a decisiones empresariales. En consonancia con Arellano et al. (2023), disponer de referentes estructurados permite reconocer brechas con mayor precisión y establecer prioridades de intervención, evitando que la gestión tecnológica dependa únicamente de percepciones dispersas.

La convivencia de COBIT 2019, ISO/IEC 27001:2022 y NIST no debería entenderse como una competencia entre marcos. Cada referente responde a una función particular y puede articularse con los demás mediante criterios de gobierno, riesgo, control y desempeño. COBIT ayuda a ordenar objetivos y responsabilidades; ISO/IEC 27001:2022 formaliza la gestión de seguridad; NIST facilita organizar capacidades cibernéticas. Arellano et al. (2023) destacan que la evaluación estructurada permite establecer oportunidades de mejora con fundamento institucional verificable.

Una implementación efectiva comienza por comprender la realidad organizacional antes de adoptar controles o procesos muy extensamente. La práctica demuestra que un marco adquiere sentido cuando sus componentes responden a prioridades verificables, recursos disponibles y responsabilidades definidas. Arellano et al. (2023) aplican COBIT 2019 para evaluar procesos de TI en una institución educativa, mostrando que el diagnóstico puede revelar diferencias entre capacidad existente y nivel esperado. Esa brecha ofrece una base concreta para planificar mejoras.

El valor de estos referentes también depende de la participación directiva. Ningún marco transforma la gestión tecnológica cuando permanece confinado al departamento de TI o se reduce a documentación para auditorías. COBIT 2019 demanda claridad sobre responsabilidades; ISO/IEC 27001:2022 requiere compromiso con la gestión de riesgos; NIST favorece una visión compartida de capacidades cibernéticas. Arellano et al. (2023) permiten advertir que evaluar procesos brinda información relevante para priorizar acciones y fortalecer decisiones institucionales mejor fundamentadas.

En organizaciones educativas, empresariales o públicas, la adopción de marcos requiere proporcionalidad. No todas las prácticas necesitan implantarse con idéntica profundidad ni al mismo ritmo. Conviene seleccionar aquellas que respondan a

riesgos, objetivos y capacidades institucionales, manteniendo trazabilidad sobre las decisiones adoptadas. El estudio de Arellano et al. (2023) refleja esta orientación al emplear COBIT 2019 como herramienta diagnóstica, desde la cual pueden definirse mejoras graduales sin convertir el gobierno tecnológico en burocracia institucional excesiva.

Figura 6

Integración práctica de marcos de gobierno de TI

La integración operativa puede materializarse mediante un mapa de correspondencias entre objetivos de COBIT, requisitos de ISO/IEC 27001:2022 y funciones de NIST. Ese ejercicio reduce duplicidades, clarifica evidencias y permite que auditoría, seguridad y dirección trabajen sobre una arquitectura común. Arellano et al. (2023) resaltan la utilidad de identificar procesos prioritarios y valorar su capacidad. Trasladada a un esquema integrado, esa lógica favorece inversiones mejor justificadas y controles vinculados con resultados institucionales observables y medibles.

En términos de madurez, la práctica responsable consiste en utilizar los marcos como instrumentos de aprendizaje organizacional y no como listas destinadas al cumplimiento mecánico. COBIT 2019 aporta dirección; ISO/IEC 27001:2022 disciplina la gestión de seguridad; NIST facilita estructurar la respuesta ante riesgos cibernéticos. Arellano et al. (2023) demuestran que una evaluación basada en COBIT permite convertir hallazgos en oportunidades de mejora, fortaleciendo progresivamente el gobierno de TI y su aporte estratégico institucional y verificable.

2.3. Integración de la ciberseguridad en la estrategia corporativa, reporting a la Junta Directiva y comités ejecutivos

La integración de la ciberseguridad en la estrategia corporativa comienza cuando deja de tratarse como una responsabilidad confinada al área técnica y pasa a formar parte de las decisiones que determinan continuidad, inversión, reputación y crecimiento. La Junta Directiva ocupa una posición decisiva en este tránsito, pues debe relacionar exposición digital con objetivos empresariales. Gale, Bongiovanni y Slapničar (2022) destacan que la supervisión desde el directorio requiere capacidades que permitan interpretar adecuadamente riesgos cibernéticos relevantes.

Llevar la ciberseguridad al espacio directivo implica modificar el lenguaje con que se presentan sus riesgos. Los indicadores puramente técnicos pueden resultar insuficientes para quienes deben decidir sobre inversiones, prioridades y exposición empresarial. Conviene traducir vulnerabilidades, incidentes y amenazas en posibles efectos financieros, operativos, regulatorios y reputacionales. Gale et al. (2022) identifican dificultades relacionadas con el conocimiento especializado dentro de los

directorios, una condición que puede limitar la calidad de la supervisión y del debate estratégico corporativo.

El reporting dirigido a la Junta requiere selección, claridad y sentido estratégico. Una abundancia de métricas puede transmitir actividad sin revelar verdadera exposición al riesgo. Por ello, los informes ejecutivos deberían vincular indicadores de seguridad con activos relevantes, tolerancia al riesgo, continuidad operativa y prioridades corporativas. Gale et al. (2022) señalan que la información disponible para los miembros del directorio influye en su capacidad de ejercer supervisión, formular preguntas pertinentes y comprender las consecuencias empresariales asociadas.

La frecuencia del reporting también merece atención. Informar sobre ciberseguridad únicamente después de un incidente reduce la capacidad preventiva del gobierno corporativo y convierte al directorio en receptor tardío de acontecimientos. Una práctica más madura establece ciclos periódicos de revisión, acompañados por mecanismos extraordinarios ante variaciones significativas del riesgo. Desde la perspectiva desarrollada por Gale et al. (2022), la gobernanza efectiva requiere que los directorios mantengan participación sostenida y dispongan de información suficiente para ejercer supervisión responsable.

Los comités ejecutivos cumplen una función de enlace entre orientación estratégica y ejecución cotidiana. En ellos convergen decisiones sobre tecnología, operaciones, finanzas, cumplimiento, talento y continuidad empresarial, áreas profundamente relacionadas con la exposición cibernética. La seguridad adquiere mayor capacidad de influencia cuando participa en estas conversaciones antes de aprobar inversiones o transformaciones digitales. Gale et al. (2022) resaltan que las estructuras de gobernanza y las responsabilidades claramente definidas favorecen una supervisión directiva más consistente del riesgo cibernético.

La responsabilidad del directorio no consiste en administrar controles técnicos ni sustituir a especialistas. Su papel radica en formular preguntas exigentes, revisar prioridades, evaluar suficiencia de recursos y comprobar que la exposición cibernética permanezca vinculada con el apetito de riesgo empresarial. Esta distinción evita confundir supervisión con gestión operativa. Gale et al. (2022) muestran que una gobernanza adecuada demanda claridad respecto de las funciones asumidas por la Junta, los ejecutivos y quienes poseen conocimiento especializado en ciberseguridad.

También resulta necesario construir confianza entre responsables de seguridad y miembros del directorio. Esa relación no nace de presentaciones esporádicas cargadas de terminología técnica, sino de interacciones que permiten comprender decisiones, incertidumbres y consecuencias. El responsable de ciberseguridad necesita conocer prioridades empresariales; la Junta, por su parte, requiere desarrollar alfabetización suficiente para interrogar la información recibida. Gale et al. (2022) reconocen el conocimiento y la experiencia como factores relevantes para fortalecer la gobernanza cibernética desde niveles directivos.

La calidad del reporting mejora cuando los indicadores muestran tendencias y relaciones, en lugar de fotografías aisladas. Evolución de incidentes relevantes, exposición de activos prioritarios, tiempos de respuesta, dependencia de terceros y avance de inversiones pueden ofrecer una lectura ejecutiva más útil. Importa, además, explicar variaciones y decisiones pendientes. Gale et al. (2022) plantean que los directorios necesitan información apropiada para desempeñar sus responsabilidades, especialmente ante una materia caracterizada por complejidad técnica e incertidumbre empresarial persistente.

Integrar ciberseguridad en la estrategia también significa incorporarla a decisiones sobre adquisiciones, alianzas, innovación, tercerización y transformación digital. Una iniciativa

comercialmente atractiva puede modificar de manera considerable la superficie de exposición de la empresa. Llevar esa conversación al comité ejecutivo permite valorar beneficios y riesgos antes de comprometer recursos. Gale et al. (2022) evidencian que diversos impulsores regulatorios, económicos y organizacionales han incrementado la atención del directorio hacia la gobernanza de la ciberseguridad corporativa.

Una organización alcanza mayor madurez cuando la ciberseguridad forma parte habitual de sus conversaciones estratégicas y deja de aparecer únicamente ante crisis o auditorías. Junta Directiva, comités ejecutivos y responsables técnicos necesitan compartir responsabilidades diferenciadas, información pertinente y criterios comunes para decidir. Gale et al. (2022) destacan que fortalecer la supervisión requiere desarrollar capacidades, estructuras y prácticas apropiadas en el directorio. La meta consiste en gobernar el riesgo digital con criterio empresarial, continuidad y responsabilidad.

2.4. Gestión de valor mediante políticas, métricas e indicadores clave de seguridad y riesgo (KRI/KPI)

La gestión de valor en ciberseguridad exige convertir decisiones técnicas en evidencias comprensibles para quienes administran recursos, riesgos y prioridades corporativas. Las políticas establecen criterios de actuación, mientras las métricas permiten observar resultados, desviaciones y tendencias con disciplina. Bhol, Mohanty y Pattnaik (2023) organizan las métricas de ciberseguridad mediante una taxonomía orientada a medir su fortaleza. Esta perspectiva facilita vincular medición, control y aprendizaje institucional sin reducir la seguridad a una acumulación de datos operativos.

Una política de seguridad adquiere valor cuando orienta comportamientos verificables y puede relacionarse con resultados. Declaraciones ofrecen dirección, pero requieren métricas capaces

de revelar cumplimiento, eficacia y exposición residual. En la propuesta de Bhol et al. (2023), clasificar las métricas ayuda a comprender diferentes dimensiones de la fortaleza cibernética. Para la dirección, esta organización resulta útil porque transforma información dispersa en señales comparables, favoreciendo decisiones sobre prioridades, inversiones y medidas correctivas con fundamento técnico institucional.

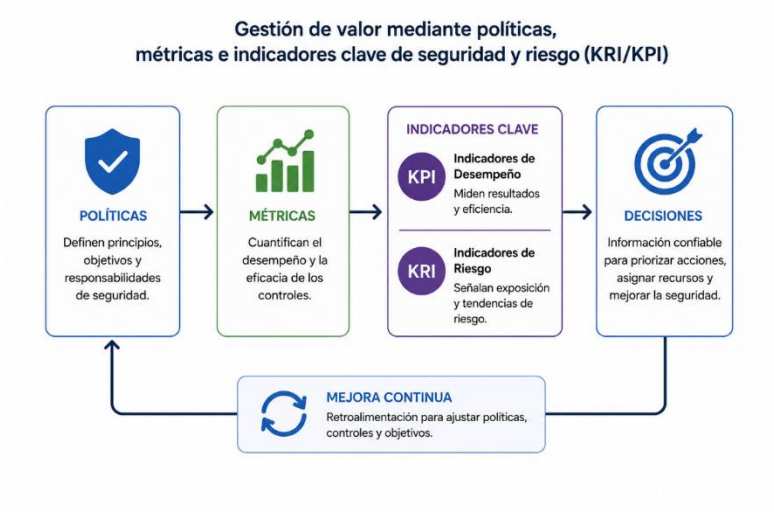
Los indicadores clave de desempeño, conocidos como KPI, permiten examinar si procesos y controles alcanzan resultados establecidos. Su utilidad depende de una definición precisa, una fuente y una periodicidad con la decisión que pretenden respaldar. Bhol et al. (2023) muestran que la medición de ciberseguridad requiere categorías capaces de representar diferentes propiedades y niveles de análisis. Un KPI bien diseñado informa desempeño; uno mal formulado puede premiar actividad mientras oculta debilidades relevantes para la organización.

Los indicadores clave de riesgo, o KRI, cumplen una función distinta: anticipan variaciones en la exposición y permiten reconocer condiciones que podrían afectar objetivos empresariales. No describen incidentes ocurridos; aportan señales para intervenir antes de que determinadas tendencias alcancen niveles inaceptables. La taxonomía presentada por Bhol et al. (2023) evidencia la diversidad de métricas disponibles para valorar fortaleza cibernética. Elegirlas exige relacionar aquello que se mide con decisiones concretas de riesgo y tolerancia organizacional definida.

La combinación de KPI y KRI permite construir una lectura completa de la seguridad. Un control puede mostrar excelente desempeño operativo y, al mismo tiempo, convivir con una exposición creciente derivada de terceros, configuraciones deficientes o activos envejecidos. Por ello, medir eficiencia sin observar riesgo produce una visión incompleta. Bhol et al. (2023) plantean una clasificación que permite distinguir métricas según

atributos de ciberseguridad, aportando una base conceptual para seleccionar indicadores relevantes en cada organización.

Figura 7
Gestión del valor mediante KPI y KRI



Las métricas también deben preservar una relación explícita con el valor empresarial. Reducir tiempos de detección, mejorar capacidades de respuesta o disminuir exposiciones vulnerables tiene sentido cuando protege operaciones, información, confianza y objetivos. Desde la perspectiva de Bhol et al. (2023), medir la fortaleza de ciberseguridad requiere reconocer múltiples componentes y propiedades. Esa diversidad recuerda que ninguna cifra aislada representa adecuadamente el estado de seguridad; la interpretación necesita combinar indicadores y comprender sus relaciones internas.

El diseño de tableros ejecutivos exige evitar una tentación frecuente: presentar todo aquello que técnicamente puede medirse. La abundancia numérica no garantiza conocimiento y puede diluir señales relevantes entre indicadores secundarios. Conviene

seleccionar métricas vinculadas con decisiones, umbrales y responsables establecidos. Bhol et al. (2023) aportan una taxonomía que facilita ordenar medidas de seguridad según características diferenciadas. Aplicada al gobierno corporativo, esta clasificación ayuda a construir reportes comprensibles, comparables y orientados hacia acciones verificables oportunas.

La medición cobra mayor utilidad cuando incorpora tendencias, umbrales y relaciones temporales. Una cifra mensual aislada dice poco sin referencia histórica, objetivo o límite aceptable. Los KRI pueden advertir deterioros progresivos, mientras los KPI permiten verificar avances derivados de inversiones y controles. Bhol et al. (2023) destacan la necesidad de estructurar métricas para evaluar fortaleza cibernética. Esta organización favorece una lectura longitudinal, donde dirección y especialistas pueden reconocer patrones y ajustar prioridades con evidencia consistente.

Las políticas, métricas e indicadores forman un sistema de gobierno cuando existe trazabilidad entre intención, ejecución y decisión. La política define expectativas; los controles materializan acciones; KPI y KRI aportan evidencia para valorar desempeño y exposición. Esta relación evita que la medición permanezca desconectada de objetivos. La clasificación desarrollada por Bhol et al. (2023) permite apreciar que las métricas poseen propósitos diferentes, por lo que seleccionarlas requiere criterio metodológico y comprensión de aquello que representan.

Gestionar valor mediante métricas implica aceptar que medir no equivale a comprender. Los indicadores necesitan interpretación, revisión periódica y capacidad para provocar decisiones cuando revelan desviaciones. Una organización madura aprende a retirar métricas que dejaron de aportar información y a incorporar otras cuando cambia su exposición. Bhol et al. (2023) ofrecen una base taxonómica para ordenar esta diversidad. El

propósito consiste en convertir evidencia de seguridad en conocimiento útil para gobernar recursos, riesgos y prioridades.

2.5. Gobernanza de la Inteligencia Artificial (NIST AI RMF, ISO/IEC 42001) y mitigación de riesgos de modelos (LLM/GenAI)

La gobernanza de la inteligencia artificial introduce una exigencia distinta en la dirección tecnológica: administrar sistemas capaces de generar contenido, inferencias y decisiones cuya conducta puede variar durante su utilización. Los modelos generativos amplifican esta necesidad por su escala, opacidad y dependencia de datos. McIntosh et al. (2024) analizan diversos marcos de ciberseguridad y gobernanza aplicables a modelos lingüísticos comerciales, destacando diferencias relevantes respecto de riesgos, oportunidades y cumplimiento regulatorio durante su adopción empresarial responsable.

El NIST AI Risk Management Framework aporta una estructura para gobernar riesgos de inteligencia artificial mediante funciones orientadas a gobernar, mapear, medir y gestionar. Su aplicación favorece una lectura continua del riesgo durante el ciclo de vida del sistema. McIntosh et al. (2024) examinan la utilidad de marcos regulatorios y de seguridad frente a modelos lingüísticos de gran escala, señalando la necesidad de aproximaciones capaces de atender particularidades tecnológicas que los esquemas tradicionales no siempre cubren adecuadamente.

ISO/IEC 42001 traslada la gobernanza de inteligencia artificial hacia un sistema de gestión institucional, donde políticas, responsabilidades, objetivos, controles y mejora continua adquieren trazabilidad. Esta orientación permite insertar la IA dentro de estructuras corporativas existentes sin tratarla como iniciativa experimental aislada. McIntosh et al. (2024) valoran ISO 42001 dentro del conjunto de marcos relevantes para comercializar modelos lingüísticos, particularmente por su capacidad para

abordar gobernanza, gestión de riesgos y exigencias regulatorias asociadas al despliegue empresarial responsable.

La complementariedad entre NIST AI RMF e ISO/IEC 42001 ofrece una vía especialmente útil para organizaciones que adoptan GenAI. El primero proporciona categorías para razonar sobre riesgos y confianza, mientras el segundo estructura responsabilidades mediante un sistema de gestión formal. McIntosh et al. (2024) sostienen que los marcos aplicados a grandes modelos lingüísticos presentan fortalezas y limitaciones diferenciadas. Integrarlos con criterio permite evitar dependencias excesivas de una referencia incapaz de cubrir toda exposición relevante empresarial.

Los LLM presentan riesgos que trascienden la seguridad informática convencional. Alucinaciones, exposición de información, manipulación de instrucciones, sesgos, contenido dañino y dependencia de proveedores pueden afectar decisiones y procesos empresariales. Frente a esta diversidad, la gobernanza requiere controles técnicos acompañados por responsabilidad organizacional. McIntosh et al. (2024) examinan riesgos asociados con la comercialización de grandes modelos lingüísticos y advierten que los marcos existentes poseen diferentes capacidades para responder a características propias de estas tecnologías generativas.

Mitigar riesgos de modelos comienza antes de su puesta en producción. La selección del proveedor, procedencia de datos, propósito previsto, usuarios autorizados y sensibilidad de la información requieren evaluación temprana. Después vienen pruebas, monitoreo y mecanismos de respuesta. McIntosh et al. (2024) plantean que la comercialización de LLM exige considerar simultáneamente ciberseguridad, cumplimiento y oportunidades empresariales. Esta visión evita que el entusiasmo por capacidades generativas desplace preguntas necesarias acerca de exposición, responsabilidad y control institucional.

La supervisión humana mantiene relevancia particular cuando GenAI participa en actividades con consecuencias financieras, jurídicas, operativas o reputacionales. No basta colocar una persona al cierre del proceso; debe definirse autoridad para revisar, cuestionar y detener resultados cuando aparezcan señales adversas. McIntosh et al. (2024) analizan la adecuación de distintos marcos frente a riesgos de LLM, mostrando que la gobernanza necesita contemplar dimensiones que exceden controles tecnológicos tradicionales y alcanzan responsabilidades corporativas, regulatorias y comerciales.

La medición del riesgo en modelos generativos requiere combinar pruebas técnicas con indicadores de comportamiento y exposición empresarial. Precisión, robustez, fuga de información, respuestas inseguras, sesgo y resistencia frente a manipulación pueden convertirse en señales de gobierno cuando poseen umbrales y responsables definidos. McIntosh et al. (2024) resaltan la necesidad de evaluar marcos considerando riesgos y cumplimiento vinculados con LLM. Esta aproximación favorece decisiones basadas en evidencia durante desarrollo, adquisición, despliegue y operación de sistemas generativos.

La gobernanza también debe alcanzar la cadena de suministro de IA. Modelos externos, interfaces, componentes abiertos, conjuntos de datos y servicios alojados distribuyen responsabilidades entre actores con capacidades e intereses diferentes. Un contrato comercial no elimina la exposición tecnológica ni transfiere completamente la responsabilidad empresarial. McIntosh et al. (2024) examinan la comercialización de LLM desde marcos de ciberseguridad y cumplimiento, destacando la importancia de evaluar riesgos asociados con adopción, operación y obligaciones regulatorias de estas tecnologías.

Gobernar LLM y GenAI exige mantener una relación disciplinada entre innovación, riesgo y responsabilidad. NIST AI

RMF aporta una lógica de gestión del riesgo, mientras ISO/IEC 42001 favorece institucionalización, trazabilidad y mejora continua. Ningún marco reemplaza el juicio directivo ni la evaluación técnica permanente. McIntosh et al. (2024) muestran que los referentes disponibles presentan coberturas distintas frente a grandes modelos lingüísticos. La madurez reside en integrarlos mediante políticas, controles, evidencia y responsabilidades claramente asignadas.

2.6. Protección de datos y privacidad: LOPDP (Ecuador) y marco legal comparado (GDPR, LGPD)

La protección de datos personales ha dejado de pertenecer al terreno periférico del cumplimiento para convertirse en una dimensión del gobierno digital. En Ecuador, la LOPDP articula derechos, principios y obligaciones que aproximan el régimen nacional a estándares internacionales. Molina-Natib y Pachano-Zurita (2025) sostienen que este desarrollo normativo representa un avance relevante, aunque su eficacia depende de aplicación institucional, fiscalización y cultura jurídica. La privacidad adquiere, entonces, valor estratégico para organizaciones públicas y privadas contemporáneas.

La LOPDP parte de principios que disciplinan el tratamiento durante su ciclo de vida. El artículo 10 establece pautas de juridicidad, lealtad, transparencia, propósito, minimización, proporcionalidad, confidencialidad y responsabilidad proactiva, entre otras. No se trata de formalidades decorativas: orientan decisiones sobre recolección, uso, conservación y eliminación. Molina-Natib y Pachano-Zurita (2025) advierten que la distancia entre reconocimiento normativo y aplicación práctica continúa requiriendo atención, especialmente ante dinámicas digitales que multiplican tratamientos de información personal contemporánea actual.

El consentimiento ocupa un lugar relevante, pero la legitimidad del tratamiento no descansa necesariamente en una autorización del titular. El artículo 7 de la LOPDP contempla diversas bases legitimadoras, entre ellas obligaciones legales, intereses vitales, interés público e interés legítimo bajo determinadas condiciones. Esta pluralidad exige documentar por qué se procesan datos. Molina-Natib y Pachano-Zurita (2025) destacan que la protección efectiva requiere fortalecer transparencia y conocimiento ciudadano, elementos vinculados con decisiones informadas sobre información personal.

Figura 8

Convergencia normativa en protección de datos

El derecho a la información constituye otra pieza central del modelo ecuatoriano. Conforme al artículo 12 de la LOPDP, el titular debe conocer, entre otros aspectos, fines, base legal, conservación, responsable, transferencias y mecanismos para ejercer sus derechos. La norma convierte la transparencia en una obligación operativa, no en una cortesía documental. Molina-Natib y Pachano-Zurita (2025) identifican precisamente la transparencia

como un ámbito donde Ecuador necesita profundizar esfuerzos para alcanzar protección efectiva en entornos digitales.

Los derechos de los titulares trasladan el control hacia la experiencia cotidiana de las personas. Los artículos 13, 14, 15 y 16 de la LOPDP regulan acceso, rectificación y actualización, eliminación y oposición, respectivamente. Su ejercicio obliga a diseñar canales internos capaces de responder con trazabilidad y oportunidad. Molina-Natib y Pachano-Zurita (2025) relacionan la eficacia del régimen ecuatoriano con una cultura jurídica más desarrollada, donde ciudadanía e instituciones comprendan responsabilidades y facultades frente al tratamiento.

La seguridad constituye un componente inseparable de la privacidad. El artículo 37 de la LOPDP exige adoptar medidas técnicas, organizativas y de cualquier otra índole adecuadas para proteger datos personales, considerando riesgos y estado de la técnica. Esta obligación conecta gobierno, ciberseguridad y responsabilidad empresarial. Molina-Natib y Pachano-Zurita (2025) señalan que la aplicación práctica del marco ecuatoriano presenta espacios de fortalecimiento institucional, cuestión especialmente relevante cuando incidentes digitales pueden comprometer derechos de numerosos titulares simultáneamente.

La responsabilidad proactiva amplía el horizonte del cumplimiento. El artículo 47 de la LOPDP atribuye al responsable obligaciones que abarcan políticas, gestión de riesgos, evaluaciones, prevención, notificación de vulneraciones y protección de datos desde el diseño y por defecto. El cumplimiento requiere evidencia, no declaraciones. Esta orientación guarda relación con la lectura crítica de Molina-Natib y Pachano-Zurita (2025), quienes resaltan la necesidad de mejorar fiscalización y aplicación para que las garantías normativas produzcan efectos materiales.

Frente al GDPR europeo, la LOPDP comparte una arquitectura reconocible: principios de tratamiento, derechos del

titular, responsabilidad del responsable, seguridad y mecanismos institucionales de control. La influencia internacional resulta visible, aunque trasladar categorías jurídicas requiere atender capacidades regulatorias nacionales. Molina-Natib y Pachano-Zurita (2025) comparan expresamente el régimen ecuatoriano con estándares internacionales y encuentran oportunidades de fortalecimiento. La convergencia normativa facilita además relaciones comerciales donde circulan datos entre organizaciones sometidas a jurisdicciones diferentes y exigencias crecientes.

La comparación con la LGPD brasileña permite apreciar una tendencia latinoamericana hacia modelos integrales de protección de datos, con bases legales, derechos, responsabilidades y autoridades especializadas. Ecuador participa de esta transformación mediante la LOPDP y su desarrollo reglamentario, aunque cada sistema conserva particularidades institucionales. Molina-Natib y Pachano-Zurita (2025) emplean el derecho comparado para valorar la experiencia ecuatoriana frente a referentes externos. Tal contraste permite distinguir entre adoptar normas avanzadas y construir capacidades efectivas para aplicarlas.

La protección de datos alcanza madurez cuando forma parte del diseño de procesos, servicios digitales, arquitecturas tecnológicas y decisiones ejecutivas. La LOPDP ofrece una base jurídica para ese propósito, reforzada por el Reglamento General y la autoridad especializada vigente. Molina-Natib y Pachano-Zurita (2025) concluyen que Ecuador debe fortalecer transparencia, fiscalización y educación digital. Frente al GDPR y la LGPD, la tarea consiste en convertir convergencia normativa en prácticas verificables que preserven autonomía, confianza y privacidad.

2.7. Cultura organizacional, liderazgo ejecutivo, concienciación y responsabilidad compartida en ciberseguridad

La cultura de ciberseguridad se construye cuando las prácticas de protección dejan de percibirse como obligaciones técnicas y pasan a formar parte del comportamiento cotidiano. Cada decisión, desde gestionar credenciales hasta compartir información, expresa valores organizacionales que pueden fortalecer o debilitar la resiliencia. Aksoy (2024) plantea que desarrollar una cultura orientada a la seguridad favorece organizaciones más resistentes frente a ataques cibernéticos. Esa transformación requiere continuidad, coherencia directiva y participación de quienes integran la institución.

El liderazgo ejecutivo ocupa una posición determinante porque las personas observan con atención aquello que la dirección prioriza, financia y practica. Cuando los líderes respetan políticas, participan en actividades formativas y preguntan por riesgos digitales, transmiten que la seguridad pertenece al negocio. Aksoy (2024) vincula el compromiso de la alta dirección con la construcción de una cultura capaz de sostener conductas protectoras. El ejemplo ejecutivo convierte principios abstractos en expectativas visibles para toda la organización.

La concienciación efectiva va más allá de impartir cursos periódicos o distribuir recordatorios sobre contraseñas y phishing. Su propósito consiste en desarrollar criterio para reconocer situaciones de riesgo y actuar con prudencia ante señales ambiguas. Según Aksoy (2024), la formación y la sensibilización constituyen elementos relevantes para fortalecer la cultura de ciberseguridad. Cuando el aprendizaje se conecta con tareas, las personas comprenden las consecuencias de sus decisiones y adquieren hábitos protectores aplicables al trabajo cotidiano.

La responsabilidad compartida modifica una idea arraigada: considerar que la seguridad corresponde exclusivamente al departamento tecnológico. Recursos humanos protege información laboral; finanzas resguarda transacciones; compras evalúa terceros; operaciones preserva continuidad; la dirección establece prioridades. Cada función administra una parte de la exposición corporativa. Aksoy (2024) destaca que una cultura de ciberseguridad requiere participación organizacional y comportamientos conscientes. Distribuir responsabilidades evita zonas grises y permite que cada persona comprenda su contribución a la resiliencia colectiva organizacional.

El comportamiento humano merece atención sin convertir a las personas en el eslabón culpable de cada incidente. Una cultura basada en temor puede desalentar reportes tempranos, ocultar errores y deteriorar confianza. Resulta más productivo promover aprendizaje, comunicación y corrección oportuna. Aksoy (2024) examina el factor humano como componente relevante de la seguridad organizacional y relaciona la cultura con mayor resistencia ante ataques. La confianza permite comunicar anomalías y aprender de ellas sin normalizar conductas negligentes.

La comunicación interna sostiene esta cultura cuando traduce riesgos técnicos en mensajes cercanos a las responsabilidades de cada audiencia. Un desarrollador, un directivo y un colaborador administrativo necesitan comprender amenazas desde perspectivas distintas. Repetir mensajes genéricos pierde eficacia con rapidez. Aksoy (2024) concede importancia a la concienciación y al intercambio de información para fortalecer comportamientos seguros. Una comunicación diseñada explica motivos, ofrece pautas accionables y mantiene presente la seguridad sin convertirla en ruido institucional permanente.

También importa reconocer que la cultura puede medirse mediante señales observables. Tasas de reporte, participación

formativa, reincidencia en conductas inseguras, tiempos de comunicación y percepción del personal ofrecen evidencias sobre hábitos colectivos. Las métricas deben interpretarse con cuidado para evitar incentivos contraproducentes. Aksoy (2024) relaciona cultura y resiliencia organizacional, vínculo que invita a evaluar no meramente conocimientos adquiridos, sino comportamientos sostenidos. Medir permite identificar áreas donde liderazgo, formación o comunicación requieren ajustes precisos y oportunos.

La incorporación de nuevos colaboradores representa un momento privilegiado para transmitir expectativas de seguridad. Desde el ingreso, políticas, responsabilidades y canales de reporte deberían presentarse como parte natural del trabajo, junto con valores y objetivos institucionales. Aksoy (2024) sostiene que la cultura de ciberseguridad requiere educación y participación de los empleados. La inducción establece una primera referencia, pero el aprendizaje posterior debe acompañar cambios tecnológicos, nuevas amenazas y modificaciones en las funciones de cada persona.

Los mandos intermedios cumplen un papel frecuentemente subestimado. Son quienes convierten prioridades ejecutivas en rutinas, asignan tiempos, resuelven tensiones operativas y validan comportamientos mediante decisiones cotidianas. Si la dirección declara importante la seguridad, pero los responsables locales premian velocidad ignorando controles, aparece una contradicción difícil de corregir. Aksoy (2024) permite comprender que la cultura depende de factores organizacionales interrelacionados. La coherencia entre discurso, incentivos y práctica determina credibilidad de las políticas de protección corporativa interna.

Una cultura madura convierte la ciberseguridad en parte de la identidad organizacional sin transformarla en una carga paralizante. Liderazgo, formación, comunicación y responsabilidad compartida deben reforzarse mutuamente para generar conductas

sostenibles. Aksoy (2024) vincula esta construcción cultural con la capacidad de las organizaciones para resistir ataques y fortalecer resiliencia. El propósito no consiste en eliminar toda posibilidad de error humano, sino en crear condiciones donde las personas detecten, comuniquen y corrijan riesgos con criterio colectivo.

2.8. Modelos de cumplimiento, auditoría continua, trazabilidad institucional y gobierno adaptativo para ecosistemas interconectados

Los modelos de cumplimiento contemporáneos necesitan responder a organizaciones cuyas operaciones atraviesan plataformas, proveedores, nubes, algoritmos y redes empresariales. Cumplir deja de ser una comprobación periódica para convertirse en capacidad permanente de demostrar decisiones, controles y responsabilidades. Saveljeva y Volkova (2025) vinculan la confianza digital con dimensiones relacionadas con gobernanza, seguridad, transparencia y cumplimiento. Desde esta perspectiva, la evidencia verificable adquiere valor institucional porque permite sostener relaciones confiables entre actores que intercambian información y servicios digitales.

La auditoría continua transforma la lógica tradicional basada en revisiones realizadas después de periodos prolongados. Mediante evidencias obtenidas con mayor frecuencia, la organización puede reconocer desviaciones, valorar controles y corregir prácticas antes de acumular exposiciones significativas. Esta capacidad adquiere importancia en ecosistemas donde los cambios tecnológicos ocurren con rapidez. Saveljeva y Volkova (2025) identifican la auditabilidad entre los elementos relacionados con confianza digital, destacando el valor de mecanismos que permitan verificar comportamientos, procesos y compromisos organizacionales de manera consistente.

La trazabilidad institucional permite reconstruir decisiones y comprender quién autorizó una acción, qué información fue

utilizada y bajo qué reglas ocurrió. En sistemas interconectados, esta memoria verificable resulta indispensable para atribuir responsabilidades sin depender de interpretaciones posteriores. Saveljeva y Volkova (2025) relacionan la trazabilidad con dimensiones relevantes de la confianza digital. Registrar evidencias no responde únicamente a necesidades auditoras; también fortalece aprendizaje, transparencia y capacidad de explicar actuaciones ante reguladores, clientes, socios y órganos directivos.

Un gobierno adaptativo reconoce que los controles apropiados pueden variar cuando cambian tecnologías, riesgos, regulaciones y relaciones empresariales. La estabilidad institucional no exige inmovilidad; requiere conservar principios mientras se revisan mecanismos de ejecución. Esta distinción permite responder a ecosistemas dinámicos sin abandonar responsabilidad ni supervisión. Saveljeva y Volkova (2025) muestran que la confianza digital posee una naturaleza multidimensional, vinculada con factores técnicos y organizacionales. Gobernar adaptativamente implica equilibrar esas dimensiones mediante decisiones revisables y evidencias verificables.

La interdependencia digital modifica profundamente las fronteras tradicionales del cumplimiento. Una organización puede proteger adecuadamente sus sistemas internos y permanecer expuesta mediante proveedores, interfaces, plataformas o servicios externos. La confianza requiere entonces criterios compartidos de responsabilidad, seguridad y verificación. Saveljeva y Volkova (2025) destacan que las relaciones digitales dependen de múltiples factores capaces de influir en la disposición de los actores para confiar. Esta visión favorece modelos de gobierno extendidos hacia terceros y cadenas tecnológicas interconectadas.

Automatizar evidencias de cumplimiento puede reducir tareas repetitivas y mejorar oportunidad, aunque la automatización necesita supervisión y criterios interpretativos. Un indicador puede señalar una desviación sin explicar sus causas ni determinar su

relevancia empresarial. Por ello, auditoría continua combina tecnología con juicio profesional. Saveljeva y Volkova (2025) sitúan elementos vinculados con seguridad, gobernanza y transparencia dentro de la construcción de confianza digital. La evidencia automatizada adquiere sentido cuando facilita decisiones responsables, comprensibles y susceptibles de revisión institucional.

La trazabilidad también cumple una función preventiva. Cuando decisiones, accesos, cambios y excepciones dejan registros verificables, las personas conocen que sus actuaciones pueden reconstruirse y evaluarse posteriormente. Esto fortalece rendición de cuentas sin convertir vigilancia en principio dominante. Saveljeva y Volkova (2025) relacionan confianza digital con atributos que abarcan transparencia, privacidad, seguridad y responsabilidad. Una arquitectura de registros bien gobernada debe proteger evidencias, limitar accesos y conservar información durante periodos coherentes con obligaciones y necesidades institucionales.

El cumplimiento basado en riesgos ofrece una alternativa a modelos que distribuyen recursos de manera uniforme entre controles con relevancia desigual. Priorizar requiere identificar activos, obligaciones, dependencias y posibles impactos, manteniendo evidencia de los criterios utilizados. En la perspectiva de Saveljeva y Volkova (2025), la confianza digital integra dimensiones diversas cuya importancia puede depender de las relaciones entre actores. Esta lectura permite orientar controles hacia áreas donde una falla tendría consecuencias mayores para operaciones, derechos o relaciones empresariales.

Los ecosistemas interconectados requieren mecanismos de aseguramiento capaces de acompañar relaciones cambiantes. Incorporar un proveedor, desplegar una plataforma o compartir datos modifica dependencias y puede demandar nuevas evidencias de cumplimiento. La gobernanza necesita detectar estos cambios y

revisar controles oportunamente. Saveljeva y Volkova (2025) presentan la confianza digital como una construcción vinculada con múltiples factores y partes interesadas. Esta característica exige que auditoría, cumplimiento y trazabilidad funcionen como capacidades permanentes, integradas con decisiones tecnológicas y empresariales.

La madurez institucional aparece cuando cumplimiento, auditoría y trazabilidad dejan de funcionar como actividades separadas y conforman un sistema de aprendizaje y rendición de cuentas. Las evidencias alimentan auditorías; los hallazgos orientan ajustes; las decisiones generan nuevos registros verificables. Saveljeva y Volkova (2025) vinculan confianza digital con una combinación de atributos técnicos, humanos y organizacionales. Bajo esta perspectiva, el gobierno adaptativo preserva responsabilidad mientras ajusta controles y relaciones frente a transformaciones continuas del ecosistema digital.

Tabla 2

Dimensiones estratégicas del gobierno digital, la gobernanza de la IA y la ciberseguridad

Dimensión de gobierno	**Orientación estratégica y aplicación organizacional**
Gobierno adaptativo de TI	Articula tecnología y estrategia mediante mecanismos de gobierno ajustables a las capacidades, prioridades y evolución de la organización. Favorece decisiones dinámicas, aprendizaje institucional y creación de valor mediante TI.
Marcos de gobierno y seguridad	COBIT 2019 estructura objetivos y responsabilidades de gobierno; ISO/IEC 27001:2022 organiza la gestión de seguridad de la información; los marcos NIST proporcionan criterios para gestionar riesgos y fortalecer capacidades de protección, detección, respuesta y recuperación.

Supervisión de la Junta Directiva	Integra el riesgo cibernético en decisiones corporativas mediante reporting ejecutivo, responsabilidades definidas, indicadores relevantes y participación periódica de la Junta Directiva y los comités ejecutivos.
Métricas de seguridad y riesgo	Vincula políticas con KPI y KRI para evaluar desempeño, exposición, tendencias y eficacia de controles. Facilita decisiones basadas en evidencia y permite relacionar inversiones en ciberseguridad con objetivos empresariales.
Gobernanza de inteligencia artificial	NIST AI RMF e ISO/IEC 42001 permiten estructurar responsabilidades, evaluación de riesgos, controles y supervisión durante el ciclo de vida de sistemas de IA. En LLM y GenAI adquieren relevancia la trazabilidad, evaluación y supervisión humana.
Protección de datos y privacidad	La LOPDP ecuatoriana, junto con referentes comparados como GDPR y LGPD, orienta el tratamiento responsable de datos mediante principios, derechos, bases legitimadoras, seguridad, responsabilidad proactiva y protección desde el diseño.
Cultura y liderazgo en ciberseguridad	Promueve comportamientos responsables mediante liderazgo ejecutivo, formación continua, comunicación, concienciación y distribución clara de responsabilidades. La seguridad se incorpora a las prácticas cotidianas y a la identidad organizacional.
Cumplimiento, auditabilidad y confianza digital	Integra auditoría continua, trazabilidad institucional, evidencia verificable y gobierno adaptativo. Facilita rendición de cuentas y control en ecosistemas digitales caracterizados por dependencias entre organizaciones, proveedores, plataformas y servicios tecnológicos.

Nota. Elaboración conceptual

Capítulo 3:

Arquitecturas Empresariales, Zero Trust y Entornos Nube

La transformación digital ha modificado profundamente la manera en que las organizaciones conciben sus arquitecturas, protegen sus activos y sostienen operaciones cada vez más distribuidas. Ya no basta con incorporar tecnologías de manera incremental. Las decisiones sobre procesos, información, aplicaciones, infraestructura y seguridad necesitan responder a una visión empresarial coherente. Hardi y Legowo (2023) destacan que la arquitectura empresarial puede habilitar cambios operativos vinculados con la transformación digital, especialmente cuando existe necesidad de adaptación ante condiciones disruptivas.

En ese escenario, la arquitectura empresarial funciona como una disciplina capaz de acercar estrategia y ejecución tecnológica. Marcos como TOGAF y Zachman permiten ordenar capacidades, procesos, datos y componentes desde perspectivas complementarias, mientras facilitan una lectura integral de las dependencias organizacionales. Hardi y Legowo (2023) vinculan esta capacidad arquitectónica con la adaptación de procesos empresariales durante periodos de cambio acelerado. La arquitectura adquiere entonces un carácter práctico: orientar decisiones presentes sin perder de vista la evolución esperada.

Sin embargo, distribuir servicios, aplicaciones y datos también transforma las fronteras tradicionales de seguridad. El perímetro corporativo pierde centralidad frente a identidades, dispositivos y recursos que interactúan desde ubicaciones diversas. En este punto, Zero Trust ofrece principios pertinentes para reconsiderar la confianza digital. Anderson et al. (2023) describen arquitecturas donde las decisiones de acceso dependen de verificaciones continuas y condiciones observables. Esta lógica resulta transferible al ámbito empresarial, donde cada interacción necesita autorización proporcional al riesgo existente.

La seguridad tampoco puede permanecer como una revisión añadida después del desarrollo tecnológico. Cuando aplicaciones y servicios cambian continuamente, detectar

vulnerabilidades en etapas tardías incrementa costos y prolonga exposiciones innecesarias. Rajapakse et al. (2022) muestran que DevSecOps procura integrar seguridad, desarrollo y operaciones mediante prácticas colaborativas y automatizadas. Tal integración lleva la protección hacia el ciclo de vida completo del software, desde requisitos y diseño hasta despliegue, operación y mantenimiento, distribuyendo responsabilidades entre quienes construyen capacidades digitales.

Figura 9

Arquitectura empresarial y seguridad digital

A esta transformación se añade la expansión de servicios cloud, multinube y arquitecturas híbridas, donde recursos corporativos conviven con infraestructuras administradas por diferentes proveedores. La flexibilidad obtenida tiene una contraparte evidente: aumenta la complejidad para mantener visibilidad, gobernar configuraciones y proteger información. Ukeje et al. (2024) identifican preocupaciones relacionadas con privacidad, confidencialidad, acceso y gobernanza en la adopción

de computación en nube. Gestionar esa diversidad requiere una postura de seguridad continua, medible y verificable.

Dentro de esta realidad tecnológica, capacidades asociadas con CSPM, CWPP y CNAPP adquieren relevancia porque permiten observar configuraciones, cargas, identidades y aplicaciones distribuidas desde perspectivas relacionadas. Más importante que la denominación comercial es la necesidad que representan: reducir fragmentación y convertir señales técnicas en decisiones de protección. Ukeje et al. (2024) evidencian que los riesgos de seguridad cloud atraviesan dimensiones interdependientes. Una organización madura necesita comprender esas relaciones para priorizar exposiciones según impacto empresarial y sensibilidad informacional.

Paralelamente, los microservicios y las APIs han modificado la construcción de ecosistemas digitales. Las aplicaciones dejan de comportarse como unidades cerradas y pasan a depender de numerosos intercambios entre servicios, plataformas y consumidores de información. Matias et al. (2024) relacionan la efectividad de arquitecturas de microservicios con mecanismos de seguridad capaces de proteger componentes e interacciones distribuidas. La resiliencia requiere entonces aislamiento, observabilidad, autenticación y recuperación, pero también una comprensión precisa de las dependencias que sostienen cada servicio empresarial.

Los datos atraviesan todas estas arquitecturas. Circulan entre aplicaciones, nubes, APIs, procesos analíticos y servicios externos, mientras adquieren valor estratégico para decisiones automatizadas y nuevos modelos empresariales. Esa movilidad obliga a preservar integridad, confidencialidad, disponibilidad y trazabilidad durante todo su tratamiento. Matias et al. (2024) destacan la importancia de mecanismos de protección dentro de arquitecturas distribuidas, mientras Ukeje et al. (2024) señalan

preocupaciones persistentes sobre privacidad y control de información almacenada o procesada mediante servicios cloud.

La continuidad operativa completa esta visión porque una arquitectura empresarial carece de verdadera madurez cuando no puede mantener o recuperar capacidades prioritarias frente a interrupciones. La resiliencia tecnológica exige reconocer dependencias, establecer prioridades y diseñar respuestas antes de que ocurra una contingencia. Hardi y Legowo (2023) muestran que la arquitectura empresarial favorece la adaptación de procesos durante condiciones disruptivas. Desde una orientación cercana a SABSA, seguridad, continuidad y arquitectura pueden vincularse mediante atributos empresariales y requisitos trazables.

Este capítulo aborda, por tanto, la convergencia entre arquitectura empresarial, Zero Trust, seguridad por diseño, DevSecOps, protección cloud, microservicios y resiliencia tecnológica como partes relacionadas de una misma transformación. Anderson et al. (2023), Rajapakse et al. (2022), Ukeje et al. (2024), Matias et al. (2024) y Hardi y Legowo (2023) permiten observar esta convergencia desde ángulos complementarios. La empresa inteligente requiere arquitecturas capaces de cambiar con rapidez, proteger recursos distribuidos y preservar continuidad sin separar innovación, gobierno y seguridad.

3.1. Arquitectura empresarial alineada con la estrategia de transformación digital (TOGAF y Zachman)

La arquitectura empresarial constituye un puente entre la estrategia y las decisiones tecnológicas para la transformación digital. Su valor aparece cuando la organización traduce objetivos de negocio en capacidades, procesos, datos, aplicaciones e infraestructura coherentes. Hardi y Legowo (2023) señalan que TOGAF ADM facilita esa articulación mediante fases iterativas orientadas al cambio organizacional. Desde esta perspectiva, la

arquitectura deja de ser documentación estática y adquiere una función directiva, capaz de ordenar prioridades y orientar inversiones.

En una transformación digital, la arquitectura empresarial necesita partir de la visión estratégica y mantenerla durante cada decisión de diseño. TOGAF aporta una secuencia metodológica que vincula visión, arquitectura de negocio, sistemas de información, tecnología, oportunidades, migración y gobierno. Según Hardi y Legowo (2023), esta lógica favorece la adaptación de procesos operativos frente a cambios del entorno empresarial. La disciplina arquitectónica permite, entonces, convertir aspiraciones digitales en iniciativas gobernables, medibles y relacionadas con resultados concretos.

El método ADM de TOGAF ofrece una dinámica cíclica pertinente para organizaciones que transforman procesos mientras continúan operando. Cada fase alimenta decisiones y permite revisar premisas cuando cambian prioridades, riesgos o capacidades. Hardi y Legowo (2023) vinculan la arquitectura empresarial con mejoras en procesos apoyados por transformación digital. Esa relación adquiere relevancia estratégica: una iniciativa tecnológica genera valor cuando modifica capacidades empresariales de manera deliberada, trazable y compatible con la dirección establecida por la organización.

La perspectiva de Zachman complementa este enfoque al organizar la arquitectura mediante preguntas fundamentales y niveles de representación empresarial. Su matriz favorece una lectura de datos, funciones, redes, personas, tiempos y motivaciones, evitando que la transformación digital quede reducida a decisiones de tecnología. En paralelo, TOGAF proporciona un método para conducir el cambio. La evidencia presentada por Hardi y Legowo (2023) respalda la utilidad de estructurar la transformación desde una arquitectura vinculada con procesos empresariales.

TOGAF y Zachman pueden entenderse como instrumentos de naturaleza distinta, aunque compatibles dentro de una práctica arquitectónica. Zachman ayuda a clasificar representaciones y detectar vacíos; TOGAF orienta entregables, decisiones y transiciones mediante ADM. Esta complementariedad resulta valiosa cuando una empresa necesita preservar coherencia entre estrategia y ejecución. Hardi y Legowo (2023) muestran que la arquitectura empresarial puede actuar como habilitadora de transformación digital al conectar cambios tecnológicos con procesos operativos y objetivos de desempeño definidos.

La alineación estratégica exige que las arquitecturas objetivo no nazcan desde preferencias técnicas, sino desde capacidades que requieren evolución. En TOGAF, la visión arquitectónica establece una dirección, mientras las arquitecturas de negocio, datos, aplicaciones y tecnología detallan estados y brechas. Hardi y Legowo (2023) señalan el papel de ADM en la articulación entre arquitectura empresarial y transformación digital. Esta relación favorece decisiones justificables, porque cada componente puede vincularse con una necesidad y una intención estratégica.

Una arquitectura empresarial orientada a transformación digital requiere gobernanza, porque diseñar estados carece de valor si las iniciativas se apartan de ellos. TOGAF incorpora mecanismos para supervisar conformidad, gestionar cambios y mantener trazabilidad entre decisiones. Hardi y Legowo (2023) relacionan la aplicación de arquitectura empresarial con la continuidad y adaptación de procesos durante condiciones disruptivas. La lección indica: gobernar arquitectura significa preservar coherencia sin convertir el método en burocracia que frene aprendizaje, innovación o respuesta.

Desde la perspectiva de ciberseguridad, alinear arquitectura y estrategia permite incorporar requisitos de protección desde las decisiones de transformación. Aunque TOGAF

no reemplaza marcos de seguridad, su estructura facilita ubicar controles, responsabilidades, datos, dependencias tecnológicas y criterios de riesgo dentro de una visión empresarial. Hardi y Legowo (2023) enfatizan la relación entre arquitectura, procesos y transformación digital; esa conexión ofrece una base para evitar que la seguridad permanezca separada de las prioridades y del diseño.

La experiencia de transformación durante periodos de disrupción mostró que la velocidad necesita una arquitectura capaz de mantener sentido. Hardi y Legowo (2023) documentan el uso de TOGAF ADM para apoyar procesos operativos y transformación digital asociados con la pandemia. Más allá de la coyuntura, el aprendizaje conserva vigencia: las organizaciones requieren mapas de transición, responsables, dependencias y criterios de evaluación que permitan cambiar con rapidez sin perder correspondencia entre capacidades digitales, procesos y metas.

En consecuencia, una arquitectura alineada con transformación digital debe funcionar como lenguaje común entre dirección, negocio, tecnología y seguridad. TOGAF aporta una ruta para conducir la evolución arquitectónica, mientras Zachman ofrece una estructura para ordenar perspectivas y artefactos. La contribución de Hardi y Legowo (2023) refuerza la idea de que la arquitectura empresarial habilita cambios operativos vinculados con transformación digital. Su aporte reside en convertir estrategia en decisiones revisables y comprensibles para actores con responsabilidades.

3.2. Implementación del Modelo Zero Trust (NIST SP 800-207) en el diseño organizacional

El modelo Zero Trust redefine la seguridad organizacional al abandonar la confianza implícita derivada de la ubicación, la red o la pertenencia institucional. Cada acceso debe evaluarse mediante identidad, dispositivo, recurso solicitado y condiciones observables. Anderson et al. (2023) describen una arquitectura

donde la verificación continua reduce la dependencia de perímetros tradicionales. Trasladado a la empresa, este principio transforma políticas, responsabilidades y flujos de autorización, acercando la seguridad a cada interacción digital relevante y estratégica.

La adopción de Zero Trust afecta el diseño organizacional porque distribuye responsabilidades que antes permanecían concentradas en equipos de infraestructura. Identidad, acceso, activos, datos y telemetría pasan a relacionarse mediante decisiones coordinadas. Anderson et al. (2023) plantean mecanismos de confianza dinámica para entornos conectados, una idea aplicable a organizaciones con usuarios y servicios. El resultado exige cooperación entre seguridad, operaciones, arquitectura y negocio, con criterios compartidos para autorizar actividades sensibles de manera consistente y verificable.

NIST SP 800-207 concibe Zero Trust desde una premisa exigente: ninguna solicitud obtiene confianza permanente por origen o ubicación. En términos organizacionales, esta orientación requiere separar autenticación, autorización y acceso efectivo, manteniendo decisiones sujetas a evidencia disponible. La arquitectura estudiada por Anderson et al. (2023) refuerza este enfoque mediante evaluación continua y control adaptativo. Para la empresa, ello implica diseñar responsabilidades capaces de revisar privilegios, comportamientos y condiciones operativas durante toda interacción con recursos corporativos.

La identidad adquiere un papel central cuando Zero Trust se incorpora al diseño empresarial. Personas, dispositivos, aplicaciones y servicios necesitan atributos verificables antes de recibir acceso a recursos. Anderson et al. (2023) destacan la autenticación y la evaluación permanente dentro de arquitecturas distribuidas, donde confiar por proximidad resulta insuficiente. En una organización, esta lógica demanda procesos claros para altas, cambios y bajas, además de coordinación entre recursos humanos, tecnología, seguridad y responsables de activos digitales.

Otro cambio relevante aparece en la segmentación de recursos y en la reducción del desplazamiento interno. Zero Trust favorece accesos delimitados según necesidad, identidad y condiciones de riesgo, en lugar de conceder amplias posibilidades después de atravesar un perímetro. Anderson et al. (2023) analizan controles distribuidos que restringen interacciones entre componentes conectados. En el ámbito empresarial, esta orientación impulsa estructuras de gobierno donde propietarios de información y servicios participan activamente en decisiones de autorización corporativa.

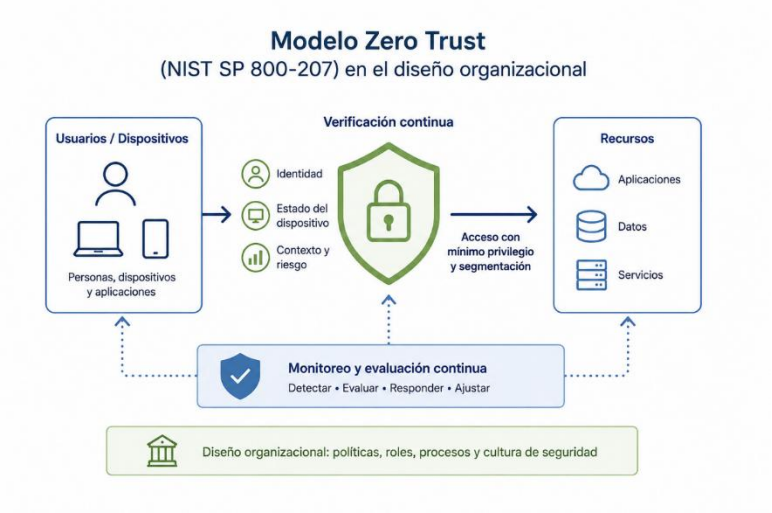
La verificación continua también modifica la relación entre seguridad y operación. Cada decisión de acceso puede nutrirse de señales procedentes de identidad, dispositivo, comportamiento y estado del recurso. Anderson et al. (2023) muestran que una arquitectura Zero Trust obtiene valor al evaluar condiciones cambiantes antes de permitir interacciones. Para las empresas, esta práctica requiere capacidades de observación, análisis y respuesta coordinadas, evitando que la autorización permanezca desligada de eventos que alteran el nivel de riesgo.

Implementar Zero Trust no equivale a adquirir tecnología aislada. Requiere revisar procesos, autoridad, responsabilidades y criterios mediante los cuales una organización concede acceso. La propuesta arquitectónica de Anderson et al. (2023) evidencia que la confianza debe gestionarse bajo condiciones variables y verificables, apoyada por información verificable. Esta perspectiva conduce a modelos operativos donde seguridad participa desde el diseño de servicios y donde las áreas propietarias definen necesidades, privilegios aceptables y condiciones para mantenerlos vigentes organizacionales.

El principio de mínimo privilegio adquiere profundidad organizacional cuando se vincula con funciones reales y recursos específicos. No basta con reducir permisos de manera indiscriminada; es necesario relacionarlos con tareas,

responsabilidades y periodos de uso. Anderson et al. (2023) presentan decisiones de acceso ajustadas a entidades y condiciones operativas. En la empresa, esta lógica favorece revisiones periódicas, autorizaciones temporales y separación de funciones, disminuyendo privilegios persistentes que podrían ampliar el impacto de una intrusión detectada.

Figura 10
Modelo Zero Trust organizacional



Zero Trust también demanda una cultura capaz de comprender que verificar no equivale a desconfiar de las personas. La verificación protege relaciones digitales mediante reglas previsibles y evidencia técnica. Anderson et al. (2023) muestran que, en sistemas conectados, la confianza está vinculada con condiciones observables y puede modificarse durante la operación. En organizaciones empresariales, comunicar este principio resulta importante para evitar resistencia, especialmente cuando nuevos controles alteran hábitos, accesos históricos o prácticas informales de colaboración.

Integrar Zero Trust en el diseño organizacional convierte la ciberseguridad en una propiedad distribuida entre arquitectura, gobierno, operación y gestión de identidades. La aportación de Anderson et al. (2023) permite observar que la confianza puede administrarse mediante decisiones continuas, controles cercanos al recurso y evaluación de entidades. En la empresa inteligente, esta orientación favorece estructuras adaptativas, donde cada acceso responde a políticas explícitas y cada cambio tecnológico conserva correspondencia con responsabilidades, riesgos y objetivos institucionales.

3.3. Seguridad por diseño y DevSecOps en el ciclo de vida de desarrollo de software (S-SDLC)

La seguridad por diseño transforma el desarrollo de software al incorporar requisitos de protección desde la concepción del producto, en lugar de agregarlos después de construirlo. Esta orientación modifica prioridades, responsabilidades y prácticas dentro del S-SDLC. Rajapakse et al. (2022) identifican que DevSecOps integra actividades de seguridad con desarrollo y operaciones, favoreciendo una responsabilidad compartida. La consecuencia organizacional es relevante: cada decisión técnica puede evaluarse tempranamente frente a riesgos, controles y objetivos empresariales previamente definidos.

Dentro del S-SDLC, la identificación temprana de requisitos de seguridad permite vincular necesidades del negocio con controles verificables durante diseño, construcción, pruebas y despliegue. DevSecOps amplía esta lógica mediante colaboración continua entre especialistas tradicionalmente separados. Rajapakse et al. (2022) destacan que la integración de seguridad enfrenta barreras relacionadas con personas, procesos y tecnología. Por ello, una práctica madura necesita acuerdos claros, capacidades técnicas y responsabilidades distribuidas durante todas las etapas del desarrollo de software empresarial.

El diseño seguro comienza antes de escribir código. Modelar amenazas, analizar superficies de ataque y definir criterios de aceptación permite anticipar exposiciones que resultarían costosas durante etapas posteriores. Desde la perspectiva DevSecOps, estas actividades deben integrarse al flujo habitual de ingeniería. Rajapakse et al. (2022) señalan que incorporar seguridad requiere superar dificultades vinculadas con conocimientos y colaboración. Esta realidad convierte la formación interdisciplinaria en una capacidad necesaria para desarrollar productos digitales modernos resistentes y mantenibles.

La automatización constituye un componente relevante de DevSecOps porque acerca controles de seguridad al ritmo cotidiano del desarrollo. Análisis de código, revisión de dependencias, pruebas y verificación de configuraciones pueden integrarse en procesos de integración y entrega continua. Rajapakse et al. (2022) describen la automatización como una respuesta pertinente recurrente ante dificultades de adopción. Sin embargo, automatizar exige criterio: una herramienta produce señales, mientras los equipos deben interpretar hallazgos, priorizar riesgos y corregir causas recurrentes.

DevSecOps también modifica la distribución de responsabilidades dentro de los equipos. La seguridad deja de permanecer confinada a una revisión tardía realizada por especialistas y pasa a formar parte de decisiones cotidianas de ingeniería. Rajapakse et al. (2022) encuentran que los factores humanos y organizacionales influyen considerablemente en la adopción. Este cambio demanda comunicación entre desarrolladores, operaciones y seguridad, además de liderazgo capaz de convertir políticas corporativas en prácticas comprensibles, aplicables y medibles para todos.

La velocidad de entrega puede generar tensiones cuando los controles de seguridad se perciben como obstáculos externos al proceso. DevSecOps busca reducir esa fricción integrando

verificaciones dentro de las mismas herramientas y rutinas utilizadas por los equipos. Rajapakse et al. (2022) observan dificultades relacionadas con la coordinación y con la integración de prácticas de seguridad. Una respuesta efectiva consiste en diseñar controles proporcionales al riesgo, con retroalimentación temprana y criterios transparentes para gestionar excepciones justificadas.

La gestión de vulnerabilidades adquiere otra dinámica dentro de un S-SDLC apoyado por DevSecOps. Detectar una debilidad carece de valor operativo cuando no existen responsables, prioridades ni mecanismos de remediación. Rajapakse et al. (2022) muestran que la adopción requiere integrar prácticas y herramientas dentro de procesos existentes. De ahí que los hallazgos deban conectarse con flujos de trabajo, niveles de riesgo y tiempos de respuesta, evitando acumulaciones que conviertan alertas técnicas en deuda de seguridad.

Las métricas permiten observar si la seguridad integrada produce mejoras o únicamente aumenta actividades administrativas. Indicadores relacionados con vulnerabilidades detectadas tempranamente, tiempos de corrección, reincidencia de fallos y cobertura de controles ofrecen evidencia para orientar decisiones. Rajapakse et al. (2022) destacan la necesidad de prácticas que faciliten integración y colaboración durante la adopción de DevSecOps. Medir con propósito permite aprender del proceso, ajustar controles y evitar que la velocidad sea evaluada separadamente de la protección.

La cultura organizacional determina buena parte de la eficacia de DevSecOps. Cuando los errores de seguridad provocan culpabilización, los equipos tienden a ocultar problemas o retrasar su comunicación; cuando existe aprendizaje disciplinado, los incidentes alimentan mejoras técnicas y procedimentales. Rajapakse et al. (2022) identifican aspectos culturales y de conocimiento entre las dificultades de adopción. Una cultura

favorable promueve transparencia, formación continua y cooperación, sin diluir la responsabilidad individual asociada con decisiones técnicas y operativas relevantes.

Seguridad por diseño, S-SDLC y DevSecOps convergen en una idea práctica: proteger software requiere decisiones continuas durante toda su vida útil. La investigación de Rajapakse et al. (2022) evidencia que adoptar DevSecOps implica atender dimensiones técnicas, humanas y organizacionales de manera coordinada. Para la empresa inteligente, esta integración permite relacionar innovación y protección desde el origen, mantener controles durante cambios frecuentes y convertir la ciberseguridad en una capacidad cotidiana del desarrollo, operación y evolución digital.

3.4. Postura de seguridad en entornos nube y multinube (CSPM, CWPP, CNAPP) y arquitecturas híbridas distribuidas

La postura de seguridad en nube requiere una visión continua de configuraciones, identidades, cargas de trabajo, datos y relaciones entre servicios distribuidos. La expansión hacia modelos multinube amplía esa necesidad, pues cada proveedor incorpora mecanismos, responsabilidades y superficies tecnológicas diferentes. Ukeje et al. (2024) identifican riesgos de seguridad y privacidad que condicionan la adopción de servicios cloud. Frente a esta realidad, gobernar la postura implica conocer activos, evaluar exposición y mantener controles coherentes entre plataformas heterogéneas.

Las arquitecturas híbridas combinan infraestructura propia con servicios públicos, privados y recursos administrados por terceros. Esta diversidad ofrece flexibilidad, aunque también fragmenta la visibilidad cuando cada entorno aplica herramientas y criterios independientes. Ukeje et al. (2024) destacan preocupaciones vinculadas con confidencialidad, privacidad, control y gestión de información en la adopción cloud. Una postura

efectiva requiere, por tanto, políticas comunes que puedan traducirse técnicamente sin ignorar particularidades regulatorias, operativas y arquitectónicas de cada plataforma utilizada.

CSPM responde a una necesidad persistente: identificar configuraciones inseguras y desviaciones respecto de políticas establecidas en recursos cloud. Su valor reside en observar continuamente infraestructura dinámica, donde cambios frecuentes pueden introducir exposiciones inadvertidas. Aunque Ukeje et al. (2024) emplean categorías generales de seguridad cloud, su revisión evidencia preocupaciones asociadas con configuraciones, acceso y protección de información. Bajo esta perspectiva, CSPM materializa capacidades de supervisión que fortalecen gobierno, trazabilidad y corrección preventiva de exposiciones técnicas recurrentes.

CWPP desplaza la atención hacia la protección de cargas de trabajo ejecutadas en máquinas virtuales, contenedores y otros componentes computacionales distribuidos. La diversidad tecnológica exige controles capaces de acompañar dichas cargas durante construcción, despliegue y operación. Ukeje et al. (2024) señalan múltiples riesgos relacionados con seguridad y privacidad en infraestructuras cloud. Desde una perspectiva empresarial, proteger cargas requiere combinar visibilidad, gestión de vulnerabilidades, endurecimiento, supervisión operativa y respuesta ante comportamientos incompatibles con políticas previamente establecidas.

CNAPP representa una convergencia de capacidades destinadas a reducir la fragmentación entre postura, cargas, identidades y desarrollo de aplicaciones nativas de nube. Más que adoptar una etiqueta comercial, interesa comprender la integración que expresa. Ukeje et al. (2024) muestran que los riesgos cloud atraviesan múltiples dimensiones técnicas y organizacionales. Integrar capacidades permite relacionar hallazgos que, vistos aisladamente, ofrecen información parcial; una configuración

vulnerable adquiere mayor significado cuando coincide con privilegios excesivos y datos sensibles expuestos.

Figura 11
Seguridad en arquitecturas multinube

En ambientes multinube, la gestión de identidades merece atención particular porque permisos equivalentes pueden representarse mediante modelos distintos entre proveedores. La acumulación de privilegios, cuentas técnicas y credenciales incrementa posibilidades de acceso indebido cuando faltan criterios comunes de gobierno. Ukeje et al. (2024) reconocen la gestión del acceso y la protección de información entre preocupaciones relevantes para organizaciones que adoptan nube. La postura debe relacionar identidad, recurso, privilegio y actividad para detectar desviaciones significativas oportunamente.

La protección de datos constituye otro eje transversal en arquitecturas distribuidas. Información corporativa puede desplazarse entre regiones, servicios administrados, repositorios y aplicaciones, creando dependencias difíciles de observar desde una

herramienta aislada. Ukeje et al. (2024) conceden especial atención a privacidad, confidencialidad y soberanía de información dentro de la adopción cloud. Por ello, una postura madura necesita clasificación, cifrado, control de acceso y trazabilidad, acompañados por criterios que determinen ubicaciones y tratamientos permitidos organizacionalmente.

La responsabilidad compartida entre proveedor y cliente modifica la manera de interpretar controles en la nube. Contratar infraestructura administrada no transfiere automáticamente todas las obligaciones de protección, pues determinadas configuraciones, identidades, aplicaciones y datos permanecen bajo responsabilidad del consumidor. Ukeje et al. (2024) describen preocupaciones relacionadas con gobernanza, confianza y control durante la adopción cloud. Comprender estas fronteras evita vacíos operativos y permite asignar responsables internos para riesgos que podrían quedar indebidamente atribuidos al proveedor externo.

Una arquitectura híbrida distribuida necesita telemetría que permita correlacionar acontecimientos entre redes, servicios, identidades y cargas. Sin esa visión transversal, los equipos pueden recibir numerosas alertas sin comprender relaciones de riesgo. Ukeje et al. (2024) evidencian que la seguridad cloud comprende factores interdependientes que exceden controles aislados. CSPM, CWPP y capacidades agrupadas bajo CNAPP adquieren mayor utilidad cuando alimentan procesos comunes de priorización, respuesta y gobierno, en lugar de operar como repositorios desconectados de hallazgos.

Gestionar la postura de seguridad cloud implica mantener correspondencia entre transformación tecnológica, riesgo y gobierno durante cambios permanentes. CSPM aporta vigilancia sobre configuraciones; CWPP protege cargas distribuidas; CNAPP procura integrar capacidades relacionadas con aplicaciones nativas de nube. La revisión de Ukeje et al. (2024) recuerda que seguridad y privacidad continúan condicionando la confianza necesaria para

adoptar estos servicios. En empresas híbridas y multinube, la madurez reside en convertir visibilidad técnica en decisiones consistentes y verificables.

3.5. Diseños de arquitecturas resilientes basadas en microservicios, APIs seguras y ecosistemas orientados a datos

Las arquitecturas resilientes basadas en microservicios responden a una necesidad empresarial concreta: mantener capacidades digitales disponibles aun cuando determinados componentes experimenten fallos o degradaciones. La separación funcional permite desplegar, escalar y recuperar servicios con mayor independencia, aunque también multiplica interacciones que requieren protección. Matias et al. (2024) relacionan la arquitectura de microservicios con mecanismos orientados a fortalecer efectividad y seguridad. La resiliencia depende, entonces, de diseñar componentes autónomos sin perder coordinación, observabilidad ni gobierno tecnológico.

La descomposición de aplicaciones monolíticas en servicios independientes modifica profundamente las fronteras de seguridad. Cada comunicación entre componentes representa una relación que necesita autenticación, autorización y protección de datos durante el tránsito. Matias et al. (2024) destacan que la arquitectura de microservicios presenta necesidades específicas de seguridad derivadas de su naturaleza distribuida. En términos empresariales, esta característica exige abandonar controles concentrados en perímetros y distribuir mecanismos defensivos cerca de servicios, identidades y recursos digitales protegidos.

Las APIs constituyen los vínculos mediante los cuales servicios, aplicaciones y actores externos intercambian capacidades e información. Su seguridad requiere mecanismos consistentes de autenticación, autorización, validación y supervisión. Matias et al. (2024) examinan prácticas destinadas a mejorar la protección de

interacciones dentro de arquitecturas de microservicios. Una API bien gobernada no representa meramente una interfaz técnica; expresa una frontera empresarial donde confluyen permisos, datos, contratos de servicio y responsabilidades que necesitan permanecer claramente definidas.

La resiliencia también depende de aceptar que los fallos ocurrirán y diseñar respuestas antes de que afecten cadenas completas de servicios. Patrones de aislamiento, límites temporales, reintentos controlados y mecanismos de recuperación permiten contener interrupciones. Matias et al. (2024) vinculan efectividad arquitectónica y seguridad en sistemas distribuidos, una relación especialmente pertinente cuando numerosas dependencias interactúan simultáneamente. Diseñar para fallar de manera controlada convierte la continuidad en una propiedad arquitectónica, no en una reacción improvisada posteriormente.

La observabilidad adquiere relevancia particular cuando una transacción atraviesa diversos microservicios antes de producir un resultado empresarial. Registros, métricas y trazas distribuidas permiten reconstruir interacciones, detectar anomalías y comprender degradaciones operativas. Matias et al. (2024) plantean mecanismos orientados a mejorar supervisión y protección en arquitecturas distribuidas. Para los equipos de seguridad, correlacionar estas señales facilita distinguir comportamientos legítimos de actividades anómalas, mientras operaciones obtiene evidencia para diagnosticar fallos con mayor precisión y rapidez.

Los ecosistemas orientados a datos añaden otra dimensión al diseño resiliente, porque la información circula entre servicios, repositorios, procesos analíticos y consumidores diversos. Cada movimiento requiere criterios de acceso, integridad y trazabilidad. Matias et al. (2024) enfatizan la necesidad de fortalecer mecanismos de seguridad dentro de arquitecturas distribuidas. Desde esta perspectiva, proteger datos exige conocer propietarios, usos autorizados y dependencias, evitando que la descentralización

tecnológica derive en una fragmentación equivalente de responsabilidades sobre información empresarial sensible.

La autonomía de los microservicios resulta valiosa cuando está acompañada por estándares compartidos. Sin acuerdos sobre autenticación, telemetría, gestión de secretos, cifrado y manejo de errores, cada equipo puede construir soluciones incompatibles que aumenten complejidad operativa. Matias et al. (2024) relacionan prácticas arquitectónicas con mejoras de seguridad y efectividad. La organización necesita establecer guardas comunes que permitan innovar sin reconstruir controles repetidamente, conservando libertad técnica dentro de límites que protejan servicios y datos corporativos.

La gestión de secretos merece atención especial en ecosistemas donde servicios se autentican entre sí mediante credenciales, certificados o tokens. Incorporar estos elementos directamente en código o configuraciones persistentes amplía exposición y dificulta rotaciones. Matias et al. (2024) examinan mecanismos de seguridad aplicables a comunicaciones entre componentes distribuidos. Una arquitectura resiliente necesita administrar credenciales durante todo su ciclo de vida, limitar su alcance y registrar usos relevantes, reduciendo posibilidades de propagación cuando una identidad técnica resulta comprometida.

La seguridad de microservicios también depende de procesos de desarrollo capaces de detectar debilidades antes del despliegue. Revisar componentes, dependencias, interfaces y configuraciones permite reducir exposiciones acumulativas en arquitecturas con frecuentes cambios. Matias et al. (2024) presentan enfoques destinados a incrementar seguridad y efectividad mediante prácticas integradas. Cuando estas verificaciones acompañan la entrega continua, la resiliencia adquiere carácter preventivo: cada modificación puede evaluarse considerando su efecto sobre dependencias, controles existentes y comportamiento general del sistema distribuido.

Microservicios, APIs y ecosistemas orientados a datos configuran arquitecturas donde resiliencia y seguridad deben avanzar como propiedades inseparables. La investigación de Matias et al. (2024) muestra que mejorar arquitecturas distribuidas requiere combinar mecanismos técnicos con decisiones estructurales capaces de proteger comunicaciones y componentes. Para la empresa inteligente, este enfoque permite construir capacidades digitales adaptables, mantener servicios ante fallos parciales y preservar confianza sobre intercambios de información que conectan procesos, plataformas, usuarios y organizaciones externas.

3.6. Integración entre arquitectura empresarial, continuidad operativa y resiliencia tecnológica (enfoque SABSA)

Integrar arquitectura empresarial, continuidad operativa y resiliencia tecnológica exige comprender la organización como un sistema de capacidades interdependientes, donde procesos, información, personas y tecnología sostienen resultados comunes. La arquitectura aporta una visión estructurada para relacionar estas dimensiones con prioridades estratégicas. Hardi y Legowo (2023) evidencian que la arquitectura empresarial facilita transformaciones orientadas a mantener procesos operativos durante periodos disruptivos. Esta perspectiva permite vincular decisiones tecnológicas con necesidades de permanencia, adaptación y recuperación organizacional efectiva.

La continuidad operativa adquiere mayor profundidad cuando deja de tratarse como un conjunto aislado de planes de contingencia y se incorpora al diseño arquitectónico. Cada capacidad empresarial posee dependencias que deben reconocerse antes de una interrupción. Hardi y Legowo (2023) muestran que la arquitectura empresarial contribuye a reorganizar procesos operativos frente a condiciones extraordinarias. Identificar

aplicaciones, datos, infraestructura y responsables asociados permite establecer prioridades de recuperación coherentes con el valor que cada proceso entrega al negocio.

Desde una perspectiva inspirada en SABSA, la seguridad puede estructurarse partiendo de atributos empresariales que expresan aquello que la organización necesita preservar. Disponibilidad, integridad, confidencialidad y capacidad de recuperación adquieren significado cuando se relacionan con objetivos concretos. La experiencia estudiada por Hardi y Legowo (2023) demuestra que articular arquitectura y transformación facilita ajustes operativos ante disrupciones. Esta orientación evita diseñar controles desconectados del negocio y permite justificar inversiones mediante necesidades empresariales claramente identificables y medibles.

La resiliencia tecnológica no consiste meramente en mantener sistemas encendidos. Implica preservar servicios prioritarios, adaptarse ante alteraciones y recuperar capacidades dentro de niveles aceptables para la organización. Hardi y Legowo (2023) relacionan arquitectura empresarial y transformación digital con la continuidad de procesos bajo circunstancias adversas. Desde esta mirada, redundancia, recuperación y disponibilidad necesitan responder a prioridades previamente establecidas. Una arquitectura resiliente distingue qué capacidades requieren mayor protección y cuáles admiten interrupciones temporales sin consecuencias graves.

El enfoque SABSA aporta una lógica de trazabilidad que vincula necesidades empresariales con requisitos de seguridad, servicios y mecanismos tecnológicos. Esta relación resulta pertinente para continuidad y resiliencia porque permite comprender la razón detrás de cada control. Hardi y Legowo (2023) evidencian que la arquitectura empresarial facilita la transformación de procesos operativos mediante una visión estructurada. Cuando existe trazabilidad, una inversión en

disponibilidad o recuperación puede justificarse por su contribución directa a capacidades empresariales prioritarias claramente reconocidas.

Las dependencias tecnológicas constituyen uno de los puntos más delicados para la continuidad empresarial. Un proceso aparentemente independiente puede depender de servicios de identidad, conectividad, datos, proveedores o aplicaciones compartidas cuya indisponibilidad produce efectos encadenados. Hardi y Legowo (2023) muestran la utilidad de la arquitectura empresarial para comprender y transformar procesos durante situaciones disruptivas. Mapear estas relaciones permite anticipar concentraciones de riesgo, establecer alternativas y diseñar mecanismos de recuperación atendiendo dependencias reales, no estructuras organizativas formales.

La arquitectura empresarial también facilita conversaciones entre responsables que suelen observar la continuidad desde perspectivas diferentes. Tecnología piensa en infraestructura; negocio, en procesos; seguridad, en riesgos; dirección, en impacto y prioridades. Hardi y Legowo (2023) evidencian que una aproximación arquitectónica permite articular transformación y operación mediante estructuras comprensibles. SABSA refuerza esta orientación al partir de necesidades empresariales para derivar requisitos de protección, creando un lenguaje que conecta decisiones técnicas con consecuencias económicas y operativas verificables.

La resiliencia requiere capacidad de adaptación además de recuperación. Una organización puede restaurar técnicamente sus plataformas y, aun entonces, resultar incapaz de responder a nuevas condiciones operativas. Hardi y Legowo (2023) describen la arquitectura empresarial como habilitadora de cambios en procesos durante la disrupción provocada por la pandemia. Esta experiencia muestra que continuidad y transformación pueden avanzar conjuntamente cuando la arquitectura permite reorganizar

capacidades, modificar dependencias y adoptar tecnologías sin perder correspondencia con prioridades institucionales definidas.

Las pruebas de continuidad adquieren mayor valor cuando reproducen dependencias arquitectónicas y decisiones reales de negocio. Verificar respaldos resulta insuficiente si no se comprueba que servicios prioritarios pueden recuperarse con identidades, conectividad, información y personal disponibles. La experiencia analizada por Hardi y Legowo (2023) destaca la importancia de adaptar procesos operativos mediante arquitectura empresarial. Desde una orientación SABSA, las pruebas pueden vincularse con atributos de negocio y evidenciar si los controles cumplen expectativas de resiliencia previamente acordadas.

Integrar arquitectura empresarial, continuidad y resiliencia tecnológica convierte la protección organizacional en una disciplina vinculada directamente con la estrategia. SABSA ofrece una orientación basada en atributos y trazabilidad, mientras la arquitectura empresarial organiza capacidades, procesos y dependencias que requieren protección. Hardi y Legowo (2023) muestran que esta disciplina puede habilitar adaptación operativa durante periodos de transformación intensa. La empresa inteligente necesita esa convergencia para preservar servicios prioritarios mientras cambia, aprende y reorganiza sus capacidades digitales.

Tabla 3

Integración de enfoques arquitectónicos y de seguridad para la empresa digital

Enfoque o componente	**Aplicación en la arquitectura empresarial y la ciberseguridad**
TOGAF y Zachman	Estructuran la relación entre estrategia, procesos, información, aplicaciones e infraestructura. TOGAF orienta la evolución arquitectónica mediante ADM, mientras Zachman organiza perspectivas y artefactos

Enfoque o componente	Aplicación en la arquitectura empresarial y la ciberseguridad
	empresariales para favorecer coherencia y trazabilidad.
Zero Trust y NIST SP 800-207	Sustituyen la confianza implícita por verificación continua de identidades, dispositivos y solicitudes de acceso. Favorecen mínimo privilegio, segmentación y decisiones de autorización vinculadas con condiciones observables de riesgo.
Seguridad por diseño, S-SDLC y DevSecOps	Incorporan requisitos y controles de seguridad durante todo el ciclo de vida del software. Integran desarrollo, operaciones y seguridad mediante colaboración, automatización, pruebas continuas y gestión temprana de vulnerabilidades.
CSPM, CWPP y CNAPP	Fortalecen la postura de seguridad en nube y multinube mediante supervisión de configuraciones, protección de cargas y correlación de riesgos asociados con aplicaciones, identidades, datos e infraestructura distribuida.
Microservicios, APIs y ecosistemas de datos	Promueven arquitecturas modulares y escalables mediante servicios independientes e interfaces controladas. Requieren autenticación, autorización, observabilidad, protección de comunicaciones y mecanismos de recuperación para preservar seguridad y resiliencia.
SABSA, continuidad y resiliencia tecnológica	Vinculan atributos empresariales con requisitos de protección, continuidad y recuperación. Facilitan trazabilidad entre necesidades del negocio, dependencias tecnológicas, controles de seguridad y capacidades necesarias para mantener servicios prioritarios frente a interrupciones.

Nota. Elaboración propia a partir de Hardi y Legowo (2023), Anderson et al. (2023), Rajapakse et al. (2022), Ukeje et al. (2024) y Matias et al. (2024).

Capítulo 4:

Protección Integral de Activos Digitales, Gestión de Cibercrisis y Resiliencia Operativa

La transformación digital ha convertido la protección de los activos empresariales en una responsabilidad que atraviesa tecnología, gobierno y continuidad operativa. Cada identidad, dato, dispositivo o servicio conectado participa en una red de dependencias cuya alteración puede extenderse rápidamente hacia procesos esenciales. Glöckler et al. (2024) explican que la gestión contemporánea de identidades empresariales requiere atender seguridad, privacidad e interoperabilidad. Esta mirada permite comprender la ciberseguridad como capacidad organizacional vinculada directamente con confianza, operación y sostenibilidad institucional.

La identidad ocupa una posición determinante porque cada interacción digital comienza con alguna forma de reconocimiento, autenticación y autorización. Personas, aplicaciones, dispositivos y terceros necesitan acceder a recursos bajo criterios verificables, evitando privilegios acumulados o permisos carentes de justificación. Glöckler et al. (2024) identifican requisitos empresariales diversos para la gestión de identidades y accesos, particularmente en entornos distribuidos. IAM, PAM e IGA adquieren, entonces, relevancia como mecanismos complementarios para gobernar relaciones digitales cada vez más complejas.

Junto con las identidades, los datos estratégicos representan activos cuya exposición puede afectar competitividad, reputación y cumplimiento regulatorio. Cifrar información resulta necesario, aunque insuficiente cuando las organizaciones desconocen dónde permanecen determinadas copias o quién puede utilizarlas. Raaj (2025) describe DSPM como un enfoque destinado a identificar información sensible y evaluar riesgos asociados con su exposición. Al combinar cifrado, prevención de pérdida de datos y visibilidad continua, la protección adquiere mayor precisión y capacidad preventiva empresarial.

La superficie tecnológica se extiende todavía más cuando sensores, controladores y dispositivos conectados intervienen directamente sobre procesos físicos. En estos entornos, una alteración digital puede producir consecuencias operacionales inmediatas. Kanamaru (2024) examina la seguridad en la era IoT destacando particularidades derivadas de la diversidad y conectividad de los dispositivos. Esta convergencia entre IoT, tecnologías operacionales y sistemas ciberfísicos exige integrar perspectivas de seguridad, ingeniería y operación, pues sus dependencias ya resultan difíciles de separar.

Figura 12

Arquitectura integral de protección digital

Las dependencias también atraviesan las fronteras de cada organización. Proveedores de software, servicios administrados, plataformas en nube y componentes tecnológicos forman cadenas donde una interrupción externa puede afectar funciones internas esenciales. Aghazadeh Ardebili et al. (2024) relacionan la resiliencia de infraestructuras críticas con métodos de evaluación de riesgos, estándares y estructuras de gobernanza. Comprender esas

interdependencias permite orientar decisiones hacia la continuidad de servicios, evaluando proveedores no como elementos periféricos, sino como participantes del riesgo empresarial.

Ahora bien, ninguna arquitectura defensiva garantiza ausencia absoluta de incidentes. La cuestión relevante pasa por la capacidad institucional para reconocer una intrusión, contenerla y recuperar operaciones sin perder dirección durante la incertidumbre. Lee et al. (2022) estudian arquitecturas de orquestación, automatización y respuesta capaces de coordinar herramientas frente a amenazas complejas. Estas capacidades tecnológicas adquieren mayor sentido cuando acompañan procedimientos estructurados, responsabilidades previamente definidas y decisiones ejecutivas capaces de equilibrar seguridad, continuidad, evidencia y comunicación corporativa.

Una cibercrisis modifica prioridades con rapidez. Lo que comienza como una alerta técnica puede alcanzar dirección, clientes, reguladores y socios comerciales en pocas horas. Por ello, la gestión de incidentes necesita canales de escalamiento, autoridad decisoria y comunicación basada en hechos verificados. Lee et al. (2022) muestran que integrar información y automatizar determinadas acciones puede favorecer respuestas coordinadas. La tecnología aporta velocidad; el juicio profesional conserva la responsabilidad de valorar consecuencias cuando las decisiones afectan operaciones esenciales.

La recuperación, por su parte, necesita algo más convincente que planes cuidadosamente redactados. BCP y DRP adquieren valor cuando han sido ejecutados, medidos y corregidos mediante ejercicios capaces de reproducir condiciones adversas. Karagiannis et al. (2024) destacan el aporte de entornos de entrenamiento realistas para desarrollar competencias en equipos SOC. Red Team, Blue Team y las simulaciones automatizadas permiten observar defensas bajo presión, revelar dependencias

inadvertidas y convertir errores controlados en oportunidades concretas de aprendizaje organizacional.

Vista en conjunto, la resiliencia digital nace de relaciones bien gobernadas entre personas, procesos, tecnologías y terceros. Aghazadeh Ardebili et al. (2024) muestran que su evaluación requiere considerar métodos, gobierno y estándares, mientras Karagiannis et al. (2024) resaltan la importancia del aprendizaje práctico para fortalecer capacidades defensivas. Ambas perspectivas convergen en una idea relevante: resistir una perturbación requiere preparación previa, pero también evidencia obtenida mediante pruebas que permitan corregir debilidades antes de una crisis real.

Este capítulo aborda, por tanto, una protección integral que comienza con identidades y privilegios, continúa sobre datos y entornos ciberfísicos, alcanza infraestructuras y cadenas de suministro, y desemboca en respuesta y continuidad. Raaj (2025) aporta la perspectiva de visibilidad sobre datos; Kanamaru (2024), la mirada sobre IoT; y Glöckler et al. (2024), el gobierno de identidades. En conjunto, estas aportaciones permiten entender la resiliencia como una práctica continua, medible y profundamente vinculada con decisiones humanas.

4.1. Gestión inteligente de identidades, accesos y privilegios corporativos (IAM, PAM, IGA)

La gestión inteligente de identidades constituye un eje de protección empresarial porque vincula personas, aplicaciones, dispositivos y permisos dentro de una arquitectura gobernada. IAM organiza la autenticación y autorización; PAM restringe cuentas con capacidades elevadas; IGA aporta gobierno, revisión y trazabilidad. Glöckler, Sedlmeir y Frank (2024) señalan que las organizaciones requieren mecanismos capaces de administrar identidades heterogéneas durante todo su ciclo de vida,

especialmente cuando proliferan servicios digitales, relaciones externas y entornos distribuidos de negocio.

En una empresa digital, conceder acceso ya no puede entenderse como un trámite administrativo aislado. Cada autorización expresa una decisión de riesgo y, por ello, debe responder a funciones, responsabilidades y necesidades verificables. La investigación de Glöckler et al. (2024) destaca requisitos empresariales relacionados con privacidad, interoperabilidad, seguridad y control de atributos. Desde esta perspectiva, IAM adquiere valor cuando conecta las políticas corporativas con decisiones de acceso consistentes, auditables y adaptables al cambio organizacional continuo.

PAM atiende una zona especialmente sensible: las credenciales privilegiadas que permiten administrar servidores, bases de datos, redes, plataformas en la nube y componentes críticos. Una cuenta administrativa comprometida puede ampliar con rapidez el alcance de un incidente. Por esa razón, conviene aplicar bóvedas de credenciales, sesiones supervisadas, elevación temporal y rotación automática más estricta. Esta disciplina coincide con la demanda de mayor control sobre datos de identidad y autorizaciones descrita por Glöckler et al. (2024).

IGA amplía la mirada al incorporar procesos de gobierno que permiten saber quién posee acceso, por qué lo posee, quién lo aprobó y cuándo debe revisarse. Esa trazabilidad resulta indispensable frente a cambios de puesto, contrataciones, desvinculaciones y relaciones con terceros. Glöckler et al. (2024) observan que la gestión empresarial de identidades enfrenta requerimientos diversos entre dominios y actores. La gobernanza reduce esa fragmentación mediante políticas comunes, certificaciones periódicas y responsabilidades claramente asignadas en conjunto.

La inteligencia aplicada a IAM, PAM e IGA permite pasar de reglas estáticas a decisiones apoyadas en señales de riesgo. Horario, ubicación, dispositivo, comportamiento y sensibilidad del recurso pueden alimentar mecanismos de autenticación adaptativa. No se trata de reemplazar el juicio profesional, sino de enriquecerlo con evidencia oportuna y verificable. Glöckler et al. (2024) resaltan la relevancia de minimizar la exposición de información personal, principio que favorece modelos de acceso más selectivos, proporcionales y respetuosos.

El principio de mínimo privilegio adquiere una dimensión práctica cuando los permisos dejan de acumularse silenciosamente. En muchas organizaciones, una persona conserva accesos heredados de funciones anteriores, proyectos concluidos o aplicaciones abandonadas. Esa deriva incrementa la superficie de ataque. La revisión continua permite retirar privilegios innecesarios y justificar excepciones. De acuerdo con Glöckler et al. (2024), los esquemas empresariales deben responder a requisitos de control, seguridad y usabilidad sin deteriorar la experiencia de los participantes.

La automatización del ciclo de vida de la identidad también fortalece la resiliencia operativa. El alta de un colaborador puede activar permisos previamente aprobados; un traslado interno puede modificar roles; una desvinculación debe revocar accesos con rapidez. Estos flujos reducen errores y ventanas de exposición. Glöckler et al. (2024) describen la interoperabilidad como una exigencia relevante en ecosistemas empresariales, aspecto que favorece integrar directorios, aplicaciones, servicios externos y plataformas corporativas de gobierno bajo criterios coherentes.

Otro componente relevante es la identidad de terceros. Proveedores, consultores, aliados y clientes participan en procesos corporativos sin pertenecer necesariamente al directorio interno. Administrar esas relaciones exige mecanismos federados, atributos verificables y límites temporales. Glöckler et al. (2024) analizan el

potencial de la identidad autosoberana para ofrecer mayor control al titular y facilitar intercambios confiables de información. Su adopción empresarial, sin embargo, requiere compatibilidad tecnológica, gobernanza definida y acuerdos entre las partes involucradas a escala.

La eficacia de IAM, PAM e IGA depende también de métricas que permitan observar el comportamiento del sistema. Resulta útil medir cuentas huérfanas, privilegios permanentes, revisiones vencidas, accesos rechazados, tiempos de revocación y excepciones corporativas abiertas periódicas. Los indicadores convierten la gobernanza en una práctica verificable, no en una declaración normativa. En línea con Glöckler et al. (2024), evaluar requisitos técnicos y organizativos ayuda a reconocer tensiones entre seguridad, privacidad, integración y facilidad de uso.

Una estrategia madura integra IAM, PAM e IGA con arquitectura empresarial, gestión de riesgos, cumplimiento y respuesta ante incidentes. La identidad deja entonces de ser una capa periférica y se convierte en un punto de decisión transversal. Glöckler et al. (2024) muestran que los requisitos de gestión de identidades abarcan dimensiones técnicas, organizativas y regulatorias. Articularlas permite proteger activos sin frenar la operación, preservar evidencias de auditoría y sostener relaciones de confianza entre actores corporativos.

4.2. Protección avanzada de datos estratégicos: cifrado, DLP y Data Security Posture Management (DSPM)

La protección de datos estratégicos exige una visión que trascienda el almacenamiento y abarque cada movimiento de la información empresarial. El cifrado protege contenidos frente a accesos indebidos, mientras DLP controla transferencias potencialmente riesgosas y DSPM aporta visibilidad sobre exposición, ubicación y configuración. Raaj (2025) plantea que DSPM permite identificar riesgos asociados con datos sensibles

distribuidos en infraestructuras diversas. Esta perspectiva favorece decisiones preventivas, especialmente cuando la información circula entre nubes, aplicaciones y repositorios corporativos.

El cifrado constituye una barrera técnica esencial para preservar confidencialidad cuando los datos permanecen almacenados o viajan entre sistemas. Su eficacia, sin embargo, depende de una gestión rigurosa de claves, certificados, algoritmos y permisos administrativos. Una clave expuesta puede neutralizar una arquitectura avanzada. Desde la perspectiva presentada por Raaj (2025), la protección moderna requiere comprender dónde residen los datos sensibles y qué riesgos acompañan su tratamiento, condición necesaria para aplicar controles proporcionales a cada activo.

Las tecnologías DLP aportan una capacidad distinta: observar el uso de la información y detener acciones contrarias a las políticas corporativas. Pueden detectar documentos confidenciales enviados por correo, copiados hacia dispositivos externos o transferidos mediante servicios externos. Esta vigilancia requiere criterios precisos para evitar interrupciones innecesarias. Raaj (2025) destaca que la visibilidad sobre datos sensibles constituye una base relevante para gestionar su postura de seguridad, particularmente en ecosistemas tecnológicos distribuidos y sujetos a cambios frecuentes.

DSPM responde a una dificultad habitual en organizaciones digitalizadas: existen datos que nadie recuerda, repositorios creados para proyectos antiguos y copias que permanecen fuera de los controles previstos. La tecnología permite descubrir, clasificar y relacionar esa información con permisos y configuraciones. Según Raaj (2025), DSPM facilita una evaluación continua de riesgos vinculados con datos sensibles. Tal capacidad transforma inventarios dispersos en conocimiento operativo, útil para priorizar correcciones según exposición, importancia empresarial y posibles consecuencias adversas.

La combinación de cifrado, DLP y DSPM adquiere valor cuando cada tecnología cumple una función complementaria. El cifrado reduce la utilidad de información obtenida ilegítimamente; DLP limita movimientos indebidos; DSPM descubre exposiciones y configuraciones inseguras. Raaj (2025) vincula este último enfoque con la identificación y mitigación continua de riesgos sobre datos. Integrar estas capacidades permite abandonar controles fragmentados y construir una protección basada en conocimiento, trazabilidad y respuesta coordinada ante variaciones del entorno tecnológico corporativo.

Clasificar la información constituye un requisito previo para protegerla con criterio. No todos los registros poseen igual valor empresarial ni generan las mismas consecuencias ante una filtración. Datos financieros, propiedad intelectual, credenciales y expedientes personales requieren tratamientos diferenciados. Raaj (2025) señala que DSPM contribuye al descubrimiento y clasificación de información sensible, facilitando la evaluación de exposición. Esta capacidad permite orientar cifrado y políticas DLP hacia activos prioritarios, evitando controles indiscriminados que pueden incrementar complejidad innecesariamente.

La expansión de servicios en nube ha multiplicado repositorios, copias, integraciones y permisos, haciendo más difícil mantener una visión de la información estratégica. Un archivo protegido inicialmente puede terminar replicado en una ubicación con controles insuficientes. Raaj (2025) relaciona DSPM con la obtención de visibilidad continua sobre datos y riesgos asociados. Esa observación permanente permite detectar desviaciones tempranas, revisar configuraciones y reducir superficies de exposición antes de que una debilidad técnica derive en incidente significativo.

La prevención de fugas también requiere comprender comportamientos humanos. Un empleado puede compartir información por error, utilizar canales inadecuados o conservar

archivos después de perder una responsabilidad funcional. DLP aporta controles frente a estas situaciones, pero su diseño necesita equilibrio y comprensión del trabajo cotidiano. Raaj (2025) sostiene que la seguridad de datos demanda identificar exposiciones y priorizar riesgos de manera continua. La tecnología gana eficacia cuando acompaña procesos comprensibles, responsabilidades y prácticas organizacionales verificables.

Figura 13
Protección estratégica de datos

La postura de seguridad de datos debe medirse mediante indicadores capaces de revelar cambios significativos. Repositorios expuestos, permisos excesivos, datos sensibles sin cifrar, transferencias bloqueadas y activos desconocidos ofrecen señales para equipos de seguridad y gobierno. De acuerdo con Raaj (2025), DSPM favorece la evaluación continua del riesgo asociado con información distribuida. Convertir estas señales en métricas facilita priorizar inversiones, justificar medidas correctivas y comunicar a la dirección una visión comprensible de la exposición empresarial.

Una estrategia avanzada de protección reconoce que el dato mantiene valor durante todo su ciclo de vida y, necesita controles persistentes. Cifrado, DLP y DSPM forman una arquitectura complementaria cuando se integran con gobierno, gestión de riesgos y respuesta ante incidentes. Raaj (2025) presenta DSPM como un enfoque orientado a descubrir y reducir exposiciones de información sensible. Esta integración permite proteger activos estratégicos con mayor precisión, preservar confianza y fortalecer continuidad operativa ante amenazas cambiantes.

4.3. Seguridad en Internet de las Cosas (IoT), tecnologías operacionales (OT) y sistemas ciberfísicos

La expansión del Internet de las Cosas ha transformado la frontera entre información digital y procesos físicos. Sensores, actuadores, plataformas industriales y dispositivos conectados intercambian datos mientras ejecutan funciones capaces de afectar operaciones reales. Kanamaru (2024) plantea que la era IoT amplía las superficies de exposición debido a la creciente interconexión entre equipos y redes. Proteger estos entornos exige reconocer que una vulnerabilidad informática puede traducirse rápidamente en consecuencias operativas, económicas e incluso físicas relevantes.

En tecnologías operacionales, la seguridad adquiere matices distintos de los habituales en sistemas administrativos. La disponibilidad, continuidad y seguridad física de procesos industriales condicionan cualquier decisión defensiva. Detener una máquina para instalar una actualización puede resultar técnicamente apropiado, aunque operacionalmente inviable en determinado momento. Kanamaru (2024) destaca que los dispositivos IoT presentan restricciones y características particulares frente a equipos informáticos convencionales. Por ello, las medidas de protección deben considerar capacidades, funciones productivas y consecuencias empresariales.

Los sistemas ciberfísicos integran procesamiento, comunicación y actuación sobre el mundo material, creando dependencias que merecen atención permanente. Una orden digital alterada puede modificar temperatura, velocidad, presión o movimiento dentro de una instalación. De acuerdo con Kanamaru (2024), la conectividad característica del IoT incrementa oportunidades de interacción, pero también amplía riesgos de seguridad. Esta relación obliga a vincular ciberseguridad con ingeniería, mantenimiento y gestión operacional, evitando tratar la protección tecnológica como una responsabilidad corporativa aislada.

El inventario de activos representa un punto de partida indispensable en entornos IoT y OT. Resulta difícil proteger dispositivos cuya existencia, versión, propietario o función permanecen desconocidos para la organización. Cámaras, controladores, sensores y pasarelas pueden conservar configuraciones antiguas durante años. Kanamaru (2024) advierte que la diversidad de dispositivos conectados plantea problemas particulares de seguridad. Mantener visibilidad sobre y dependencias facilita detectar anomalías, priorizar intervenciones y reducir espacios donde una amenaza podría permanecer inadvertida.

La segmentación de redes permite limitar el movimiento de un atacante entre dispositivos conectados y sistemas industriales. Separar funciones críticas, restringir comunicaciones y controlar puntos de intercambio disminuye la propagación de incidentes. Esta arquitectura debe responder a flujos operativos reales, no a divisiones diseñadas desde escritorios distantes. Kanamaru (2024) relaciona la seguridad IoT con la necesidad de afrontar amenazas derivadas de conexiones. Una segmentación bien gobernada preserva operaciones mientras reduce exposición entre dominios tecnológicos diferentes.

La autenticación de dispositivos merece tanta atención como la identidad de las personas. Cada sensor, controlador o pasarela que intercambia información debería demostrar su legitimidad antes de participar en procesos corporativos. Credenciales predeterminadas, certificados vencidos y claves compartidas deterioran esa confianza técnica. Kanamaru (2024) examina riesgos asociados con dispositivos IoT y sus mecanismos de comunicación. Gestionar identidades técnicas, renovar credenciales y verificar integridad permite establecer relaciones entre máquinas dentro de ecosistemas crecientemente automatizados y distribuidos.

La actualización de firmware plantea una tensión persistente entre protección y continuidad. Muchos dispositivos permanecen instalados durante periodos prolongados, mientras sus fabricantes modifican productos, interrumpen soporte o publican correcciones con ritmos diferentes. Kanamaru (2024) señala particularidades de seguridad vinculadas al ciclo tecnológico del IoT. Una política madura evalúa vulnerabilidades, disponibilidad de parches, criticidad operativa y ventanas de mantenimiento. Cuando actualizar resulta imposible, controles compensatorios pueden reducir exposición sin comprometer innecesariamente procesos esenciales de la organización.

La supervisión continua permite reconocer comportamientos que una revisión periódica podría pasar por alto. Cambios inesperados de tráfico, conexiones hacia destinos desconocidos o modificaciones en controladores pueden revelar actividad anómala. En la perspectiva de Kanamaru (2024), el crecimiento del IoT demanda atención a amenazas asociadas con conectividad y heterogeneidad. Correlacionar eventos digitales con variables operacionales aporta una lectura más rica del riesgo y ayuda a distinguir incidentes reales de variaciones normales propias del proceso productivo.

La respuesta ante incidentes en OT e IoT requiere coordinación entre especialistas de seguridad, ingeniería, operaciones y dirección. Una acción defensiva precipitada podría detener procesos o afectar equipos físicos. Por esta razón, los procedimientos deben ensayarse antes de una crisis. Kanamaru (2024) enfatiza las particularidades que acompañan la protección de entornos conectados. Preparar escenarios, responsabilidades y canales de comunicación permite responder con criterio cuando cada minuto importa y las decisiones digitales producen efectos materiales inmediatos.

La seguridad de IoT, OT y sistemas ciberfísicos debe integrarse al gobierno empresarial desde el diseño de nuevas capacidades digitales. Comprar dispositivos conectados sin evaluar soporte, comunicaciones, actualizaciones y dependencia tecnológica puede trasladar riesgos hacia años posteriores. Kanamaru (2024) presenta la ciberseguridad IoT como una materia que requiere respuestas acordes con sus características particulares. Vincular arquitectura, riesgo, continuidad e ingeniería permite construir operaciones resilientes donde innovación y protección avanzan mediante decisiones conscientes, medibles y sostenibles.

4.4. Resiliencia de infraestructuras críticas y aseguramiento de la cadena de suministro tecnológica

La resiliencia de infraestructuras críticas representa una capacidad empresarial orientada a mantener servicios esenciales frente a incidentes tecnológicos, fallos operativos o ataques deliberados. No basta prevenir intrusiones; también importa resistir, responder y recuperar funciones dentro de márgenes aceptables. Aghazadeh Ardebili et al. (2024) vinculan la resiliencia cibernética con métodos de evaluación de riesgos, estructuras de gobierno y estándares. Esta visión desplaza la seguridad desde controles aislados hacia capacidades organizacionales preparadas para condiciones adversas.

Las infraestructuras críticas dependen crecientemente de ecosistemas tecnológicos donde convergen redes, aplicaciones, plataformas industriales, comunicaciones y servicios externos. Una interrupción localizada puede propagarse mediante dependencias difíciles de advertir durante operaciones normales. Aghazadeh Ardebili et al. (2024) destacan la necesidad de evaluar riesgos considerando interdependencias y dimensiones organizacionales. Mapear relaciones entre activos, procesos y proveedores permite reconocer puntos de concentración cuya pérdida afectaría funciones esenciales, facilitando decisiones de protección basadas en consecuencias operativas verificables y prioridades.

La evaluación del riesgo adquiere mayor utilidad cuando abandona fotografías estáticas y acompaña la evolución de amenazas, vulnerabilidades y dependencias. Las infraestructuras cambian, los proveedores actualizan servicios y nuevas conexiones alteran exposiciones previamente aceptadas. Según Aghazadeh Ardebili et al. (2024), diversos métodos contribuyen a valorar la resiliencia cibernética desde perspectivas complementarias. Combinar análisis técnicos con conocimiento operativo permite identificar escenarios plausibles, estimar impactos y decidir inversiones donde la reducción del riesgo ofrece mayor valor institucional.

El gobierno de la resiliencia requiere responsabilidades definidas antes de que ocurra una interrupción. Dirección, tecnología, seguridad, operaciones y gestión de proveedores deben conocer sus atribuciones y mecanismos de coordinación. Durante una crisis, la ambigüedad consume tiempo valioso. Aghazadeh Ardebili et al. (2024) reconocen la gobernanza como componente relevante en la evaluación y fortalecimiento de infraestructuras críticas. Establecer autoridad, criterios de escalamiento y mecanismos de rendición de cuentas convierte la preparación técnica en capacidad institucional efectiva.

La cadena de suministro tecnológica amplía el perímetro de riesgo más allá de las fronteras corporativas. Software, componentes, servicios administrados y plataformas externas incorporan dependencias que pueden convertirse en vías indirectas de compromiso. Aghazadeh Ardebili et al. (2024) examinan la resiliencia desde una perspectiva donde las relaciones e interdependencias afectan la evaluación del riesgo. Conocer proveedores críticos, servicios contratados y conexiones autorizadas permite priorizar controles y anticipar consecuencias cuando un tercero experimenta una interrupción severa o incidente cibernético.

Figura 14

Resiliencia de infraestructuras y cadena tecnológica

Asegurar proveedores tecnológicos requiere criterios de evaluación durante contratación, operación, renovación y terminación de servicios. Certificaciones o cuestionarios aportan evidencia, pero pierden valor cuando se convierten en formalidades documentales. Resulta preferible relacionar requisitos con el riesgo del servicio prestado. Aghazadeh Ardebili et al. (2024) resaltan la

contribución de estándares y marcos de gobierno para estructurar prácticas de resiliencia. Contratos, auditorías y métricas pueden traducir esas expectativas en obligaciones verificables durante toda relación comercial.

La diversidad de proveedores puede reducir dependencias excesivas, aunque también incrementa complejidad de integración y supervisión. Concentrar servicios esenciales en una plataforma genera eficiencia, pero una interrupción puede afectar simultáneamente numerosos procesos. La resiliencia demanda examinar estos compromisos con criterios empresariales. Aghazadeh Ardebili et al. (2024) relacionan la evaluación con el análisis de riesgos y capacidades de recuperación. Identificar alternativas, redundancias y procedimientos manuales permite sostener funciones prioritarias cuando tecnologías habituales dejan de estar disponibles temporalmente.

La preparación para incidentes requiere ejercicios que representen situaciones creíbles: indisponibilidad de proveedores, compromiso de software, interrupciones de comunicaciones o pérdida de plataformas compartidas. Estos ensayos revelan dependencias que los documentos rara vez muestran. Aghazadeh Ardebili et al. (2024) destacan la importancia de metodologías capaces de valorar dimensiones múltiples de resiliencia. Practicar decisiones bajo presión permite evaluar tiempos de recuperación, coordinación interinstitucional y capacidad de mantener servicios esenciales mientras equipos técnicos contienen y reparan daños.

Los estándares ofrecen lenguaje común para ordenar controles, responsabilidades y métricas, aunque su adopción requiere adaptación a características operativas particulares. Cumplir requisitos formales no garantiza capacidad real para resistir una crisis. Aghazadeh Ardebili et al. (2024) analizan distintos estándares relacionados con evaluación y gobierno de la resiliencia cibernética. Su utilidad aumenta cuando sirven para comparar capacidades, identificar brechas y orientar mejoras

medibles, vinculando cumplimiento normativo con continuidad de servicios y gestión efectiva del riesgo empresarial.

La resiliencia madura se reconoce cuando la organización puede anticipar perturbaciones, absorber impactos, recuperar operaciones y aprender de cada incidente. Esta capacidad depende tanto de arquitectura tecnológica como de gobierno, proveedores y cultura institucional. Aghazadeh Ardebili et al. (2024) plantean que métodos, estándares y estructuras de gobernanza contribuyen conjuntamente a evaluar la resiliencia de infraestructuras críticas. Integrar cadena de suministro y riesgo cibernético permite preservar servicios esenciales aun cuando determinadas defensas preventivas resulten superadas.

4.5. Respuesta a incidentes (NIST SP 800-61/ISO 27035) y gestión ejecutiva de cibercrisis

La respuesta a incidentes constituye una capacidad organizacional que articula preparación, detección, análisis, contención, recuperación y aprendizaje. Marcos como NIST SP 800-61 e ISO 27035 aportan estructuras para ordenar decisiones cuando la presión aumenta y la información permanece incompleta. Lee et al. (2022) destacan que la orquestación y automatización permiten coordinar herramientas y procesos de seguridad. Esta integración reduce demoras operativas y facilita que los especialistas concentren su atención en eventos de mayor impacto empresarial.

Un incidente tecnológico puede transformarse en cibercrisis cuando compromete operaciones, reputación, obligaciones regulatorias o relaciones con clientes. En ese punto, la respuesta deja de pertenecer exclusivamente al equipo técnico y exige dirección ejecutiva responsable. Lee et al. (2022) describen arquitecturas capaces de integrar detección, análisis y respuesta mediante mecanismos automatizados. Para la dirección, disponer de información oportuna resulta esencial al decidir prioridades,

autorizar medidas extraordinarias y comunicar consecuencias sin alimentar incertidumbre innecesaria entre actores involucrados.

La preparación determina buena parte de la calidad de una respuesta. Equipos definidos, canales alternativos, criterios de escalamiento y procedimientos ensayados permiten actuar con mayor disciplina cuando aparece un incidente. NIST SP 800-61 e ISO 27035 orientan esta organización mediante procesos estructurados de manejo de eventos. En paralelo, Lee et al. (2022) señalan que la automatización puede integrar capacidades dispersas de seguridad, favoreciendo respuestas coordinadas ante amenazas que atraviesan distintos dominios tecnológicos y operativos empresariales.

Detectar un incidente con rapidez requiere combinar telemetría, inteligencia de amenazas y capacidad analítica. Sin embargo, acumular alertas no equivale a comprender una crisis. El valor aparece cuando los datos permiten establecer alcance, severidad y posibles consecuencias. Lee et al. (2022) plantean que las arquitecturas SOAR facilitan la coordinación de información procedente de herramientas. Esta capacidad favorece la priorización de eventos y reduce tareas repetitivas durante etapas donde el tiempo condiciona decisiones técnicas y ejecutivas.

La contención plantea decisiones delicadas porque detener una amenaza puede afectar servicios necesarios para el negocio. Aislar servidores, bloquear cuentas o suspender conexiones requiere ponderar seguridad, continuidad y evidencia disponible. Lee et al. (2022) muestran que la orquestación permite coordinar acciones de respuesta entre componentes tecnológicos heterogéneos. Bajo una gestión ejecutiva madura, estas medidas responden a criterios acordados, evitando improvisaciones que podrían ampliar pérdidas, destruir evidencia o prolongar innecesariamente la interrupción de operaciones esenciales corporativas.

La automatización aporta velocidad, aunque requiere límites. Un procedimiento automatizado puede bloquear indicadores conocidos, recopilar evidencias o ejecutar verificaciones sin esperar intervención manual. Lee et al. (2022) destacan el papel de SOAR para integrar herramientas, automatizar tareas y coordinar respuestas frente a amenazas complejas. Las decisiones con efectos severos sobre operaciones, clientes o cumplimiento deben mantener supervisión humana, pues la rapidez pierde valor cuando una acción técnicamente correcta genera consecuencias desproporcionadas o difíciles de revertir.

Durante una cibercrisis, la comunicación ejecutiva adquiere tanta importancia como la contención técnica. Directivos, reguladores, clientes y socios necesitan información, aunque cada audiencia demanda niveles distintos de detalle. Comunicar demasiado pronto puede difundir datos incorrectos; hacerlo tarde puede deteriorar confianza. Lee et al. (2022) resaltan la integración de información como elemento relevante para respuestas coordinadas. Una estructura de crisis debe establecer vocerías, frecuencias de actualización y mecanismos para validar hechos antes de comunicar decisiones institucionales.

La recuperación no consiste meramente en reactivar sistemas. Antes de restablecer servicios, conviene verificar cuidadosamente integridad, eliminar persistencias maliciosas, renovar credenciales y confirmar que las condiciones han disminuido. Lee et al. (2022) presentan mecanismos de respuesta automatizada capaces de apoyar acciones coordinadas frente a incidentes complejos. Esta capacidad puede acelerar tareas repetibles, mientras especialistas validan componentes. Recuperar con prudencia evita que la urgencia por operar reintroduzca vulnerabilidades o permita al atacante conservar acceso residual inadvertido.

El aprendizaje posterior convierte cada incidente en una fuente de mejora institucional. Revisar decisiones, tiempos,

evidencias, comunicaciones y fallos de coordinación permite identificar cambios en controles y procedimientos. NIST SP 800-61 e ISO 27035 conceden relevancia a esta retroalimentación dentro de la gestión de incidentes. Lee et al. (2022) muestran que las arquitecturas de respuesta pueden integrar múltiples capacidades defensivas. Registrar lecciones con franqueza fortalece procesos y evita repetir errores bajo nuevas formas de ataque.

La gestión ejecutiva de cibercrisis alcanza madurez cuando integra preparación técnica, autoridad decisoria, comunicación y continuidad operativa dentro de una misma disciplina. NIST SP 800-61 e ISO 27035 proporcionan referencias para estructurar la respuesta, mientras la automatización amplía capacidad y velocidad. Lee et al. (2022) destacan arquitecturas orientadas a coordinar herramientas y acciones frente a amenazas complejas. La combinación de gobierno y tecnología permite responder con criterio, preservar evidencia y recuperar confianza tras una interrupción.

4.6. Continuidad operativa (BCP/DRP) y resiliencia probada mediante simulaciones de ciberataques (Red/Blue Team, BAS)

La continuidad operativa convierte la resiliencia en una capacidad verificable para sostener procesos esenciales durante interrupciones graves. BCP organiza prioridades, responsabilidades y alternativas de operación, mientras DRP orienta la recuperación de plataformas, datos y servicios tecnológicos. Karagiannis et al. (2024) destacan el valor de entornos de entrenamiento realistas para desarrollar competencias de ciberseguridad en equipos SOC. Esta perspectiva recuerda que los planes adquieren verdadero significado cuando las personas pueden ejecutarlos bajo presión controlada y medible.

Diseñar BCP y DRP exige comprender dependencias entre procesos, aplicaciones, infraestructura, personas y proveedores.

Una recuperación técnicamente exitosa pierde utilidad cuando llega después del tiempo tolerable para el negocio. Por ello, objetivos como RTO y RPO deben vincularse con prioridades operativas verificadas. Karagiannis et al. (2024) plantean que los entornos de práctica permiten desarrollar capacidades mediante experiencias cercanas a situaciones reales. Ese aprendizaje ayuda a descubrir brechas organizacionales que permanecen ocultas en procedimientos meramente documentales.

Los ejercicios Red Team permiten observar la organización desde la perspectiva de un adversario autorizado, utilizando tácticas orientadas a alcanzar objetivos previamente acordados. Su propósito trasciende encontrar vulnerabilidades aisladas: busca comprobar cadenas de ataque, controles y capacidad de reacción. Karagiannis et al. (2024) resaltan que los cyber ranges favorecen entrenamiento práctico para profesionales de operaciones de seguridad. En condiciones controladas, estas experiencias revelan debilidades técnicas y humanas sin exponer procesos productivos a riesgos empresariales innecesarios.

El Blue Team representa la disciplina defensiva encargada de detectar, investigar, contener y aprender frente a actividades adversarias. Su desempeño depende de herramientas, procedimientos y criterio profesional, especialmente cuando las señales aparecen dispersas entre numerosos sistemas. Según Karagiannis et al. (2024), los ambientes de entrenamiento diseñados para equipos SOC favorecen el desarrollo estructurado de competencias. Practicar con escenarios realistas permite evaluar tiempos de detección, calidad del análisis y coordinación entre especialistas durante incidentes reales exigentes.

La confrontación controlada entre Red Team y Blue Team convierte la simulación en una oportunidad de aprendizaje. El equipo ofensivo revela rutas de compromiso; el defensivo demuestra capacidad para reconocerlas y responder. Después, ambas miradas permiten revisar controles sin buscar culpables.

Karagiannis et al. (2024) vinculan los entornos de entrenamiento con marcos de competencias que ayudan a estructurar capacidades profesionales. Esta práctica fortalece la cooperación y transforma hallazgos técnicos en mejoras operativas concretas y medibles.

Breach and Attack Simulation aporta una modalidad automatizada para comprobar controles mediante la ejecución recurrente de técnicas adversarias definidas. A diferencia de ejercicios puntuales, BAS facilita verificaciones frecuentes y comparables frente a cambios tecnológicos. La investigación de Karagiannis et al. (2024) enfatiza el aprendizaje práctico y la reproducción controlada de escenarios de seguridad. Aplicado con criterios de gobierno, este enfoque permite identificar degradaciones defensivas y priorizar correcciones antes de que una amenaza real las aproveche.

Las simulaciones adquieren mayor valor cuando incorporan decisiones de continuidad, no únicamente acciones técnicas. Un ransomware puede obligar a operar manualmente, restaurar respaldos, trasladar cargas o activar proveedores alternativos. Cada decisión consume tiempo y recursos. Karagiannis et al. (2024) destacan que los escenarios prácticos facilitan el desarrollo de habilidades relacionadas con funciones profesionales específicas. Integrar BCP y DRP en ejercicios de seguridad permite comprobar si procedimientos, responsables y recursos responden adecuadamente ante condiciones adversas realistas.

Probar respaldos constituye una práctica elemental, aunque frecuentemente confundida con verificar que una copia fue creada. La resiliencia exige restaurar información, medir tiempos y comprobar integridad en condiciones cercanas a una crisis. Los ejercicios permiten descubrir credenciales ausentes, dependencias olvidadas o procedimientos desactualizados. Karagiannis et al. (2024) muestran la utilidad de ambientes controlados para desarrollar destrezas mediante actividades prácticas. Trasladar esa

lógica al DRP convierte la recuperación en evidencia observable verificable, no en confianza documental.

Las métricas permiten convertir cada simulación en conocimiento comparable. Tiempo de detección, contención, recuperación, decisiones escaladas y objetivos alcanzados ofrecen evidencia para evaluar capacidades. Sin medición, el ejercicio corre el riesgo de convertirse en una demostración vistosa con aprendizaje limitado. Karagiannis et al. (2024) relacionan el diseño de cyber ranges con competencias profesionales definidas. Vincular resultados con BCP, DRP y funciones SOC facilita priorizar inversiones y observar avances entre ejercicios realizados en distintos periodos organizacionales.

La continuidad operativa madura cuando la organización acepta que ningún plan merece confianza sin haber sido probado. Red Team, Blue Team y BAS aportan perspectivas complementarias para someter defensas, personas y procedimientos a presión controlada. Karagiannis et al. (2024) evidencian el valor de entornos realistas para formar y evaluar capacidades de equipos SOC. Integrar estas prácticas con BCP y DRP transforma la resiliencia en una disciplina demostrable, capaz de aprender antes de enfrentar una crisis.

Tabla 4

Componentes de la protección integral de activos digitales y la resiliencia operativa

Ámbito de gestión y protección	**Propósito estratégico en la organización**
Gestión de identidades, accesos y privilegios (IAM, PAM, IGA)	Controlar identidades digitales, autorizaciones y privilegios durante su ciclo de vida, aplicando mínimo privilegio, segregación de funciones, trazabilidad y revisiones periódicas para reducir accesos indebidos y fortalecer el gobierno de la identidad.
Protección avanzada de datos (cifrado, DLP, DSPM)	Preservar confidencialidad e integridad mediante cifrado, prevención de fugas, descubrimiento de información sensible y evaluación continua de su

	exposición, ubicación, permisos y configuraciones de seguridad.
Seguridad de IoT, OT y sistemas ciberfísicos	Proteger dispositivos conectados, tecnologías industriales y procesos físicos mediante inventario de activos, segmentación, autenticación, supervisión continua y gestión de vulnerabilidades, considerando las particularidades operacionales de estos entornos.
Infraestructuras críticas y cadena de suministro tecnológica	Fortalecer la capacidad de resistencia y recuperación de servicios esenciales mediante evaluación de riesgos, análisis de interdependencias, gobierno de proveedores, redundancia y controles aplicados durante todo el ciclo de relación con terceros.
Respuesta a incidentes y gestión ejecutiva de cibercrisis	Coordinar preparación, detección, análisis, contención, recuperación, comunicación y aprendizaje mediante procedimientos estructurados, automatización y responsabilidades ejecutivas previamente definidas para responder con rapidez y criterio ante eventos de alto impacto.
Continuidad operativa y recuperación (BCP/DRP)	Mantener procesos prioritarios y recuperar servicios tecnológicos dentro de parámetros aceptables, estableciendo dependencias, responsables, alternativas operativas, respaldos verificables y objetivos de recuperación alineados con las necesidades empresariales.
Simulación y validación de la resiliencia (Red Team, Blue Team, BAS)	Comprobar periódicamente la efectividad de controles, capacidades defensivas y procedimientos de recuperación mediante ejercicios adversariales y simulaciones controladas que permitan medir desempeño, identificar brechas y orientar mejoras continuas.

Nota. IAM = Identity and Access Management; PAM = Privileged Access Management; IGA = Identity Governance and Administration; DLP = Data Loss Prevention; DSPM = Data Security Posture Management; IoT = Internet of Things; OT = Operational Technology; BCP = Business Continuity Plan; DRP = Disaster Recovery Plan; BAS = Breach and Attack Simulation. Elaboración propia con base en Glöckler et al. (2024), Raaj (2025), Kanamaru (2024), Aghazadeh Ardebili et al. (2024), Lee et al. (2022) y Karagiannis et al. (2024).

Capítulo 5:

Inteligencia Artificial, Analítica Avanzada y Automatización de la Ciberseguridad

La ciberseguridad empresarial atraviesa una transformación marcada por la incorporación de inteligencia artificial, analítica avanzada y automatización en actividades antes dominadas por reglas estáticas y revisión manual. El cambio no responde únicamente al aumento del volumen de datos, sino a la velocidad con que evolucionan las amenazas. Vourganas y Michala (2024) describen un campo donde el aprendizaje automático participa crecientemente en detección, clasificación y análisis de actividades maliciosas, abriendo nuevas posibilidades para anticipar comportamientos difíciles de reconocer.

En este escenario, la capacidad predictiva adquiere una relevancia particular. Detectar un incidente cuando el daño ya se ha producido resulta insuficiente para organizaciones cuyas operaciones dependen de servicios digitales interconectados. El interés se desplaza hacia señales tempranas, patrones anómalos y relaciones que permitan actuar antes de una afectación significativa. Vourganas y Michala (2024) examinan aplicaciones del aprendizaje automático que aprovechan grandes conjuntos de datos para identificar amenazas, aunque su rendimiento permanece estrechamente vinculado con información representativa.

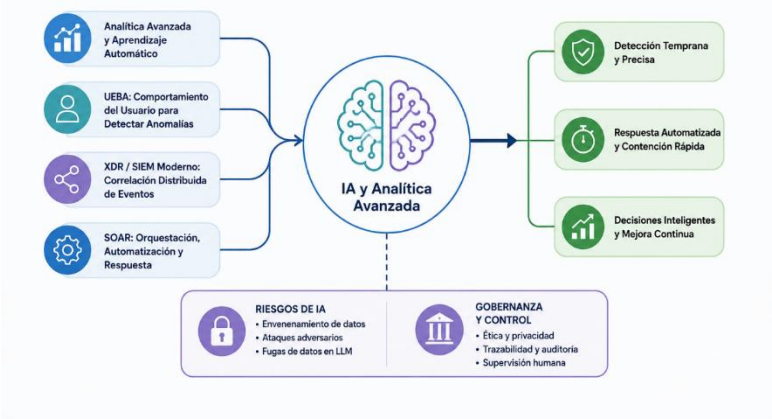
La mirada analítica también se dirige hacia usuarios y entidades, cuyas actividades cotidianas generan huellas capaces de revelar desviaciones significativas. Horarios, accesos, dispositivos y secuencias operativas construyen patrones que pueden ser examinados sin depender enteramente de firmas conocidas. Artioli et al. (2024) muestran que los algoritmos de agrupamiento ofrecen alternativas relevantes para UEBA, pues permiten identificar estructuras conductuales y observaciones atípicas. Una anomalía, sin embargo, requiere interpretación antes de convertirse en evidencia de actividad maliciosa.

La velocidad introduce otra exigencia. Una señal detectada varias horas después puede conservar utilidad forense, pero perder

buena parte de su valor preventivo. De ahí el interés por arquitecturas capaces de procesar eventos en tiempo real y relacionarlos mientras la actividad permanece en curso. Artioli et al. (2024) evidencian diferencias importantes entre algoritmos empleados en análisis conductual, recordando que precisión y eficiencia deben evaluarse conjuntamente cuando la detección opera sobre flujos continuos provenientes de infraestructuras empresariales complejas.

Figura 15

Ecosistema inteligente de ciberseguridad empresarial



Junto con estas capacidades analíticas aparece la necesidad de convertir hallazgos en acciones coordinadas. Las plataformas SOAR responden a esta necesidad mediante flujos que articulan herramientas, procedimientos y decisiones dentro de operaciones repetibles. Lee et al. (2022) presentan una arquitectura orientada a integrar orquestación, automatización y respuesta en ambientes tecnológicos heterogéneos. El propósito trasciende la rapidez: también interesa preservar trazabilidad, reducir inconsistencias y liberar capacidad humana para investigaciones que requieren experiencia, criterio profesional y comprensión organizacional profunda.

Esta integración cobra mayor importancia cuando los eventos de seguridad se encuentran distribuidos entre terminales, redes, identidades, aplicaciones y servicios digitales. Ninguna señal aislada cuenta necesariamente toda la historia. Lee et al. (2022) plantean mecanismos de cooperación entre componentes de seguridad que permiten comprender operaciones desarrolladas en ambientes combinados. Desde esta perspectiva, la ciberinteligencia, el SIEM moderno y XDR convergen alrededor de una necesidad compartida: relacionar evidencias dispersas para construir una representación operativa más completa de cada incidente.

La automatización avanza, además, hacia sistemas con mayores capacidades de razonamiento y actuación. Los agentes inteligentes pueden interpretar alertas, consultar información, organizar evidencias y participar en procedimientos de contención bajo políticas previamente definidas. Ferrag et al. (2025) documentan múltiples aplicaciones de modelos lingüísticos de gran escala dentro de la ciberseguridad. Este desarrollo amplía las posibilidades defensivas, pero obliga a determinar con cuidado qué decisiones pueden delegarse, cuáles requieren aprobación humana y qué límites deben acompañar cada nivel de autonomía.

La inteligencia artificial presenta, en efecto, una dualidad difícil de ignorar. La misma tecnología que ayuda a reconocer amenazas puede incorporar vulnerabilidades aprovechables por adversarios. Ferrag et al. (2025) analizan riesgos relacionados con manipulación de modelos, ataques adversarios, exposición de información y otras debilidades asociadas con sistemas generativos. En consecuencia, proteger algoritmos, datos de entrenamiento e interfaces deja de ser una tarea periférica y pasa a formar parte de la arquitectura general de seguridad de la organización digital.

Esta realidad coloca al gobierno de TI ante responsabilidades renovadas. Adoptar modelos avanzados no consiste meramente en incorporar herramientas capaces de

procesar más información o responder con mayor velocidad. También exige trazabilidad, delimitación de privilegios, criterios de supervisión y mecanismos de rendición de cuentas. Ferrag et al. (2025) destacan vulnerabilidades que acompañan la expansión de los modelos generativos, mientras Lee et al. (2022) evidencian el valor de arquitecturas coordinadas para mantener control sobre operaciones automatizadas de seguridad.

Este capítulo aborda, por tanto, una transición desde la detección basada en evidencia histórica hacia capacidades predictivas, conductuales, distribuidas y progresivamente autónomas. Aprendizaje automático, UEBA, SOAR, ciberinteligencia, XDR, SIEM y agentes inteligentes forman partes relacionadas de una transformación más amplia. Vourganas y Michala (2024), Artioli et al. (2024), Lee et al. (2022) y Ferrag et al. (2025) permiten examinar esa evolución desde perspectivas complementarias, manteniendo presente una premisa esencial: automatizar también exige gobernar.

5.1. IA y aprendizaje automático aplicados al análisis predictivo de amenazas cibernéticas

La inteligencia artificial y el aprendizaje automático han transformado el análisis predictivo de amenazas cibernéticas al permitir que grandes volúmenes de eventos sean examinados con una velocidad difícil de alcanzar mediante procedimientos tradicionales. En lugar de depender exclusivamente de firmas conocidas, los modelos aprenden regularidades, identifican desviaciones y estiman comportamientos potencialmente maliciosos. Vourganas y Michala (2024) señalan que estas capacidades han ganado relevancia ante ataques cada vez más sofisticados y dinámicos en entornos digitales empresariales.

El valor predictivo de estos sistemas reside en su capacidad para reconocer patrones previos a un incidente y relacionar señales que, observadas por separado, podrían parecer irrelevantes.

Registros de red, autenticaciones, comportamiento de usuarios y actividad de dispositivos aportan indicios para construir modelos de riesgo. Desde esta perspectiva, el aprendizaje automático convierte datos operativos en evidencia anticipatoria. Según Vourganas y Michala (2024), la detección avanzada de patrones y anomalías fortalece la respuesta frente a amenazas.

No obstante, predecir una amenaza no equivale a adivinar el futuro. La utilidad del modelo depende de la representatividad, calidad y diversidad de los datos empleados durante su entrenamiento. Un conjunto sesgado puede aprender asociaciones engañosas y producir alertas que distraigan al equipo de seguridad. Vourganas y Michala (2024) advierten que los conjuntos disponibles presentan diferencias importantes en características, métodos de recolección y requisitos de preprocesamiento, circunstancia que dificulta comparaciones fiables entre soluciones predictivas empresariales.

En los sistemas de detección de intrusiones, el aprendizaje automático ofrece una ventaja especialmente visible: puede examinar tráfico continuo y distinguir comportamientos normales de secuencias potencialmente hostiles. Esta capacidad resulta valiosa cuando los atacantes modifican técnicas para evadir reglas estáticas. La revisión de Vourganas y Michala (2024) destaca la detección de anomalías como un campo estrechamente vinculado con inteligencia artificial. Sin embargo, una predicción útil requiere calibración, validación periódica y comprensión del entorno operativo real.

Las técnicas supervisadas permiten entrenar clasificadores con ejemplos previamente etiquetados de actividad legítima y maliciosa. Su desempeño puede ser elevado cuando las categorías están bien representadas, aunque pierde eficacia frente a conductas novedosas o muestras escasas. Los métodos no supervisados, por otra parte, buscan estructuras y desviaciones sin depender enteramente de etiquetas. Vourganas y Michala (2024) remarcan

que la disponibilidad de datos condiciona profundamente la investigación, cuestión especialmente sensible cuando las amenazas evolucionan con rapidez.

El aprendizaje profundo amplía estas posibilidades mediante arquitecturas capaces de captar relaciones complejas en grandes conjuntos de datos. Redes neuronales pueden apoyar la detección de malware, phishing y patrones anómalos, pero su capacidad predictiva debe evaluarse junto con sus costos computacionales y su interpretabilidad. Vourganas y Michala (2024) documentan el interés creciente por estas técnicas en ciberseguridad. Para una empresa inteligente, precisión sin explicación suficiente puede generar resistencia operativa y decisiones difíciles de auditar internamente.

La analítica predictiva adquiere mayor sentido cuando se integra con procesos de gestión del riesgo y operaciones de seguridad. Una puntuación de probabilidad, por ejemplo, puede ayudar a priorizar incidentes, asignar recursos y orientar investigaciones antes de que una actividad hostil produzca daños mayores. Sin embargo, automatizar la clasificación no elimina el juicio profesional. Vourganas y Michala (2024) resaltan la importancia de mantener supervisión humana, especialmente cuando la incertidumbre del modelo exige revisión experta especializada.

También debe considerarse la exposición de los propios modelos a manipulación adversaria. Un atacante puede intentar alterar datos, diseñar entradas engañosas o aprovechar debilidades del proceso de entrenamiento para reducir la eficacia de la detección. Por ello, la seguridad del modelo forma parte de la seguridad empresarial. Vourganas y Michala (2024) destacan el entrenamiento adversarial como vía para incrementar resistencia. La predicción confiable exige proteger datos, modelos, canales de actualización y mecanismos de evaluación continua.

La gobernanza de la inteligencia artificial aporta disciplina a este enfoque predictivo. Documentar fuentes de datos, criterios de selección, métricas, versiones y decisiones de ajuste permite comprender por qué un modelo cambia su comportamiento. La trazabilidad resulta relevante para auditoría, cumplimiento y rendición de cuentas. De acuerdo con Vourganas y Michala (2024), transparencia, explicabilidad y auditabilidad deben acompañar las aplicaciones de inteligencia artificial en ciberseguridad. La confianza organizacional nace tanto del rendimiento como de evidencia.

En la empresa inteligente, el análisis predictivo de amenazas debe entenderse como una capacidad evolutiva, conectada con arquitectura empresarial, gobierno de TI y automatización responsable. Su aporte consiste en anticipar señales, reducir tiempos de detección y favorecer respuestas proporcionadas al riesgo observado. Con avances relevantes, persisten limitaciones asociadas a datos heterogéneos y evaluación de modelos. Vourganas y Michala (2024) plantean preguntas abiertas que invitan a mejorar representación, ética, robustez y utilidad práctica de estas tecnologías.

5.2. Analítica avanzada y comportamiento del usuario (UEBA) para detección de anomalías en tiempo real

La analítica avanzada aplicada al comportamiento de usuarios y entidades ha adquirido relevancia en arquitecturas modernas de ciberseguridad, especialmente ante actividades que escapan de reglas estáticas. UEBA permite observar patrones de acceso, frecuencia de operaciones, recursos consultados y variaciones temporales para reconocer conductas atípicas. Artioli et al. (2024) destacan que las técnicas de agrupamiento facilitan la identificación de perfiles conductuales sin requerir etiquetas previas, una ventaja significativa frente a escenarios empresariales caracterizados por datos dinámicos.

El principio operativo de UEBA parte de una idea sencilla: cada usuario desarrolla cierta regularidad al interactuar con sistemas, aplicaciones y recursos corporativos. Horarios de conexión, ubicaciones, dispositivos empleados y secuencias de actividad forman huellas conductuales susceptibles de análisis estadístico. Cuando dichas pautas cambian de manera considerable, aparecen señales que merecen atención. Artioli et al. (2024) examinan algoritmos de clustering capaces de organizar observaciones según semejanzas, facilitando la detección de comportamientos alejados de grupos habituales.

La detección de anomalías en tiempo real exige procesar flujos continuos sin perder capacidad interpretativa. No basta con generar alertas rápidamente; resulta necesario establecer qué comportamiento produjo la desviación y cuánto difiere respecto del patrón esperado. En esta tarea, el agrupamiento ofrece mecanismos para descubrir estructuras internas entre usuarios y entidades. Artioli et al. (2024) comparan diversas familias de algoritmos y muestran que su rendimiento varía dependiendo de las características presentes en cada conjunto analizado.

Entre las fortalezas de UEBA destaca su capacidad para abordar amenazas internas, cuentas comprometidas y movimientos poco habituales dentro de una infraestructura digital. Un acceso legítimo puede convertirse en vehículo de ataque cuando las credenciales han sido sustraídas, circunstancia difícil de reconocer mediante controles basados únicamente en identidad. Artioli et al. (2024) plantean que el análisis conductual mediante clustering permite establecer agrupaciones representativas y localizar observaciones anómalas cuya distancia respecto de patrones frecuentes merece investigación especializada.

La selección del algoritmo influye directamente en la calidad de los perfiles generados. Métodos basados en centroides, densidad, jerarquías u otras estrategias responden de manera diferente ante ruido, dimensionalidad y distribuciones irregulares.

No existe, por tanto, una técnica universalmente adecuada para toda organización. La investigación de Artioli et al. (2024) evidencia diferencias relevantes entre algoritmos evaluados para UEBA, reforzando la necesidad de valorar cada método mediante criterios técnicos vinculados con datos, desempeño y capacidad discriminatoria operativa.

Otro aspecto relevante corresponde al tratamiento de variables antes de ejecutar los modelos analíticos. Registros empresariales contienen atributos heterogéneos, valores categóricos, escalas distintas y eventos cuya frecuencia puede variar considerablemente. Una preparación deficiente altera las distancias entre observaciones y termina afectando los grupos obtenidos. Artioli et al. (2024) prestan atención al procesamiento de características dentro de su evaluación experimental. Esta etapa demanda decisiones cuidadosas, pues pequeños cambios metodológicos pueden modificar sensiblemente la interpretación posterior del comportamiento observado.

La velocidad añade otra dimensión al problema. En entornos empresariales distribuidos, millones de eventos pueden producirse mientras una sesión permanece activa, de modo que una anomalía detectada horas después quizá llegue demasiado tarde. UEBA adquiere valor cuando aproxima el análisis al instante en que ocurre la desviación. Los hallazgos presentados por Artioli et al. (2024) permiten comprender que eficiencia computacional y calidad del agrupamiento deben evaluarse conjuntamente cuando estas técnicas respaldan sistemas operativos de vigilancia continua.

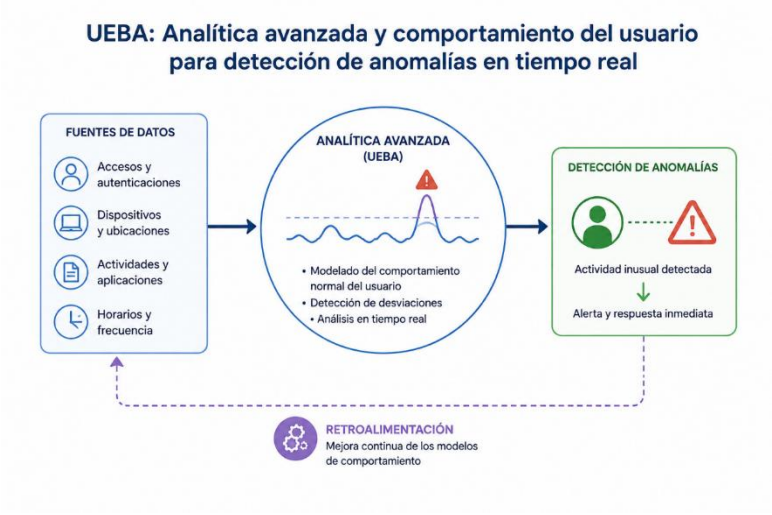
La interpretación humana permanece vinculada al valor práctico de UEBA. Una conducta estadísticamente infrecuente no representa necesariamente una amenaza: un empleado puede viajar, asumir nuevas funciones o acceder excepcionalmente a información relacionada con una tarea legítima. Por esta razón, las anomalías requieren valoración antes de convertirse en incidentes confirmados. Artioli et al. (2024) muestran que diferentes métodos

producen agrupaciones y resultados distintos, hecho que aconseja complementar métricas algorítmicas con conocimiento operativo y criterios profesionales de seguridad.

Desde la perspectiva de gobierno de TI, UEBA requiere políticas claras respecto de recolección, conservación y utilización de datos conductuales. La capacidad técnica para analizar actividades individuales debe convivir con principios de privacidad, proporcionalidad y rendición de cuentas. Esta dimensión adquiere particular importancia cuando los modelos generan puntuaciones que pueden influir en investigaciones internas. La comparación desarrollada por Artioli et al. (2024) aporta criterios técnicos para seleccionar algoritmos, mientras la organización debe establecer límites responsables para su aplicación empresarial.

Figura 16

Detección conductual de anomalías mediante UEBA



Integrar UEBA con plataformas de monitoreo, gestión de eventos y automatización permite convertir patrones conductuales en decisiones oportunas. Una anomalía relevante puede elevar el

nivel de riesgo, solicitar autenticación adicional o activar una investigación antes de producirse una afectación mayor. Artioli et al. (2024) demuestran que la elección del algoritmo de clustering modifica significativamente los resultados obtenidos. Para la empresa inteligente, esta evidencia invita a combinar analítica avanzada, evaluación continua y supervisión experta con una gobernanza tecnológica responsable.

5.3. Automatización e integración de operaciones de seguridad mediante plataformas SOAR

Las plataformas de orquestación, automatización y respuesta de seguridad, conocidas como SOAR, representan una evolución significativa en la gestión contemporánea de operaciones cibernéticas. Su propósito consiste en articular herramientas, datos y procedimientos dentro de flujos coordinados que reduzcan tareas manuales repetitivas. Lee et al. (2022) plantean una arquitectura orientada a integrar funciones de seguridad en entornos tecnológicos heterogéneos. Esta integración permite que los equipos concentren atención especializada en incidentes cuya complejidad requiere análisis humano profundo.

La automatización mediante SOAR adquiere especial valor cuando un centro de operaciones recibe volúmenes elevados de alertas procedentes de múltiples fuentes. Revisar cada señal manualmente consume tiempo y favorece inconsistencias durante jornadas de alta presión. Mediante reglas, flujos predefinidos y mecanismos coordinados, determinadas acciones pueden ejecutarse con mayor rapidez. Lee et al. (2022) describen la orquestación como componente capaz de vincular tecnologías diferentes, favoreciendo respuestas estructuradas ante eventos producidos dentro de infraestructuras digitales ampliamente interconectadas.

El concepto de orquestación trasciende la ejecución automática de tareas aisladas. Implica establecer relaciones entre

herramientas que tradicionalmente operaban de manera separada, permitiendo compartir información y desencadenar acciones según condiciones previamente definidas. Una alerta puede enriquecerse con datos adicionales antes de determinar su prioridad. En la arquitectura presentada por Lee et al. (2022), la coordinación entre componentes busca mejorar las capacidades de detección y respuesta dentro de ambientes donde convergen dispositivos, servicios y redes con características diversas.

Los playbooks constituyen una pieza relevante dentro de la operación de SOAR porque traducen procedimientos organizacionales en secuencias ejecutables y repetibles. Ante determinadas alertas, un flujo puede recopilar evidencias, consultar fuentes internas, clasificar indicadores y derivar el caso hacia especialistas. Esta estandarización disminuye variaciones innecesarias entre respuestas semejantes. Lee et al. (2022) destacan que la automatización coordinada permite administrar eventos de seguridad mediante procesos estructurados, particularmente valiosos cuando diferentes tecnologías participan simultáneamente en una investigación operativa.

La velocidad de respuesta constituye otra aportación importante. Durante un incidente, cada minuto puede ampliar la exposición de sistemas, usuarios y activos informacionales. Automatizar actividades de verificación, correlación y contención reduce intervalos que anteriormente dependían de intervención manual. La propuesta de Lee et al. (2022) integra capacidades de respuesta dentro de una arquitectura diseñada para ambientes tecnológicos combinados. Tal enfoque favorece acciones oportunas frente a amenazas cuya propagación puede atravesar componentes físicos, virtuales y conectados entre sí.

Integrar SOAR con tecnologías existentes evita convertir la automatización en una capa aislada. Sistemas de monitoreo, herramientas de detección, repositorios de inteligencia y mecanismos de control pueden intercambiar información

mediante interfaces coordinadas. El beneficio aparece cuando cada componente aporta evidencia al mismo proceso operativo. Lee et al. (2022) consideran la interoperabilidad entre elementos de seguridad dentro de su arquitectura para ambientes combinados, donde la diversidad tecnológica demanda mecanismos capaces de articular datos y respuestas sin fragmentar la gestión institucional.

Sin embargo, automatizar una operación de seguridad exige prudencia. Una acción ejecutada rápidamente también puede amplificar errores cuando las reglas han sido configuradas de manera deficiente. Bloquear una cuenta legítima, aislar un activo necesario o descartar una alerta relevante puede afectar procesos empresariales. Por ello, conviene establecer niveles de autorización según riesgo e impacto. Lee et al. (2022) vinculan automatización y respuesta dentro de una arquitectura coordinada, ofreciendo bases para distribuir funciones entre mecanismos automáticos y supervisión especializada.

La arquitectura SOAR también contribuye a preservar conocimiento operativo. Cuando procedimientos de respuesta quedan formalizados mediante flujos reproducibles, la organización reduce dependencia de prácticas informales conservadas por determinados especialistas. Esta característica favorece continuidad, aprendizaje y revisión periódica de procesos. En el planteamiento de Lee et al. (2022), los componentes arquitectónicos cooperan para gestionar información y acciones de seguridad. Tal cooperación facilita convertir experiencia acumulada en procedimientos consistentes que pueden ajustarse conforme evolucionan amenazas y tecnologías corporativas.

Desde la perspectiva del gobierno de TI, la automatización requiere trazabilidad suficiente para reconstruir decisiones, acciones y resultados. Cada ejecución debe dejar evidencia verificable: qué evento inició el proceso, qué herramientas participaron y qué respuesta fue aplicada. Esta información fortalece auditoría y mejora continua. Lee et al. (2022) presentan

una arquitectura que articula múltiples componentes dentro de operaciones coordinadas de seguridad, característica que favorece una visión integrada del incidente y permite evaluar posteriormente la efectividad de las respuestas.

Para la empresa inteligente, SOAR representa más que una tecnología destinada a acelerar operaciones. Constituye una capacidad organizacional que conecta personas, procedimientos y herramientas alrededor de respuestas coherentes frente al riesgo cibernético. Su madurez depende de integración, diseño cuidadoso de flujos y revisión permanente de resultados. La arquitectura propuesta por Lee et al. (2022) evidencia el valor de coordinar automatización y respuesta en ambientes heterogéneos, donde actuar con rapidez debe conservar control, trazabilidad y criterio profesional.

5.4. Ciberinteligencia de amenazas y correlación distribuida de eventos (XDR/SIEM moderno)

La ciberinteligencia de amenazas adquiere valor cuando transforma señales dispersas en conocimiento operativo capaz de orientar decisiones oportunas. En infraestructuras empresariales heterogéneas, los eventos proceden de redes, aplicaciones, dispositivos, identidades y servicios externos, formando un panorama difícil de interpretar manualmente. Lee et al. (2022) plantean una arquitectura de seguridad orientada a coordinar componentes diversos dentro de ambientes tecnológicos combinados, principio que favorece la correlación distribuida y una comprensión más amplia de actividades potencialmente maliciosas actuales.

Los sistemas SIEM modernos amplían la función tradicional de recopilar registros mediante capacidades analíticas destinadas a relacionar acontecimientos producidos en múltiples capas tecnológicas. Una autenticación irregular puede parecer menor hasta relacionarse con tráfico sospechoso, cambios de

privilegios o actividad inusual en otro activo. La arquitectura descrita por Lee et al. (2022) enfatiza la cooperación entre componentes de seguridad, perspectiva pertinente para construir procesos de correlación donde cada evidencia adquiere significado al vincularse con otras señales.

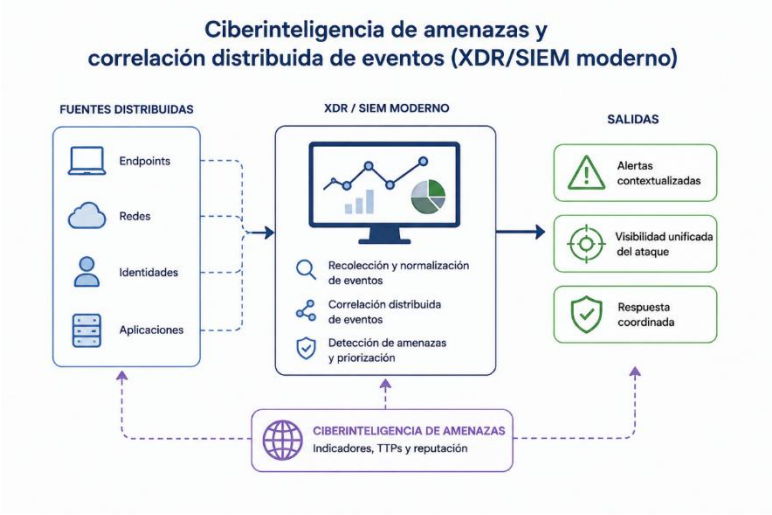
XDR extiende esta lógica al reunir telemetría procedente de terminales, redes, cargas de trabajo, identidades y servicios digitales bajo mecanismos coordinados de detección y respuesta. Su aporte reside en reconstruir cadenas de actividad que permanecerían fragmentadas entre herramientas independientes. Lee et al. (2022) destacan la necesidad de integrar tecnologías de seguridad en ambientes caracterizados por dispositivos y sistemas diversos. Esa visión arquitectónica respalda modelos donde la información distribuida puede convertirse en evidencia coherente y accionable.

La ciberinteligencia complementa la correlación técnica al aportar información acerca de indicadores, tácticas, patrones y comportamientos asociados con actores maliciosos. Cuando esa información dialoga con telemetría interna, una alerta deja de ser un dato aislado y adquiere mayor relevancia investigativa. Lee et al. (2022) proponen mecanismos de integración orientados a mejorar detección y respuesta mediante componentes interrelacionados. Esta perspectiva permite entender la inteligencia como insumo dinámico que enriquece decisiones frente a eventos distribuidos complejos actuales.

La correlación distribuida resulta especialmente valiosa en arquitecturas empresariales donde los activos ya no permanecen concentrados dentro de un perímetro convencional. Servicios en nube, dispositivos conectados y plataformas remotas generan registros desde ubicaciones distintas y con formatos diversos. Lee et al. (2022) estudian un ambiente combinado en el que convergen tecnologías heterogéneas y plantean mecanismos coordinados de seguridad. Tal enfoque favorece una lectura transversal de

incidentes que atraviesan dominios técnicos antes administrados de manera independiente.

Figura 17
Correlación inteligente de eventos mediante XDR y SIEM



Un beneficio relevante del SIEM moderno consiste en reducir el ruido producido por grandes volúmenes de eventos. Correlacionar señales según temporalidad, identidad, origen, destino y comportamiento permite priorizar aquellas combinaciones que presentan mayor riesgo. Esta capacidad requiere reglas bien diseñadas y fuentes confiables. Lee et al. (2022) señalan que la coordinación entre tecnologías fortalece la gestión de eventos en ambientes complejos, donde detectar relaciones significativas puede acelerar la identificación de actividades hostiles, orientando respuestas proporcionadas.

La eficacia de XDR y SIEM depende también de la calidad de la telemetría incorporada. Registros incompletos, marcas temporales inconsistentes o configuraciones deficientes pueden fragmentar la secuencia de un incidente y conducir a

interpretaciones equivocadas. La propuesta arquitectónica de Lee et al. (2022) concede importancia a la interacción organizada entre componentes de seguridad. Desde esta mirada, recopilar datos no basta: deben normalizarse, relacionarse y mantenerse disponibles para que la investigación conserve continuidad entre dominios tecnológicos.

La automatización puede convertir una correlación relevante en una acción inmediata, aunque requiere controles proporcionales al impacto esperado. Una secuencia compatible con compromiso de credenciales podría activar enriquecimiento de indicadores, elevar prioridad o solicitar validación antes de ejecutar medidas restrictivas. Lee et al. (2022) vinculan orquestación, automatización y respuesta mediante una arquitectura integrada. Este planteamiento resulta pertinente para XDR y SIEM modernos, pues conecta detección distribuida con procedimientos repetibles, auditables y sujetos a supervisión humana.

Desde el gobierno de TI, la correlación de eventos demanda trazabilidad, criterios de retención y responsabilidades claramente asignadas. La capacidad de reunir información procedente de usuarios, dispositivos y aplicaciones debe acompañarse de controles que preserven privacidad, integridad y acceso autorizado. Lee et al. (2022) presentan una arquitectura donde componentes participan coordinadamente en operaciones de seguridad. Esta organización facilita reconstruir decisiones y evaluar respuestas, elementos necesarios para auditoría, aprendizaje institucional y mejora permanente de capacidades defensivas.

Para la empresa inteligente, ciberinteligencia, XDR y SIEM moderno forman una capacidad integrada destinada a convertir datos dispersos en conocimiento operativo. La ventaja no proviene únicamente de acumular eventos, sino de relacionarlos con rapidez, significado y criterios de riesgo. Lee et al. (2022) muestran que la integración arquitectónica favorece operaciones coordinadas frente a amenazas presentes en ambientes tecnológicos heterogéneos.

Esta visión permite articular detección, investigación y respuesta bajo una gobernanza capaz de sostener decisiones informadas.

5.5. Agentes inteligentes y sistemas autónomos para contención y respuesta automatizada frente a incidentes

Los agentes inteligentes están modificando la respuesta ante incidentes al incorporar capacidades de interpretación, decisión y ejecución dentro de operaciones tradicionalmente dependientes de intervención humana. Estos sistemas pueden analizar alertas, relacionar evidencias y recomendar medidas de contención con una velocidad compatible con amenazas de rápida propagación. Ferrag et al. (2025) examinan el creciente papel de los modelos generativos en ciberseguridad, destacando aplicaciones capaces de apoyar actividades defensivas mediante procesamiento automatizado de información técnica y conocimiento especializado disponible.

La autonomía adquiere verdadero sentido cuando el sistema puede pasar de interpretar una alerta a ejecutar acciones controladas según políticas previamente establecidas. Un agente podría consultar telemetría, evaluar indicadores, determinar el nivel de riesgo y activar medidas autorizadas. Ferrag et al. (2025) describen aplicaciones de modelos lingüísticos en diferentes tareas de ciberseguridad, mostrando su capacidad para procesar información compleja. Esta evolución aproxima las operaciones defensivas hacia esquemas donde razonamiento computacional y automatización trabajan estrechamente coordinados.

La contención automatizada busca reducir el intervalo existente entre detección y respuesta, una ventana durante la cual un atacante puede ampliar privilegios, desplazarse entre sistemas o extraer información. Ante evidencia suficiente, un agente podría aislar temporalmente un dispositivo, revocar sesiones o restringir determinadas comunicaciones. Ferrag et al. (2025) identifican

múltiples aplicaciones defensivas de inteligencia artificial generativa. Su incorporación en procesos de respuesta permite concebir mecanismos adaptativos capaces de seleccionar acciones según características observadas durante cada incidente.

Sin embargo, conceder capacidad ejecutiva a un agente introduce riesgos que deben ser tratados desde el diseño. Una interpretación equivocada puede provocar bloqueos innecesarios, interrupciones operativas o alteraciones sobre activos legítimos. La revisión de Ferrag et al. (2025) advierte que los modelos lingüísticos presentan vulnerabilidades propias y pueden ser objeto de manipulaciones adversarias. Por ello, autonomía no equivale a libertad irrestricta: requiere permisos delimitados, validaciones, registros de actividad y mecanismos que permitan detener decisiones potencialmente perjudiciales.

La supervisión humana mantiene un papel determinante cuando las consecuencias de una acción automatizada pueden afectar procesos sensibles. Los agentes pueden filtrar evidencias, resumir incidentes y proponer respuestas, mientras determinadas decisiones permanecen sujetas a aprobación profesional. Ferrag et al. (2025) analizan riesgos asociados con resultados incorrectos y vulnerabilidades presentes en sistemas generativos. Frente a estas limitaciones, los modelos de autonomía graduada permiten distribuir responsabilidades según criticidad, confianza analítica e impacto empresarial previsto para cada intervención.

Una capacidad especialmente prometedora reside en el uso de agentes para apoyar investigaciones de incidentes mediante interacción con diversas fuentes de información. Estos sistemas pueden organizar registros, interpretar hallazgos y relacionar indicadores con conocimiento disponible para facilitar el trabajo analítico. Ferrag et al. (2025) documentan aplicaciones de modelos lingüísticos vinculadas con análisis de amenazas y operaciones defensivas. El valor práctico aparece cuando dicha asistencia reduce

tareas repetitivas sin desplazar el razonamiento experto requerido ante situaciones ambiguas.

Los sistemas autónomos también pueden contribuir al aprendizaje operativo después de cada incidente. Registros de decisiones, resultados de contención y evaluaciones humanas ofrecen información para ajustar procedimientos y mejorar respuestas posteriores. Este ciclo requiere gobernanza rigurosa para evitar que errores anteriores sean incorporados como prácticas aceptables. Ferrag et al. (2025) examinan vulnerabilidades y riesgos inherentes a modelos generativos, recordando que la capacidad de aprendizaje debe acompañarse de evaluación permanente, protección de datos y mecanismos de verificación.

La seguridad del propio agente constituye una preocupación inevitable. Instrucciones maliciosas, manipulación de entradas o exposición de información sensible pueden alterar decisiones y convertir una herramienta defensiva en superficie adicional de ataque. Ferrag et al. (2025) analizan vulnerabilidades asociadas con modelos lingüísticos, entre ellas técnicas destinadas a modificar su comportamiento esperado. Una arquitectura responsable debe separar privilegios, validar entradas, limitar accesos y registrar cada acción ejecutada para facilitar investigación, auditoría y recuperación ante comportamientos inesperados posteriores.

Desde la perspectiva del gobierno de TI, incorporar agentes autónomos requiere definir responsabilidades antes de delegar decisiones. Debe conocerse qué acciones pueden ejecutar, bajo qué condiciones, con cuáles datos y quién responde cuando una decisión produce consecuencias adversas. Ferrag et al. (2025) resaltan preocupaciones de seguridad relacionadas con aplicaciones generativas en entornos cibernéticos. La trazabilidad, explicabilidad y delimitación de privilegios adquieren entonces relevancia institucional, pues permiten combinar velocidad

automatizada con control organizacional y rendición de cuentas efectiva.

Para la empresa inteligente, los agentes representan una evolución hacia operaciones de seguridad capaces de reaccionar con mayor rapidez y adaptación frente a incidentes dinámicos. Su aporte no reside en reemplazar indiscriminadamente al especialista, sino en ampliar su capacidad mediante análisis, coordinación y ejecución controlada. Ferrag et al. (2025) muestran oportunidades y vulnerabilidades vinculadas con inteligencia artificial generativa en ciberseguridad. El equilibrio entre autonomía, supervisión y gobernanza determinará la confianza depositada en estas capacidades defensivas.

5.6. Desafíos de seguridad de la IA: envenenamiento de datos, ataques adversarios y fugas de datos en LLM

La incorporación de inteligencia artificial en procesos empresariales amplía capacidades analíticas, pero también introduce riesgos vinculados con la integridad de datos, modelos y resultados. Los sistemas generativos pueden convertirse en objetivos atractivos cuando participan en decisiones, automatizaciones o tratamiento de información sensible. Ferrag et al. (2025) identifican diversas vulnerabilidades asociadas con modelos lingüísticos de gran escala, desde manipulación de entradas hasta exposición informativa. Proteger estas tecnologías requiere considerar su ciclo de vida como superficie permanente de ataque.

El envenenamiento de datos representa una amenaza especialmente delicada porque interviene sobre el material utilizado para entrenar o ajustar modelos. Datos manipulados pueden introducir asociaciones engañosas, sesgos intencionales o comportamientos activables bajo determinadas condiciones. La alteración quizá permanezca inadvertida durante evaluaciones convencionales y manifestarse posteriormente. Ferrag et al. (2025)

examinan amenazas dirigidas contra sistemas generativos y resaltan riesgos relacionados con datos y modelos, cuestión que demanda controles de procedencia, integridad y validación antes del entrenamiento.

La procedencia de los datos adquiere, por ello, importancia estratégica. Organizaciones que reúnen información desde repositorios públicos, proveedores externos o interacciones internas necesitan conocer origen, transformaciones y permisos asociados con cada conjunto. Una cadena documental incompleta dificulta identificar alteraciones deliberadas. Ferrag et al. (2025) describen un panorama donde las vulnerabilidades de los modelos generativos abarcan diferentes etapas de utilización. Frente a esta realidad, verificar fuentes y conservar trazabilidad reduce oportunidades para introducir contenido malicioso inadvertidamente.

Los ataques adversarios operan mediante entradas cuidadosamente elaboradas para provocar comportamientos diferentes de aquellos esperados durante condiciones normales. Pequeñas modificaciones pueden inducir clasificaciones incorrectas, respuestas inadecuadas o evasión de mecanismos defensivos basados en inteligencia artificial. Ferrag et al. (2025) revisan técnicas ofensivas dirigidas contra modelos generativos y sistemas apoyados por aprendizaje automático. Esta fragilidad revela que un buen rendimiento estadístico no garantiza resistencia ante adversarios que conocen, estudian o infieren características funcionales del modelo desplegado.

En los modelos lingüísticos, la manipulación mediante instrucciones constituye una preocupación adicional. Entradas diseñadas estratégicamente pueden intentar modificar prioridades del sistema, evadir restricciones o inducir acciones contrarias a las políticas establecidas. Ferrag et al. (2025) analizan vulnerabilidades relacionadas con ataques dirigidos a LLM y mecanismos capaces de alterar sus respuestas. La defensa requiere separar instrucciones

confiables de contenido externo, restringir privilegios y verificar acciones antes de permitir que una salida generada afecte recursos empresariales sensibles directamente.

Las fugas de datos presentan consecuencias particularmente graves cuando un modelo procesa documentos internos, credenciales, información personal o conocimiento corporativo reservado. Una respuesta aparentemente inocente puede revelar fragmentos que nunca debieron abandonar un dominio autorizado. Ferrag et al. (2025) reconocen riesgos de privacidad y exposición de información asociados con aplicaciones de inteligencia artificial generativa. Reducir esta superficie demanda clasificación de datos, controles de acceso, filtrado de entradas y salidas, además de políticas estrictas de conservación informativa.

También existe riesgo cuando empleados incorporan información empresarial sensible en servicios generativos sin evaluar previamente condiciones de almacenamiento y tratamiento. El problema deja entonces de pertenecer exclusivamente al modelo y alcanza prácticas organizacionales, contratos, capacitación y gobierno de datos. Ferrag et al. (2025) vinculan la adopción de LLM con preocupaciones de privacidad y seguridad que requieren atención integral. Una política responsable debe delimitar qué información puede procesarse, mediante cuáles servicios y bajo qué mecanismos de protección institucional.

La evaluación de seguridad de un LLM necesita superar las pruebas convencionales de precisión. Conviene examinar resistencia ante manipulación, exposición de información, instrucciones hostiles y comportamientos inesperados bajo combinaciones poco frecuentes de entradas. Ferrag et al. (2025) reúnen vulnerabilidades y vectores de ataque que evidencian la amplitud de esta superficie. Las pruebas adversarias, auditorías periódicas y ejercicios controlados permiten descubrir debilidades

antes de que sean aprovechadas, aunque ninguna evaluación elimina completamente la incertidumbre operativa residual.

Desde el gobierno de TI, proteger sistemas de inteligencia artificial implica asignar responsabilidades durante adquisición, entrenamiento, despliegue, actualización y retiro. Cada modificación del modelo o de sus fuentes de datos puede alterar el perfil de riesgo previamente evaluado. Ferrag et al. (2025) presentan un panorama amplio de vulnerabilidades asociadas con aplicaciones generativas en ciberseguridad. Esta evidencia respalda una gobernanza continua basada en trazabilidad, gestión de accesos, evaluación de proveedores y vigilancia permanente del comportamiento tecnológico desplegado.

Para la empresa inteligente, la seguridad de la inteligencia artificial debe concebirse como una disciplina integrada con ciberseguridad, privacidad y gobierno de datos. Envenenamiento, manipulación adversaria y fugas informativas muestran que los modelos pueden ser objetivo, medio y superficie de ataque simultáneamente. Ferrag et al. (2025) evidencian esta dualidad al examinar aplicaciones defensivas junto con vulnerabilidades propias de los LLM. La confianza tecnológica dependerá de combinar innovación, controles verificables y supervisión humana durante toda su operación.

Tabla 5

Capacidades de inteligencia artificial, analítica avanzada y automatización aplicadas a la ciberseguridad empresarial

Capacidad tecnológica	Aplicación en la ciberseguridad empresarial
IA y aprendizaje automático para análisis predictivo	Procesan grandes volúmenes de datos para reconocer patrones, estimar comportamientos maliciosos y anticipar amenazas. Su desempeño depende de la calidad de los datos, el entrenamiento de los modelos y la evaluación periódica frente a cambios en las tácticas de ataque.

Capacidad tecnológica	Aplicación en la ciberseguridad empresarial
Analítica avanzada y UEBA	Analizan patrones de comportamiento de usuarios y entidades mediante variables como accesos, horarios, dispositivos y secuencias de actividad. Las desviaciones respecto de perfiles habituales permiten detectar cuentas comprometidas, amenazas internas y comportamientos anómalos en tiempo real.
Orquestación, automatización y respuesta mediante SOAR	Integran herramientas y procedimientos de seguridad mediante flujos automatizados y playbooks. Facilitan el enriquecimiento de alertas, la clasificación de incidentes, la ejecución de acciones de contención y la coordinación entre plataformas, manteniendo trazabilidad y supervisión profesional.
Ciberinteligencia, XDR y SIEM moderno	Correlacionan telemetría procedente de terminales, redes, identidades, aplicaciones y servicios digitales. La integración de evidencias distribuidas permite reconstruir cadenas de ataque, priorizar alertas y ofrecer una visión integral del incidente para orientar decisiones de investigación y respuesta.
Agentes inteligentes y sistemas autónomos	Incorporan capacidades de interpretación, razonamiento y ejecución para apoyar investigaciones y respuestas automatizadas. Pueden consultar información, organizar evidencias y ejecutar medidas previamente autorizadas, aunque requieren delimitación de privilegios, trazabilidad, mecanismos de validación y supervisión humana según el riesgo involucrado.
Seguridad de sistemas basados en IA y LLM	Comprende la protección frente al envenenamiento de datos, manipulación adversaria, instrucciones maliciosas y exposición de información sensible. Requiere controles durante entrenamiento, despliegue y operación, además de gestión de accesos, validación de entradas, protección de datos y evaluación continua de vulnerabilidades.

Nota. La tabla presenta las principales capacidades tecnológicas abordadas en el Capítulo 5 y su aplicación dentro de las operaciones de ciberseguridad empresarial. Elaboración propia con base en Vourganas y Michala (2024), Artioli et al. (2024), Lee et al. (2022) y Ferrag et al. (2025).

Capítulo 6:

Innovación, Inteligencia Empresarial y Futuro de la Ciberseguridad

La transformación digital ha llevado a las organizaciones hacia una etapa en la que innovar implica mucho más que incorporar tecnologías avanzadas. Significa aprender a gobernarlas, comprender sus implicaciones y preservar la confianza mientras cambian las formas de producir, decidir y relacionarse. Saveljeva y Volkova (2025) plantean que la confianza digital reúne dimensiones vinculadas con seguridad, gobernanza, transparencia, trazabilidad y sostenibilidad. Bajo esta perspectiva, la empresa inteligente necesita conjugar innovación y protección dentro de una misma visión estratégica.

En ese escenario, la ciberseguridad deja de ocupar una posición periférica frente a la estrategia empresarial. Participa directamente en la creación de valor, condiciona decisiones de inversión y acompaña relaciones cada vez más dependientes de plataformas digitales. Tan et al. (2025) vinculan la gobernanza de ciberseguridad con el valor corporativo mediante la confianza de inversionistas y cadenas de suministro. Esta relación permite entender la seguridad como una capacidad organizacional que protege activos y, al mismo tiempo, fortalece legitimidad empresarial.

La velocidad del cambio tecnológico añade otra dimensión al debate. Algunas capacidades que hace pocos años pertenecían al terreno experimental comienzan a incorporarse en agendas estratégicas, arquitecturas y programas de investigación empresarial. Liu y Moody (2024) señalan que los avances de la computación cuántica obligan a preparar la transición hacia mecanismos criptográficos resistentes a futuras capacidades de procesamiento. No se trata de anticipar fechas exactas, sino de reconocer que determinadas decisiones de seguridad requieren horizontes temporales considerablemente amplios.

La preparación post-cuántica ilustra una cuestión recurrente en la empresa inteligente: proteger el presente exige pensar con anticipación. Inventarios criptográficos, arquitecturas

adaptables y planes de migración adquieren valor cuando la incertidumbre tecnológica forma parte de la planificación. Liu y Moody (2024) explican que la criptografía post-cuántica responde a riesgos derivados de capacidades que podrían comprometer esquemas actualmente utilizados. La prospectiva, por tanto, se convierte en una práctica de gobierno capaz de conectar innovación científica con continuidad empresarial.

Figura 18

Ecosistema de innovación y ciberseguridad inteligente

Al mismo tiempo, las organizaciones necesitan experimentar con nuevas decisiones sin trasladar cada prueba directamente hacia sus operaciones reales. Los gemelos digitales ofrecen una respuesta particularmente interesante. Homaei et al. (2024) describen su aplicación en ciberseguridad junto con técnicas de inteligencia artificial, destacando posibilidades relacionadas con simulación, análisis y protección. Mediante representaciones virtuales vinculadas con procesos reales, la empresa puede observar comportamientos, evaluar modificaciones y aprender de escenarios

simulados antes de intervenir sobre infraestructuras que sostienen operaciones sensibles.

La inteligencia artificial introduce, además, una transformación en la distribución de la capacidad de decisión. Plataformas autónomas, agentes digitales y sistemas cognitivos pueden interpretar información y ejecutar acciones con velocidades que exceden los ciclos tradicionales de supervisión. Cao et al. (2024) examinan la automatización y orquestación de arquitecturas Zero Trust como mecanismos capaces de adaptar controles de seguridad a entornos tecnológicos dinámicos. La autonomía empresarial requiere, en consecuencia, verificación permanente, políticas gobernables y mecanismos capaces de conservar trazabilidad.

Esta evolución modifica también la relación entre innovación y responsabilidad. Una organización puede desplegar capacidades avanzadas y, aun entonces, generar fragilidad cuando sus decisiones tecnológicas carecen de criterios de gobernanza, sostenibilidad o rendición de cuentas. Tan et al. (2025) muestran que la gestión de ciberseguridad mantiene vínculos con confianza y valoración empresarial. La mirada ESG amplía esta relación al situar la seguridad digital entre las prácticas mediante las cuales una empresa demuestra disciplina institucional frente a inversionistas, proveedores y demás participantes.

Por otra parte, la expansión del edge computing acerca procesamiento e inteligencia a los lugares donde los datos son producidos. Las decisiones pueden ejecutarse cerca de dispositivos, instalaciones y procesos, reduciendo latencias y ampliando capacidades operativas. Wang et al. (2025) plantean que la inteligencia confiable en el borde requiere integrar seguridad, confiabilidad, transparencia y sostenibilidad. Esta combinación anticipa arquitecturas empresariales distribuidas donde velocidad y autonomía deberán convivir con controles capaces de mantener integridad y comportamiento previsible.

La convergencia de estas tendencias configura una empresa más conectada, distribuida y dependiente de decisiones algorítmicas. Nada ocurre de manera aislada. La confianza digital dialoga con la gobernanza; la computación cuántica obliga a revisar decisiones criptográficas; los gemelos digitales amplían las capacidades de simulación; la inteligencia artificial transforma la autonomía operativa; y el borde redistribuye procesamiento. Saveljeva y Volkova (2025) recuerdan que la confianza tecnológica requiere integrar múltiples dimensiones, precisamente porque las relaciones digitales forman sistemas profundamente interdependientes.

Este capítulo aborda esa convergencia desde una mirada orientada hacia el futuro de la ciberseguridad y la inteligencia empresarial. El interés no reside únicamente en describir tecnologías, sino en comprender las capacidades de gobierno necesarias para utilizarlas responsablemente. Wang et al. (2025) destacan que seguridad, confiabilidad, transparencia y sostenibilidad deben avanzar conjuntamente en sistemas inteligentes distribuidos. Desde esta perspectiva, innovar significa construir organizaciones capaces de anticipar cambios, aprender continuamente y preservar confianza mientras sus fronteras tecnológicas continúan transformándose.

6.1. Ecosistemas digitales inteligentes orientados a la creación de valor y confianza digital

Los ecosistemas digitales inteligentes articulan personas, datos, plataformas y capacidades analíticas para producir valor mediante relaciones tecnológicas confiables. Su relevancia empresarial reside en convertir interacciones dispersas en experiencias coordinadas, verificables y sostenibles. La confianza digital, según Saveljeva y Volkova (2025), integra seguridad, transparencia, gobernanza y cumplimiento como dimensiones interdependientes. Desde esta perspectiva, innovar exige diseñar

vínculos donde la eficiencia tecnológica avance junto con la legitimidad percibida por clientes, colaboradores, aliados y reguladores contemporáneos diversos involucrados.

La creación de valor en un ecosistema inteligente no depende únicamente de automatizar procesos, sino de establecer condiciones que permitan compartir información con seguridad y propósito. Las organizaciones obtienen ventajas cuando los participantes reconocen reglas comprensibles, responsabilidades definidas y mecanismos verificables de protección. Saveljeva y Volkova (2025) relacionan la confianza digital con arquitecturas seguras y prácticas de gobernanza capaces de reducir incertidumbre. Esa relación favorece cooperación, continuidad operativa y decisiones empresariales mejor fundamentadas y responsables.

En estos entornos, los datos adquieren una función económica y relacional. Alimentan modelos analíticos, personalizan servicios y facilitan decisiones oportunas, pero también demandan trazabilidad respecto de su origen, tratamiento y destino. La propuesta de Saveljeva y Volkova (2025) vincula la confianza con transparencia y trazabilidad, dos atributos que fortalecen la percepción de integridad. Cuando una empresa puede explicar sus prácticas digitales con claridad, transforma la gestión informacional en reputación, aprendizaje organizacional y valor compartido sostenible.

La inteligencia empresarial amplía esta lógica al convertir grandes volúmenes de información en conocimiento accionable. Sin embargo, una recomendación algorítmica pierde valor cuando sus fundamentos resultan opacos o cuando los usuarios perciben riesgos injustificados. Saveljeva y Volkova (2025) sitúan la seguridad y la transparencia entre los componentes de la confianza digital. Por ello, la analítica avanzada requiere controles, documentación y criterios de responsabilidad que permitan

aprovechar su potencia sin deteriorar relaciones construidas durante muchos años.

La arquitectura tecnológica también expresa decisiones de gobierno. Cada identidad, interfaz, servicio compartido y repositorio de datos configura límites de acceso y responsabilidades entre actores. Una arquitectura segura, en la visión sistematizada por Saveljeva y Volkova (2025), contribuye directamente a formar confianza digital. Este planteamiento desplaza la ciberseguridad desde una función defensiva hacia una capacidad de negocio: proteger intercambios, preservar evidencias y sostener experiencias confiables se convierte en una fuente tangible de diferenciación competitiva empresarial.

La gobernanza aporta dirección a esa arquitectura mediante políticas, roles, métricas y mecanismos de rendición de cuentas. En ecosistemas donde participan proveedores, clientes, plataformas, las fronteras organizacionales pierden nitidez y la responsabilidad necesita acuerdos explícitos. Saveljeva y Volkova (2025) destacan gobernanza y cumplimiento dentro de la construcción de confianza digital. La empresa inteligente debe traducir esos principios en prácticas observables, porque la confianza se fortalece cuando las promesas institucionales encuentran correspondencia en conductas verificables cotidianas.

El cumplimiento normativo adquiere mayor sentido cuando deja de tratarse como una obligación aislada y pasa a integrarse en el diseño de productos y servicios digitales. Las reglas pueden convertirse en criterios de calidad, previsibilidad y respeto hacia quienes participan del ecosistema. De acuerdo con Saveljeva y Volkova (2025), el cumplimiento forma parte de una concepción amplia de confianza digital. Esta lectura permite vincular regulación, ética corporativa y competitividad sin reducirlas a ejercicios documentales rutinarios.

La transparencia merece una atención particular porque conecta decisiones técnicas con expectativas humanas. Informar acerca del uso de datos, las responsabilidades y los mecanismos de protección reduce asimetrías entre organizaciones y usuarios. Saveljeva y Volkova (2025) incorporan la transparencia como componente de la confianza digital, junto con seguridad y trazabilidad. En términos empresariales, comunicar de manera comprensible no debilita la innovación; por el contrario, puede favorecer aceptación, cooperación y permanencia dentro de relaciones digitales complejas.

La sostenibilidad amplía la discusión más allá del rendimiento inmediato. Un ecosistema inteligente debe conservar capacidad de adaptación, legitimidad y continuidad sin trasladar costos desproporcionados a participantes futuros. Saveljeva y Volkova (2025) consideran la sostenibilidad dentro del entramado conceptual asociado con la confianza digital. Esta mirada invita a evaluar decisiones tecnológicas por su permanencia, gobernabilidad y efectos acumulativos. Crear valor implica entonces equilibrar innovación, protección, responsabilidad institucional y relaciones duraderas entre múltiples actores interdependientes actuales.

Desde una perspectiva estratégica, la confianza digital puede entenderse como capital relacional que habilita innovación y cooperación entre actores interdependientes. No se obtiene mediante una herramienta aislada; se construye con seguridad, gobernanza, cumplimiento, transparencia, trazabilidad y sostenibilidad, dimensiones reunidas por Saveljeva y Volkova (2025). Cuando estas capacidades se integran en la gestión empresarial, la ciberseguridad participa activamente en la creación de valor, fortalece decisiones inteligentes y ofrece bases confiables para futuras transformaciones tecnológicas responsables sostenibles.

6.2. Computación cuántica, criptografía post-cuántica (PQC) y preparación para la era cuántica

La computación cuántica introduce una transformación profunda en la relación entre capacidad computacional y protección criptográfica. Su desarrollo plantea una etapa en la que determinados problemas matemáticos, hoy resistentes al cálculo convencional, podrían resolverse con mayor eficiencia mediante algoritmos cuánticos. Liu y Moody (2024) advierten que este avance modifica las expectativas de seguridad asociadas con sistemas criptográficos ampliamente utilizados. Para las organizaciones, anticipar esta transición constituye una decisión estratégica vinculada con continuidad, innovación y resiliencia tecnológica futura.

La preocupación empresarial nace especialmente de la posible vulnerabilidad de esquemas de clave pública empleados para proteger comunicaciones, identidades y transacciones digitales. La capacidad de ciertos algoritmos cuánticos para alterar las premisas matemáticas tradicionales obliga a revisar arquitecturas construidas durante décadas. Liu y Moody (2024) describen la criptografía post-cuántica como una respuesta orientada a mantener protección frente a adversarios con recursos cuánticos. Esta transición demanda planificación institucional antes de que dichas capacidades alcancen madurez operativa.

La criptografía post-cuántica, conocida mediante las siglas PQC, reúne mecanismos diseñados para resistir ataques ejecutados tanto por computadores convencionales como por futuras máquinas cuánticas. Su adopción representa mucho más que sustituir algoritmos dentro de aplicaciones existentes. Liu y Moody (2024) señalan que la preparación requiere comprender las implicaciones técnicas de nuevos esquemas criptográficos y su incorporación progresiva. Cada organización deberá reconocer dependencias, compatibilidades y restricciones antes de

transformar infraestructuras donde la confianza descansa sobre criptografía tradicional.

Uno de los riesgos que merece atención procede de la captura actual de información cifrada para intentar descifrarla posteriormente mediante recursos cuánticos suficientemente avanzados. Esta posibilidad modifica la evaluación temporal del riesgo, pues datos protegidos hoy pueden conservar valor durante años. Desde la perspectiva presentada por Liu y Moody (2024), la transición hacia mecanismos resistentes debe comenzar antes de disponer de computadores cuánticos capaces de comprometer sistemas vigentes. Esperar demasiado puede convertir decisiones aplazadas en exposiciones difíciles.

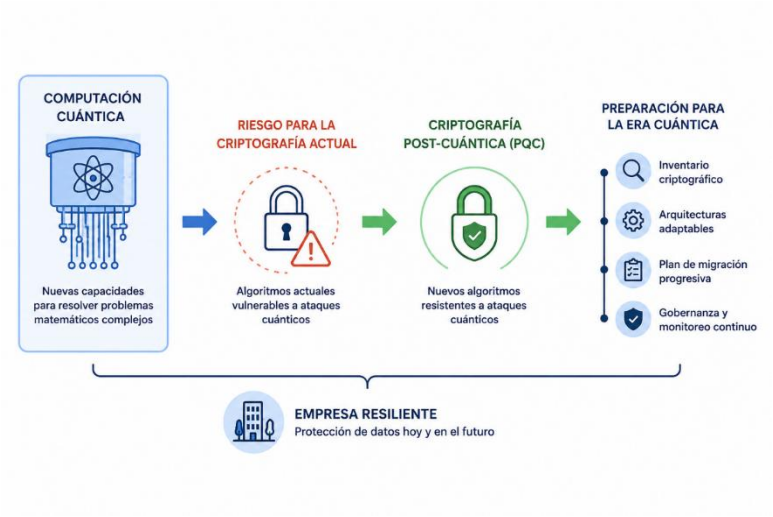
La preparación empresarial requiere elaborar inventarios criptográficos que permitan identificar algoritmos, certificados, protocolos, bibliotecas y dependencias presentes en sistemas internos y servicios externos. Sin visibilidad, cualquier programa de migración corre el riesgo de dejar componentes vulnerables inadvertidos. Liu y Moody (2024) plantean la transición post-cuántica como un proceso que demanda atención anticipada y coordinación técnica. Conocer dónde reside la criptografía permite priorizar activos, estimar esfuerzos y diseñar secuencias de cambio compatibles con las operaciones empresariales existentes.

La agilidad criptográfica adquiere especial relevancia ante este panorama. Una organización preparada necesita capacidad para sustituir algoritmos y parámetros sin reconstruir por completo sus sistemas cada vez que evolucionen los estándares o aparezcan nuevas evidencias técnicas. Liu y Moody (2024) examinan la transición post-cuántica desde una perspectiva donde la adaptación tecnológica resulta determinante para mantener protección. Diseñar arquitecturas flexibles reduce dependencias rígidas y facilita incorporar mecanismos resistentes conforme maduren las tecnologías cuánticas y los estándares internacionales aplicables.

La migración hacia PQC también plantea decisiones relacionadas con rendimiento, interoperabilidad y administración de claves. Los nuevos mecanismos pueden presentar tamaños, requisitos computacionales y comportamientos diferentes respecto de soluciones anteriores, algo relevante en infraestructuras heterogéneas. Liu y Moody (2024) destacan que la transición debe considerar cuidadosamente las propiedades prácticas de los algoritmos post-cuánticos. Evaluarlos mediante pruebas controladas permite detectar incompatibilidades, medir efectos operativos y evitar que una mejora criptográfica produzca dificultades inesperadas en servicios empresariales críticos existentes.

Figura 19

Transición hacia la seguridad post-cuántica



La era cuántica requiere además una gobernanza capaz de conectar decisiones científicas, arquitectónicas y empresariales. Los responsables de seguridad necesitan dialogar con áreas de infraestructura, desarrollo, riesgos, cumplimiento y dirección para establecer prioridades coherentes. De acuerdo con Liu y Moody

(2024), la evolución hacia criptografía resistente demanda una transición consciente frente al progreso tecnológico. Esta preparación convierte un asunto aparentemente distante en una responsabilidad presente, vinculada con inversiones, ciclos tecnológicos y protección prolongada de información sensible corporativa.

Conviene comprender que prepararse para tecnologías cuánticas no significa predecir una fecha exacta para la aparición de máquinas capaces de afectar sistemas criptográficos relevantes. La incertidumbre forma parte del problema y obliga a trabajar mediante escenarios. Liu y Moody (2024) muestran que la seguridad post-cuántica responde precisamente a la necesidad de anticipar capacidades futuras sin abandonar las necesidades actuales. Esta perspectiva favorece programas graduales, evaluaciones periódicas y decisiones reversibles frente a una evolución tecnológica todavía dinámica.

La computación cuántica representa, en consecuencia, una frontera donde innovación y ciberseguridad vuelven a encontrarse. Las empresas inteligentes deberán observar avances científicos mientras desarrollan inventarios criptográficos, agilidad arquitectónica, pruebas de interoperabilidad y planes progresivos de migración. Liu y Moody (2024) sitúan la criptografía post-cuántica dentro de una transformación necesaria para preservar seguridad ante capacidades futuras. Prepararse desde ahora permite distribuir esfuerzos, reducir incertidumbre y proteger el valor digital durante ciclos tecnológicos que trascienden decisiones inmediatas.

6.3. Gemelos digitales como soporte para simulación y gestión segura de procesos empresariales

Los gemelos digitales representan una evolución significativa en la manera de observar, comprender y gestionar procesos empresariales mediante representaciones virtuales

vinculadas con sistemas físicos o digitales. Estas réplicas permiten analizar comportamientos, anticipar variaciones y ensayar decisiones sin intervenir directamente sobre operaciones productivas. Homaei et al. (2024) destacan su creciente relación con inteligencia artificial y ciberseguridad. Esta convergencia convierte al gemelo digital en un recurso estratégico para organizaciones interesadas en combinar eficiencia, aprendizaje continuo y protección operacional responsable.

La capacidad de reproducir dinámicas empresariales dentro de entornos virtuales ofrece una ventaja especialmente valiosa: experimentar antes de actuar. Un cambio operativo, una configuración tecnológica o una política de seguridad pueden evaluarse mediante simulaciones que reduzcan incertidumbre. De acuerdo con Homaei et al. (2024), los gemelos digitales facilitan análisis avanzados apoyados por inteligencia artificial. Para la empresa inteligente, esta posibilidad transforma la simulación en una práctica de gestión capaz de respaldar decisiones con evidencia y previsión.

La utilidad del gemelo digital depende, en buena medida, de la calidad de los datos que alimentan su representación. Sensores, aplicaciones empresariales, dispositivos conectados y plataformas analíticas proporcionan señales que mantienen correspondencia entre operación real y modelo virtual. Homaei et al. (2024) describen esta integración como fundamento para aplicaciones vinculadas con seguridad y análisis inteligente. Datos incompletos, manipulados o tardíos pueden distorsionar resultados; por ello, integridad y trazabilidad adquieren especial relevancia en estas arquitecturas.

Desde la perspectiva de ciberseguridad, los gemelos digitales ofrecen espacios controlados para estudiar incidentes sin comprometer directamente activos productivos. Es posible reproducir configuraciones, observar patrones anómalos y evaluar respuestas ante determinadas amenazas dentro de

representaciones diseñadas para experimentación. Homaei et al. (2024) relacionan estas capacidades con aplicaciones de inteligencia artificial orientadas a fortalecer la seguridad. El aprendizaje obtenido mediante simulaciones puede alimentar procedimientos preventivos y mejorar la preparación institucional frente a eventos potencialmente disruptivos futuros.

La inteligencia artificial amplía notablemente las posibilidades de estas representaciones al identificar patrones difíciles de reconocer mediante observación convencional. Algoritmos de aprendizaje pueden analizar datos históricos y señales operativas para detectar desviaciones relevantes. Homaei et al. (2024) examinan precisamente la convergencia entre gemelos digitales, inteligencia artificial y ciberseguridad como un campo de creciente desarrollo. Esta combinación permite avanzar desde modelos descriptivos hacia capacidades predictivas que apoyan mantenimiento, seguridad y continuidad de procesos empresariales complejos actuales.

Un gemelo digital también puede convertirse en instrumento para evaluar modificaciones arquitectónicas antes de trasladarlas al entorno productivo. Nuevas conexiones, controles o configuraciones pueden probarse virtualmente y observar sus efectos sobre rendimiento y seguridad. Según Homaei et al. (2024), estas tecnologías ofrecen posibilidades relevantes para modelar sistemas y apoyar mecanismos inteligentes de protección. La experimentación previa reduce intervenciones improvisadas y permite documentar evidencias útiles para decisiones técnicas, auditorías y procesos internos de gestión del riesgo tecnológico.

Sin embargo, la representación virtual también requiere protección. Un gemelo digital conectado con procesos empresariales puede concentrar información detallada acerca de configuraciones, comportamientos y dependencias operativas. Homaei et al. (2024) reconocen cuestiones de seguridad asociadas con estas tecnologías y con los datos utilizados por ellas. Proteger

accesos, comunicaciones e integridad de los modelos resulta indispensable. Una representación alterada deliberadamente podría producir interpretaciones equivocadas y conducir decisiones empresariales hacia respuestas poco adecuadas frente a situaciones reales relevantes.

La gestión segura de procesos mediante gemelos digitales exige gobernanza sobre datos, modelos, accesos y responsabilidades. No basta con disponer de una representación técnicamente avanzada; resulta necesario determinar quién puede modificarla, qué información recibe y qué decisiones pueden apoyarse en sus resultados. Homaei et al. (2024) muestran que la aplicación de estas tecnologías en ciberseguridad requiere considerar múltiples componentes interrelacionados. La gobernanza aporta disciplina para convertir capacidad técnica en conocimiento confiable y operacionalmente útil para organizaciones contemporáneas.

Otra aportación relevante aparece en la formación y preparación de equipos. Los escenarios virtuales permiten practicar respuestas, analizar comportamientos y estudiar consecuencias sin interrumpir operaciones reales. La revisión de Homaei et al. (2024) evidencia el potencial de los gemelos digitales para aplicaciones de seguridad apoyadas por inteligencia artificial. En una organización orientada al aprendizaje, estas prácticas pueden fortalecer capacidades humanas y técnicas, creando experiencias donde equivocarse durante una simulación aporta conocimiento antes de enfrentar incidentes verdaderos complejos.

Los gemelos digitales proyectan una forma distinta de relacionar innovación, inteligencia empresarial y ciberseguridad. Su valor procede de conectar representación, datos, simulación y aprendizaje para comprender procesos antes de intervenir sobre ellos. Homaei et al. (2024) muestran que su convergencia con inteligencia artificial abre oportunidades relevantes para protección y análisis avanzado. Integrados mediante criterios de

seguridad y gobernanza, pueden transformar la experimentación virtual en una capacidad empresarial permanente para anticipar riesgos y orientar decisiones responsables futuras.

6.4. Ciberseguridad en plataformas autónomas, sistemas cognitivos y organizaciones impulsadas por IA

Las plataformas autónomas modifican profundamente la relación entre decisión, velocidad y responsabilidad dentro de la empresa inteligente. Sistemas capaces de interpretar señales, ejecutar acciones y ajustar comportamientos reducen la intervención humana en múltiples operaciones, pero amplían la superficie que debe protegerse. Cao et al. (2024) vinculan automatización y orquestación con arquitecturas Zero Trust orientadas a verificar continuamente las interacciones digitales. La ciberseguridad adquiere entonces una función dinámica, integrada directamente en decisiones tecnológicas ejecutadas a velocidad algorítmica.

Los sistemas cognitivos incorporan capacidades analíticas que permiten reconocer patrones, procesar información y apoyar decisiones empresariales con creciente autonomía. Esta condición exige abandonar modelos de seguridad sustentados principalmente en perímetros estáticos. Cao et al. (2024) analizan la automatización de Zero Trust mediante mecanismos capaces de adaptar controles frente a condiciones cambiantes. En organizaciones impulsadas por inteligencia artificial, verificar identidades, dispositivos, aplicaciones y solicitudes de acceso constituye una práctica permanente que acompaña cada interacción digital relevante.

La automatización de controles permite responder con rapidez cuando una plataforma gestiona miles de interacciones simultáneas. Una decisión tardía puede resultar insuficiente frente a sistemas que operan en milisegundos. La orquestación estudiada por Cao et al. (2024) busca coordinar componentes de Zero Trust

para aplicar políticas de manera dinámica y consistente. Esta capacidad resulta particularmente pertinente cuando agentes inteligentes consumen servicios, intercambian datos y ejecutan tareas sin requerir autorización humana explícita durante cada operación empresarial cotidiana.

La identidad adquiere nuevas dimensiones cuando las acciones dejan de proceder exclusivamente de usuarios humanos. Agentes inteligentes, servicios automatizados, interfaces y cargas de trabajo también requieren atributos verificables que permitan determinar privilegios adecuados. Cao et al. (2024) relacionan la automatización de Zero Trust con mecanismos destinados a gestionar decisiones de acceso bajo criterios adaptativos. Esta perspectiva favorece una seguridad donde cada entidad demuestra legitimidad antes de utilizar recursos, independientemente de su ubicación o de autorizaciones concedidas anteriormente.

En organizaciones impulsadas por inteligencia artificial, los datos representan tanto materia prima para aprender como activos que requieren protección permanente. Una alteración inadvertida o maliciosa puede modificar resultados analíticos y desencadenar decisiones automatizadas incorrectas. El planteamiento de Cao et al. (2024) acerca de arquitecturas Zero Trust automatizadas refuerza la necesidad de evaluar continuamente accesos y comportamientos. Proteger flujos informacionales significa preservar confidencialidad e integridad, pero también cuidar la calidad de las decisiones derivadas de ellos.

La orquestación aporta coordinación entre herramientas que tradicionalmente han funcionado como componentes independientes. Gestión de identidades, análisis de comportamiento, políticas de acceso y mecanismos de respuesta pueden intercambiar señales para construir decisiones más oportunas. Cao et al. (2024) estudian esta integración dentro de Zero Trust y destacan el papel de la automatización para administrar entornos tecnológicos complejos. La empresa obtiene

mayor capacidad de reacción cuando sus controles comparten información y actúan mediante políticas previamente gobernadas coherentes.

Una plataforma autónoma necesita libertad operativa suficiente para cumplir sus objetivos, aunque esa autonomía no debería confundirse con ausencia de supervisión. Políticas, límites y registros permiten establecer espacios de actuación compatibles con el riesgo aceptado por la organización. Cao et al. (2024) presentan la automatización de Zero Trust como una vía para adaptar decisiones de seguridad mediante información continuamente actualizada. La autonomía responsable nace, precisamente, de combinar capacidad de acción con mecanismos persistentes de verificación y control.

La velocidad algorítmica plantea también preguntas acerca de trazabilidad y responsabilidad. Cuando una decisión automatizada bloquea un servicio, modifica permisos o responde ante una anomalía, la organización necesita comprender las razones que motivaron esa actuación. Cao et al. (2024) examinan mecanismos de orquestación capaces de coordinar políticas dentro de arquitecturas Zero Trust. Mantener registros interpretables permite auditar decisiones, ajustar reglas y conservar supervisión humana sobre sistemas cuyo comportamiento puede variar ante señales operativas cambiantes de manera continua.

La adopción de inteligencia artificial en funciones empresariales requiere que la seguridad participe desde el diseño de procesos y arquitecturas. Incorporarla después puede producir controles fragmentados, incompatibilidades y dependencias difíciles de administrar. La propuesta analizada por Cao et al. (2024) muestra el valor de automatizar y orquestar principios Zero Trust para responder a infraestructuras dinámicas. Este enfoque favorece arquitecturas donde verificación, mínimo privilegio y evaluación permanente acompañan naturalmente la evolución de plataformas inteligentes y servicios autónomos empresariales.

Figura 20
Ciberseguridad en organizaciones impulsadas por IA

La empresa impulsada por inteligencia artificial necesita una ciberseguridad capaz de aprender, coordinar controles y responder al ritmo de sus sistemas automatizados. Zero Trust ofrece principios pertinentes para esta transformación cuando sus mecanismos pueden operar de manera adaptable. Cao et al. (2024) vinculan automatización y orquestación con una aplicación más dinámica de estas arquitecturas. El propósito empresarial consiste en preservar confianza y gobernabilidad mientras máquinas, personas y servicios colaboran dentro de procesos progresivamente autónomos, distribuidos e inteligentes.

6.5. Innovación tecnológica sostenible y gobernanza ESG aplicada a la seguridad digital

La innovación tecnológica sostenible exige comprender la seguridad digital como parte de la responsabilidad corporativa y no como una función técnica separada del gobierno empresarial. Proteger datos, infraestructuras y relaciones digitales influye sobre

la continuidad operativa, la reputación y las expectativas de quienes aportan capital. Tan et al. (2025) vinculan la gobernanza de ciberseguridad con el valor de mercado corporativo mediante mecanismos asociados con confianza. Esta relación aproxima naturalmente seguridad, sostenibilidad y gestión estratégica empresarial responsable.

La perspectiva ESG amplía la lectura tradicional de la ciberseguridad al relacionarla con compromisos ambientales, sociales y de gobernanza que condicionan la legitimidad empresarial. Una organización digitalmente responsable necesita demostrar capacidad para administrar riesgos tecnológicos sin comprometer derechos, relaciones comerciales ni continuidad. Tan et al. (2025) encuentran conexiones entre gobierno de ciberseguridad, confianza de inversionistas y valoración corporativa. La protección digital adquiere, desde esta mirada, significado económico y reputacional dentro de las decisiones estratégicas de largo plazo.

La dimensión ambiental también dialoga con la innovación digital mediante decisiones relacionadas con infraestructura, eficiencia computacional y renovación tecnológica. Adoptar nuevas capacidades de seguridad implica considerar consumo energético, vida útil de dispositivos y sostenibilidad de arquitecturas cada vez más intensivas en datos. Aunque Tan et al. (2025) centran su análisis en gobernanza, confianza y valor empresarial, su perspectiva permite entender que las decisiones de ciberseguridad participan en marcos corporativos donde rendimiento económico y responsabilidad sostenible mantienen vínculos crecientes.

En la dimensión social, la seguridad digital protege relaciones que dependen de confianza, privacidad y continuidad de los servicios. Clientes, empleados, proveedores e inversionistas esperan que las organizaciones administren responsablemente la información confiada a sus plataformas. Tan et al. (2025) muestran que la confianza de los inversionistas constituye un mecanismo

relevante entre gobernanza de ciberseguridad y valor corporativo. Una gestión responsable puede comunicar madurez institucional y reducir percepciones de incertidumbre asociadas con incidentes tecnológicos y prácticas deficientes.

La gobernanza representa el punto donde ESG y ciberseguridad encuentran una conexión particularmente directa. Consejos de administración y equipos ejecutivos necesitan integrar el riesgo digital dentro de decisiones sobre estrategia, inversiones y supervisión. Tan et al. (2025) relacionan una mejor gobernanza de ciberseguridad con efectos favorables sobre la confianza y el valor empresarial. La seguridad deja entonces de pertenecer exclusivamente al área tecnológica y pasa a formar parte de responsabilidades directivas vinculadas con transparencia, control y rendición de cuentas.

Las cadenas de suministro digitales amplían esta responsabilidad porque una organización depende de proveedores tecnológicos, plataformas, servicios externos y múltiples relaciones interconectadas. La seguridad de cada participante puede afectar la estabilidad del conjunto. Tan et al. (2025) identifican la confianza en la cadena de suministro como una vía mediante la cual la gobernanza de ciberseguridad puede relacionarse con el valor corporativo. Gestionar terceros responsablemente contribuye a proteger operaciones y preservar relaciones comerciales sostenibles durante periodos prolongados.

La confianza de los inversionistas ofrece otra lectura significativa de la seguridad digital. Las decisiones de inversión consideran perspectivas financieras, pero también señales acerca de calidad directiva, exposición al riesgo y capacidad institucional para responder ante incertidumbre. Según Tan et al. (2025), la gobernanza de ciberseguridad puede fortalecer dicha confianza y favorecer el valor de mercado. Comunicar políticas, responsabilidades y mecanismos de supervisión permite convertir

prácticas internas de protección en señales externas de disciplina organizacional y previsión estratégica.

La innovación sostenible requiere evitar una paradoja frecuente: incorporar tecnologías avanzadas mientras aumentan dependencias, vulnerabilidades o costos difíciles de gobernar. Cada iniciativa digital debería evaluarse atendiendo beneficios empresariales, riesgos tecnológicos y consecuencias para grupos interesados. Los hallazgos de Tan et al. (2025) refuerzan la relación entre gobernanza de ciberseguridad y creación de valor mediante confianza. Innovar responsablemente significa, entonces, desarrollar capacidades digitales cuya expansión pueda mantenerse bajo criterios verificables de control, responsabilidad y continuidad empresarial futura.

Las métricas ESG pueden enriquecerse cuando la ciberseguridad se traduce en indicadores comprensibles para órganos de gobierno e inversionistas. Frecuencia de incidentes, exposición de terceros, tiempos de respuesta, madurez de controles y supervisión directiva ofrecen señales acerca de capacidad institucional. Tan et al. (2025) aportan evidencia sobre la relación entre gobernanza de seguridad, confianza y valoración corporativa. Medir con criterio permite abandonar reportes meramente técnicos y conectar protección digital con decisiones empresariales, sostenibilidad y responsabilidad corporativa efectiva.

Integrar innovación sostenible, ESG y seguridad digital conduce hacia una concepción más amplia del valor empresarial. La organización protege activos mientras preserva confianza entre inversionistas, proveedores y demás participantes de su ecosistema económico. Tan et al. (2025) muestran que la gobernanza de ciberseguridad puede relacionarse positivamente con valoración corporativa mediante confianza inversora y confianza en cadenas de suministro. Esta perspectiva convierte la seguridad digital en una capacidad de gobierno vinculada con resiliencia, legitimidad y crecimiento responsable.

6.6. Prospectiva de la empresa inteligente en escenarios de hiperconectividad, edge computing y automatización avanzada

La empresa inteligente avanza hacia escenarios donde dispositivos, plataformas, personas y algoritmos intercambian información con una velocidad creciente. La hiperconectividad modifica la arquitectura organizacional porque distribuye capacidades de decisión entre múltiples puntos tecnológicos. Wang et al. (2025) relacionan la inteligencia en el borde con seguridad, confiabilidad, transparencia y sostenibilidad, dimensiones necesarias para construir sistemas confiables. Esta perspectiva anticipa organizaciones donde procesar información cerca de su origen permitirá responder con rapidez sin abandonar criterios rigurosos de protección.

El edge computing desplaza parte del procesamiento desde infraestructuras centralizadas hacia dispositivos y nodos próximos a las fuentes de datos. Esta distribución reduce latencias y favorece respuestas inmediatas en operaciones sensibles al tiempo. Wang et al. (2025) examinan la inteligencia confiable en el borde como una convergencia entre capacidades computacionales, aprendizaje automático y requisitos de seguridad. Para la empresa, acercar análisis y decisión puede transformar procesos industriales, logísticos y comerciales mediante respuestas adaptativas ante variaciones operativas frecuentes.

La hiperconectividad empresarial incrementará el número de relaciones digitales que deben administrarse simultáneamente. Sensores, equipos industriales, vehículos, aplicaciones y agentes inteligentes intercambiarán señales dentro de infraestructuras distribuidas, generando oportunidades de coordinación y nuevas exposiciones. Según Wang et al. (2025), la inteligencia en el borde necesita mecanismos que garanticen seguridad y confiabilidad frente a condiciones cambiantes. La empresa inteligente deberá

combinar conectividad amplia con políticas capaces de preservar integridad, disponibilidad y comportamiento previsible entre componentes tecnológicos heterogéneos.

La automatización avanzada añadirá capacidad de acción a esa infraestructura distribuida. Los sistemas no se limitarán a recopilar información; podrán interpretar señales, seleccionar respuestas y ejecutar operaciones con intervención humana reducida. Wang et al. (2025) destacan la confiabilidad como una propiedad central de la inteligencia desplegada en el borde. Este principio resulta especialmente relevante cuando decisiones automatizadas afectan producción, logística o servicios, pues cada acción requiere mecanismos que permitan mantener rendimiento previsible incluso ante fallos, perturbaciones o comportamientos adversos.

La seguridad adquiere características particulares cuando datos y modelos se procesan fuera de centros tecnológicos tradicionales. Cada nodo del borde puede convertirse en punto de decisión y, simultáneamente, en superficie susceptible de ataques. Wang et al. (2025) examinan amenazas y mecanismos de protección asociados con inteligencia distribuida confiable. La prospectiva empresarial deberá considerar arquitecturas capaces de proteger dispositivos, comunicaciones, datos y modelos mientras mantienen flexibilidad suficiente para operar en escenarios dinámicos, heterogéneos y geográficamente dispersos de manera eficiente.

La transparencia será igualmente importante porque las decisiones tomadas cerca del borde pueden producir efectos inmediatos sobre procesos físicos y digitales. Comprender por qué un sistema seleccionó determinada acción facilita supervisión, auditoría y corrección. Wang et al. (2025) reconocen la transparencia como una dimensión relevante para establecer inteligencia confiable en entornos distribuidos. En la empresa futura, explicar decisiones automatizadas contribuirá a mantener gobernabilidad cuando numerosos modelos actúen

simultáneamente sobre recursos, usuarios y operaciones sensibles del negocio cotidiano.

La sostenibilidad tecnológica adquiere especial relevancia ante la multiplicación de dispositivos, modelos y cargas computacionales distribuidas. Mayor inteligencia no debería traducirse necesariamente en consumo indiscriminado de energía y recursos. Wang et al. (2025) integran sostenibilidad dentro de las dimensiones que caracterizan una inteligencia confiable en el borde. Esta mirada invita a diseñar arquitecturas eficientes, capaces de equilibrar rendimiento y utilización responsable de recursos, especialmente cuando millones de dispositivos participen en redes empresariales crecientemente automatizadas y conectadas.

Desde una perspectiva organizacional, estas transformaciones modificarán también la distribución de responsabilidades. La toma de decisiones tecnológicas ocurrirá en múltiples niveles, desde centros corporativos hasta dispositivos instalados en instalaciones remotas. Wang et al. (2025) muestran que seguridad, confiabilidad, transparencia y sostenibilidad deben considerarse conjuntamente para desarrollar inteligencia confiable en el borde. Gobernar esta diversidad requerirá políticas coherentes, mecanismos de supervisión y capacidades humanas capaces de interpretar sistemas cuya autonomía aumentará progresivamente durante los próximos ciclos tecnológicos.

La prospectiva no consiste en predecir exactamente qué tecnología dominará cada sector, sino en reconocer fuerzas capaces de modificar estructuras empresariales y preparar respuestas flexibles. Edge computing, inteligencia artificial e hiperconectividad forman una combinación que redistribuye procesamiento y decisión. Wang et al. (2025) presentan una visión de inteligencia en el borde donde múltiples propiedades de confianza deben coexistir. Preparar arquitecturas adaptables permitirá aprovechar innovaciones futuras sin comprometer

seguridad, rendimiento, transparencia ni sostenibilidad de las operaciones empresariales.

La empresa inteligente del futuro probablemente funcionará como una red distribuida de capacidades cognitivas, servicios digitales y decisiones automatizadas coordinadas entre nube y borde. En esa configuración, la confianza tecnológica deberá construirse desde múltiples dimensiones complementarias. Wang et al. (2025) articulan seguridad, confiabilidad, transparencia y sostenibilidad como fundamentos de una inteligencia en el borde digna de confianza. Integrar estos principios permitirá convertir hiperconectividad y automatización avanzada en capacidades empresariales orientadas a innovación responsable y resiliencia.

Tabla 6

Tecnologías emergentes y dimensiones estratégicas de ciberseguridad para la empresa inteligente

Ámbito tecnológico y estratégico	**Implicaciones para la ciberseguridad y la empresa inteligente**
Ecosistemas digitales inteligentes	Articulan datos, plataformas, actores y servicios bajo principios de confianza digital. Requieren seguridad, transparencia, trazabilidad, gobernanza y cumplimiento para sostener relaciones digitales confiables y favorecer la creación de valor.
Computación cuántica y criptografía post-cuántica	Plantean la necesidad de anticipar la transición desde esquemas criptográficos vulnerables frente a futuras capacidades cuánticas hacia mecanismos resistentes, acompañados de inventarios criptográficos, agilidad arquitectónica y planes progresivos de migración.
Gemelos digitales	Permiten representar procesos y activos para realizar simulaciones, evaluar modificaciones y estudiar escenarios de seguridad sin intervenir directamente sobre operaciones reales. Su confiabilidad depende de la integridad de los datos, la protección del modelo y una gobernanza adecuada.
Plataformas autónomas y sistemas cognitivos	Incrementan la autonomía en decisiones y operaciones empresariales. Demandan verificación continua de identidades, accesos y comportamientos,

	junto con mecanismos de trazabilidad, supervisión y orquestación compatibles con principios Zero Trust.
Innovación sostenible y gobernanza ESG	Vinculan la protección digital con responsabilidad corporativa, confianza de inversionistas, relaciones con terceros y valor empresarial. La ciberseguridad adquiere relevancia dentro de la gobernanza y de los criterios utilizados para valorar sostenibilidad, transparencia y rendición de cuentas.
Hiperconectividad, edge computing y automatización avanzada	Distribuyen procesamiento, inteligencia y capacidad decisoria entre nube, borde y dispositivos conectados. Requieren integrar seguridad, confiabilidad, transparencia y sostenibilidad para preservar operaciones resilientes dentro de arquitecturas crecientemente distribuidas y automatizadas.

Nota. La tabla relaciona los principales ámbitos abordados en el capítulo con sus implicaciones para la seguridad digital y la evolución de la empresa inteligente. Elaboración basada en Saveljeva y Volkova (2025), Liu y Moody (2024), Homaei et al. (2024), Cao et al. (2024), Tan et al. (2025) y Wang et al. (2025).

Conclusiones

La ciberseguridad constituye una capacidad estratégica para conducir la transformación digital con niveles adecuados de confianza, continuidad y generación de valor. Su integración en la dirección organizacional permite vincular las decisiones tecnológicas con prioridades empresariales, exposición al riesgo y expectativas de crecimiento sostenible. Esta perspectiva supera una visión centrada exclusivamente en controles técnicos. La Empresa Inteligente requiere seguridad incorporada desde la planificación, capaz de acompañar la innovación y preservar los activos que sostienen sus procesos, servicios y decisiones.

La gestión integral del riesgo digital representa el punto de partida para establecer prioridades coherentes con los objetivos del negocio. Identificar activos, amenazas, vulnerabilidades, dependencias e impactos permite orientar recursos hacia exposiciones relevantes y fundamentar decisiones ejecutivas con mayor precisión. La cuantificación fortalece esta capacidad al traducir el riesgo cibernético a términos comprensibles para la dirección. El monitoreo continuo completa este enfoque mediante perfiles dinámicos que permiten ajustar controles, inversiones y respuestas conforme evoluciona la superficie digital de la organización.

El gobierno de TI y la gobernanza de la ciberseguridad convierten las prioridades derivadas del riesgo en responsabilidades, políticas, métricas y mecanismos de supervisión. Esta relación aproxima la seguridad a juntas directivas, comités ejecutivos y responsables de procesos empresariales. La responsabilidad deja de concentrarse en las áreas tecnológicas. Una Empresa Inteligente necesita estructuras de decisión capaces de equilibrar innovación, cumplimiento, privacidad, desempeño y exposición digital, promoviendo una cultura donde cada actor

comprenda su participación en la construcción de confianza y resiliencia institucional.

La arquitectura empresarial materializa las decisiones de riesgo y gobierno mediante estructuras tecnológicas coherentes con la estrategia. Zero Trust, seguridad por diseño, DevSecOps, arquitecturas híbridas, servicios en nube, microservicios y APIs conforman componentes de una visión que integra protección desde las etapas iniciales del diseño. Esta articulación reduce fragmentaciones entre estrategia y operación. La arquitectura adquiere, por tanto, una función de enlace entre necesidades empresariales, información, aplicaciones e infraestructura, favoreciendo capacidades digitales adaptables, interoperables, protegidas y preparadas para cambios tecnológicos acelerados.

La protección de activos digitales alcanza mayor efectividad cuando identidades, accesos, privilegios, datos, infraestructuras y cadenas de suministro forman parte de una estrategia integrada. Prevenir continúa siendo indispensable, aunque resulta insuficiente frente a entornos altamente interconectados. Las organizaciones necesitan detectar anomalías, contener incidentes, recuperar servicios y aprender de cada evento. La resiliencia operativa amplía entonces el propósito de la seguridad: además de reducir probabilidades de materialización, busca conservar funciones esenciales y recuperar capacidades empresariales ante perturbaciones de distinta naturaleza.

La inteligencia artificial y la analítica avanzada transforman las operaciones de ciberseguridad mediante detección de anomalías, análisis predictivo, correlación de eventos y automatización de respuestas. Estas capacidades permiten procesar volúmenes de información difíciles de gestionar mediante intervención humana permanente. Al mismo tiempo, introducen riesgos relacionados con modelos, datos, privacidad, decisiones automatizadas y nuevas modalidades de ataque. La innovación responsable requiere mecanismos de supervisión, trazabilidad y

evaluación que permitan aprovechar estas tecnologías sin desvincularlas del gobierno institucional ni del apetito de riesgo establecido.

Las preguntas formuladas al inicio de la obra encuentran una respuesta convergente: riesgo, gobierno, arquitectura, protección, operación e innovación deben funcionar como componentes relacionados de una misma capacidad organizacional. Ninguna dimensión alcanza madurez cuando permanece aislada. La secuencia desarrollada permite pasar de la identificación de aquello que puede afectar al negocio hacia decisiones de gobierno, diseños tecnológicos protegidos, capacidades operativas resilientes y mecanismos de innovación responsable. Esta integración constituye uno de los fundamentos distintivos de la Empresa Inteligente propuesta en esta obra.

La Empresa Inteligente puede comprenderse, en consecuencia, como una organización capaz de aprender, decidir y adaptarse mediante la integración responsable de personas, procesos, datos y tecnologías. Su inteligencia no depende exclusivamente del grado de automatización alcanzado, sino de la calidad de sus decisiones y de la confianza que pueda sostener en sus ecosistemas digitales. Seguridad, gobernanza y arquitectura adquieren carácter habilitador. Innovar con responsabilidad implica desarrollar capacidades tecnológicas que generen valor sin debilitar continuidad, privacidad, cumplimiento, trazabilidad ni sostenibilidad empresarial.

El futuro del riesgo, el gobierno y la arquitectura estará condicionado por la expansión de la IA generativa, la hiperconectividad, los sistemas autónomos, la inteligencia distribuida y la computación cuántica. Estas transformaciones ampliarán las superficies de exposición y modificarán los criterios tradicionales de control. Los modelos de gobierno necesitarán mayor adaptabilidad, mientras las arquitecturas deberán incorporar confianza verificable, segmentación, automatización y

preparación criptográfica. El riesgo adquirirá un carácter progresivamente dinámico, demandando evaluación continua y decisiones capaces de responder a entornos tecnológicos en permanente transformación.

La resiliencia será, bajo este horizonte, una expresión de madurez organizacional y no una capacidad reservada para momentos de crisis. La empresa preparada para el futuro será aquella que pueda anticipar, resistir, responder, recuperarse y aprender mientras mantiene su capacidad de innovar. La ciberseguridad adquiere entonces un propósito profundamente empresarial: proteger la confianza que permite transformar. Frente a la IA generativa y la hiperconectividad, gobernar el riesgo con inteligencia permitirá construir organizaciones adaptables, sostenibles y capaces de crear valor digital perdurable.

Referencias Bibliográficas

Asamblea Nacional del Ecuador. (2021)**.** *Ley Orgánica de Protección de Datos Personales***.** Quinto Suplemento del Registro Oficial No. 459, 26 de mayo de 2021

Aflakhah, E., & Soewito, B. (2023). Assessing information security using COBIT 2019 and ISO 27001:2013 for developing a mitigation plan. *International Journal of Engineering Trends and Technology, 71*(10), 223–237. https://doi.org/10.14445/22315381/IJETT-V71I10P221

Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. *Applied Sciences, 14*(24), 11807. https://doi.org/10.3390/app142411807

Aksoy, C. (2024). Building a cyber security culture for resilient organizations against cyber attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, 7*(1), 96–110. https://doi.org/10.33416/baybem.1374001

Anderson, J., Huang, Q., Cheng, L., & Hu, H. (2023). A zero-trust architecture for connected and autonomous vehicles. *IEEE Internet Computing, 27*(5), 7–14. https://doi.org/10.1109/MIC.2023.3304893

Arellano, A., et al. (2023). Aplicación de COBIT 2019 al gobierno y gestión de las tecnologías de información en instituciones educativas sin fines de lucro. *South Florida Journal of Development, 4*(3), 1388–1410. https://doi.org/10.46932/sfjdv4n3-027

Artioli, P., Maci, A., & Magrì, A. (2024). A comprehensive investigation of clustering algorithms for user and entity behavior analytics. *Frontiers in Big Data, 7*, 1375818. https://doi.org/10.3389/fdata.2024.1375818

Bhol, S. G., Mohanty, J. R., & Pattnaik, P. K. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings, 80*, 2274–2279. https://doi.org/10.1016/j.matpr.2021.06.228

Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and orchestration of zero trust architecture: Potential solutions and challenges. *Machine Intelligence Research, 21*(2), 294–317.

Chong, W. F., Feng, R., Hu, H., & Zhang, L. (2025). Cyber risk assessment for capital management. *Journal of Risk and Insurance, 92*(2), 424–471. https://doi.org/10.1111/jori.12504

Cyber supply chain resilience: Analyzing ISO, NIST, and NIS2 frameworks for mitigating third-party risks. (2025). *Procedia Computer Science, 263*, 591–599. https://doi.org/10.1016/j.procs.2025.07.071

Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2025). Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities. *Internet of Things and Cyber-Physical Systems, 5*, 1–46. https://doi.org/10.1016/j.iotcps.2025.01.001

Gale, M., Bongiovanni, I., & Slapničar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security, 121*, 102840. https://doi.org/10.1016/j.cose.2022.102840

Glöckler, J., Sedlmeir, J., & Frank, M. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering, 66*, 421–440. https://doi.org/10.1007/s12599-023-00830-x

Goshikonda, N., & Pulipati, K. (2024). Continuous cyber security risk assessment using zero-trust architecture and machine learning intelligence. *Journal of Computational Analysis and Applications*. https://doi.org/10.48047/jocaaa.2024.33.08.440

Hardi, K. V., & Legowo, N. (2023). Enterprise architecture: Enabling digital transformation for operational business process during COVID-19. *HighTech and Innovation Journal, 4*(1), 1–18. https://doi.org/10.28991/HIJ-2023-04-01-01

Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. C., Ávila, M., & Caro, A. (2024). A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review, 57*, 201. https://doi.org/10.1007/s10462-024-10805-3

Kanamaru, H. (2024). Cybersecurity in the IoT era. *Systems, Control and Information, 68*(5), 167–172. https://doi.org/10.11509/isciesci.68.5_167

Karagiannis, S., Magkos, E., Karavaras, E., Karnavas, A., Nikiforos, M. N., & Ntantogian, C. (2024). Towards NICE-by-design cybersecurity learning environments: A cyber range for SOC

teams. *Journal of Network and Systems Management, 32*(2), 42. https://doi.org/10.1007/s10922-024-09816-w

Lee, M., Jang-Jaccard, J., & Kwak, J. (2022). Novel architecture of security orchestration, automation and response in Internet of blended environment. *Computers, Materials & Continua, 73*(1), 199–223. https://doi.org/10.32604/cmc.2022.028495

Levstek, A., Pucihar, A., & Hovelja, T. (2022). Towards an adaptive strategic IT governance model for SMEs. *Journal of Theoretical and Applied Electronic Commerce Research, 17*(1), 230–252. https://doi.org/10.3390/jtaer17010012

Liu, Y.-K., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. *Physical Review Applied, 21*, 040501. https://doi.org/10.1103/PhysRevApplied.21.040501

Matias, M., Ferreira, E., Mateus-Coelho, N., & Ferreira, L. (2024). Enhancing effectiveness and security in microservices architecture. *Procedia Computer Science, 239*, 2260–2269. https://doi.org/10.1016/j.procs.2024.06.417

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security, 144*, 103964. https://doi.org/10.1016/j.cose.2024.103964

Molina-Natib, K. E., & Pachano-Zurita, A. C. (2025). La protección de datos personales en el entorno digital ecuatoriano: Análisis crítico del marco normativo y su aplicación práctica. *Sociedad & Tecnología, 8*(S3). https://doi.org/10.51247/st.v8iS3.350

Raaj, N. (2025). Understanding data security posture management (DSPM). *International Journal of Information Technology, 6*(2), 1–6. https://doi.org/10.34218/IJIT_06_02_001

Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. *Information and Software Technology, 141*, 106700. https://doi.org/10.1016/j.infsof.2021.106700

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666

Saveljeva, J., & Volkova, T. (2025). A survey on digital trust: Towards a validated definition. *Digital, 5*(2), 14. https://doi.org/10.3390/digital5020014

Seid, E., Satheesh, S., Popov, O., & Blix, F. (2024). FAIR: Cyber security risk quantification in logistics sector. *Procedia Computer Science, 237,* 783–792. https://doi.org/10.1016/j.procs.2024.05.166

Tan, W., Guo, B., & Zhang, Q. (2025). Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. *Pacific-Basin Finance Journal, 90*, 102646. https://doi.org/10.1016/j.pacfin.2024.102646

Ukeje, N., Gutierrez, J., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. *International Journal of Information Security*, *23*, 1459–1475. https://doi.org/10.1007/s10207-023-00797-6

Vourganas, I. J., & Michala, A. L. (2024). Applications of machine learning in cyber security: A review. *Journal of Cybersecurity and Privacy, 4*(4), 972–992. https://doi.org/10.3390/jcp4040045

Wang, X., Wang, B., Wu, Y., Ning, Z., Guo, S., & Yu, F. R. (2025). A survey on trustworthy edge intelligence: From security and reliability to transparency and sustainability. *IEEE Communications Surveys & Tutorials, 27*(3), 1729–1757. https://doi.org/10.1109/COMST.2024.3446585

Red de Investigación
Científica y Desarrollo
Tecnológico **Del Pacífico**

Una guia práctica y estratégica para **proteger**, **gobernar** e **innovar** con TI, impulsando la transformación digital y construyendo empresas inteligentes y resilientes.

EDITORIAL
SAGA

ISBN: 978-9907-803-62-4