Compliance y ciberseguridad: Guía para la empresa (prevención y resiliencia)

Obligaciones legales, gestión del riesgo y ciberresiliencia para proteger datos, sistemas y continuidad de negocio

Liderando la próxima generación de ciberseguridad

GORKA ARROYUELOS GOROSTIZA

ARANZADI

ARANZADI LA LEY, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es
Atención al cliente: https://areacliente.aranzadilaley.es/publicaciones

Primera edición: 2026

Depósito Legal: M-11022-2026
ISBN versión impresa: 978-84-1085-852-7
ISBN versión electrónica: 978-84-1085-853-4

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.
Printed in Spain

En ningún caso, el autor, el editor o cualquier parte afiliada serán responsables de ninguna pérdida o daño, incluidos, entre otros, pérdidas o daños indirectos o consecuentes o cualquier pérdida o daño que surja de la pérdida de datos o ganancias que surjan de o en conexión con, el uso de este documento técnico.

Las opiniones y puntos de vista expresados en este documento técnico son los del autor y no necesariamente reflejan la política o la posición oficial de ninguna otra agencia, corporación o usuario. La información proporcionada está sujeta a cambios sin previo aviso y no debe interpretarse como un compromiso por parte de los autores o editores.

La información proporcionada en esta publicación, ***Compliance* y ciberseguridad: Guía para la empresa (prevención y resiliencia)**, es solo para fines informativos generales. Si bien hemos hecho todo lo posible para garantizar la precisión e integridad de la información contenida en este documento, el autor y el editor no realizan declaraciones ni garantías de ningún tipo, expresas o implícitas, sobre la integridad, precisión, confiabilidad, idoneidad o disponibilidad con respecto al informe técnico o la información, los productos, los servicios o los gráficos relacionados que contiene para cualquier propósito.

Por lo tanto, cualquier confianza que deposite en dicha información es estrictamente bajo su propio riesgo.

Se recomienda a los lectores que busquen asesoramiento profesional antes de tomar cualquier decisión basada en la información proporcionada en esta publicación. El autor y el editor no asumen ninguna responsabilidad por las acciones que se tomen en función del contenido de este documento técnico.

Índice General

Página

Página

Página

Página

Página

Página

Página

Página

PARTE IV
GESTIÓN DE CIBERCRISIS, RESILIENCIA INSTITUCIONAL Y APRENDIZAJE POSFALLO

Página

PARTE V
GOBERNANZA EN INCERTIDUMBRE PERMANENTE Y SOBERANÍA DEL MANDO ALGORÍTMICO

CAPÍTULO 8

Página

Página

Índice de ilustraciones y tablas

Índice de Ilustraciones

Índice de Tablas

El autor. Un arquitecto de resiliencia en la era de la IA

Nacido en el País Vasco, donde aprendí que navegar la incertidumbre es tanto un arte como una necesidad. Hoy, mi brújula profesional es la ciberseguridad, no como un escudo invisible, sino como un puente entre la **innovación tecnológica, la ética y la confianza institucional**.

He recorrido todos los niveles de la transformación digital desde los primeros roles operativos en sistemas hasta liderar como CIO y el CISO, protegiendo infraestructuras críticas en entornos públicos y privados. He diseñado arquitecturas *Zero Trust* que redefinen la confianza más allá del perímetro tradicional, integrando regulaciones como ENS, NIS2 y *AI Act*, mientras garantizo que la eficiencia y la soberanía de los datos caminen de la mano.

Mi pasión es traducir la complejidad en claridad. A través de artículos y conferencias, mezclo **rigor técnico, ética y un toque de humor** para hacer accesible lo inaccesible, la gestión de riesgos, la protección de datos y los desafíos de la IA en la ciberseguridad.

Este libro es la culminación de años de experiencia. Una **guía para líderes que quieren navegar la incertidumbre digital con visión, integridad y curiosidad**. En un mundo donde los sistemas autónomos toman decisiones complejas, sigo fiel al mantra de que, en el vasto océano digital, el conocimiento es nuestro barco y la curiosidad nuestra vela.

Transparencia metodológica y autoría. Sistema de Iconografía HMC (Human-Machine Collaboration)

Este libro analiza la transformación de la ciberseguridad en el horizonte 2026, donde el riesgo digital se consolida como un desafío estratégico y jurídico bajo el marco de la Directiva NIS2, el *AI Act* y el ENS. Ante la insuficiencia de los modelos tradicionales de gestión de identidades y accesos (IAM), se propone la transición hacia la *Identidad operativa*, entendida como paradigma ampliado y dinámico de identidad digital que abarca toda entidad actuante (humana o no humana) bajo verificación continua, contexto dinámico y mandato revocable y la emergencia de las *Identidades Artificiales* (entidades no humanas dotadas de agencia algorítmica emergente) como instrumentos de sujeción técnica para sistemas autónomos, permitiendo su gobernanza sin abdicación de soberanía.

La investigación fundamenta cómo el modelo *Zero Trust* y la Arquitectura de la Evidencia permiten materializar la responsabilidad proactiva (*accountability*) de la alta dirección. El estudio concluye que la gobernanza de identidades no humanas es esencial para preservar la soberanía digital y la legitimidad institucional en entornos altamente automatizados, asegurando una supervisión humana significativa y una gestión de riesgos alineada con los valores democráticos europeos.

Esta obra adopta el estándar de transparencia algorítmica desarrollado por la *Dubai Future Foundation* (julio 2025) para declarar visualmente el grado de intervención de sistemas de inteligencia artificial en la elaboración de contenido académico.

Los contenidos sustantivos de esta obra (análisis conceptual, propuestas normativas, taxonomías operativas y conclusiones) han sido desarrollados mediante:

- **Nivel 1 (Solo Humano).** Análisis crítico, deliberación estratégica, propuesta de reforma legislativa (Art. 41bis Ley 39/2015).
- **Nivel 2 (Liderado por Humano).** Revisión bibliográfica sistemática, sistematización de marcos normativos, verificación de referencias.

Los Niveles 4 y 5 NO han sido empleados en ninguna sección sustantiva por incompatibilidad con estándares de autoría científica.

Esta declaración cumple con los principios de transparencia algorítmica propuestos en la Parte III, Capítulo 5.6 de la presente obra.

Todo ser humano

Líder

Prólogo

Gobernanza tecnológica, responsabilidad organizativa y el nuevo estatuto del CISO

La progresiva incorporación de sistemas de inteligencia artificial a la operativa institucional ha alterado el modo en que las organizaciones producen decisiones, gestionan riesgos y estructuran responsabilidades. Si durante décadas la transformación digital se interpretó como un fenómeno de eficiencia operativa, el actual marco regulatorio europeo revela algo distinto como es que la tecnología se ha convertido en un vector central de imputación jurídica.

El Reglamento europeo de Inteligencia Artificial, la Directiva NIS2, el Reglamento DORA y los desarrollos nacionales en materia de seguridad configuran un escenario en el que la gobernanza tecnológica deja de ser una cuestión interna para adquirir relevancia normativa directa. Las organizaciones ya no son evaluadas únicamente por sus resultados, sino por la arquitectura preventiva y probatoria que sustenta sus sistemas.

En este contexto, la figura del CISO experimenta una transformación silenciosa pero profunda. Tradicionalmente asociado a la protección técnica de la información, su función evoluciona hacia un papel estructural en la gestión del riesgo institucional. El CISO se convierte en un actor clave dentro del sistema de cumplimiento normativo, no como mero responsable operativo, sino como pieza esencial en la trazabilidad, supervisión y documentación del riesgo tecnológico.

La obra que el lector tiene ante sí aborda esta transformación desde una perspectiva integradora. No se limita a describir obligaciones regulatorias ni a detallar controles técnicos. Propone, en cambio, una lectura sistemática en la que derecho, arquitectura tecnológica y responsabilidad organizativa se articulan en un mismo plano.

Uno de los principales aciertos del trabajo reside en identificar que la verdadera exigencia normativa no recae únicamente sobre el sistema de inteligencia artificial, sino sobre la estructura que lo habilita y lo supervisa. La gobernanza

no es un documento programático; es una arquitectura verificable. La *compliance* tecnológica no se agota en la declaración de políticas, sino que exige la trazabilidad, la segregación de funciones, el control de privilegios y la capacidad probatoria.

Desde esta perspectiva, la noción de «Arquitectura de la Evidencia» adquiere especial relevancia. La responsabilidad contemporánea no se basa exclusivamente en la existencia de un daño, sino en la posibilidad de demostrar que la organización desplegó medidas estructurales adecuadas para prevenirlo y controlarlo. El estándar de diligencia se desplaza hacia la configuración previa del sistema.

En este marco, el CISO deja de ser un perfil estrictamente técnico para integrarse en la lógica de gobierno corporativo y responsabilidad institucional. Su función se aproxima a la de un garante estructural del riesgo tecnológico, especialmente en entornos donde la automatización influye en derechos, servicios públicos o decisiones estratégicas.

La obra articula esta transformación mediante categorías propias que permiten ordenar un campo todavía en consolidación doctrinal. Conceptos como la identidad operativa de los sistemas automatizados o la gobernanza del privilegio ofrecen herramientas útiles para interpretar las obligaciones emergentes en materia de supervisión y control.

Pero quizá el valor más relevante del libro radique en su afirmación implícita de que la inteligencia artificial no plantea únicamente un desafío técnico, sino un desafío de diseño organizativo. La cuestión central no es si el sistema funciona, sino si la organización está estructurada para asumir su responsabilidad.

En un momento en que el cumplimiento normativo en materia de IA corre el riesgo de convertirse en una suma de check-list formales, esta obra propone un enfoque más exigente: comprender la gobernanza tecnológica como arquitectura institucional.

Se trata, por ello, de un trabajo especialmente pertinente para responsables de seguridad, directivos, juristas y profesionales del *compliance*, llamados a integrar tecnología y derecho en un mismo sistema de responsabilidad. El libro no ofrece soluciones simplistas; ofrece un marco estructural desde el que pensar la imputación del riesgo en la era de la automatización.

La solidez técnica del análisis y su coherencia normativa lo convierten en una aportación valiosa para el debate jurídico contemporáneo. En un entorno donde la responsabilidad puede diluirse entre capas técnicas y organizativas, la claridad conceptual es una exigencia imprescindible. Esta obra contribuye a proporcionarla.

Prefacio del autor. Gobernar la tecnología cuando la responsabilidad no es delegable

Este libro no nace únicamente de una reflexión teórica, sino que lo hace desde una tensión profesional constante marcada por la distancia entre lo que la norma exige y la forma en que las organizaciones están realmente estructuradas para cumplirla.

Durante años he observado cómo la transformación digital avanzaba con rapidez, mientras la gobernanza y la arquitectura de responsabilidad evolucionaban con mucha mayor lentitud. La seguridad se trataba como una cuestión técnica, el cumplimiento, como una obligación documental y la inteligencia artificial, como una promesa de eficiencia.

Sin embargo, en la práctica diaria, las preguntas eran otras. ¿Quién responde cuando un sistema automatizado condiciona una decisión relevante? ¿Dónde se sitúa la supervisión real cuando los procesos se fragmentan entre proveedores, desarrolladores y unidades internas? ¿Puede una organización demostrar, no solo afirmar, que ha diseñado su arquitectura tecnológica conforme a estándares de diligencia exigibles?

El marco normativo europeo reciente (*AI Act*, NIS2, DORA y desarrollos nacionales en materia de seguridad) ha hecho visible lo que en la práctica ya era evidente, la responsabilidad no desaparece con la automatización. Se desplaza hacia el diseño organizativo.

Este libro es el resultado de intentar responder a esa constatación. No he querido escribir un manual técnico ni un comentario exhaustivo de normas. He querido proponer una estructura conceptual que ayude a ordenar el problema desde dentro de la organización.

De ahí surgen categorías como la *arquitectura de la evidencia, la identidad operativa o la gobernanza del privilegio*. No como ejercicios terminológicos, sino como herramientas para comprender cómo se articula imputación del riesgo cuando la decisión se apoya en sistemas automatizados.

En mi dilatada experiencia profesional, la mayor vulnerabilidad no suele estar en la ausencia de tecnología, sino en la ambigüedad estructural marcadas por las responsabilidades difusas, los controles no integrados y la supervisión no documentada.

La inteligencia artificial amplifica esa ambigüedad si no se corrige mediante diseño institucional y he querido situar en el centro de esta reflexión la figura del CISO y, en general, de los responsables de seguridad y cumplimiento.

No como perfiles exclusivamente técnicos, sino como actores clave en la arquitectura de responsabilidad. En el entorno actual, cada vez más exigente, su función trasciende la protección operativa y se inserta en la lógica de gobierno corporativo e institucional.

Este libro no ofrece recetas cerradas, sino que ofrece la tesis de que la gobernanza tecnológica es una cuestión de arquitectura organizativa verificable. La responsabilidad no puede delegarse en el algoritmo, ni diluirse en la complejidad técnica, sino que debe estructurarse.

Si estas páginas contribuyen a que las organizaciones reflexionen con mayor rigor sobre cómo diseñan sus sistemas y cómo asumen sus obligaciones, el esfuerzo habrá merecido la pena.

Parte I
Fundamentos normativos del nuevo paradigma

Objetivo: Esta Parte I establece el marco fundacional normativo-técnico para la gobernanza del riesgo digital en Europa (2025-2026), analizando la transición desde paradigmas técnico-reactivos hacia obligaciones estructurales de supervisión corporativa.

Marco teórico: Desarrollamos el concepto de síntesis interseccional como convergencia obligatoria entre dimensiones normativas (NIS2, *AI Act*, ENS), técnicas (*Zero Trust*, IAM) y organizativas (redefinición rol CISO).

Método: Realismo jurídico-tecnológico que combina análisis doctrinal normativo, *Design Science Research* y etnografía de gestión.

Hallazgos principales: (1) NIS2 Art. 20 configura responsabilidad fiduciaria del Consejo comparable a *Chief Risk Officers*; (2) *AI Act* introduce tensión irresoluble entre autonomía algorítmica y supervisión humana que solo arquitecturas *Zero Trust* pueden materializar; (3) CISO emerge como arquitecto de responsabilidad institucional, no gestor técnico.

Contribución: Primera articulación sistemática de arquitectura de la evidencia como traducción operativa de *accountability* jurídica en controles técnicos auditables, preparando marco teórico para gobernanza de identidades artificiales (Partes II-III).

Capítulo 1

Introducción y gobernanza estratégica de la ciberseguridad

Introducción

La ciberseguridad en Europa ha dejado de ser, de forma definitiva, una cuestión eminentemente técnica. A partir de 2025-2026, el riesgo digital se consolida como un **riesgo organizativo, jurídico y estratégico**, sujeto a un marco regulatorio vinculante que redefine responsabilidades, procesos de decisión y modelos de gobernanza tanto en el sector privado como en las administraciones públicas.

Para comprender la magnitud de este cambio, es imperativo contrastar *el Estado del Arte (2023-2024)* con la *Realidad Operativa de 2026*. Hasta hace apenas veinticuatro meses, la ciberseguridad se articulaba sobre el *paradigma del perímetro y la reacción*. Bajo este modelo, el éxito se medía por la robustez de las barreras técnicas y la capacidad de respuesta ante incidentes aislados.

La identidad digital era tratada como un mero atributo de acceso humano (una combinación de credencial y rol) y el cumplimiento normativo se percibía como un ejercicio de *check-list* estático para evitar sanciones administrativas.

Este modelo ha colapsado bajo el peso de tres vectores disruptivos:

Primero, la disolución del perímetro tradicional. La adopción masiva de nubes híbridas y arquitecturas *Edge* distribuidas ha borrado las fronteras físicas sobre las que se construía la seguridad clásica.

Segundo, la hiperautomatización algorítmica. Los agentes de IA ya no ejecutan instrucciones, sino que toman decisiones autónomas que escapan al modelo de control basado en supervisión humana directa.

Tercero, el desplazamiento de la responsabilidad jurídica hacia la alta dirección. La Directiva NIS2 (Art. 20) convierte la ciberseguridad en una obligación fiduciaria del Consejo, no del departamento técnico.

Estos tres vectores convergen en una realidad ineludible: ya no estamos en la era de la protección de sistemas, sino en la etapa de la gobernanza del privilegio. Mientras que en el estado del arte previo la identidad era el acceso, en el escenario de 2026 la identidad es el poder.

La magnitud de esta transición queda ilustrada por datos recientes como el último informe de ENISA (2025), el 68% de los incidentes de ciberseguridad notificados en entidades críticas europeas derivaron de *fallos de gobernanza organizativa*, no de vulnerabilidades técnicas. En España, la Sentencia del Tribunal Supremo 1119/2025 (caso BOSCO) estableció un precedente al imputar responsabilidad administrativa a la dirección de una corporación por ausencia de trazabilidad en decisiones automatizadas, un fallo de arquitectura institucional, no de *firewall.*

Ya no estamos en la era de la protección de sistemas sino en la etapa de la Gobernanza del Privilegio. Mientras que en el estado del arte previo la identidad era el acceso, en el escenario de 2026 la identidad es el poder. La realidad actual exige que el CISO no gestione cortafuegos sino infraestructuras de legalidad donde cada bit de acción sea imputable, trazable y soberano. Esta transición del enfoque técnico-reactivo al estratégico-administrativo constituye la fractura epistemológica que este libro analiza.

La entrada en vigor y aplicación efectiva de instrumentos como la *Directiva NIS2*, el *Reglamento General de Protección de Datos (RGPD)*, el *Reglamento de Inteligencia Artificial (AI Act)*, junto con marcos sectoriales como *DORA*, el nuevo *ecosistema de identidad y confianza derivado de eIDAS2* y, en el caso español, el *Esquema Nacional de Seguridad (ENS)*, configuran un escenario en el que la ciberseguridad ya no puede abordarse como una función aislada ni delegarse exclusivamente en áreas técnicas.

Este nuevo contexto normativo no se limita a imponer controles o medidas de seguridad adicionales. Introduce, de forma explícita o implícita, una obligación estructural de gobernanza del riesgo digital, desplazando el foco desde la mera protección de infraestructuras hacia la responsabilidad organizativa, la trazabilidad de las decisiones y la rendición de cuentas de la alta dirección. La ciberseguridad pasa así a formar parte del núcleo del gobierno corporativo y administrativo, al mismo nivel que otros riesgos estratégicos tradicionales.

Paralelamente, la acelerada adopción de sistemas de inteligencia artificial, servicios automatizados y arquitecturas distribuidas tensiona los modelos clásicos de control, supervisión e identidad. Los sistemas digitales ya no se limitan a ejecutar instrucciones predefinidas, sino que aprenden, se adaptan y actúan de forma parcialmente autónoma, generando nuevos desafíos para la imputación de responsabilidades, el control de accesos y la gestión del riesgo operativo.

Este fenómeno pone en cuestión los enfoques tradicionales basados en perímetros, confianza implícita y supervisión ex post.

En este escenario, emerge una tensión central que atraviesa todo el marco regulatorio europeo contemporáneo, cómo conciliar la creciente autonomía tecnológica de los sistemas digitales con la exigencia de responsabilidad jurídica personal, control organizativo y protección efectiva de los derechos fundamentales.

Ni la normativa de protección de datos, ni la regulación de ciberseguridad, ni el incipiente marco de la inteligencia artificial resuelven plenamente, por sí solas, esta tensión.

Ante esta insuficiencia fragmentaria, esta obra propone y se fundamenta en la síntesis híbrida como marco metodológico y operativo. No se trata simplemente de un enfoque multidisciplinar, sino de una necesidad ontológica en la gobernanza moderna. La síntesis híbrida sostiene que el riesgo digital no puede ser mitigado eficazmente si no se aborda desde la colisión y refuerzo mutuo de tres dimensiones irreductibles: la normativa, la técnica y la organizativa.

- **La dimensión normativa (arquitectura de la legalidad).** Donde el cumplimiento (NIS2, *AI Act*, ENS) deja de ser una carga para convertirse en el mandato de delegación que legitima la acción digital.
- **La dimensión técnica (arquitectura de la evidencia).** Donde el modelo *Zero Trust* y la criptografía de clave pública no solo aseguran el dato, sino que generan la prueba irrefutable de la diligencia debida del administrador.
- **La dimensión organizativa (gobernanza del poder).** Donde se definen los límites de la autonomía algorítmica y se preserva el control humano significativo en los puntos de no retorno.

Justificamos esta síntesis por el fracaso sistémico de los enfoques en silo. Un control técnico sin anclaje jurídico es arbitrariedad ya que una norma sin capacidad de verificación técnica es *cumplimiento de papel*. Solo a través de esta intersección es posible construir una identidad consciente de la privacidad y una resiliencia soberana.

Esta metodología permite al CISO moderno actuar como un arquitecto de confianza institucional, transformando la complejidad regulatoria en una ventaja competitiva y en un escudo de responsabilidad personal para la alta dirección.

Este capítulo sostiene que la respuesta europea a este desafío no se articula a través de una única norma o tecnología sino mediante la convergencia de tres planos inseparables representados por un marco regulatorio exigente orientado a la gestión del riesgo y la responsabilidad junto con una arquitectura técnica

coherente basada en principios de verificación continua, minimización de confianza y control de identidades además de una gobernanza organizativa madura en la que la ciberseguridad se integra en la toma de decisiones estratégicas.

Desde esta perspectiva, el capítulo analiza cómo las políticas de seguridad, la Directiva NIS2, el *AI Act*, el ENS y la adopción de arquitecturas como *Zero Trust* no constituyen elementos independientes, sino piezas de un mismo modelo de gobernanza del riesgo digital.

Asimismo, se examina el papel emergente del *Chief Information Security Officer* (CISO) como figura clave en la articulación de este modelo, no solo como responsable técnico, sino como actor estratégico con un mandato delegado de gestión y supervisión.

El objetivo de este capítulo no es ofrecer un catálogo de buenas prácticas ni un análisis normativo exhaustivo, sino establecer el marco fundacional sobre el que se construye el resto de la obra. Un marco que permita comprender por qué, en el contexto europeo actual, la ciberseguridad debe abordarse como una cuestión de identidad, control y responsabilidad y por qué los modelos tradicionales resultan insuficientes ante la emergencia de sistemas digitales cada vez más autónomos.

A partir de este punto, los capítulos siguientes profundizarán en una de las consecuencias más relevantes de este cambio de paradigma, la aparición de identidades no humanas e identidades artificiales como elementos operativos dentro de organizaciones reguladas y los desafíos jurídicos, técnicos y democráticos que ello plantea para la gobernanza del sector público y privado en Europa.

1.1. POLÍTICAS GENERALES DE SEGURIDAD Y PROCEDIMIENTOS

En el contexto regulatorio europeo actual, las políticas generales de seguridad ya no pueden entenderse como documentos meramente formales ni como expresiones abstractas de buenas intenciones organizativas. Constituyen, por el contrario, instrumentos centrales de gobernanza del riesgo digital, con efectos jurídicos-organizativos y operativos directos.

Tanto el RGPD, como la Directiva NIS2 y, en el ámbito del sector público español, el Esquema Nacional de Seguridad (ENS), convergen en una misma exigencia estructural como es la necesidad de que las corporaciones definan, formalicen, apliquen y revisen de manera sistemática un marco de seguridad que permita gestionar el riesgo de forma demostrable. En este sentido, las políticas de seguridad no son un complemento del cumplimiento normativo, sino uno de sus pilares constitutivos.

Desde una perspectiva de gobernanza, las políticas generales de seguridad cumplen al menos tres funciones esenciales. En primer lugar, articulan la voluntad organizativa en materia de protección de activos, datos y servicios, traduciendo principios normativos abstractos en criterios operativos concretos. En segundo lugar, habilitan la delegación de responsabilidades, permitiendo que la dirección ejerza su deber de supervisión a través de mandatos claros, trazables y verificables. Y, en tercer lugar, actúan como elementos probatorios fundamentales en caso de incidente, auditoría o procedimiento sancionador, al reflejar el grado de diligencia adoptado por la organización.

Este último aspecto resulta especialmente relevante en el marco del **principio de responsabilidad proactiva (*accountability*)** del RGPD y de la responsabilidad explícita atribuida a los órganos de dirección por la NIS2. En ambos casos, la ausencia, obsolescencia o inadecuación de políticas de seguridad no se interpreta como una mera deficiencia documental, sino como un **indicador de fallo organizativo** en la gestión del riesgo. Las políticas se convierten así en una pieza clave para demostrar que las decisiones adoptadas fueron razonables, informadas y coherentes con el estado del arte y el marco normativo aplicable.

En el ámbito del *ENS*, esta función se refuerza de manera particular. El esquema configura la política de seguridad como el elemento vertebrador del sistema, del que se derivan normas de desarrollo, procedimientos operativos y medidas técnicas.

Lejos de constituir un *check-list* de controles, el ENS presupone una arquitectura de gobierno en la que la política de seguridad define el marco común de actuación para toda la organización, garantizando coherencia, continuidad y control, especialmente relevante en entornos administrativos complejos y sujetos a rotación de responsabilidades.

Desde el punto de vista operativo, las políticas generales de seguridad deben concebirse como documentos vivos, alineados con la gestión continua del riesgo y sujetos a revisión periódica. La acelerada evolución del entorno digital (marcada por la adopción de servicios en la nube, el trabajo remoto, la externalización de procesos críticos y la incorporación progresiva de sistemas de inteligencia artificial) hace inviable cualquier enfoque estático. Una política de seguridad que no se revisa, no se comunica o no se aplica de forma efectiva pierde rápidamente su valor normativo y organizativo.

Asimismo, resulta imprescindible distinguir entre la política de seguridad como marco estratégico y los procedimientos como instrumentos de ejecución. Mientras la primera establece principios objetivos y criterios de decisión, los segundos concretan cómo se aplican estos principios en situaciones específicas como pueden ser la gestión de accesos, el tratamiento de incidentes, la continuidad de negocio, la relación con terceros o el uso de sistemas automatizados.

Esta distinción no es meramente formal, sino que permite mantener la estabilidad del marco de gobernanza al tiempo que se adapta la operativa a contextos cambiantes.

En este sentido, la creciente incorporación de sistemas automatizados y componentes de inteligencia artificial introduce una presión adicional sobre las políticas de seguridad tradicionales. Estos sistemas, que pueden operar de forma parcialmente autónoma, requieren que las políticas amplíen su alcance para incluir no solo usuarios humanos, sino también identidades técnicas, servicios y agentes digitales, cuya actuación debe quedar igualmente sujeta a control, supervisión y rendición de cuentas. Aunque esta cuestión se desarrollará en capítulos posteriores, resulta ya evidente que las políticas de seguridad constituyen el primer nivel en el que esta ampliación conceptual debe materializarse.

En definitiva, las políticas generales de seguridad y los procedimientos asociados no deben entenderse como un requisito administrativo ni como un artefacto de cumplimiento, sino como el núcleo organizativo desde el que se gobierna el riesgo digital. En el marco europeo post-2025, su calidad, coherencia y grado de integración con la toma de decisiones estratégicas se convierten en un factor determinante para la resiliencia, la responsabilidad y la legitimidad de las organizaciones, tanto públicas como privadas.

En este contexto de políticas generales y procedimientos, la opacidad decisional representa el principal riesgo democrático residual. La iconografía HMC, como mecanismo de transparencia radical, complementa estas obligaciones al materializar la trazabilidad visual en actos administrativos, alineándose con la supervisión humana significativa (*AI Act* Art. 14) y el control democrático (vid. STS 1119/2025, caso BOSCO).

1.1.1. LA DIRECTIVA NIS2 COMO OBLIGACIÓN ESTRUCTURAL DE GOBERNANZA DEL RIESGO DIGITAL

La Directiva (UE) 2022/2555 (NIS2) marca un punto de inflexión en la concepción europea de la ciberseguridad. Frente a enfoques anteriores centrados en sectores críticos o en requisitos técnicos fragmentados, NIS2 introduce una obligación estructural de gestión del riesgo digital, con alcance transversal y consecuencias directas sobre la gobernanza organizativa.

La principal innovación de NIS2 no reside únicamente en la ampliación del número de entidades obligadas ni en el endurecimiento del régimen sancionador, sino en el desplazamiento explícito de la ciberseguridad hacia el ámbito del gobierno corporativo y administrativo. La directiva exige que las corporaciones adopten medidas técnicas operativas y organizativas adecuadas y proporcionadas, pero, sobre todo, que estas medidas estén integradas en un sistema de gestión del riesgo supervisado por la alta dirección.

Este enfoque implica una ruptura con la tradicional externalización de la seguridad hacia áreas técnicas o proveedores especializados. NIS2 establece que los órganos de dirección aprueben, supervisen y respondan por las medidas de ciberseguridad adoptadas, introduciendo una lógica de responsabilidad personal que aproxima la gestión del riesgo digital a otros ámbitos regulados del *compliance* europeo. La ciberseguridad deja así de ser una cuestión delegable sin control efectivo y se convierte en una obligación indelegable de supervisión.

Esta obligación de supervisión cristaliza en el Artículo 20 de la NIS2, que introduce un régimen de responsabilidad para los órganos de dirección que trasciende la *mera culpa in eligendo o in vigilando*. En 2026, la *diligencia debida* del administrador no se agota en la aprobación de un presupuesto ya que exige la verificación de que las medidas adoptadas son *adecuadas y proporcionadas* al estado del arte.

Desde una perspectiva de defensa jurídica, la diligencia debida actúa como un marco de exclusión de responsabilidad personal. Para que este escudo sea efectivo, el directivo debe demostrar que su decisión se basó en una *ignorancia no culpable*, apoyada en informes técnicos (CISO) que traduzcan el riesgo de vulnerabilidad en riesgo de impacto institucional.

No se castiga el incidente, sino la *falta de gobernanza previa al incidente*. Por ello, el análisis profundo de la NIS2 revela que el legislador europeo busca forzar un *conocimiento experto* en los consejos de administración, convirtiendo la ciberseguridad en un activo de responsabilidad fiduciaria.

Desde una perspectiva jurídica, esta obligación tiene implicaciones relevantes. La directiva no impone únicamente la adopción de controles, sino la capacidad de demostrar una gestión diligente del riesgo, basada en evaluaciones periódicas, decisiones documentadas y mecanismos de mejora continua. En este sentido, NIS2 refuerza una lógica de responsabilidad *ex ante*, alineada con el principio de *accountability* del RGPD, pero aplicada al conjunto de los activos y servicios digitales críticos para la organización.

En el ámbito del sector público y de las entidades reguladas, esta exigencia encuentra una clara convergencia con marcos nacionales como el Esquema Nacional de Seguridad (ENS). Mientras NIS2 define el deber jurídico de gestión y supervisión del riesgo, el ENS proporciona una estructura operativa y metodológica para materializar dicho deber, especialmente en organizaciones complejas con múltiples niveles de responsabilidad. Esta complementariedad refuerza la idea de que la gobernanza de la ciberseguridad no puede entenderse sin una adecuada articulación entre normativa europea y marcos nacionales de implementación.

Otro elemento central de NIS2 es su énfasis en la gestión de la cadena de suministro y de los servicios externalizados. La directiva reconoce explícita-

mente que el riesgo digital ya no se limita a los sistemas internos, sino que se extiende a proveedores, plataformas y terceros sobre los que la organización mantiene un control limitado pero una responsabilidad persistente. Esta ampliación del perímetro de responsabilidad obliga a revisar las políticas de seguridad, los contratos y los mecanismos de supervisión, integrando la seguridad como criterio estructural en la toma de decisiones de negocio y de contratación pública.

Asimismo, NIS2 introduce obligaciones reforzadas en materia de gestión de incidentes, notificación y cooperación con autoridades competentes. Estas obligaciones no deben interpretarse únicamente como cargas administrativas, sino como mecanismos de aprendizaje sistémico y resiliencia colectiva orientados a reducir el impacto de incidentes graves y a mejorar la capacidad de respuesta del ecosistema europeo. La gestión de incidentes se configura, así como un componente esencial de la gobernanza del riesgo y no como un mero procedimiento reactivo.

En conjunto, NIS2 redefine la ciberseguridad como un problema organizativo y jurídico de primer orden, cuya gestión requiere liderazgo, estructura y coherencia. Su aportación fundamental no es tanto prescribir qué tecnologías deben adoptarse, sino exigir que exista un sistema de decisión, supervisión y responsabilidad claramente identificable. Este enfoque prepara el terreno para la adopción de modelos arquitectónicos más avanzados y para la redefinición de roles estratégicos, cuestiones que se desarrollarán en los apartados siguientes.

Por tanto, la Directiva NIS2 no debe leerse como un reglamento técnico más, sino como la base legal que define la responsabilidad última del Consejo de Administración ante la resiliencia de la entidad.

En este contexto y centrándonos en el marco español, esta gobernanza encuentra su traducción práctica más robusta en el *Esquema Nacional de Seguridad (ENS)*. Es vital que el CISO traslade al Consejo una jerarquía clara, mientras que la NIS2 establece el marco de obligaciones y el régimen sancionador europeo, el ENS se consolida como el instrumento técnico y operativo de referencia para su cumplimiento efectivo.

Para la mayoría de las organizaciones, el ENS ha dejado de ser una certificación opcional para convertirse en el lenguaje oficial de reporte de madurez. Cumplir con el ENS es, de facto, la vía más sólida para garantizar la *diligencia debida* que la NIS2 exige. En los informes de gobernanza el ENS aporta la estructura de controles, mientras que la NIS2 aporta el peso de la responsabilidad administrativa y penal, transformando al ENS de un requisito técnico en un activo estratégico de defensa jurídica.

Esta obligación estructural de gobernanza del riesgo digital (NIS2) se intensifica con la entrada en vigor del Reglamento de Inteligencia Artificial (*AI Act*),

que introduce una tensión regulatoria específica en sistemas autónomos de alto riesgo, donde la autonomía algorítmica puede colisionar con principios de supervisión humana y transparencia decisional.

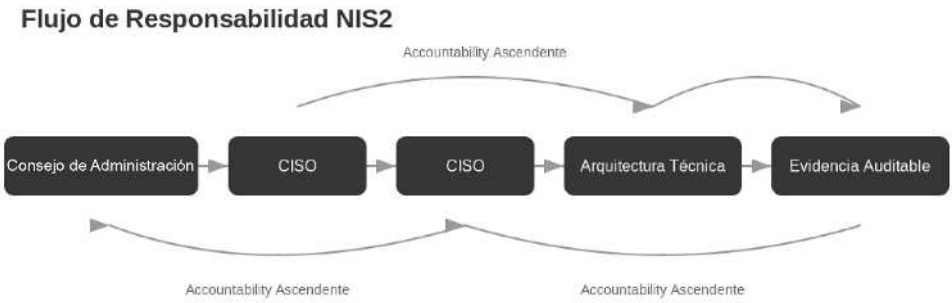

Ilustración 1. Flujo de responsabilidad NIS2

1.1.2. EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL (*AI ACT*) Y LA TENSIÓN REGULATORIA DE LOS SISTEMAS AUTÓNOMOS

La aprobación del Reglamento (UE) 2024/1689, conocido como el RIA (o *AI Act*), introduce una nueva dimensión en el marco de la ciberseguridad y la gobernanza del riesgo digital en Europa.

A diferencia de otros instrumentos normativos centrados en la protección de infraestructuras, datos o servicios, el RIA constituye el primer marco jurídico exhaustivo a nivel mundial que se ocupa de sistemas capaces de tomar decisiones, generar resultados y actuar de forma autónoma. Esto plantea desafíos críticos para los modelos tradicionales de control, supervisión y responsabilidad.

Desde la perspectiva de la ciberseguridad, el RIA no puede entenderse como una norma aislada. Su enfoque basado en el riesgo sitúa a esta norma en una intersección obligatoria con el RGPD, la Directiva NIS2 y el Esquema Nacional de Seguridad (ENS).

Sin embargo, el RIA introduce una tensión estructural ya que regula sistemas cuyo comportamiento no siempre es predecible *ex ante*, cuestionando los supuestos clásicos de control sobre los que se ha construido la seguridad digital hasta hoy.

Uno de los pilares del RIA es su arquitectura de clasificación la cual no regula tecnología *per se* sino el uso que se le da mediante la división de los sistemas en cuatro categorías representadas por el riesgo inaceptable vinculado a los sistemas prohibidos, el alto riesgo, el riesgo limitado sujeto a obligaciones de transparencia y finalmente el riesgo mínimo.

La calificación de Alto Riesgo implica obligaciones reforzadas que impactan directamente en la función del CISO como son la gestión del riesgo (Art. 9), la documentación técnica, la trazabilidad y, fundamentalmente, la robustez y ciberseguridad (Art. 15).

Esta lógica tiene implicaciones directas en la operativa de 2026. La protección de sistemas de inteligencia artificial ya no se limita a evitar accesos no autorizados, sino que debe extenderse a la integridad funcional del sistema, la prevención de manipulaciones del comportamiento (ataques adversarios), la gestión de sesgos y la detección de usos indebidos. En este sentido, el riesgo ya no es únicamente técnico, sino sistémico.

La tensión entre innovación y regulación se resuelve mediante la aplicación de marcos de gobernanza híbridos. En este sentido, la investigación integra los trabajos de la OCDE (2025) sobre la clasificación de riesgos en sistemas agentes con la taxonomía de amenazas para inteligencia artificial de ENISA. El resultado es una gestión del riesgo digital que no solo es reactiva, sino que se apoya en evidencias técnicas inmutables y en el consenso de los principales organismos reguladores internacionales.

El RIA introduce además una redefinición implícita de la noción de control mediante dos conceptos que este libro desarrolla técnica y organizativamente representados por la supervisión humana contemplada en el Artículo 14 y el sistema de gestión de calidad establecido en el Artículo 17.

Respecto a la *supervisión humana* el reglamento exige que los sistemas de alto riesgo se diseñen para ser vigilados por personas físicas con el objetivo de prevenir o minimizar el llamado sesgo de automatización o tendencia humana a confiar ciegamente en las decisiones del sistema. Aquí es donde la noción de Identidad operativa que propondremos se vuelve vital debido a que cada agente de IA debe tener una identidad trazable que permita al supervisor humano ejercer un control real y si fuera necesario una revocación inmediata de sus facultades.

Por su parte el *sistema de gestión de calidad* no constituye una recomendación ética sino un requisito imperativo que obliga a los implementadores o *deployers* representados por las organizaciones que utilizan el sistema bajo su autoridad a establecer políticas, procedimientos y estructuras de gestión de riesgos auditables. Esto otorga una base legal indiscutible a la creación de Comités de Gobernanza Algorítmica elevando la responsabilidad del CISO a un rango fiduciario.

En este contexto, emerge la gran tensión de la gobernanza moderna de cómo integrar sistemas autónomos en organizaciones obligadas a demostrar control y responsabilidad (*accountability*), cuando dichos sistemas operan con un grado inherente de adaptación. Si la Directiva NIS2 establece el *quién* y el *cómo* de la

resiliencia mediante la gobernanza estructural, el RIA aborda la naturaleza misma de la tecnología que redefine la capacidad operativa.

Esta convergencia normativa genera una situación inédita. El CISO de 2026 se encuentra ante el desafío de gestionar identidades que no solo acceden a información, sino que ejecutan procesos de forma delegada. Por tanto, el cumplimiento ya no reside en la adopción de un catálogo estático de controles, sino en la capacidad de la organización para demostrar una supervisión efectiva sobre agentes cuya opacidad es un riesgo sistémico.

En definitiva, el RIA pone en evidencia las limitaciones de los enfoques clásicos de control frente a tecnologías autónomas. Al obligar a los *deployers* a garantizar la trazabilidad y la supervisión bajo una cadena de mando humana identificable, el reglamento prepara el terreno para la adopción de arquitecturas de seguridad basadas en la verificación continua y la minimización de la confianza (*Zero Trust*), que se analizan en el apartado siguiente.

La tensión entre autonomía y supervisión humana se agrava en el ámbito de la soberanía de datos, Donde el *Data Act* impone requisitos de interoperabilidad y acceso de terceros que exigen una respuesta arquitectónica integral.

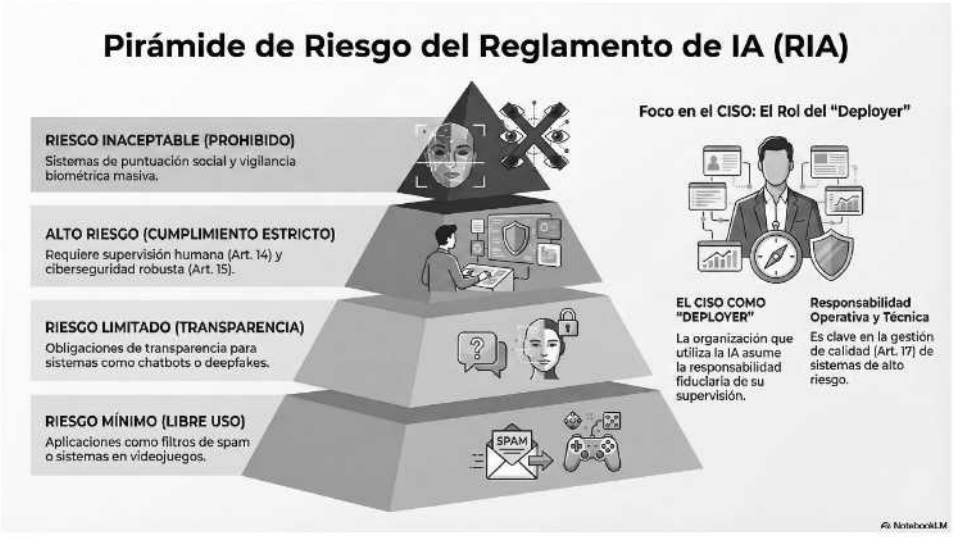

Ilustración 2. Para operar bajo el Reglamento, es vital entender que no todos los sistemas exigen la misma diligencia. La siguiente pirámide desglosa las obligaciones técnicas y de supervisión que el CISO, en su rol de implementador, debe garantizar.

1.1.3. EL *DATA ACT*. SOBERANÍA, INTEROPERABILIDAD Y ACCESO DE TERCEROS

El Triángulo Regulatorio se cierra con el *Data Act* (Ley de Datos), cuya función es romper los monopolios de datos y garantizar la soberanía tecnológica. En el horizonte actual, el CISO moderno debe gestionar no solo la seguridad, sino el derecho de acceso a los datos generados por el uso de productos conectados.

La categoría de Alto Riesgo, especialmente en infraestructuras críticas y servicios públicos esenciales, constituye el núcleo de la presión operativa para el CISO debido a que bajo este nivel *AI Act* impone obligaciones proactivas de autoevaluación que prefiguran una homologación interna obligatoria.

En este escenario destacan tres ejes críticos representados en primer lugar por la gestión de riesgos contemplada en el Artículo 9 como un proceso continuo que debe iterar durante todo el ciclo de vida de la IA identificando sesgos y riesgos de seguridad específicos. A esto se suma la trazabilidad y registros o *logging* que impone la obligación de que el sistema genere registros automáticos que permitan supervisar su funcionamiento y en caso de fallo reconstruir la cadena de eventos de forma crucial para la NIS2.

Finalmente, la robustez y ciberseguridad exigidas por el Artículo 15 determinan que los sistemas deben ser resistentes a intentos de terceros de alterar su uso o comportamiento mediante ataques adversarios o *poisoning*. Estas obligaciones transforman la IA de ser un producto comprado a ser un sistema gobernado Donde el cumplimiento no representa un hito de entrega sino un estado de vigilancia técnica permanente.

Esta insuficiencia del *Data Act* para gestionar simultáneamente soberanía de datos e interoperabilidad revela una paradoja más profunda, que ningún instrumento normativo aislado logra garantizar un control técnico efectivo en ecosistemas distribuidos y altamente dinámicos.

Zero Trust emerge precisamente como respuesta arquitectónica a esta fragmentación regulatoria, al desplazar el enfoque de perímetros estáticos hacia una verificación continua de confianza basada en identidad, contexto y comportamiento, complementando así las obligaciones de resiliencia operativa (NIS2, art. 21) y robustez algorítmica (*AI Act*, art. 15).

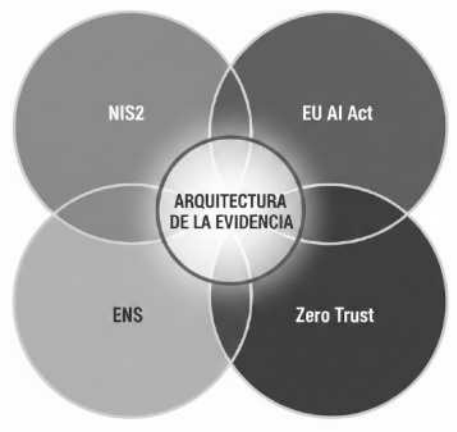

Ilustración 3 Diagrama de Síntesis Interseccional

En el ámbito administrativo, esta arquitectura se materializa en propuestas concretas de transparencia radical, como la adopción obligatoria de la iconografía de Colaboración Humano-Máquina (HMC), lanzada por la *Dubai Future Foundation* el 16 de julio de 2025, que clasifica visualmente (mediante cinco niveles primarios y nueve iconos funcionales) el grado de intervención humana *versus* máquina en la generación de decisiones o contenidos, constituyendo un nuevo contrato social que legitima la automatización al eliminar la opacidad estructural y vincular explícitamente el nivel de autonomía algorítmica con la imputación jurídica y la responsabilidad administrativa.

1.2. *ZERO TRUST* COMO RESPUESTA ARQUITECTÓNICA A LA INSUFICIENCIA REGULATORIA Y TÉCNICA

La convergencia de marcos normativos exigentes (RGPD, NIS2, ENS y *AI Act*) con entornos tecnológicos cada vez más distribuidos y automatizados pone de manifiesto una limitación estructural como es que la regulación, por sí sola, no garantiza el control efectivo del riesgo digital.

Para que las obligaciones jurídicas de diligencia, supervisión y responsabilidad sean operativas, deben apoyarse en arquitecturas técnicas coherentes capaces de materializarlas de forma continua y verificable. En este contexto, el modelo de *Zero Trust* emerge como una respuesta estructural a la insuficiencia de los enfoques tradicionales de seguridad.

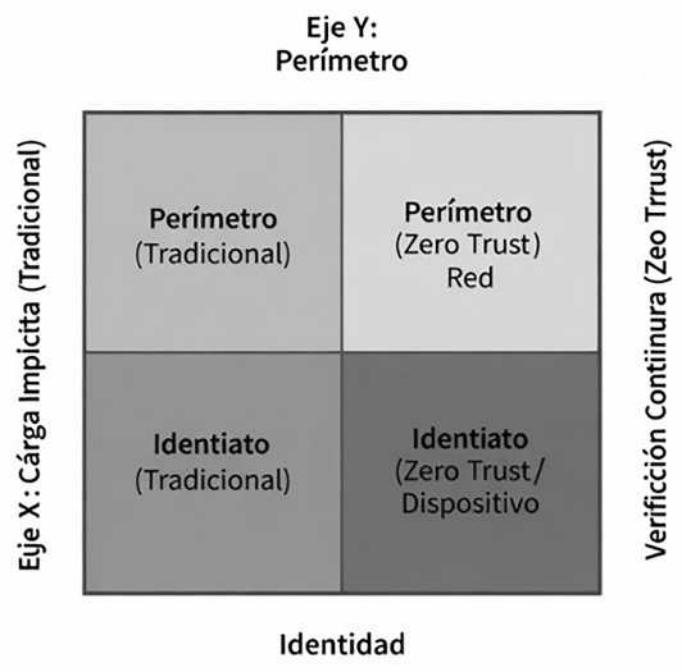

Ilustración 4. Comparativa confianza implícita Vs Verificación continua

Zero Trust no debe entenderse como una tecnología concreta ni como un producto, sino como un principio arquitectónico que redefine la forma en que se conciben la confianza, el acceso y el control en los sistemas digitales. Frente a los modelos basados en perímetros y confianza implícita, *Zero Trust* parte de una premisa radicalmente distinta, ninguna identidad, dispositivo o servicio es confiable por defecto, con independencia de su ubicación o pertenencia organizativa. Todo acceso debe ser evaluado, autorizado y supervisado de manera dinámica.

Desde una perspectiva jurídica y organizativa, este enfoque resulta especialmente relevante porque alinea la arquitectura técnica con las exigencias normativas de gestión del riesgo y *accountability*. La verificación continua, la segmentación de accesos y la aplicación del principio de mínimo privilegio permiten traducir obligaciones abstractas (como la seguridad adecuada, la supervisión efectiva o la trazabilidad de las decisiones) en mecanismos técnicos observables y auditables.

En el marco de la Directiva NIS2, *Zero Trust* facilita la implementación de medidas proporcionadas y adaptativas, capaces de responder a un entorno de amenazas en constante evolución. La capacidad de limitar el impacto de inci-

dentes, detectar comportamientos anómalos y aislar componentes comprometidos refuerza la resiliencia organizativa exigida por la directiva. De forma similar, en el ámbito del ENS, los principios de *Zero Trust* encajan de manera natural con la gestión continua del riesgo, la defensa en profundidad y la segregación de funciones, proporcionando un soporte técnico sólido a los principios básicos del esquema.

La relevancia de *Zero Trust* se intensifica con la incorporación de servicios en la nube, trabajo remoto y sistemas automatizados, donde los límites tradicionales de la organización se difuminan. En estos entornos, el perímetro deja de ser una referencia válida y la identidad se convierte en el principal vector de control. *Zero Trust* desplaza así el foco desde la protección del entorno hacia la protección del acceso, independientemente del lugar desde el que se produzca.

Este desplazamiento tiene implicaciones directas para la *gestión de identidades y accesos (IAM)*. En un modelo *Zero Trust*, la identidad ya no se concibe como un atributo estático asociado a un usuario humano, sino como un conjunto dinámico de atributos contextuales que deben evaluarse de forma continua, entre otros, el rol, el dispositivo, el comportamiento, la ubicación, el nivel de riesgo o el tipo de servicio solicitado.

Esta lógica resulta especialmente pertinente en organizaciones que comienzan a integrar identidades técnicas, servicios automatizados y agentes de inteligencia artificial, cuya actuación debe quedar igualmente sujeta a control y supervisión.

Asimismo, *Zero Trust* introduce una nueva relación entre automatización y control. Lejos de debilitar la gobernanza, la automatización bien diseñada permite reforzar la capacidad de supervisión, al hacer posible la aplicación consistente de políticas, la detección temprana de anomalías y la respuesta rápida a incidentes. No obstante, esta automatización debe integrarse en un marco claro de responsabilidad organizativa, evitando que la delegación técnica diluya la rendición de cuentas.

Desde esta perspectiva, *Zero Trust* no constituye una solución mágica ni un sustituto de la gobernanza, sino un habilitador técnico de los modelos de control exigidos por el marco normativo europeo. Su adopción exige decisiones estratégicas, inversión sostenida y una revisión profunda de las políticas de seguridad y los procedimientos organizativos. Sin una gobernanza madura, el riesgo de implementar *Zero Trust* como un conjunto fragmentado de controles técnicos es elevado.

En definitiva, *Zero Trust* representa un punto de encuentro entre regulación, tecnología y organización. Permite materializar, a nivel arquitectónico, la exigencia europea de gestión continua del riesgo, control efectivo e imputación clara de responsabilidades. Sobre esta base técnica se hace posible redefinir los

roles estratégicos en materia de ciberseguridad y avanzar hacia modelos de identidad y gobernanza más adecuados para un entorno digital en evolución, cuestiones que se abordan en los apartados siguientes.

Bajo este escenario, el modelo *Zero Trust* (ZTA) debe ser rescatado de su reducción comercial como simple solución tecnológica para ser comprendido como una doctrina de gobernanza y un axioma de desconfianza administrativa necesaria. En el horizonte de la ciberseguridad, la confianza se ha revelado como una vulnerabilidad de diseño insostenible.

Por ello, la transición hacia arquitecturas de *Zero Trust* no responde únicamente a una mejora en la seguridad de la red, sino a la necesidad de construir una arquitectura de la evidencia que satisfaga los estándares de responsabilidad proactiva exigidos por la NIS2 y el *AI Act*.

Esta doctrina invierte la lógica tradicional de seguridad perimetral sustituir la confianza implícita por la verificación continua y dinámica de cada transacción. Desde una perspectiva jurídico-técnica, *Zero Trust* actúa como la materialización del principio de precaución debido a que ante la imposibilidad de garantizar la integridad absoluta de un actor sea este un empleado, un dispositivo IoT o un agente de IA autónomo, el sistema deniega el acceso por defecto. La legitimidad de la acción digital ya no reside en la ubicación del sujeto dentro de una red corporativa sino en la validación en tiempo real de su identidad operativa, su contexto y su comportamiento.

Para el CISO y los órganos de dirección, este enfoque permite una fragmentación de la responsabilidad administrativa mediante el uso de micro perímetros. Al compartimentar los activos críticos, la organización no solo contiene la propagación técnica de un incidente (movimiento lateral), sino que delimita el alcance del riesgo jurídico.

En caso de una brecha, la capacidad de demostrar que cada acceso fue verificado individualmente y bajo el principio de privilegio mínimo se constituye como la prueba irrefutable de *diligencia debida*. Así, el micro perímetro deja de ser una barrera técnica para convertirse en un límite de imputación ya que el administrador puede probar que tomó las medidas adecuadas y proporcionales para proteger el núcleo de la institución, transformando una infraestructura de red en un blindaje de responsabilidad legal.

En última instancia, *Zero Trust* en 2026 es el único marco capaz de gestionar la identidad consciente de la privacidad y la autonomía algorítmica. Al exigir una revalidación constante, el sistema genera un registro de *logs* de alta fidelidad que funciona como un diario de legalidad de la organización, permitiendo que la auditoría algorítmica y la supervisión del CISO sean, por primera vez, procesos basados en datos objetivos y no en presunciones de seguridad.

1.3. EL MARCO ESTRATÉGICO DEL CISO MODERNO. MÁS ALLÁ DE LOS CONTROLES TÉCNICOS

En este contexto, el marco estratégico del CISO en 2026 debe abandonar definitivamente el silo de la tecnología para integrarse en la Arquitectura de Decisión de la organización. Este desplazamiento implica que la ciberseguridad ya no se mide por la ausencia de incidentes (una métrica técnica a menudo engañosa) sino por la resiliencia del proceso de negocio o administrativo. El CISO moderno actúa como un Chief Risk Officer especializado que traduce vulnerabilidades binarias en impactos financieros operativos y, sobre todo, reputacionales.

La estrategia debe pivotar sobre tres ejes de valor representados por la alineación con la autonomía estratégica, la ética algorítmica y la protección del valor fiduciario. Esto significa que el diseño de seguridad debe ser consciente del propósito. en el sector público, por ejemplo, la estrategia del CISO debe garantizar que la digitalización no erosione los derechos fundamentales de la ciudadanía. Por tanto, el marco estratégico se convierte en un ejercicio de equilibrio ponderado mediante el cual CISO debe decidir dónde se sitúa el umbral de riesgo aceptable en función de la misión de la entidad, documentando estas decisiones para que sirvan de base a la gobernanza corporativa. Ya no se trata de implementar el mejor cortafuegos sino de diseñar la estrategia que permita a la organización seguir operando bajo ataque, cumpliendo con su mandato legal y protegiendo sus activos críticos.

Para materializar este equilibrio ponderado, el CISO moderno debe operacionalizar los tres ejes de valor mencionados mediante una nueva *gramática del riesgo.*

A. La alineación con la autonomía estratégica (soberanía digital)

En un ecosistema hiperconectado la estrategia de seguridad no puede ser agnóstica a la procedencia de la tecnología. El CISO debe evaluar la dependencia crítica de proveedores externos, especialmente en servicios de nube y modelos de lenguaje (LLM). La autonomía estratégica exige que el diseño de la arquitectura permita una reversibilidad operativa mediante la capacidad de migrar activos críticos o mantener funciones básicas ante un fallo sistémico del proveedor o un conflicto geopolítico. Aquí la seguridad se funde con la política de continuidad asegurando que la soberanía de la institución no quede secuestrada por opacidades técnicas de terceros.

B. La ética algorítmica y la integridad del dato

Cuando la ciberseguridad integra agentes de IA el riesgo se desplaza del acceso al contenido. La estrategia debe contemplar la protección del ciclo de vida del aprendizaje debido a que un sistema de seguridad que utiliza IA para

detectar amenazas es vulnerable a sesgos o a envenenamiento de datos (*data poisoning*[1]). Por tanto, el CISO debe auditar no solo quién accede al sistema sino cómo piensa el sistema. La ética algorítmica se convierte en un control de seguridad preventivo mediante el cual garantizar que las decisiones automatizadas sean explicables (*explainability*) y no discriminatorias representa en 2026 una obligación de cumplimiento tanto bajo el *AI Act* como bajo el RGPD.

C. La protección del valor fiduciario y la resiliencia de los derechos

En el ámbito de la Administración Pública, este eje adquiere una dimensión constitucional. La estrategia del CISO debe proteger el valor público. Esto implica que el umbral de riesgo aceptable es mucho más bajo cuando lo que está en juego es la privacidad de la historia clínica de un ciudadano o la integridad del censo electoral. El CISO actúa aquí como un fideicomiso de la confianza ciudadana. Su estrategia debe documentar formalmente la ponderación entre la eficiencia de la automatización y la salvaguarda de los derechos fundamentales, creando un expediente de Diligencia Debida que proteja a la organización ante futuras impugnaciones judiciales.

Finalmente, este marco estratégico se apoya en una Métrica de Resiliencia. Ya no basta con reportar el número de ataques bloqueados. El CISO debe informar al consejo de dirección sobre el tiempo de supervivencia operativa ante escenarios de fallo total y el impacto en el cumplimiento de cada decisión técnica. Esta transición del dato técnico al dato de gobernanza es lo que consolida al CISO como un pilar fundamental de la Arquitectura de Decisión, transformando la ciberseguridad de un centro de costes a un motor de legitimidad institucional.

Esta transformación estratégica no ocurre en el vacío, sino que se inserta en un ecosistema regulatorio y organizativo que define las nuevas reglas del juego en Europa. En el contexto europeo, la ciberseguridad ha dejado de ser una función puramente técnica para convertirse en un elemento central de la gobernanza organizativa. La entrada en vigor de NIS2, la aplicación del RGPD y la integración de sistemas de inteligencia artificial obligan a las organizaciones a repensar no solo sus arquitecturas técnicas, sino también los roles estratégicos encargados de gestionar el riesgo digital. En este marco, el CISO emerge como figura clave, no únicamente como responsable de la implementación de controles, sino como actor estratégico con mandato delegado de supervisión y coordinación.

1. El *data poisoning* (envenenamiento de datos) es un ciberataque en el que actores maliciosos corrompen los datos de entrenamiento de un modelo de IA o *Machine Learning* (ML) inyectando información falsa, sesgada o malintencionada. Esto manipula el comportamiento del modelo, provocando decisiones erróneas, fallos de seguridad o resultados sesgados sin necesidad de alterar el algoritmo principal.

El CISO moderno debe operar en la intersección de tres dominios críticos, a saber, la regulación, la arquitectura técnica y la estrategia organizativa. Desde el punto de vista regulatorio, actúa como garante del cumplimiento de NIS2, RGPD, *AI Act* y ENS, asegurando que las políticas y procedimientos de seguridad se traduzcan en prácticas efectivas y verificables. Desde el plano técnico, supervisa la adopción de arquitecturas avanzadas, como *Zero Trust*, que materializan la gobernanza del riesgo y habilitan la trazabilidad continua. Desde el punto de vista estratégico, influye en la toma de decisiones de la alta dirección, condicionando la priorización de recursos, la asignación de responsabilidades y la respuesta a incidentes.

Este enfoque requiere que el CISO sea más que un gestor de seguridad y devenga en ser un facilitador de la resiliencia organizativa, capaz de integrar las exigencias normativas con las capacidades técnicas de la organización y de anticipar riesgos emergentes, incluyendo aquellos derivados de sistemas autónomos y agentes de inteligencia artificial. La dirección de la organización depende de sus análisis, recomendaciones y métricas, aunque la responsabilidad última permanezca en el órgano directivo, en cumplimiento con la NIS2 y principios de *accountability*.

El CISO moderno también desempeña un papel central en la gestión de la cadena de suministro y servicios externalizados. La ampliación del perímetro de riesgo a terceros, prevista en NIS2 y reforzada por las obligaciones de control y supervisión del *AI Act*, requiere que la función del CISO abarque no solo sistemas internos, sino también componentes externos sobre los que la organización mantiene una responsabilidad indirecta. En este sentido, el CISO actúa como interlocutor técnico y jurídico, garantizando la coherencia de las políticas de seguridad con la operativa de proveedores y socios estratégicos.

En corporaciones públicas, la figura del CISO se encuentra particularmente articulada con el Esquema Nacional de Seguridad (ENS), desempeñando la función de garante operativo del cumplimiento y la supervisión de riesgos. Esta integración permite que las políticas y procedimientos no solo existan formalmente, sino que se implementen y se supervisen de manera efectiva, proporcionando evidencia de diligencia y trazabilidad ante inspecciones o auditorías.

Finalmente, el CISO moderno debe ser capaz de traducir los principios de gobernanza en criterios medibles y verificables, vinculando la arquitectura técnica, las políticas de seguridad y los procesos de decisión con indicadores de riesgo y desempeño. Solo de este modo es posible garantizar la continuidad operativa, la seguridad de los activos críticos y la protección de los derechos fundamentales, cumpliendo simultáneamente con las exigencias normativas y las expectativas estratégicas de la organización.

En síntesis, el CISO moderno deja de ser un simple responsable técnico para convertirse en actor estratégico de primer nivel, cuya labor integra regulación, arquitectura y estrategia, constituyendo un eje central en la gestión del riesgo digital europeo. Esta conceptualización prepara el terreno para abordar la asunción directa de responsabilidad del CISO, que se analiza en la sección siguiente.

1.4. EL CISO COMO DIRECTIVO. RESPONSABILIDAD, IMPUTACIÓN Y LÍMITES EN LA GOBERNANZA DEL RIESGO DIGITAL

La metamorfosis del CISO en un perfil directivo de alto nivel conlleva una asunción de responsabilidades que trascienden lo puramente operativo para adentrarse en el terreno de la responsabilidad fiduciaria. Bajo el marco de la *Directiva NIS2*, específicamente en su *Artículo 20*, se establece un mandato imperativo como es que la responsabilidad de la gestión de riesgos de ciberseguridad recae de forma efectiva en los órganos de dirección.

Esta disposición genera un efecto cascada sobre la figura del CISO moderno, quien deja de ser un mero ejecutor técnico para convertirse en un fiduciario del riesgo. Su función primordial en este nuevo orden es garantizar que el órgano de administración no incurra en una ignorancia culpable, actuando como el arquitecto del nexo causal entre la inversión tecnológica y la protección de la responsabilidad personal de los administradores. La imputación jurídica, por tanto, se desplaza desde la falta técnica aislada hacia la deficiencia estructural en la gobernanza.

Para navegar esta exposición legal, es imprescindible que el CISO adopte y documente sus acciones bajo la doctrina del Juicio de Empresa (*Business Judgment Rule*) adaptada al ámbito digital.

Esta regla, pilar del derecho de sociedades, protege a los directivos de la responsabilidad por decisiones que resulten en daños, siempre que estas hayan sido tomadas de buena fe, sin intereses personales y tras un el proceso de decisión racional basado en información adecuada. En nuestro ecosistema actual, implica que la defensa del CISO no debe basarse en la pretensión de una infalibilidad técnica (imposible en el actual estado del arte), sino en la perfección procesal.

Si el CISO puede demostrar fehacientemente que la estrategia se fundamenta en estándares reconocidos, que los riesgos han sido evaluados de forma sistemática y que la dirección ha sido informada puntualmente de las carencias, su responsabilidad queda blindada. La resiliencia jurídica reside, por tanto, en la solidez del expediente administrativo de toma de decisiones.

No obstante, la responsabilidad del CISO debe entenderse siempre como una *responsabilidad derivada y cualificada*. Es fundamental delimitar este rol

para evitar que se convierta en una figura de chivo expiatorio organizacional. La NIS2 es clara, el CISO no sustituye a la alta dirección ni asume su responsabilidad indelegable ya que actúa como una figura de *imputación funcional*.

Su actuación se evalúa mediante el principio de responsabilidad proactiva (*accountability*), presente tanto en el RGPD como en el Esquema Nacional de Seguridad (ENS). Mientras que el RGPD exige demostrar la adopción de medidas técnicas apropiadas para proteger los derechos fundamentales, el ENS articula un modelo de roles Donde el CISO garantiza la operatividad del sistema dentro de una estructura jerárquica definida. Esta corresponsabilidad estructural asegura que la gestión del riesgo no dependa de la voluntad de una persona, sino de la madurez de la institución.

Este equilibrio de responsabilidades enfrenta su mayor desafío en la automatización extrema y el uso de agentes de IA. La emergencia de la *Delegación Opaca* (la cesión de decisiones críticas a sistemas autónomos cuya lógica interna es inescrutable en tiempo real) representa la nueva frontera de la imputación jurídica. La jurisprudencia europea de 2026 subraya que la complejidad del algoritmo no exime al directivo de su deber de supervisión.

Aquí, el CISO actúa como mediador entre la autonomía técnica y la exigencia jurídica de control, aplicando el principio de *responsabilidad por el diseño del control*. Si un sistema autónomo provoca un daño, la responsabilidad administrativa recaerá en el CISO si no se establecieron los *guardrails* o mecanismos de desconexión (*kill-switches*[2]) adecuados. En última instancia, la autonomía de la tecnología no altera la heteronomía de la norma.

En conclusión, el reconocimiento del CISO como figura con dimensión directiva no implica una personalización indebida del riesgo, sino una clarificación de roles acorde con la complejidad del entorno digital.

Sin un mandato claro, recursos adecuados y apoyo efectivo de la alta dirección, la exigencia de responsabilidad se convierte en una ficción organizativa. Por ello, el éxito del CISO en 2026 no se mide por la ausencia de incidentes, sino por su capacidad de construir una *arquitectura de la evidencia*. Este marco de gobernanza, que desarrollaremos operativamente en capítulos posteriores, permite transitar de una seguridad basada en la fe a una basada en la prueba, protegiendo la integridad legal de la institución y abriendo el camino hacia el análisis de las identidades artificiales.

2. Un *kill switch* (interruptor de apagado) es un mecanismo de seguridad diseñado para detener o apagar maquinaria, sistemas informáticos o redes inmediatamente en caso de emergencia, fallo o peligro. Evita daños mayores al cortar el funcionamiento o la conexión de manera rápida y automática.

Ilustración 5. La ciberseguridad ya no es un silo técnico. El Radar de Convergencia ilustra cómo la responsabilidad directiva nace de la intersección inevitable de estas tres corrientes normativas.

La metamorfosis del CISO en un perfil directivo de alto nivel conlleva una asunción de responsabilidades que trascienden lo puramente operativo para adentrarse en el terreno de la responsabilidad fiduciaria. Esta convergencia de obligaciones normativas, que hasta ahora hemos analizado de forma secuencial, requiere una lectura sincrónica que identifique no solo los mandatos formales de cada instrumento, sino sus puntos de solapamiento funcional y sus vacíos compartidos. La Tabla 1.1 sistematiza esta intersección, revelando cómo NIS2, *AI Act* y ENS articulan un sistema de gobernanza digital que, paradójicamente, no contempla de forma explícita la gestión de las identidades artificiales (núcleo del riesgo algorítmico contemporáneo y objeto central de este libro).

Tabla 1. Tabla. Convergencia normativa NIS2, AI Act y ENS en la gobernanza de identidades artificiales

Dimensión de análisis	Directiva NIS2 (UE) 2022/2555	Reglamento *AI Act* (UE) 2024/1689	Esquema Nacional de Seguridad (RD 311/2022)
Ámbito de aplicación			
Sujetos obligados	Entidades esenciales e importantes (sectores críticos: energía, transporte, salud, finanzas, agua, infraestructuras digitales, administración pública)	Proveedores e Implementadores (*Deployers*) de sistemas IA de alto riesgo; Usuarios de sistemas prohibidos	Administraciones Públicas españolas y entidades que presten servicios a las mismas (obligatorio el sector público)
Alcance territorial	UE + Estados Miembros (transposición 17/10/2024)	UE + efecto extraterritorial si IA se usa en UE	España (alineado con normativa UE)
Objeto regulado	**Redes y sistemas de información críticos** Cadena de suministro TIC	**Sistemas de Inteligencia Artificial** según nivel de riesgo (prohibido, alto, limitado, mínimo)	**Información electrónica y servicios públicos digitales** Sistemas de información de AAPP
Obligaciones principales			
Gestión de riesgos	Art. 21: Medidas técnicas organizativas y operativas **adecuadas y proporcionadas** para gestionar riesgos de ciberseguridad	Art. 9: Sistema de **gestión de riesgos continua** durante ciclo de vida (identificación de riesgos conocidos/previsibles, incluidos sesgos)	**Análisis y gestión de riesgos** (op.pl.1): Identificación, valoración, tratamiento y seguimiento sistemático
Gobernanza corporativa	Art. 20: **Responsabilidad del órgano de dirección**: aprobación, supervisión efectiva, formación obligatoria	Art. 17: **Sistema de gestión de calidad** para implementadores Art. 26: Obligaciones de *governance* para proveedores	**Política de seguridad aprobada por máxima autoridad** (op.pl.2); Asignación de responsabilidades (roles definidos)
Seguridad por diseño	Implícito en medidas técnicas (Art. 21.2: seguridad de sistemas, redes, cadena suministro)	Art. 15: **Robustez, precisión, ciberseguridad desde el diseño** Resistencia a manipulación/*adversarial AI*	**Protección desde el diseño** (op.acc): Principio de mínimo privilegio, segregación de funciones
Supervisión humana	No explícita (centrada en procesos organizativos)	Art. 14: **Supervisión humana significativa** obligatoria en sistemas alto riesgo, prevención de *automation bias*	Implícita en **responsabilidad de uso** (op.exp.8): Control efectivo sobre sistemas automatizados

Trazabilidad/*Logs*	Art. 21.2.e: Políticas y procedimientos para evaluar eficacia de medidas	Art. 12: **Registro automático de eventos** (*logging*); Art. 11: Documentación técnica exhaustiva	op.exp.9: **Registro de actividad** de usuarios; mp.info.3: **Protección de registros de auditoría**
Notificación de incidentes	Art. 23: **Alerta temprana (24h)** + Informe de incidente (72h) + Informe final Umbral: impacto significativo	Art. 73: Notificación de incidentes graves de IA a autoridades de vigilancia del mercado	CCN-CERT: **Notificación obligatoria** de incidentes de seguridad según categorización del sistema
Cadena de suministro	Art. 21.2.g: Seguridad en **relaciones proveedor-cliente** (debido *diligence* terceros)	Art. 28: Obligaciones de **transparencia en cadena de valor** responsabilidad compartida proveedor-*deployer*	mp.si.2: **Análisis de riesgos de servicios externalizados** control de acceso de terceros
Identidades artificiales: tratamiento específico			
Reconocimiento conceptual	**No explícito** (enfoque en protección de sistemas, no agentes)	**Implícito**: Sistemas IA son sujetos operativos que requieren control humano (Art. 14)	**No explícito**, pero identidades técnicas incluidas en op.acc (control de acceso lógico)
Mecanismos de control	Control de accesos genérico (usuarios autorizados)	**Supervisión humana efectiva** (Art. 14.3): diseño para permitir intervención/interrupción	**Gestión de identidades** (op.acc.5): Identificación unívoca, autenticación robusta, control de privilegios
Imputación de responsabilidad	Responsabilidad organizativa del **órgano de dirección** (Art. 20)	Responsabilidad del **implementador** (*deployer*) que usa IA bajo su autoridad (Art. 26) Proveedor responde por diseño	**Responsable del servicio** + responsable de la información + **responsable de seguridad** (roles segregados)
Trazabilidad de decisiones	*Logs* de actividad de sistemas	Art. 12.1: **Capacidad de *logging* automático** durante operación del sistema IA	**Trazabilidad completa** de accesos y acciones (op.exp.9)
Régimen sancionador			
Autoridad competente	Autoridad nacional NIS (España: CCN-CERT + INCIBE + sectoriales)	Autoridad nacional de vigilancia del mercado (España: **AESIA** - Agencia Española Supervisión IA)	CCN (Centro Criptológico Nacional) + Autoridades sectoriales
Sanciones económicas	**Hasta 10M € o 2% facturación global** (lo mayor) para entidades esenciales Hasta 7M € o 1.4% para importantes	**Hasta 35M € o 7% facturación global** (sistemas prohibidos); Hasta 15M € o 3% (incumplimiento obligaciones Art. 9-15) Hasta 7.5M € o 1.5% (información incorrecta)	**Sanciones administrativas** según LPAC (hasta 1M € el sector público) Responsabilidad patrimonial

Sanciones personales	Art. 20.4: **Responsabilidad personal de administradores** (sanciones y medidas según derecho nacional)	Art. 99: Posibilidad de sanciones a **personas físicas responsables** según derecho nacional	**Responsabilidad disciplinaria** funcionarios Responsabilidad penal por delitos informáticos (CP)
Medidas no pecuniarias	Suspensión de certificaciones Prohibición temporal de operar	**Retirada del mercado** de sistemas IA Prohibición de comercialización	**Declaración de no conformidad** Obligación de subsanación
	Principios rectores		
Principio clave	**Resiliencia y gestión de crisis** Seguridad de la cadena de suministro	**Confianza y supervisión humana** Prevención de riesgos a derechos fundamentales	**Defensa en profundidad** Proporcionalidad Gestión continua del riesgo
Enfoque de cumplimiento	***Risk-based approach*** (proporcionalidad a impacto servicio)	***Risk-based regulation*** (4 niveles: prohibido, alto, limitado, mínimo)	**Categorización de sistemas** (Bajo, Medio, Alto) con medidas graduales
Relación con identidad	Identidad como **vector de acceso** a sistemas críticos	Identidad artificial como **sujeto de supervisión** (agente autónomo a controlar)	Identidad como **base de imputación** y trazabilidad en sistemas públicos
	Interoperabilidad y convergencia		
Punto de convergencia con otros marcos	Compatible con ISO 27001, RGPD (Art. 32 medidas seguridad), DORA (sector financiero)	Compatible con RGPD (Art. 22 decisiones automatizadas), NIS2 (ciberseguridad de IA)	**Complementario a NIS2** como marco operativo español Alineado con CCN-STIC
Tratamiento de la opacidad algorítmica	No aborda (enfoque en infraestructura)	Art. 13: **Transparencia y provisión de información** a usuarios Art. 86: Derecho a explicación	**Necesidad de motivación** del acto administrativo (LPA 39/2015) Explicabilidad implícita
Mecanismos de evidencia	Documentación de medidas de seguridad adoptadas	**Documentación técnica completa** (Art. 11) *Logs* automáticos (Art. 12)	**Sello de órgano + CSV** como evidencia de autenticidad Expediente electrónico único

El análisis comparativo revela tres hallazgos críticos para el CISO moderno. Primero, la escalada sancionadora del *AI Act* (hasta 35M€) supera ampliamente la de NIS2 (10M€), lo que implica que una identidad artificial mal gobernada puede generar sanciones acumulativas por violación simultánea de ambos marcos.

Segundo, el vacío regulatorio en la fila identidades artificiales demuestra que ningún marco europeo define mecanismos específicos de control para agentes no humanos con agencia algorítmica emergente, validando la necesidad de los constructos teóricos que desarrollaremos en el Capítulo 2.

Tercero, la responsabilidad indelegable del órgano de dirección (NIS2 Art. 20, *AI Act* Art. 26, ENS política de máxima autoridad) transforma al CISO en facilitador de la *accountability* directiva, no en chivo expiatorio técnico. Sobre esta base normativa consolidada, la sección siguiente propone la arquitectura de gobernanza que permite materializar estas exigencias.

1.5. LA SÍNTESIS DEL ESCUDO. HACIA UNA ARQUITECTURA DE GOBERNANZA INTEGRADA

La gestión del riesgo digital en la segunda mitad de esta década ha dejado de ser una disciplina técnica para convertirse en una arquitectura jurídica multidimensional. El CISO de 2026 ya no opera en el vacío, sino en el centro de una convergencia de mandatos que forman un escudo de protección institucional, pero que también delimitan el perímetro de su responsabilidad personal y corporativa.

En la base de este escudo encontramos el eje de la resiliencia estructural, donde la Directiva NIS2 establece el marco de gobernanza general, elevando la ciberseguridad a una responsabilidad estratégica del órgano de dirección. Esta base se vuelve aún más exigente en sectores específicos a través del Reglamento DORA, que traslada las obligaciones generales a un plano de resiliencia operativa financiera obligando a una vigilancia estrecha de la cadena de suministro y de la continuidad del negocio ante incidentes sistémicos.

Sobre esta base de resiliencia se despliega el eje del control funcional y algorítmico. Aquí, el Reglamento de Inteligencia Artificial (RIA) define las reglas del juego para la autonomía, exigiendo que cualquier sistema de alto riesgo sea robusto y auditable. Sin embargo, para que estos requisitos no queden en una declaración de intenciones, el CISO encuentra en España su herramienta operativa fundamental, el Esquema Nacional de Seguridad (ENS). Es el ENS el que proporciona los controles técnicos y organizativos necesarios para materializar la seguridad que NIS2 y el RIA exigen, convirtiéndose en el lenguaje común que traduce la ley en configuraciones, cifrados y niveles de acceso verificables.

Finalmente, el escudo se cierra con el eje de la legitimidad y la privacidad, Donde el RGPD y la reciente Guía de la AEPD de diciembre de 2025 actúan como los garantes de los derechos fundamentales. Este marco establece los

ARANZADI DERECHO EMPRESA

En el año 2026, la ciberseguridad ha trascendido definitivamente la protección de sistemas para consolidarse como una cuestión estratégica de poder, responsabilidad y control institucional. Bajo la presión regulatoria de la Directiva NIS2, el Reglamento de Inteligencia Artificial y el Esquema Nacional de Seguridad, las organizaciones europeas ya no son evaluadas por sus promesas de protección, sino por su capacidad real de aportar evidencias verificables de diligencia debida.

El colapso del perímetro tradicional marca el fin de una visión obsoleta de la defensa digital, dando paso a un cambio de paradigma en el que la identidad deja de actuar como un simple mecanismo de acceso para transformarse en el núcleo del poder operativo soberano, donde, a través de la trazabilidad inmutable, la verificación continua y la capacidad efectiva de revocación, cada acción, humana o artificial, queda sometida a un nuevo contrato con la realidad digital.

Mediante el paradigma de la Identidad Operativa, el autor redefine quién actúa, bajo qué responsabilidad y dentro de qué límites de mandato en entornos hiperautomatizados, situando al CISO como el arquitecto jefe de las condiciones de legitimidad, encargado de asegurar que la organización opere sin perder el mando estratégico sobre sus agentes autónomos.

La pregunta crítica de nuestra era deja de ser si una institución está protegida y pasa a ser si puede demostrarlo de forma irrefutable cuando la tecnología falla, cuando la automatización toma decisiones con impacto jurídico y cuando la responsabilidad exige pruebas.

Con un enfoque fundamentado en el realismo jurídico-tecnológico, este libro proporciona a la alta dirección un marco de defensa basado en el sellado epistémico, la supervisión humana significativa y los protocolos de desconexión inmediata, conocidos como kill-switches, diseñados para intervenir cuando la tecnología desborda el control humano.

Este tratado no constituye una simple mejora técnica, sino un manual imprescindible sobre cómo sostener el poder y la integridad en un entorno algorítmico donde cada decisión debe ser explicable, auditable y reversible para preservar la confianza ciudadana.

ISBN: 978-84-1085-852-7

ARANZADI