Ciberseguridad como dominio organizacional: condiciones estructurales del liderazgo técnico

Federico Pacheco[1]

[1] Universidad Tecnológica Nacional, Buenos Aires, Argentina
federico.pacheco@gmail.com

Resumen. Las funciones de ciberseguridad operan bajo condiciones estructurales que desafían los supuestos tradicionales sobre toma de decisiones en sistemas organizacionales. Estas condiciones incluyen incertidumbre adversarial persistente, conocimiento altamente distribuido, presión temporal y responsabilidad institucional no delegable. Si bien la literatura existente aborda estos elementos de manera fragmentada, suele asumir que la incertidumbre puede reducirse progresivamente, que el conocimiento puede integrarse de forma suficiente y que la autoridad puede alinearse con el expertise técnico. Este trabajo cuestiona dichos supuestos al caracterizar la ciberseguridad como un dominio en el cual estas condiciones se encuentran estructuralmente limitadas. En consecuencia, se argumenta que la relación entre evaluación técnica y decisión organizacional no puede entenderse como un problema de alineación progresiva, sino como una tensión persistente bajo restricciones del dominio. El trabajo contribuye al explicitar estas condiciones estructurales, delimitar el alcance de los modelos existentes y presentar un conjunto de proposiciones teóricas orientadas a guiar futuras investigaciones.

Palabras clave: Ciberseguridad, liderazgo técnico, toma de decisiones, autoridad epistémica, diseño organizacional, sistemas sociotécnicos.

1. Introducción

La ciberseguridad se consolidó como función crítica en organizaciones actuales, en la medida en que la dependencia de infraestructuras digitales, la sofisticación de actores adversariales y la expansión de marcos regulatorios incrementaron su impacto sobre la continuidad operativa, la exposición al riesgo y la responsabilidad institucional. En este contexto, la toma de decisiones en ciberseguridad dejó de ser un problema puramente técnico para convertirse en un proceso organizacional que articula evaluación experta, arbitraje estratégico y rendición de cuentas.

La literatura abordó el liderazgo en ciberseguridad desde múltiples perspectivas, incluyendo marcos de gobernanza del riesgo, desarrollo de competencias profesionales y enfoques de liderazgo distribuido. Estos trabajos contribuyeron a caracterizar estructuras de supervisión, trayectorias de formación y dinámicas relacionales en funciones técnicas complejas. Sin embargo, tienden a compartir un conjunto de supuestos implícitos sobre las condiciones bajo las cuales se coordinan decisiones en contextos organizacionales intensivos en conocimiento.

En particular, dichos enfoques presuponen que por lo general la incertidumbre puede ser progresivamente reducida mediante información o análisis, que el conocimiento relevante puede integrarse de manera coherente en procesos decisionales, y que la autoridad organizacional puede alinearse gradualmente con el expertise técnico. Estos supuestos, si bien razonables en otros dominios de ingeniería o gestión, resultan problemáticos en el contexto específico de la ciberseguridad.

A diferencia de otras funciones técnicas, la ciberseguridad opera bajo condiciones de incertidumbre adversarial persistente, donde los actores relevantes adaptan activamente su comportamiento en función de las decisiones defensivas; conocimiento altamente distribuido, donde la información necesaria para evaluar una situación se encuentra fragmentada entre múltiples especialistas; presión temporal, que limita la viabilidad de procesos deliberativos extensos; e implicancias organizacionales que exceden el dominio técnico, involucrando dimensiones operativas, legales y estratégicas bajo responsabilidad institucional no delegable.

Estas condiciones alteran las bases sobre las cuales se construyen la autoridad, la legitimidad y los derechos de decisión en funciones técnicas. En particular, la coexistencia de conocimiento distribuido y responsabilidad institucional introduce una tensión estructural: quienes poseen la capacidad de evaluar técnicamente una situación no son necesariamente quienes detentan la autoridad para decidir, y quienes asumen la responsabilidad por la decisión no poseen necesariamente el conocimiento suficiente para evaluarla de manera autónoma.

Por ejemplo, durante la gestión de incidentes críticos en ciberseguridad, es frecuente que múltiples expertos técnicos sostengan interpretaciones divergentes sobre la naturaleza, alcance o impacto de una amenaza, basadas en información parcial y en dominios de conocimiento especializados. Sin embargo, decisiones como la contención de sistemas, la interrupción de servicios o la notificación a terceros deben ser tomadas por actores con responsabilidad institucional, cuyas decisiones no dependen exclusivamente de dichas interpretaciones técnicas, sino también de consideraciones operativas, legales y estratégicas. Este tipo de situaciones ilustra la separación entre evaluación técnica y decisión organizacional que este trabajo busca formalizar.

El problema central puede formularse, por tanto, en los siguientes términos: ¿qué propiedades estructurales de la ciberseguridad como dominio organizacional modifican las condiciones bajo las cuales se ejerce el liderazgo técnico y se coordinan decisiones en funciones intensivas en conocimiento?

Este trabajo propone una reformulación del liderazgo técnico en ciberseguridad a partir de la caracterización de un desacople estructural entre evaluación técnica y decisión organizacional. En particular, se argumenta que la separación entre evaluación técnica y decisión organizacional no constituye una disfunción ni una contingencia organizacional, sino una propiedad estructural derivada de la organización del trabajo experto bajo condiciones de adversarialidad, distribución del conocimiento y accountability institucional.

El resto del trabajo se estructura de la siguiente manera. En la Sección II se analizan los supuestos implícitos en la literatura existente. La Sección III caracteriza las propiedades estructurales del dominio de la ciberseguridad. La Sección IV examina las implicancias de estas propiedades sobre los modelos tradicionales de liderazgo

técnico. Finalmente, se discuten las consecuencias teóricas y se plantean líneas de trabajo futuro.

A diferencia de enfoques existentes que abordan la incertidumbre, la distribución del conocimiento o la autoridad decisional de manera aislada, este trabajo los considera en su configuración conjunta como determinantes estructurales del problema decisional en ciberseguridad.

2. Trabajo relacionado

La literatura sobre liderazgo técnico y toma de decisiones en contextos complejos ha sido ampliamente desarrollada en campos como la teoría organizacional, los sistemas sociotécnicos y los sistemas de alta confiabilidad. Sin embargo, estos enfoques no abordan explícitamente escenarios en los cuales la incertidumbre es activamente generada por actores adversarios, ni las implicancias de esta condición sobre la posibilidad de convergencia evaluativa entre expertos.

A. Liderazgo técnico y coordinación organizacional

Los modelos de liderazgo técnico han evolucionado desde enfoques centrados en la autoridad jerárquica hacia concepciones que enfatizan la distribución del liderazgo, la coordinación lateral y la integración de conocimiento especializado. En particular, la literatura sobre liderazgo distribuido sostiene que la capacidad de decisión emerge de la interacción entre múltiples actores con expertise diferenciado.

En paralelo, los enfoques sociotécnicos destacan la necesidad de diseñar sistemas organizacionales que articulen componentes humanos y técnicos de manera coherente, reconociendo la interdependencia entre ambos. Estos marcos han contribuido a desplazar el foco desde el individuo hacia la configuración del sistema.

No obstante, estos enfoques suelen presuponer que la coordinación permite integrar el conocimiento distribuido en procesos decisionales relativamente coherentes, y que las tensiones entre actores pueden resolverse mediante mecanismos de alineación progresiva.

B. Toma de decisiones bajo incertidumbre

La toma de decisiones en contextos complejos ha sido abordada desde múltiples perspectivas, incluyendo la racionalidad limitada, la toma de decisiones naturalista y los modelos de sistemas de alta confiabilidad.

Estos enfoques coinciden en que las decisiones se toman bajo condiciones de información incompleta y presión temporal, y destacan el rol del expertise en la interpretación de situaciones ambiguas. En particular, la literatura sobre naturalistic decision making muestra que los expertos no comparan alternativas de manera exhaustiva, sino que reconocen patrones y actúan en consecuencia.

Sin embargo, incluso estos enfoques tienden a asumir que la incertidumbre puede ser gestionada o reducida mediante experiencia, entrenamiento o mejora de los procesos de decisión, sin considerar escenarios en los cuales la incertidumbre es activamente generada por actores adversarios.

C. Conocimiento distribuido y coordinación

El problema de la distribución del conocimiento ha sido extensamente analizado en teoría organizacional. Autores como Hayek argumentan que el conocimiento relevante para la toma de decisiones se encuentra disperso entre múltiples actores, lo que limita la posibilidad de centralizarlo. En línea con esto, la literatura sobre coordinación enfatiza la necesidad de mecanismos que permitan articular contribuciones parciales en contextos de interdependencia.

En entornos técnicos complejos, esta distribución se intensifica debido a la especialización creciente, lo que incrementa la dependencia entre expertos y la necesidad de coordinación transversal.

No obstante, estos enfoques suelen asumir que, mediante estructuras adecuadas, es posible lograr niveles suficientes de integración del conocimiento para sostener decisiones coherentes a nivel organizacional.

D. Limitaciones de los enfoques existentes en ciberseguridad

En el campo específico de la ciberseguridad, la literatura ha abordado principalmente aspectos de gobernanza, gestión del riesgo, desarrollo de capacidades y madurez organizacional. Estos enfoques han sido fundamentales para estructurar funciones de seguridad dentro de las organizaciones.

Sin embargo, tienden a tratar los problemas de decisión como cuestiones de mejora de procesos, alineación organizacional o desarrollo de competencias, sin problematizar las condiciones estructurales que limitan la integración del conocimiento y la alineación entre expertise y autoridad.

En particular, la combinación de adversarialidad persistente, conocimiento altamente distribuido y responsabilidad institucional no delegable introduce restricciones que no son abordadas explícitamente por estos marcos.

En conjunto, la literatura existente proporciona herramientas valiosas para comprender la coordinación organizacional y la toma de decisiones en contextos complejos. En contraste con estos enfoques, el presente trabajo no asume que la integración del conocimiento o la alineación entre expertise y autoridad sean alcanzables mediante mejoras organizacionales, sino que las considera estructuralmente limitadas bajo ciertas condiciones del dominio. Además, se apoyan en tres supuestos que no se sostienen plenamente en el dominio de la ciberseguridad: que la incertidumbre es progresivamente reducible, que el conocimiento distribuido puede integrarse de manera suficiente, y que la autoridad puede alinearse con el expertise

Este trabajo parte de la hipótesis de que estos supuestos se encuentran estructuralmente limitados en ciberseguridad, y que dicha limitación requiere una reformulación del problema del liderazgo técnico.

3. Propiedades estructurales de la ciberseguridad

Las limitaciones identificadas en la literatura no se derivan exclusivamente de enfoques incompletos, sino de la aplicación de supuestos organizacionales que no se sostienen bajo las condiciones estructurales del dominio de la ciberseguridad. En esta sección se caracterizan dichas condiciones no como atributos contextuales, sino como propiedades que configuran el espacio de posibilidades del sistema decisional.

Estas propiedades no operan de manera independiente, sino como un conjunto interrelacionado de restricciones que afectan simultáneamente la evaluación técnica, la coordinación organizacional y el ejercicio de la autoridad.

A. Incertidumbre adversarial como límite estructural de la inferencia

En ciberseguridad, la incertidumbre no es únicamente consecuencia de información incompleta, sino de la presencia de actores que adaptan activamente su comportamiento en función de las decisiones defensivas. Esta condición introduce una forma de incertidumbre estratégica en la cual el entorno relevante no es estable ni exógeno, sino reactivo.

Como consecuencia, la incertidumbre no puede ser eliminada mediante acumulación de información, mejora de modelos o refinamiento analítico. En cambio, persiste como una propiedad estructural del dominio, limitando la posibilidad de fundamentar decisiones sobre bases predictivas estables.

Este carácter no reducible de la incertidumbre implica que la evaluación técnica no converge necesariamente hacia una única interpretación óptima, sino que permanece sujeta a juicio experto bajo ambigüedad irreductible. En este contexto, el desacuerdo técnico no constituye una anomalía, sino una condición esperable del sistema.

B. Distribución estructural del conocimiento relevante

El conocimiento necesario para evaluar situaciones en ciberseguridad se encuentra fragmentado entre múltiples dominios especializados (infraestructura, aplicaciones, identidad, threat intelligence, cumplimiento, entre otros), sin que exista una instancia capaz de integrarlo completamente en tiempo real.

Esta distribución no es contingente ni organizacionalmente accidental, sino inherente a la complejidad técnica del dominio. Como resultado, ningún actor individual posee acceso completo al conjunto de información relevante para la toma de decisiones.

En consecuencia, la evaluación técnica depende de la coordinación de múltiples fuentes de expertise, lo que introduce dependencias interpersonales y limita la posibilidad de centralizar el proceso de análisis. Esta condición restringe la capacidad de alinear conocimiento y decisión dentro de un mismo actor.

C. Urgencia temporal y compresión del espacio deliberativo

Las decisiones en ciberseguridad suelen desarrollarse bajo condiciones de presión temporal asociadas a incidentes, vulnerabilidades activas o ventanas de exposición

limitadas. Esta urgencia reduce el tiempo disponible para integrar conocimiento distribuido, evaluar alternativas y construir consenso.

La compresión del tiempo decisional amplifica los efectos de la incertidumbre y la fragmentación del conocimiento, forzando decisiones bajo condiciones de información incompleta y coordinación parcial. En este contexto, los mecanismos deliberativos extensos pierden viabilidad operativa, y la toma de decisiones se desplaza hacia esquemas de arbitraje bajo presión.

D. Interdependencia sistémica de las decisiones

Las decisiones en ciberseguridad no afectan únicamente al sistema técnico, sino que generan consecuencias sobre múltiples dimensiones organizacionales, incluyendo continuidad operativa, costos, cumplimiento regulatorio, exposición legal y reputación.

Esta interdependencia implica que las decisiones no pueden optimizarse exclusivamente desde criterios técnicos, sino que requieren arbitraje entre objetivos potencialmente conflictivos. Como resultado, la evaluación técnica constituye una condición necesaria pero no suficiente para la toma de decisiones.

Esta característica introduce una disociación funcional entre la capacidad de evaluar técnicamente una situación y la capacidad de decidir sobre ella en términos organizacionales.

E. Responsabilidad institucional no transferible

A diferencia del conocimiento técnico, la responsabilidad por las decisiones en ciberseguridad —incluyendo sus consecuencias operativas, legales y estratégicas— no puede delegarse completamente en actores técnicos. La accountability permanece asociada a posiciones organizacionales con mandato formal de decisión.

Esta condición introduce una asimetría estructural: mientras que la evaluación depende de actores distribuidos con expertise especializado, la decisión recae en actores con responsabilidad institucional, independientemente de su nivel de conocimiento técnico.

Esta asimetría no es contingente ni resoluble mediante capacitación o comunicación, sino que responde a la necesidad organizacional de asignar responsabilidad por la acción.

F. Configuración conjunta de restricciones

Las propiedades descritas no operan de manera aislada, sino que configuran conjuntamente un conjunto de restricciones sobre el sistema decisional:

la incertidumbre limita la convergencia analítica
la distribución del conocimiento impide su centralización
la urgencia reduce la capacidad de coordinación
la interdependencia exige arbitraje no técnico
la accountability separa evaluación de decisión

En conjunto, estas condiciones generan un entorno en el cual los supuestos de reducibilidad de la incertidumbre, integración del conocimiento y alineación entre expertise y autoridad no se sostienen.

4. Consecuencias organizacionales y límites actuales

Las propiedades estructurales del dominio de la ciberseguridad introducen restricciones que afectan directamente los supuestos sobre los cuales se apoyan los modelos tradicionales de liderazgo técnico y coordinación organizacional. Estas restricciones no implican la invalidez de dichos modelos en términos generales, pero sí delimitan su alcance explicativo en contextos caracterizados por adversarialidad, distribución del conocimiento, presión temporal y responsabilidad institucional no delegable.

En particular, las condiciones descritas alteran tres supuestos centrales: la reducibilidad de la incertidumbre, la integrabilidad del conocimiento y la alineación progresiva entre expertise y autoridad.

A. Límite de la reducibilidad de la incertidumbre

En modelos convencionales de toma de decisiones, la incertidumbre es tratada como una variable que puede ser progresivamente reducida mediante mayor información, análisis o modelización. Bajo este supuesto, el rol del liderazgo técnico consiste en mejorar la calidad de la evaluación hasta alcanzar un nivel suficiente de certeza para la decisión.

Sin embargo, bajo condiciones de incertidumbre adversarial, este supuesto no se sostiene. La información relevante es incompleta, dinámica y, en muchos casos, estratégicamente manipulada por actores externos. En consecuencia, la evaluación técnica no converge necesariamente hacia una única interpretación estabilizada.

Esto implica que la decisión no puede derivarse linealmente de la evaluación, sino que requiere arbitraje bajo ambigüedad persistente. El liderazgo técnico no puede en general definirse, por tanto, como la capacidad de eliminar la incertidumbre, sino como la capacidad del sistema de operar en su presencia.

B. Límite de la integración del conocimiento

Los modelos organizacionales suelen asumir que el conocimiento distribuido puede integrarse en procesos decisionales coherentes, ya sea mediante jerarquía, coordinación transversal o mecanismos colaborativos.

No obstante, la distribución estructural del conocimiento en ciberseguridad, combinada con restricciones temporales, limita la posibilidad de integrar completamente la información relevante antes de decidir. La evaluación técnica se realiza sobre bases parciales y desde perspectivas especializadas que no siempre son plenamente compatibles.

Como resultado, la coordinación no puede basarse en una síntesis completa del conocimiento, sino en la articulación de contribuciones parciales bajo condiciones de incompletitud. Esto introduce una separación operativa entre el proceso de evaluación técnica y el momento de decisión organizacional.

C. Límite de la alineación entre expertise y autoridad

Una premisa extendida en modelos de liderazgo técnico es que la autoridad decisional puede alinearse progresivamente con el expertise, ya sea mediante promoción, acumulación de experiencia o reconocimiento organizacional.

Sin embargo, en ciberseguridad, la coexistencia de conocimiento distribuido e implicancias organizacionales amplias limita significativamente esta alineación completa. Ningún actor concentra simultáneamente el conocimiento técnico necesario para evaluar todas las dimensiones de una situación y la responsabilidad institucional para decidir sobre sus consecuencias.

En consecuencia, la evaluación técnica y la decisión organizacional quedan necesariamente desacopladas. Este desacople no constituye una falla organizacional, sino una consecuencia directa de las condiciones estructurales del dominio.

D. Desacople estructural entre evaluación y decisión

Las limitaciones anteriores convergen en una implicancia central: la imposibilidad de sostener modelos en los cuales la decisión se deriva directamente del conocimiento técnico.

En ciberseguridad, la evaluación técnica depende de actores distribuidos con expertise especializado, mientras que la decisión requiere arbitraje entre criterios técnicos, organizacionales y regulatorios bajo responsabilidad institucional. Esta doble dependencia introduce una separación estructural entre evaluación y decisión.

Esta separación no puede resolverse mediante mejoras en comunicación, capacitación o procesos, ya que no responde a déficits operativos sino a restricciones del dominio. En ausencia de mecanismos que articulen ambas dimensiones, el sistema decisional tiende a exhibir comportamientos como latencia, sobreescalamiento o conflicto interfuncional.

E. Redefinición del problema del liderazgo técnico

A partir de lo anterior, el liderazgo técnico en ciberseguridad no puede en general definirse adecuadamente como una propiedad individual, una posición jerárquica o un conjunto de competencias.

En cambio, emerge como un problema de coordinación entre:

evaluación técnica distribuida, dependiente del expertise

decisión organizacional centralizada, dependiente de la responsabilidad institucional

Bajo esta reformulación, el problema no es quién lidera ni quién posee mayor conocimiento, sino cómo el sistema organiza la relación entre saber y decidir bajo condiciones de incertidumbre, fragmentación del conocimiento y presión temporal.

5. Hacia una reformulación del liderazgo técnico

Las condiciones estructurales analizadas en las secciones anteriores muestran que los modelos tradicionales de liderazgo técnico resultan insuficientes para explicar la coordinación decisional en funciones de ciberseguridad. En particular, la imposibilidad de reducir la incertidumbre, la fragmentación del conocimiento relevante y la no transferibilidad de la responsabilidad institucional impiden sostener supuestos de convergencia analítica, integración completa del conocimiento y alineación entre expertise y autoridad.

En este contexto, el liderazgo técnico no puede comprenderse adecuadamente como una propiedad individual, una función jerárquica ni un conjunto de competencias. Estas aproximaciones presuponen condiciones de estabilidad, integrabilidad y alineación que no se sostienen bajo las restricciones del dominio.

En cambio, el problema del liderazgo técnico en ciberseguridad puede reformularse como un problema de coordinación entre dos dimensiones estructuralmente diferenciadas: la evaluación técnica, dependiente de conocimiento especializado distribuido, y la decisión organizacional, asociada a la responsabilidad institucional por la acción bajo incertidumbre.

Esta reformulación implica desplazar el foco analítico desde atributos individuales o estructuras formales hacia las configuraciones mediante las cuales las organizaciones articulan conocimiento experto y autoridad decisional en contextos de alta complejidad.

Bajo esta reformulación, el liderazgo técnico se define como la capacidad del sistema organizacional de articular evaluación técnica distribuida en decisiones institucionales bajo condiciones de incertidumbre.

Esta perspectiva establece las condiciones conceptuales para modelos que interpretan el liderazgo técnico como un problema de diseño institucional de la autoridad y de los derechos de decisión, en los cuales la relación entre conocimiento, legitimidad y decisión no se resuelve mediante alineación, sino mediante mecanismos de articulación bajo restricciones estructurales.

La reformulación propuesta puede representarse como un sistema en el cual la evaluación técnica y la decisión organizacional operan bajo condiciones estructurales diferenciadas. En este sistema, el conocimiento relevante se encuentra distribuido entre múltiples actores con expertise especializado, mientras que la responsabilidad por la decisión permanece concentrada en instancias institucionales. La articulación entre ambas dimensiones se produce bajo restricciones de tiempo, coordinación e incertidumbre, lo que limita la convergencia evaluativa y condiciona el proceso decisional. La Figura 1 sintetiza esta dinámica, destacando la separación estructural entre evaluación técnica distribuida y decisión organizacional centralizada.

Figura 1. Representación conceptual de la dinámica entre evaluación técnica distribuida y decisión organizacional centralizada en contextos de ciberseguridad. La articulación entre ambas dimensiones ocurre bajo restricciones estructurales que limitan la convergencia evaluativa e introducen un desacople entre evaluar y decidir.

La representación anterior describe la dinámica interna del sistema decisional en ciberseguridad. Sin embargo, esta configuración puede entenderse también como un caso particular dentro de un espacio más general definido por la relación entre distribución del conocimiento y centralización de la autoridad, lo cual se desarrolla en la siguiente sección.

6. Proposiciones teóricas

A partir de las propiedades estructurales del dominio de la ciberseguridad y sus implicancias sobre los modelos de liderazgo técnico y coordinación decisional, se proponen las siguientes proposiciones teóricas. Estas no constituyen afirmaciones empíricamente verificadas en este trabajo, sino hipótesis estructurales derivadas del análisis conceptual desarrollado, orientadas a guiar investigaciones futuras.

P1. Límite estructural de la convergencia evaluativa

En dominios caracterizados por incertidumbre adversarial persistente, la evaluación técnica de una misma situación no converge necesariamente hacia una interpretación única, aun en presencia de actores altamente expertos.

P2. Incompletitud estructural del conocimiento decisional

Cuando el conocimiento relevante para la evaluación técnica se encuentra distribuido entre múltiples dominios especializados, ningún actor individual posee una representación completa del estado decisional en tiempo operativo.

P3. Compresión temporal y degradación de la coordinación

Bajo condiciones de presión temporal, la capacidad de integrar conocimiento distribuido disminuye de manera significativa, incrementando la probabilidad de decisiones basadas en información parcial.

P4. Necesidad de arbitraje no técnico

En contextos donde las decisiones técnicas generan consecuencias organizacionales interdependientes, la decisión no puede derivarse exclusivamente de criterios técnicos, requiriendo arbitraje entre dimensiones heterogéneas.

P5. Desacople estructural entre evaluación y decisión

Cuando coexisten conocimiento distribuido y responsabilidad institucional no delegable, se genera una tensión persistente entre evaluación técnica y decisión organizacional.

En conjunto, estas proposiciones describen un sistema en el cual la relación entre conocimiento y decisión no puede entenderse como un proceso de alineación progresiva, sino como una articulación bajo restricciones estructurales.

La configuración estructural descrita en este trabajo puede representarse también como una posición dentro de un espacio conceptual definido por la distribución del conocimiento relevante y la centralización de la autoridad decisional. En este espacio, distintos dominios organizacionales pueden ubicarse según el grado en que el conocimiento necesario para la evaluación se encuentra concentrado o distribuido, y según el nivel en que la autoridad para decidir se encuentra centralizada o distribuida. La ciberseguridad se caracteriza por una combinación particular de alta distribución del conocimiento y alta centralización de la autoridad decisional, lo que introduce una tensión estructural entre evaluación y decisión.

La Figura 2 representa esta configuración, destacando la naturaleza no contingente del desacople analizado. No busca representar un modelo dinámico, sino más bien una ubicación conceptual del problema en un espacio estructural más amplio. Esta representación permite además comparar la ciberseguridad con otros dominios técnicos, identificando configuraciones en las cuales las tensiones entre conocimiento y autoridad pueden variar en intensidad o forma.

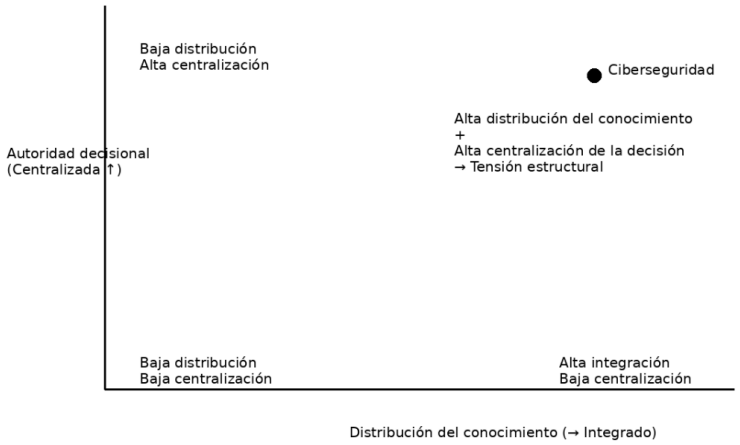

Figura 2. Ubicación conceptual de la ciberseguridad en un espacio definido por la distribución del conocimiento y la centralización de la autoridad decisional. La combinación de conocimiento altamente distribuido y autoridad decisional centralizada introduce una tensión estructural entre evaluación técnica y decisión organizacional.

La configuración identificada en ciberseguridad puede compararse con otros dominios técnicos y organizacionales en función de la distribución del conocimiento, la naturaleza de la incertidumbre y la centralización de la autoridad decisional. La Tabla 1 sintetiza estas diferencias, destacando que el desacople entre evaluación técnica y decisión organizacional no es exclusivo de la ciberseguridad, pero alcanza en este dominio una intensidad particular debido a la combinación simultánea de adversarialidad persistente, fragmentación del conocimiento y responsabilidad institucional no delegable.

Dominio	**Incertidumbre**	**Distribución del conocimiento**	**Autoridad decisional**	**Relación evaluación–decisión**
Ingeniería tradicional	Baja–moderada, reducible	Moderada	Alineada con expertise	Alta convergencia
Sistemas de alta confiabilidad (HRO)	Moderada–alta, gestionable	Alta	Parcialmente distribuida	Coordinación adaptativa
Operaciones militares	Alta, adversarial	Alta	Altamente centralizada	Tensión operativa
Gestión de crisis	Alta, dinámica	Alta	Centralizada	Coordinación bajo presión
Ciberseguridad	Alta, adversarial persistente	Muy alta, fragmentada	Centralizada (accountability)	Desacople estructural
Modelo ideal (su-	reducible	integrable	alineable	natural

Dominio	Incertidumbre	Distribución del conocimiento	Autoridad decisional	Relación evaluación–decisión
puesto clásico)				

Tabla 1. Comparación entre dominios organizacionales en función de incertidumbre, distribución del conocimiento y autoridad decisional.

7. Discusión y trabajo futuro

El análisis desarrollado en este trabajo propone una caracterización de la ciberseguridad como dominio organizacional cuyas propiedades estructurales alteran los supuestos bajo los cuales se han construido los modelos tradicionales de liderazgo técnico y coordinación decisional. Esta caracterización no busca reemplazar dichos modelos en términos generales, sino delimitar las condiciones bajo las cuales su capacidad explicativa resulta limitada. El trabajo no aborda los mecanismos específicos mediante los cuales estas tensiones se manifiestan o se regulan en sistemas organizacionales, sino que se limita a caracterizar las condiciones estructurales que las hacen inevitables.

En particular, los resultados sugieren que la separación entre evaluación técnica y decisión organizacional no debe interpretarse como una disfunción, un déficit de competencias o una falla de gobernanza, sino como una consecuencia estructural de la coexistencia de incertidumbre adversarial, conocimiento distribuido y responsabilidad institucional no delegable. Esta interpretación permite reubicar fenómenos recurrentes —como latencia decisional, sobreescalamiento o conflicto interfuncional— como manifestaciones esperables bajo determinadas configuraciones del dominio, en lugar de anomalías organizacionales.

Una posible objeción a este enfoque es que las condiciones analizadas no son exclusivas de la ciberseguridad, sino que pueden observarse en otros dominios caracterizados por alta complejidad técnica o incertidumbre, tales como sistemas de alta confiabilidad, operaciones militares o gestión de crisis. Sin embargo, el argumento no se basa en la exclusividad de cada propiedad de manera aislada, sino en su configuración conjunta. La combinación de adversarialidad persistente, fragmentación del conocimiento, presión temporal e implicancias organizacionales no delegables genera un entorno en el cual los supuestos de reducibilidad, integración y alineación resultan simultáneamente restringidos.

Otra posible crítica refiere a la ausencia de validación empírica directa de las proposiciones planteadas. Este trabajo se posiciona como un desarrollo conceptual orientado a explicitar condiciones estructurales y a reformular el problema del liderazgo técnico en ciberseguridad. En este sentido, su contribución no radica en la verificación empírica, sino en la construcción de un marco analítico que permita orientar investigaciones futuras.

A partir de este marco, se abren diversas líneas de trabajo empírico. Estudios cualitativos podrían analizar cómo se configuran en la práctica las relaciones entre evaluación técnica y decisión organizacional en distintos tipos de organizaciones, así como los mecanismos mediante los cuales se gestionan tensiones asociadas a la distribución

del conocimiento y la responsabilidad. Investigaciones cuantitativas podrían examinar la relación entre condiciones estructurales del dominio, configuraciones organizacionales y resultados observables, tales como tiempos de decisión, patrones de escalamiento o niveles de conflicto interfuncional.

Asimismo, estudios comparativos entre dominios —por ejemplo, entre ciberseguridad y otras funciones técnicas expuestas a incertidumbre estratégica— permitirían evaluar el alcance y los límites del modelo propuesto, así como identificar condiciones bajo las cuales sus supuestos pueden variar.

El valor de este trabajo no radica en identificar elementos aislados previamente conocidos, sino en formalizar su interacción como una configuración estructural que condiciona de manera sistemática la relación entre evaluación técnica y decisión organizacional.

Finalmente, este trabajo establece una base conceptual para el desarrollo de modelos que aborden el liderazgo técnico como un problema de diseño institucional de la autoridad y de los derechos de decisión. La formalización de dichos modelos, así como su validación empírica, constituye una línea de investigación futura necesaria para avanzar en la comprensión del fenómeno.

8. Conclusiones

El presente trabajo ha argumentado que la ciberseguridad constituye un dominio organizacional cuyas condiciones estructurales —incertidumbre adversarial persistente, conocimiento altamente distribuido, presión temporal y responsabilidad institucional no delegable— alteran los supuestos bajo los cuales se han construido los modelos tradicionales de liderazgo técnico y coordinación decisional.

En este contexto, la separación entre evaluación técnica y decisión organizacional no puede interpretarse como una disfunción ni como una contingencia organizacional, sino como una consecuencia estructural de la organización del trabajo experto bajo accountability institucional. Esta separación limita la aplicabilidad de enfoques basados en la reducibilidad de la incertidumbre, la integración completa del conocimiento y la alineación progresiva entre expertise y autoridad.

En consecuencia, el liderazgo técnico en ciberseguridad no puede comprenderse como una propiedad individual ni como una función jerárquica, sino como un problema organizacional de articulación entre conocimiento experto distribuido y decisión institucional bajo condiciones de incertidumbre.

Este marco conceptual establece las condiciones de posibilidad para modelos que abordan el liderazgo técnico como un problema de diseño institucional de la autoridad y de los derechos de decisión, donde la relación entre saber y decidir no se resuelve mediante alineación, sino mediante mecanismos explícitos de coordinación bajo restricciones estructurales.

Bibliografía

Afrin, S., et al. (2025). Smart infrastructure project decision-making under cyber uncertainty. Journal of Computer Science and Technology Studies, 7(8), 912–936.

Gaudenzi, A., et al. (2025). Uncertainty-aware attack stage inference using evidential deep learning. CEUR Workshop Proceedings.

Hayek, F. A. (1945). The use of knowledge in society. American Economic Review, 35(4), 519–530.

ISO. (2022). ISO/IEC 27001:2022 Information security management systems — Requirements. International Organization for Standardization.

Kashtalian, A., et al. (2025). Control and decision-making in deceptive multi-computer systems for cybersecurity. Applied Sciences, 15(22), 12286. https://doi.org/10.3390/app152212286

Klein, G. (1998). Sources of power: How people make decisions. MIT Press.

Kojukhov, A., & Bovshover, A. (2026). Agentic AI for cybersecurity: A meta-cognitive architecture for governable autonomy. arXiv preprint.

Kotter, J. P. (1996). Leading change. Harvard Business School Press.

Lempert, R. J., Popper, S. W., & Bankes, S. C. (2022). Decision making under deep uncertainty: From theory to practice.

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. ACM Computing Surveys, 26(1), 87–119. https://doi.org/10.1145/174666.174668

McFadden, S., et al. (2026). SoK: The pitfalls of deep reinforcement learning for cybersecurity. arXiv preprint.

Mintzberg, H. (1979). The structuring of organizations. Prentice-Hall.

Mohamed, N., et al. (2025). Advances in artificial intelligence and machine learning for cybersecurity. Cogent Engineering.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). https://doi.org/10.6028/NIST.CSWP.04162018

Simon, H. A. (1997). Administrative behavior: A study of decision-making processes in administrative organizations (4th ed.). Free Press. (Original work published 1947)

Spillane, J. P. (2006). Distributed leadership. Jossey-Bass.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. Human Relations, 4(1), 3–38. https://doi.org/10.1177/001872675100400101

Weick, K. E., & Sutcliffe, K. M. (2007). Managing the unexpected: Resilient performance in an age of uncertainty (2nd ed.). Jossey-Bass.

Zhang, Y., & Malacaria, P. (2024). Dealing with uncertainty in cybersecurity decision support. Computers & Security, 148, 104153. https://doi.org/10.1016/j.cose.2024.104153

Zhou, H., et al. (2025). Adversarial decision-making in partially observable multi-agent systems. arXiv preprint.