



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Estrategias de virtualización para la optimización
de CPD en entornos militares*

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Francisco Javier Fernández Díaz

DIRECTORES: Fernando Suárez Lorenzo

Milagros Fernández Gavilanes

CURSO ACADÉMICO: 2025–2026

UniversidadeVigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Estrategias de virtualización para la optimización
de CPD en entornos militares*

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_{de}Vigo

RESUMEN

La creciente dependencia de las capacidades de defensa en infraestructuras de computación demanda soluciones que aseguren resiliencia, eficiencia y trazabilidad en escenarios caracterizados por conectividad degradada y restricciones energéticas severas. En este contexto, los centros de proceso de datos militares —estratégicos, operacionales y tácticos— deben armonizar sostenibilidad, continuidad del servicio y cumplimiento normativo, de acuerdo con el Esquema Nacional de Seguridad, las guías CCN-STIC y la doctrina OTAN FMN.

Esta investigación desarrolla un marco metodológico unificado para la evaluación de infraestructuras virtualizadas en defensa, estructurado en torno al **Índice Global de Eficiencia Operativa**. Este integra tres dimensiones críticas: eficiencia energética, resiliencia operativa y conformidad normativa. Su desarrollo se sustenta en la principal contribución del trabajo: la definición formal de la métrica ***Military Power Usage Effectiveness***, que supera las limitaciones de su equivalente en el ámbito civil mediante factores de penalización logística, ambiental y de virtualización, adaptados específicamente al dominio militar.

La validación del modelo, realizada mediante un enfoque analítico paramétrico multiescala, evidencia que la eficiencia y la resiliencia dependen del nivel de empleo: las máquinas virtuales mantienen su mayor idoneidad en el nivel estratégico por su robustez normativa, mientras que las micro-VM y los contenedores bastionados ofrecen ventajas energéticas y tiempos de recuperación significativamente inferiores en escenarios tácticos. Estos hallazgos respaldan la adopción de una arquitectura híbrida federada, capaz de optimizar la huella logística sin comprometer la soberanía del dato ni la seguridad de la misión.

En conjunto, el trabajo proporciona un marco analítico reproducible que permite objetivar decisiones de planificación, orientar la evolución doctrinal y facilitar la transición hacia infraestructuras de computación más sostenibles, seguras y adaptadas a la operación distribuida en defensa.

PALABRAS CLAVE

Virtualización, Eficiencia energética, DDIL, *Edge Computing*, Micro-VM.

AGRADECIMIENTOS

A mi familia, por ser el origen de todo esfuerzo y el refugio incondicional a lo largo del camino. Gracias por vuestra paciencia infinita y por brindarme la estabilidad y el aliento necesarios para la culminación de este proyecto. Este logro es, ante todo, vuestro.

A mis tutores, Fernando y Milagros, por su inestimable guía y calidad humana. Agradezco profundamente que me hayan enseñado a elevar mis propios estándares de exigencia y a mirar la investigación con rigor y perspectiva.

A mis compañeros, por el viaje compartido. De todos y cada uno he aprendido lecciones valiosas que me llevo para el futuro, y que han convertido este máster en una experiencia inolvidable.

CONTENIDO

Índice de Figuras	3
Índice de Tablas	5
Lista de Acrónimos y Abreviaturas	7
1 Introducción	11
1.1 Contexto y motivación	11
1.2 Problema y oportunidad	13
1.3 Hipótesis y enfoque metodológico	14
1.4 Objetivos del trabajo	16
1.5 Estructura de la memoria	16
2 Fundamentos tecnológicos y marco doctrinal	19
2.1 Clasificación y funciones de los CPD en Defensa	20
2.2 Principios y tecnologías de virtualización en entornos de Defensa	26
2.3 Principios de eficiencia energética en infraestructuras virtualizadas	31
2.4 Propuesta de métrica energética: M-PUE	33
2.5 Marco doctrinal y normativo: ENS, CCN-STIC y FMN Spiral 5	39
2.6 Riesgos y barreras de implementación	42
2.7 Síntesis de fundamentos técnicos y doctrinales	44
3 Estado del arte, tendencias y análisis comparativo	47
3.1 Virtualización y <i>edge computing</i> en el ámbito militar	47
3.2 Estrategias de eficiencia energética y consolidación dinámica	50
3.3 Tendencias y aproximaciones en la gestión y evolución tecnológica	53
3.4 Limitaciones y retos actuales	55
3.5 Brecha metodológica y oportunidad de innovación	58
4 Metodología integrada y marco de evaluación para entornos virtualizados de Defensa	61
4.1 Fundamentación y propósito estratégico del método	61
4.2 Principios doctrinales, operativos y energéticos del marco	63
4.3 Estructura conceptual del método	64
4.4 Métricas e indicadores	65
4.5 Ejemplo ilustrativo de aplicación del método	70
4.6 Validación conceptual del método en escenarios doctrinales representativos	72
4.7 Síntesis metodológica y proyección del marco	74
5 Resultados y análisis de escenarios	77
5.1 Planteamiento metodológico del análisis	77
5.2 Parámetros de configuración y escenarios de prueba	79
5.3 Resultados del modelado	81
5.4 Análisis de sensibilidad del M-PUE	82
5.5 Análisis del escenario estratégico (E1)	84
5.6 Análisis del escenario operacional (E2)	85

5.7	Análisis del escenario táctico (E3)	86
5.8	Discusión y síntesis de hallazgos	88
6	Conclusiones, aportaciones y líneas futuras	91
6.1	Conclusiones estratégicas y validación de la hipótesis	91
6.2	Aportaciones metodológicas y doctrinales	92
6.3	Limitaciones y líneas futuras de investigación	93
7	Bibliografía.....	97

ÍNDICE DE FIGURAS

Figura 2-1	Alcalá Data Center	22
Figura 2-2	CPD modular en contenedor con dimensiones personalizadas (no-ISO)	22
Figura 2-3	CPD táctico sobre HPE Edgeline EL8000	23
Figura 2-4	Clasificación doctrinal de los CPD en defensa por nivel de despliegue	24
Figura 2-5	Diferencia entre arquitectura física y virtual	27
Figura 2-6	Comparativa de pilas de virtualización y reducción de sobrecarga	30
Figura 2-7	Medición de PUE en los CPD de Google.	37
Figura 2-8	Marco conceptual integrado	45
Figura 4-1	Estructura conceptual del continuo de computación en Defensa	62
Figura 4-2	Arquitectura funcional del método IGEO	69
Figura 5-1	Arquitectura de referencia y topología física de los escenarios (E1, E2, E3)	80
Figura 5-2	Evolución del M-PUE por escenario	81
Figura 5-3	Sensibilidad del M-PUE ante la degradación ambiental en el escenario táctico (E3)	83
Figura 5-4	Perfil de competencia tecnológica en escenario táctico (E3)	87
Figura 6-1	Hoja de ruta y proyección de líneas futuras (L1–L6)	95

ÍNDICE DE TABLAS

Tabla 2-1	Clasificación y características técnicas de los CPD por nivel de despliegue.	25
Tabla 2-2	Niveles de virtualización y tecnologías representativas.	27
Tabla 2-3	Comparativa de tecnologías de virtualización y nivel TRL estimado en defensa. . .	30
Tabla 2-4	Distribución estimada del consumo energético por tipo de CPD.	32
Tabla 2-5	Sobrecoste y densidad energética media por tecnología de virtualización.	32
Tabla 2-6	Justificación de fuentes para los factores M-PUE.	35
Tabla 2-7	Clasificación orientativa del M-PUE según el entorno de operación.	37
Tabla 2-8	Correspondencia entre guías CCN-STIC y tecnologías de virtualización.	40
Tabla 2-9	Convergencia doctrinal y normativa.	41
Tabla 3-1	Modelos de despliegue de <i>edge computing</i> en entornos de defensa.	48
Tabla 3-2	Análisis comparativo de tecnologías de virtualización para entornos <i>edge</i> militares. .	49
Tabla 3-3	Principales estrategias de consolidación y aplicabilidad en defensa.	51
Tabla 3-4	Tipos de escalado adaptativo aplicables a entornos virtualizados de defensa. . . .	51
Tabla 3-5	Escenarios de consolidación energética federada en el marco OTAN/UE.	52
Tabla 3-6	Evolución de la gestión de recursos virtualizados.	53
Tabla 3-7	Métricas aplicadas en infraestructuras virtualizadas.	54
Tabla 3-8	Principales limitaciones tecnológicas en la virtualización aplicada a defensa. . . .	55
Tabla 3-9	Principales vacíos normativos y doctrinales en la virtualización de defensa.	56
Tabla 3-10	Síntesis de brechas estructurales en la virtualización de defensa.	57
Tabla 3-11	Vacíos metodológicos en la evaluación de infraestructuras virtualizadas de defensa. .	58
Tabla 3-12	Relación entre limitaciones del estado del arte y soluciones metodológicas aportadas. .	59
Tabla 4-1	Principios doctrinales, operativos y energéticos del marco metodológico.	64
Tabla 4-2	Niveles L1–L3 para el cálculo del M-PUE en entornos de defensa.	67
Tabla 4-3	Comparativa de resultados obtenidos en los escenarios analizados.	74
Tabla 5-1	Fuentes de referencia para los parámetros del modelo.	79
Tabla 5-2	Perfiles tecnológicos y factores de virtualización.	80
Tabla 5-3	Parámetros energéticos y logísticos por escenario.	80
Tabla 5-4	Escenarios doctrinales y ponderaciones IGEO.	81
Tabla 5-5	Resultados consolidados del M-PUE.	81
Tabla 5-6	Indicadores de resiliencia operativa (IRO): SLA medio y MTTR.	82
Tabla 5-7	Comparativa de conformidad normativa.	82

LISTA DE ACRÓNIMOS Y ABREVIATURAS

Acrónimo	Definición
ACE	Allied Software for Cloud and Edge Services
AIM	Automated Infrastructure Management
AMD-V	Advanced Micro Devices – Virtualization
ARM	Advanced RISC Machines
C2	Command and Control (Mando y Control)
CCN	Centro Criptológico Nacional
CCN-STIC	Guías de Seguridad de las TIC (CCN)
CIS	Communication and Information Systems
CM	Capacidad de Microsegmentación
CNCF	Cloud Native Computing Foundation
COP	Coefficient of Performance
CPD	Centro de Proceso de Datos
CPU	Central Processing Unit
CUE	Carbon Usage Effectiveness
DCIM	Data Center Infrastructure Management
DDIL	Denied, Degraded, Intermittent, and Limited
DIANA	Defence Innovation Accelerator for the North Atlantic
DNS	Domain Name System
DPDK	Data Plane Development Kit
E2C	European Edge Computing
EAL	Evaluation Assurance Level
EDOCC	European Defence Operational Collaborative Cloud
ENS	Esquema Nacional de Seguridad
EPT	Extended Page Tables
ERF	Energy Reuse Factor
FMN	Federated Mission Networking
FPGA	Field Programmable Gate Array
GA	Grado de Aislamiento
GPU	Graphics Processing Unit
HVAC	Heating, Ventilation and Air Conditioning
HVP	High Visibility Project
IA	Inteligencia Artificial
ICOMP	Índice de Conformidad Normativa
IEC	International Electrotechnical Commission
IGEO	Índice Global de Eficiencia Operativa

Acrónimo	Definición
IOMMU	Input-Output Memory Management Unit
IoT	Internet of Things
IPMI	Intelligent Platform Management Interface
IPN	I-Profile Normal
IRO	Índice de Resiliencia Operativa
iSCSI	Internet Small Computer Systems Interface
ISO	International Organization for Standardization
ISR	Intelligence, Surveillance and Reconnaissance
IST	Information Systems Technology
KSM	Kernel Samepage Merging
KVM	Kernel-based Virtual Machine
LEED	Leadership in Energy and Environmental Design
LTS	Long Term Support
LVM	Logical Volume Manager
LXC	Linux Containers
M-PUE	Military Power Usage Effectiveness
MIL-STD	Military Standard
MPE	Mission Partner Environment
MTBF	Mean Time Between Failures
MTTR	Mean Time To Recovery (o Repair)
NATO	North Atlantic Treaty Organization
NDBB	NATO Digital Backbone
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
NT	Nivel de Trazabilidad
NUMA	Non-Uniform Memory Access
OTAN	Organización del Tratado del Atlántico Norte
PDU	Power Distribution Unit
PII	Personally Identifiable Information
PUE	Power Usage Effectiveness
RAID	Redundant Array of Independent Disks
SDI	Software-Defined Infrastructure
SDN	Software Defined Networking
SDS	Software Defined Storage
SLA	Service Level Agreement
SLO	Service Level Objective
STANAG	Standardization Agreement
SWaP	Size, Weight, and Power

Acrónimo	Definición
TCB	Trusted Computing Base
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions
THD	Total Harmonic Distortion
TIC	Tecnologías de la Información y las Comunicaciones
TRL	Technology Readiness Level
UE	Unión Europea
UPS	Uninterruptible Power Supply
VDI	Virtual Desktop Infrastructure
VFIO	Virtual Function I/O
VLAN	Virtual Local Area Network
VM	Virtual Machine (Máquina Virtual)
VXLAN	Virtual Extensible LAN
WUE	Water Usage Effectiveness
ZTNA	Zero Trust Network Access

1 INTRODUCCIÓN

1.1 Contexto y motivación

En los últimos años, la transformación digital de las Fuerzas Armadas europeas ha dejado de ser una aspiración tecnológica para convertirse en una necesidad operativa estratégica. Este proceso responde a la creciente complejidad de los teatros de operaciones contemporáneos, al auge de las amenazas híbridas y al rápido desarrollo de las tecnologías de la información. En este nuevo paradigma, la digitalización no implica únicamente incorporar capacidades avanzadas. Requiere asumir una integración transversal de principios como la interoperabilidad multinacional, la sostenibilidad operativa y el cumplimiento normativo riguroso. Todo ello debe realizarse en estrecha conexión con los marcos doctrinales de resiliencia en entornos caracterizados por conectividad degradada o intermitente, denominados DDIL (*Denied, Degraded, Intermittent and Limited*). Este concepto, consolidado en la doctrina OTAN, tiene su origen en la documentación técnica del NIST [1], donde se emplea la variante *Denied, Disrupted, Intermittent and Limited*. De forma complementaria, esta integración debe converger con los principios de arquitectura de seguridad moderna, haciendo especial énfasis en el modelo *Zero Trust*.

Uno de los ámbitos donde esta transformación resulta más evidente es el rediseño y la operación de los centros de proceso de datos (CPD). Estas infraestructuras, tradicionalmente asociadas al soporte administrativo, son hoy elementos críticos para sistemas de mando y control, inteligencia, logística, comunicaciones seguras, ciberdefensa y apoyo a fuerzas desplegadas. Su papel se ha ampliado para aportar capacidades modulares y resilientes que sostienen la superioridad informativa y la continuidad operativa. Este trabajo adopta el término estándar de la industria, *edge computing*, para referirse a los despliegues más avanzados, móviles y cercanos al punto de necesidad, evaluando sus implicaciones técnicas y estratégicas bajo el principio de que la «gravedad del dato» obliga a mover el cómputo hacia la información, y no al revés.

En el plano doctrinal, la OTAN ha consolidado esta evolución mediante la iniciativa *Federated Mission Networking* (FMN) [2], que define requisitos técnicos y operativos destinados a garantizar interoperabilidad, seguridad y resiliencia en entornos multinacionales. Su iteración más reciente, Spiral 5, actualmente en fase de validación, introduce capacidades específicas para asegurar servicios críticos incluso en escenarios DDIL, demandando infraestructuras capaces de operar de forma autónoma ante fallos de enlace o ataques adversarios.

De forma complementaria, la Alianza ha lanzado dos iniciativas que consolidan la transición hacia arquitecturas distribuidas en el borde. Por un lado, el programa *Allied Software for Cloud and Edge Services* (ACE) [3], designado como *High Visibility Project* (HVP), persigue habilitar el desarrollo y despliegue de servicios clasificados en nodos *edge*. Por su parte, el concepto *NATO Digital Backbone* (NDBB) [4] establece una arquitectura de referencia basada en la federación de nubes nacionales y nodos de misión, conectando de forma segura los niveles estratégico, operacional y táctico.

Ambas iniciativas consolidan la idea de que la computación distribuida y resiliente en el borde no es una aspiración futura, sino un requisito operativo vigente. En este contexto, los CPD tácticos analizados en este trabajo representan la base técnica sobre la que deben operar estos servicios federados, reforzando la necesidad de marcos de decisión capaces de equilibrar eficiencia, resiliencia y conformidad normativa en escenarios multinacionales y DDIL.

En paralelo, el marco normativo nacional ha intensificado sus exigencias en materia de seguridad y auditoría. El Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad (ENS) [5], clasifica los sistemas de información en categorías básica, media o alta, según el impacto potencial de una brecha de seguridad sobre la confidencialidad, integridad, disponibilidad y trazabilidad de los activos gestionados. Dada la naturaleza crítica de muchos sistemas del Ministerio de Defensa, especialmente aquellos vinculados al tratamiento de información clasificada, una parte significativa de estos activos se categoriza como alta, lo que implica la aplicación de controles reforzados de seguridad física, lógica y de gestión de la configuración.

De forma complementaria, el Centro Criptológico Nacional ha publicado guías técnicas que desarrollan los requisitos específicos para entornos virtualizados y arquitecturas en la nube. La Guía CCN-STIC-220 [6] establece los controles de seguridad aplicables a entornos de virtualización, incluyendo el despliegue y la administración de hipervisores, el aislamiento de cargas de trabajo y la protección de redes virtualizadas. Por su parte, la Guía CCN-STIC-823 [7] detalla los requisitos aplicables a infraestructuras *cloud* públicas o híbridas, con especial atención a la segregación de recursos y la gestión de credenciales privilegiadas.

A estos requisitos técnicos y normativos se suman condicionantes logísticos y medioambientales de creciente relevancia. Según estimaciones del grupo de trabajo IST-208 de la OTAN [8], el consumo anual de gasóleo asociado al funcionamiento eléctrico y la climatización de CPD desplegados en operaciones supera las 150.000 toneladas, con un impacto económico y medioambiental significativo. El ahorro energético en zona de operaciones no es solo una cuestión de eficiencia técnica, sino una necesidad táctica: reducir el consumo implica disminuir la frecuencia de los convoyes de suministro de combustible y, por tanto, la exposición de las fuerzas a ataques. Consecuentemente, la sostenibilidad se convierte en una dimensión estratégica del diseño de infraestructuras TIC. A este respecto, diversos estudios han demostrado que el uso combinado de virtualización avanzada, consolidación dinámica de cargas y mecanismos de apagado selectivo puede reducir el consumo energético agregado entre un 35 % y un 40 % [9, 10, 11], especialmente en entornos operativos con despliegues prolongados.

Este potencial ahorro energético no solo contribuye a optimizar la sostenibilidad logística y reducir la dependencia energética en teatros de operaciones, sino que también favorece el alineamiento con los objetivos de eficiencia, resiliencia y soberanía definidos en las directrices de interoperabilidad de la OTAN y en iniciativas estratégicas de la Unión Europea. Entre estas últimas destaca el programa European Edge Computing (E2C) [12], que impulsa el desarrollo de capacidades de procesamiento distribuido, virtualización estandarizada y control soberano de datos como pilares de una infraestructura de defensa más ágil, interoperable y resiliente.

En el ámbito nacional, esta evolución se refleja en los esfuerzos actuales del Ministerio de Defensa orientados al desarrollo de una *Nube de Combate* española, identificada como capacidad prioritaria en el Boletín de Observación Tecnológica [13]. Esta iniciativa responde directamente a los objetivos de «ciberresiliencia y acceso rápido a capacidades críticas» establecidos en la Brújula Estratégica de la Unión Europea [14], alineándose con las prioridades del Plan Industrial y Tecnológico para la Seguridad y la Defensa del ejercicio 2025 [15].

Dada esta coyuntura, están emergiendo arquitecturas híbridas basadas en *cloud privado* y *edge computing*, que combinan elasticidad, proximidad al dato y soberanía técnica. Este ecosistema tecnológico impulsa la adopción de soluciones avanzadas de virtualización capaces de mejorar rendimiento, reducir consumo y ofrecer garantías verificables de aislamiento y trazabilidad exigidas por el Esquema Nacional de Seguridad (ENS) y los estándares OTAN. Estas capacidades constituyen habilitadores técnicos fundamentales para implementar arquitecturas *Zero Trust Network Access* (ZTNA) mediante técnicas como la microsegmentación y el aislamiento multinivel.

No obstante, pese a los avances logrados en entornos civiles, la adopción de estas tecnologías en defensa sigue siendo desigual, especialmente en los niveles operacional y táctico. Actualmente no existe un marco metodológico plenamente integrado que permita evaluar de forma sistemática la relación entre eficiencia energética, resiliencia operativa y cumplimiento normativo verificable. Esta carencia dificulta el diseño de CPD optimizados para escenarios adversos, impidiendo dotar a la fuerza de una capacidad de supervivencia digital cuantificable.

Ante esta necesidad, el presente Trabajo Fin de Máster propone un **marco analítico de evaluación comparativa** para analizar las principales tecnologías de virtualización aplicables a CPD militares, con el objetivo de determinar configuraciones óptimas según el nivel de despliegue —estratégico, operacional y táctico— y el equilibrio entre rendimiento, sostenibilidad y conformidad regulatoria. Este trabajo se articula en torno a tres aportaciones principales:

- La definición de una métrica específica de eficiencia energética orientada a entornos militares desplegados denominada *Military Power Usage Effectiveness* (M-PUE), planteada como una extensión del estándar *Power Usage Effectiveness* (PUE) propuesto por The Green Grid [16], que integra factores ambientales y logísticos asociados a escenarios tácticos y condiciones operativas exigentes;
- El desarrollo de un marco analítico comparativo para evaluar diferentes tecnologías de virtualización bajo criterios integrados de eficiencia, resiliencia y seguridad;
- La formulación de recomendaciones estratégicas para la adopción progresiva de soluciones virtualizadas en el ecosistema TIC de Defensa.

Estas contribuciones sientan las bases del problema a abordar y delimitan el alcance operativo, normativo y metodológico del trabajo que se desarrolla a continuación.

1.2 Problema y oportunidad

La adopción de tecnologías de virtualización en entornos de defensa ha estado tradicionalmente asociada a infraestructuras de propósito general, ubicadas en centros de datos estratégicos y operando bajo condiciones estables de conectividad, suministro energético y soporte logístico. En este contexto, la consolidación de servicios sobre hipervisores convencionales ha permitido racionalizar recursos, simplificar la administración y mejorar la eficiencia operativa.

Sin embargo, la extrapolación directa de este paradigma a niveles operacional y táctico revela importantes limitaciones. Estos entornos, caracterizados por su variabilidad, hostilidad y dependencia de recursos limitados, exigen capacidades técnicas adaptadas que superen los modelos heredados de despliegue. En particular, la aplicación de arquitecturas virtualizadas convencionales se enfrenta a tres retos operativos críticos:

- **Disponibilidad degradada de comunicaciones.** En escenarios DDIL, la intermitencia o baja capacidad de los enlaces dificulta la sincronización de cargas, el aprovisionamiento remoto y la recuperación ante incidentes, comprometiendo la coordinación efectiva entre los nodos desplegados y el nivel superior.

- **Restricciones energéticas y logísticas.** Los CPD tácticos dependen para su operación de generadores de campaña con autonomía limitada y cadenas de suministro vulnerables. Esta condición impone restricciones estrictas en términos de SWaP (*Size, Weight, and Power*), exigiendo estrategias de eficiencia capaces de reducir drásticamente el consumo sin degradar la disponibilidad de los servicios de misión.
- **Seguridad multinivel y aislamiento reforzado.** La convivencia de cargas con distinta clasificación en una misma infraestructura física requiere mecanismos de segregación robustos. Es imperativo garantizar un aislamiento lógico verificable que cumpla con los requisitos establecidos por el marco normativo del ENS, asegurando la confidencialidad e integridad de la información sensible en alineación con las políticas *Zero Trust*.

A estas limitaciones técnicas se suman condicionantes estructurales de carácter estratégico:

- La obligación de acreditar el cumplimiento del ENS en su categoría ALTA, lo que conlleva controles rigurosos sobre segmentación lógica, trazabilidad y gestión de configuración, incluso en entornos dinámicos y distribuidos.
- La presión creciente por reducir la huella logística y energética de los despliegues, en línea con los objetivos de sostenibilidad definidos en iniciativas como el programa europeo *E2C* y los estándares OTAN de eficiencia.
- La necesidad de garantizar la continuidad de los servicios críticos ante fallos, interferencias deliberadas o ataques adversarios, en conformidad con los principios de resiliencia definidos por la iniciativa FMN Spiral 5.

En conjunto, estas circunstancias configuran un *trade-off* estructural: aunque la virtualización ha alcanzado un alto grado de madurez en el ámbito civil, aún no existe un marco metodológico específico que permita su aplicación sistemática, segura y eficiente en infraestructuras militares distribuidas, particularmente en niveles operacional y táctico. La ausencia de criterios integrados que equilibren eficiencia energética, resiliencia operativa y conformidad normativa limita la capacidad de estos CPD para sostener operaciones en escenarios adversos y altamente exigentes.

Al mismo tiempo, este reto representa una oportunidad estratégica para transformar el paradigma actual. La evolución de tecnologías como los micro-VM, los *unikernels*, los orquestadores distribuidos ligeros o las plataformas *cloud-edge* soberanas, permite plantear una aproximación adaptativa que combine eficiencia energética, aislamiento fuerte, trazabilidad reforzada y elasticidad operativa. Este nuevo enfoque ofrece la posibilidad de optimizar los CPD militares más allá de la simple consolidación, integrando capacidades avanzadas que respondan a las demandas de entornos DDIL, interoperabilidad multinacional y cumplimiento regulatorio exigente.

Como estrategia de transformación digital a medio y largo plazo, esta aproximación convertiría la virtualización en un pilar de modernización del entorno TIC de defensa, reforzando la autonomía tecnológica, reduciendo la huella logística y elevando la resiliencia distribuida. Todo ello en plena coherencia con las prioridades nacionales en materia de ciberdefensa, con los estándares doctrinales OTAN y con las líneas estratégicas de la UE en materia de digitalización segura, sostenible y soberana.

1.3 Hipótesis y enfoque metodológico

Partiendo del análisis de las brechas detectadas en los modelos de despliegue actuales, este estudio asume como premisa la inexistencia de una solución universal para todos los escalones de mando. La complejidad del teatro de operaciones moderno exige superar la visión monolítica de la infraestructura TIC en favor de modelos adaptativos, que integren las dimensiones operativa, logística y normativa, donde la tecnología se subordina a las restricciones del entorno y a la criticidad de la misión. Bajo este prisma conceptual, la investigación se fundamenta la siguiente hipótesis:

Los CPD en defensa, adaptados a los niveles estratégico, operacional y táctico, requieren arquitecturas de virtualización alineadas con el contexto doctrinal, capaces de garantizar simultáneamente la soberanía del dato y una ciberseguridad avanzada mediante esquemas ZTNA, especialmente en entornos operativos DDIL. En función del escenario, estas arquitecturas pueden adoptar configuraciones híbridas que combinen tecnologías con distintos perfiles de aislamiento, eficiencia y resiliencia. Esta necesidad responde al conflicto estructural de los CPD militares, donde deben equilibrarse de forma concurrente la eficiencia energética y logística, la resiliencia en condiciones DDIL y el cumplimiento normativo verificable, dimensiones que ninguna tecnología de virtualización maximiza por sí sola.

Se postula, además, que la evaluación de estas arquitecturas no puede basarse en métricas tradicionales, siendo necesario un marco metodológico específico –el Índice Global de Eficiencia Operativa (IGEO)– que integre de manera equilibrada la sostenibilidad energética (M-PUE), la resiliencia operativa (IRO) y el grado de conformidad normativa (ICOMP). Este índice permite identificar la tecnología óptima para cada nivel doctrinal y para cada prioridad operativa, proporcionando un criterio comparativo homogéneo, reproducible y ajustable a la intención del mando.

Para contrastar esta hipótesis se adopta un enfoque metodológico analítico-comparativo, orientado a evaluar tecnologías de virtualización bajo condiciones representativas del ámbito de defensa, tanto desde el punto de vista operativo como regulatorio. El procedimiento metodológico se articula en las siguientes fases:

- F-1: Caracterización doctrinal y tecnológica.** Se realiza una revisión del marco normativo vigente (ENS, guías CCN-STIC, directrices FMN) y se definen las tipologías de CPD empleadas en el entorno de defensa, distinguiendo los niveles estratégico, operacional y táctico, junto con sus restricciones específicas en cuanto a energía, logística y conectividad.
- F-2: Definición de métricas y criterios de evaluación.** Se formula la métrica M-PUE como indicador de eficiencia energética para entornos desplegados, y se definen las métricas IRO e ICOMP, que permiten evaluar de forma integrada sostenibilidad, resiliencia y cumplimiento normativo.
- F-3: Construcción del marco analítico comparativo.** Se elabora una matriz de evaluación que vincula las tecnologías de virtualización –hipervisores, contenedores, micro-VM y *unikernels*– con los criterios definidos, permitiendo ponderar su idoneidad y madurez tecnológica (TRL) en función del contexto operativo y regulatorio.
- F-4: Análisis de escenarios representativos.** Se evalúan escenarios doctrinales parametrizados (E1, E2 y E3) mediante un modelado analítico paramétrico multiescala, valorando la idoneidad relativa de cada tecnología según las prioridades estratégicas del Mando y las restricciones energéticas, logísticas y normativas.
- F-5: Síntesis y recomendaciones.** Se formulan conclusiones y recomendaciones orientadas a la adopción progresiva de soluciones virtualizadas seguras, sostenibles y eficientes, compatibles con las prioridades estratégicas del entorno TIC de la Defensa.

Este enfoque proporciona un marco de análisis riguroso, estructurado y reproducible, que permite comparar alternativas tecnológicas sin requerir validación experimental directa, manteniendo coherencia con los imperativos doctrinales de la OTAN y la UE, con los requisitos regulatorios nacionales y con las necesidades operativas propias de entornos militares en transformación digital.

A partir de la hipótesis planteada, este trabajo responde a las siguientes preguntas de investigación:

- P-1:** ¿Cómo se compara el comportamiento operativo, energético y de seguridad de las distintas tecnologías de virtualización en entornos DDIL?
- P-2:** ¿Cómo varía su idoneidad en función del nivel doctrinal de despliegue (estratégico, operacional, táctico)?
- P-3:** ¿Hasta qué punto un índice compuesto como IGEO puede servir como herramienta objetiva para apoyar decisiones en el diseño de CPD militares?

1.4 Objetivos del trabajo

El objetivo general de este Trabajo Fin de Máster es diseñar y validar un marco de decisión para la selección de tecnologías de virtualización en CPD de defensa, capaz de resolver el *trade-off* entre eficiencia energética y logística, resiliencia operativa en entornos DDIL y el grado de conformidad normativa verificable ENS/ZTNA, identificando la tecnología óptima para cada contexto doctrinal (E1, E2, E3).

A partir de este planteamiento, se establecen los siguientes objetivos específicos:

- OE-1: Caracterizar el contexto doctrinal, normativo y operativo.** Analizar los requisitos establecidos por el ENS, las guías CCN-STIC y las directrices OTAN-FMN, así como las condiciones energéticas, logísticas y de conectividad propias de CPD estratégicos, operacionales y tácticos.
- OE-2: Comparar las principales tecnologías de virtualización.** Evaluar hipervisores, contenedores, micro-VM y *unikernels* en términos de aislamiento, eficiencia, resiliencia, madurez normativa y sostenibilidad logística.
- OE-3: Formalizar una métrica de eficiencia energética adaptada a entornos militares.** Definir la métrica M-PUE como extensión del PUE, integrando factores ambientales, energéticos y logísticos relevantes para escenarios DDIL.
- OE-4: Desarrollar un marco integrado de evaluación operativa.** Construir el Índice IGEO, que combine sostenibilidad energética (M-PUE), resiliencia operativa (IRO) y cumplimiento normativo (ICOMP), permitiendo comparar tecnologías en función del nivel doctrinal.
- OE-5: Validar el marco mediante modelado analítico paramétrico.** Evaluar las tecnologías bajo escenarios doctrinales parametrizados (E1–E3), analizando el comportamiento de cada métrica y su integración en el IGEO.
- OE-6: Formular una hoja de ruta y recomendaciones estratégicas de adopción.** Derivar una hoja de ruta tecnológica basada en los resultados integrados del IGEO y del análisis multi-escala, alineada con las prioridades doctrinales de los escenarios E1–E3.

1.5 Estructura de la memoria

La presente memoria se organiza siguiendo una estructura progresiva y coherente con los objetivos del trabajo, avanzando desde los fundamentos doctrinales y tecnológicos hasta el análisis comparativo y las conclusiones estratégicas. Cada capítulo responde a una fase lógica del estudio y contribuye a desarrollar una visión integral de la virtualización aplicada a CPD en entornos de defensa.

El Capítulo 2, Fundamentos tecnológicos y marco doctrinal, establece la base conceptual del trabajo. Se analiza la evolución doctrinal y funcional de los CPD –desde infraestructuras estratégicas hasta nodos tácticos– y se describen los principios y tecnologías de virtualización (máquinas virtuales, contenedores, micro-VM y *unikernels*) junto con los marcos normativos y operativos relevantes, como el ENS, las guías CCN-STIC y la iniciativa aliada FMN.

El Capítulo 3, Estado del arte, tendencias y análisis comparativo, recoge una revisión crítica de la literatura científica, técnica y doctrinal. Se identifican las principales líneas de investigación y tendencias en eficiencia energética, resiliencia operativa y seguridad en entornos virtualizados de defensa, así como las lagunas existentes que justifican el desarrollo de un marco analítico específico.

El Capítulo 4, Metodología y marco de evaluación, describe el enfoque seguido para el análisis comparativo. Se definen las métricas y criterios de evaluación –incluyendo la métrica M–PUE como indicador de eficiencia energética– y se construye una matriz que relaciona tecnologías de virtualización con requisitos operativos, normativos y energéticos, diferenciando niveles de despliegue (estratégico, operacional y táctico).

El Capítulo 5, Resultados y análisis de escenarios, presenta los hallazgos obtenidos mediante la aplicación del marco comparativo. Se identifican las configuraciones tecnológicas más adecuadas según el entorno, y se formulan recomendaciones orientadas a facilitar una adopción progresiva, eficiente y segura de la virtualización en el ecosistema TIC del ámbito militar.

El Capítulo 6, Conclusiones, aportaciones y líneas futuras, sintetiza las contribuciones del trabajo y su valor estratégico. Se validan los objetivos iniciales y se propone una agenda de trabajo futura centrada en la estandarización de métricas, el desarrollo de pilotos y la integración con iniciativas europeas y aliadas en transformación digital, sostenibilidad y ciberdefensa.

La memoria se completa con la **Bibliografía**, que recoge las fuentes doctrinales, normativas y científicas consultadas, y con un anexo de **Acrónimos** para facilitar la lectura técnica. En su conjunto, el documento ofrece una exposición rigurosa y estructurada, alineada con las prioridades del entorno de defensa y los estándares académicos del Máster.

2 FUNDAMENTOS TECNOLÓGICOS Y MARCO DOCTRINAL

Este capítulo establece las bases conceptuales, tecnológicas y normativas que sustentan el análisis desarrollado en esta memoria. Su propósito es ofrecer una visión integrada del papel de los CPD en la defensa moderna, las tecnologías de virtualización que los habilitan y los marcos doctrinales y regulatorios que condicionan su diseño, operación y acreditación.

La transformación digital del ámbito militar ha impulsado una evolución significativa en la manera en que se conciben, despliegan y gestionan las infraestructuras de información. La doctrina OTAN y los programas europeos de modernización TIC enfatizan la transición hacia arquitecturas distribuidas, modulares y resilientes, capaces de operar bajo restricciones severas de conectividad, disponibilidad energética y condiciones ambientales. En este entorno, las infraestructuras tradicionales, fuertemente centralizadas y dependientes de enlaces estables, resultan insuficientes para garantizar la continuidad del mando y control en escenarios caracterizados por comunicaciones DDIL, coaliciones multinacionales e interoperabilidad intensiva.

De este modo, los CPD dejan de ser instalaciones monolíticas para convertirse en capacidades desplegadas, federadas y energéticamente sostenibles. Esta tendencia se alinea con estudios recientes sobre infraestructuras críticas –incluyendo arquitecturas modulares, *container data centers* y nodos tácticos rugerizados– que evidencian cómo la madurez tecnológica permite hoy integrar computación estratégica, operacional y táctica en una malla coherente de servicios, conocida en el ámbito europeo como el «*Continuum de Computación*» [17].

Sobre esta evolución doctrinal se articula el uso de tecnologías de virtualización, que permiten desacoplar cargas de trabajo de la infraestructura física, optimizar recursos, reforzar el aislamiento de dominios de seguridad y reducir la huella logística y energética. Su adopción posibilita arquitecturas híbridas que combinan estabilidad (nivel estratégico), modularidad (nivel operacional) y despliegue rápido (nivel táctico), en consonancia con los principios de interoperabilidad y resiliencia definidos en FMN Spiral 5.

La operación de estas tecnologías está condicionada por un marco normativo exigente –Esquema Nacional de Seguridad, guías CCN–STIC y estándares OTAN/UE– que establece controles de segregación lógica, continuidad operativa y trazabilidad energética. Este marco regulador define requisitos de seguridad y, al mismo tiempo, impulsa modelos de operación auditables y sostenibles.

Este capítulo introduce, por tanto, los conceptos fundamentales que permitirán, en las secciones posteriores, evaluar comparativamente las distintas opciones tecnológicas y su adecuación a cada nivel de despliegue –estratégico, operacional y táctico– constituyendo el marco doctrinal y técnico sobre el que se construye el análisis.

2.1 Clasificación y funciones de los CPD en Defensa

Los CPD en defensa proporcionan recursos de computación, almacenamiento y comunicaciones esenciales para sistemas de mando y control (C2), inteligencia, comunicaciones militares, logística, ciberdefensa y apoyo al planeamiento. Su función es asegurar la prestación continua de estos servicios en entornos donde disponibilidad, protección de la información y continuidad operativa resultan determinantes para la misión.

La evolución doctrinal ha impulsado una transición hacia arquitecturas distribuidas y resilientes, capaces de sostener operaciones incluso bajo conectividad degradada y restricciones energéticas. En este marco, los CPD dejan de concebirse como instalaciones fijas para configurarse como capacidades virtualizadas, escalables y aptas para distintos grados de movilidad. Esta transformación permite integrar infraestructuras permanentes, modulares o desplegables dentro de un modelo federado coherente con los niveles estratégico, operacional y táctico.

Con el fin de caracterizar estas capacidades de forma coherente, se adopta una clasificación conceptual basada en dichos niveles. Aunque no constituye una organización formal, esta aproximación permite distinguir infraestructuras orientadas a la estabilidad y capacidad (nivel estratégico), nodos modulares que extienden servicios hacia zonas adelantadas (nivel operacional) y soluciones ligeras que proporcionan computación cercana al usuario en condiciones variables o degradadas (nivel táctico).

Las subsecciones siguientes desarrollan las particularidades de cada tipo de CPD, atendiendo a su diseño físico, sus requisitos funcionales y su adecuación al entorno operativo.

2.1.1 Evolución doctrinal y tecnológica

La evolución de los CPD en defensa ha estado determinada tanto por los avances tecnológicos como por los cambios doctrinales y operativos. Durante la segunda mitad del siglo XX, los primeros CPD militares, inspirados en modelos civiles basados en *mainframes* centralizados, se orientaban a funciones administrativas y logísticas. La seguridad se fundamentaba en la separación física y en el control jerárquico de accesos, con escasa flexibilidad o capacidad de integración.

A partir de la década de 1990, la expansión de los sistemas de C2, inteligencia y apoyo logístico introdujo nuevas exigencias de disponibilidad y flexibilidad. Las operaciones en los Balcanes, Afganistán e Irak pusieron de manifiesto las limitaciones de los modelos centralizados en escenarios caracterizados por redes inestables, coaliciones multinacionales y entornos de comunicaciones degradadas. Este periodo marcó el inicio del desarrollo de CPD modulares y transportables, capaces de operar de forma parcial o completamente autónoma.

El salto decisivo se produjo con la consolidación de las tecnologías de virtualización a mediados de los 2000. La posibilidad de ejecutar múltiples sistemas operativos sobre un mismo hardware físico redujo drásticamente los tiempos de despliegue, mejoró la eficiencia energética y permitió replicar servicios críticos sin infraestructura adicional. La virtualización introdujo el concepto de *infraestructura lógica desplegable*, en la que la movilidad, la resiliencia y el aislamiento de cargas pasaron a ser propiedades inherentes a la arquitectura [6, 10].

A partir de 2010, la irrupción del *edge computing*, los contenedores y las micro-VM desplazó las capacidades de cómputo hacia el borde de la red, reduciendo la dependencia del núcleo estratégico. En paralelo, el ámbito europeo ha comenzado a materializar esta transición en iniciativas concretas, entre las que destaca el proyecto European Defence Operational Collaborative Cloud (EDOCC) [18], orientado a desarrollar una plataforma federada, modular e interoperable capaz de soportar operaciones multinivel. En el entorno nacional, la reciente puesta en marcha del centro de datos *Numant-IA* [19] por parte del Ministerio de Defensa ejemplifica la modernización hacia una nube privada segura y orientada a la soberanía digital.

En la actualidad, los CPD militares se desarrollan bajo criterios de interoperabilidad, sostenibilidad y soberanía tecnológica. Se conciben como nodos interconectados capaces de desplegarse, federarse o replicarse según la misión, configurando un ecosistema digital resiliente y energéticamente eficiente, plenamente coherente con los marcos estratégicos de la OTAN, la Unión Europea y el Estado español.

2.1.2 Clasificación y características de los CPD militares por nivel de despliegue

La organización de los Centros de Proceso de Datos (CPD) en el ámbito de la defensa puede alinearse conceptualmente con los tres niveles doctrinales de mando —**estratégico, operacional y táctico**— establecidos en la doctrina OTAN (AAP-06, AJP-01) y en la doctrina conjunta española (PDC-00). Esta correspondencia no constituye una jerarquía rígida de instalaciones, sino una aproximación a un marco funcional que permite asociar cada tipo de infraestructura a los requisitos característicos de su categoría funcional: continuidad estratégica, sostenimiento operacional y capacidad de mando en primera línea.

Cada nivel presenta patrones diferenciados de escala, disponibilidad, movilidad, resistencia ambiental, protección física e integración arquitectónica. A continuación se describen sus características específicas.

2.1.2.1 CPD estratégico

Los CPD estratégicos constituyen el núcleo del ecosistema TIC de defensa. Son infraestructuras fijas de gran escala, ubicadas generalmente en territorio nacional o bases permanentes aliadas. Su diseño toma como referencia las mejores prácticas de los estándares civiles —TIA-942 [20], EN 1047 [21] y BICSI 002 [22]— buscando niveles de redundancia y protección física equivalentes o superiores para garantizar la máxima resiliencia ante amenazas físicas y lógicas, asegurando también interoperabilidad, trazabilidad y buenas prácticas en infraestructuras críticas.

Estas instalaciones constituyen el nodo central de continuidad de operaciones críticas y de servicios clasificados, alojando servicios corporativos, plataformas de C2, sistemas de inteligencia, ciberdefensa y logística, por lo que requieren disponibilidad cercana al 100 %. Operan bajo esquemas normativos estrictos, destacando la categoría ENS-ALTA del ENS, que impone requisitos máximos en Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, junto con certificaciones como ISO/IEC 27001 [23].

Desde el punto de vista eléctrico, utilizan un esquema 2N puro, con acometidas, transformadores y líneas totalmente duplicadas, de modo que el 100 % de la carga pueda mantenerse con cualquiera de las dos líneas sin necesidad de conmutación o transferencia.

La climatización se basa en sistemas de precisión redundante N+1, basados en unidades de expansión directa, con control automático de temperatura y humedad. El aire se distribuye mediante plenum bajo suelo técnico, garantizando una impulsión uniforme y una eficiencia térmica elevada.

La electrónica de red se rige por la norma ISO/IEC 18598 [24], que define los requisitos de los sistemas de *Automated Infrastructure Management* (AIM). Estos sistemas permiten la administración inteligente del cableado, la integración con procesos de gestión de infraestructuras y la generación de alertas asociadas a la seguridad física y lógica del entorno. Se utilizan paneles y bandejas de parcheo inteligentes, así como armarios y cerramientos con protección electromagnética (TEMPEST) y resistencia ante pulso electromagnético de gran altitud (HEMP) [25], conforme a las directivas IEC 61000 [26] e ISO/IEC 11801 [27], garantizando confidencialidad incluso ante inteligencia de señales adversaria.

En conjunto, el CPD estratégico representa el nivel máximo de resiliencia y seguridad dentro del ecosistema TIC de defensa, tal y como se ilustra en el ejemplo de la Figura 2-1.

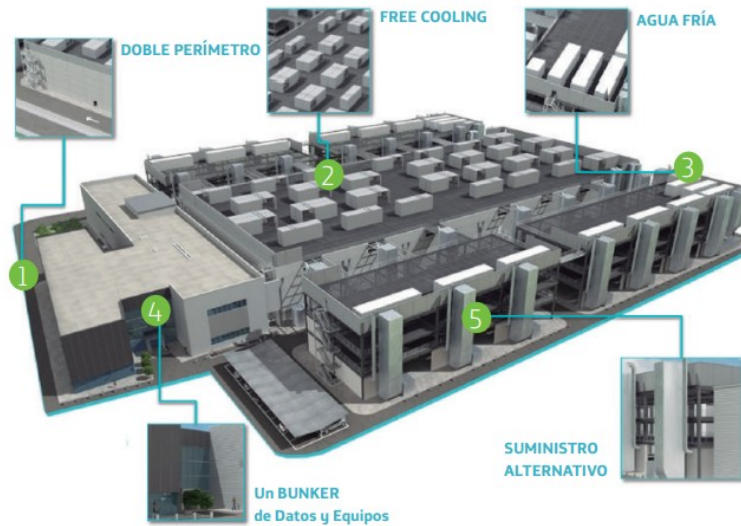


Figura 2-1: Alcalá Data Center [28].

2.1.2.2 CPD modular operacional

Los CPD modulares operacionales actúan como nodos intermedios que enlazan los niveles estratégico y táctico. Se despliegan en bases avanzadas o zonas seguras del teatro de operaciones, combinando infraestructura fija con módulos transportables. Su diseño se orienta a la escalabilidad, facilidad de mantenimiento y rapidez de despliegue, siguiendo modelos de *container data center* o módulos prefabricados. Diversos proveedores europeos especializados en infraestructuras críticas ofrecen soluciones modulares con equivalencia TIER III, adecuadas para despliegues militares y coherentes con el concepto OTAN de *deployable data center* definido en FMN Spiral 5, así como con la categoría ENS–MEDIA según el ENS.

Estas características estructurales reflejan configuraciones típicas ofrecidas por fabricantes europeos de CPD modulares, pudiendo variar según contrato y entorno operativo, pero ilustran adecuadamente los requisitos funcionales del nivel operacional.

Su estructura física, ilustrada en la Figura 2-2, se basa en contenedores metálicos de alta resistencia, generalmente configurados como módulos tipo *all in one* de altura variable. La envolvente está construida en acero al carbono con soldadura continua, paredes exteriores de chapa corrugada reforzada y techo embutido, garantizando resistencia mecánica y estanqueidad. Todo el conjunto recibe un tratamiento anticorrosivo C5-M (350 µm) conforme a la UNE–EN ISO 12944, adecuado para entornos marinos, ambientes corrosivos o bases avanzadas expuestas.



Figura 2-2: CPD modular en contenedor con dimensiones personalizadas (no-ISO) [29].

El diseño suele incorporar una estructura portante mediante vigas de perfil en I normalizado (IPN), que permite la superposición vertical de módulos o la adición escalonada de nuevos bloques funcionales. En la parte inferior se dispone un plenum técnico (habitualmente ≥ 75 cm) destinado al paso de canalizaciones eléctricas, redes y anillos de climatización. Este espacio cumple una función dual: facilita la sectorización térmica y actúa como barrera pasiva frente a inundaciones o impactos mecánicos.

A nivel eléctrico, los CPD operacionales emplean configuraciones de redundancia $2N$ parcial o $N+1$, apoyadas por sistemas UPS $2 \times (N+1)$ y distribución segmentada. La climatización suele resolverse mediante unidades $N+1$ optimizadas para espacios confinados, con controlador térmico distribuido y capacidad para soportar densidades de 12–17 kW por rack.

Estos CPD resultan idóneos para despliegues prolongados en bases avanzadas o centros logísticos, donde la infraestructura debe poder ampliarse, mantenerse y operar de forma autónoma con mínima obra civil y con medidas de seguridad proporcionales a la criticidad de la misión.

2.1.2.3 CPD táctico

El CPD Táctico representa la implementación militar del paradigma de *edge computing*, ofreciendo capacidades de procesamiento y almacenamiento cercanas al punto de necesidad. Representan el extremo de la movilidad y la eficiencia operativa dentro del ecosistema TIC de defensa. Su función es sostener capacidades esenciales de C2, inteligencia y comunicaciones en unidades desplegadas en primera línea, operando con recursos limitados y bajo condiciones ambientales adversas. Aunque de menor capacidad, mantienen principios equivalentes de redundancia lógica y aislamiento de cargas, aplicados dentro de las restricciones de espacio, energía y entorno propias del nivel táctico.

Estas infraestructuras suelen materializarse en servidores compactos, como el mostrado en la Figura 2-3, equipos hiperconvergentes de baja potencia o *appliances* reforzadas, integrables en cajas ruggedizadas tipo *pelican*, bastidores ligeros o plataformas vehiculares. Incorporan sistemas de refrigeración *in-row* de pequeña escala o soluciones de *cooling* por conducción/líquido de bajo mantenimiento. La protección física y ambiental se ajusta a los estándares MIL-STD-810H (vibración, choque, humedad, polvo, temperatura) [30] y MIL-STD-461G (compatibilidad electromagnética) [31], garantizando operatividad en condiciones extremas.



Figura 2-3: CPD táctico sobre HPE Edgeline EL8000 [32].

El suministro energético se optimiza mediante microrredes híbridas (diésel–solar–batería), cargadores inteligentes y mecanismos de *power gating* o apagado selectivo de módulos. Estas medidas buscan maximizar la autonomía y reducir el consumo en posiciones avanzadas, donde la logística de combustible o el acceso a generadores puede ser limitada.

Desde el punto de vista funcional, los CPD tácticos emplean virtualización ligera, micro-VM y contenedores minimalistas para ejecutar servicios críticos en entornos *DDIL*. Esto permite mantener capacidades esenciales incluso bajo pérdida parcial de conectividad con los niveles superiores, facilitando la sincronización diferida, la operación autónoma temporal y la resiliencia frente a interrupciones de red.

En este nivel, la prioridad es preservar la operatividad con el mínimo consumo, la máxima resiliencia y un tiempo de despliegue del orden de minutos. Estas infraestructuras encarnan los principios de sostenibilidad, modularidad y autonomía energética que exige la doctrina FMN para el borde táctico, adaptando las medidas de seguridad del ENS mediante el principio de proporcionalidad previsto en el ENS.

2.1.2.4 Representación gráfica y comparativa por niveles

En la Figura 2-4 se resume visualmente una aproximación a la jerarquía doctrinal de los CPD según su nivel de despliegue. Esta diferenciación no implica compartimentos estancos: la tendencia actual es la adopción de arquitecturas federadas, donde los tres niveles cooperan mediante sincronización dinámica de servicios, replicación segura de datos y gestión unificada, conformando una malla funcional continua acorde con los principios de interoperabilidad de la OTAN y la UE.



Figura 2-4: Clasificación doctrinal de los CPD en defensa por nivel de despliegue. Fuente: Elaboración propia mediante generación asistida.

Para dotar de concreción técnica a esta jerarquía, la Tabla 2-1 sistematiza los parámetros fundamentales de cada nivel. En ella se presentan las diferencias en infraestructura, tecnología y normativa, definiendo el perfil operativo que servirá de referencia para el análisis posterior.

Parámetro	Estratégico	Operacional	Táctico
Infraestructura	Fija de alta disponibilidad	Despliegue semipermanente	Nodos ligeros desplegables
Estructura física	Obra civil permanente	Contenedores modulares	Chasis ligero / ruggedizado
Tecnología de virtualización	Hipervisores tipo 1 (KVM, VMware ESXi, Xen)	Virtualización híbrida (hipervisores + contenedores)	Micro-VMs y contenedores minimalistas
Función principal	C2 estratégico, ciberdefensa, inteligencia	Enlace federado y redundante de misión	C2 táctico, despliegue rápido en entornos DDIL
Normativa aplicable	ENS-ALTA, ISO/IEC 27001, AC/35-D/2004, CCN-STIC-220, ISO/IEC 18598	ENS-MEDIA, FMN Spiral 5	MIL-STD-810H / 461, FMN Spiral 5

Tabla 2-1: Clasificación y características técnicas de los CPD por nivel de despliegue.

2.1.3 Condicionantes de los entornos operativos modernos

Los CPD contemporáneos deben mantener su operatividad en entornos caracterizados por tres condicionantes críticos: degradación de la conectividad, exigencias de ciberseguridad multinivel y sostenibilidad energética [7, 11]. Estos factores determinan el diseño técnico, la arquitectura de red y las políticas de operación, y han adquirido un papel central en doctrinas OTAN como *Mission Partner Environment* (MPE) [33], *Federated Mission Networking* (FMN) y en los marcos nacionales definidos por el ENS y las guías CCN-STIC.

2.1.3.1 Operación en entornos DDIL

La conectividad intermitente o degradada obliga a desplegar mecanismos de replicación local de servicios esenciales (autenticación, DNS, catálogos), sincronización asíncrona de datos y orquestadores capaces de funcionar en modo desconectado. La resiliencia autónoma es un requisito doctrinal clave para mantener la continuidad del mando y control.

Además, los despliegues en coalición y las misiones multinacionales requieren capacidades de *store-and-forward*, gestión tolerante a fallos, colas persistentes y mecanismos de coherencia eventual entre nodos federados. Estos principios permiten operar de manera sostenida incluso cuando la red troncal está interrumpida y posibilitan la validación diferida de transacciones cuando la conectividad se restablece. Este enfoque es coherente con las arquitecturas distribuidas orientadas al borde que se emplean en operaciones con alta movilidad o enlaces WAN inestables.

2.1.3.2 Seguridad multinivel

La coexistencia de dominios clasificados y no clasificados exige aislamiento lógico robusto, control de acceso reforzado y auditoría verificable. Se aplican principios de *zero trust*, segmentación por VLAN/VXLAN y cumplimiento estricto de los marcos normativos. Específicamente, se requiere la segregación robusta de dominios (medida [op.sep] del ENS) y la protección de redes (medida [op.net]), tal como detallan las guías CCN-STIC-220 y FMN Spiral 5. El equilibrio entre aislamiento, rendimiento y eficiencia resulta esencial para mantener la integridad de la información sin comprometer la operatividad.

Adicionalmente, en despliegues combinados se incorporan mecanismos de control reforzado de flujos como soluciones de transferencia controlada entre dominios, filtrado unidireccional, autenticación multifactor y autorización basada en atributos. La federación de identidades y el control granular sobre los patrones de acceso condicionan la arquitectura de virtualización y la distribución de cargas entre los niveles estratégico, operacional y táctico.

2.1.3.3 Sostenibilidad energética

Los despliegues prolongados imponen restricciones severas de consumo y reposición logística. La eficiencia se optimiza mediante consolidación dinámica de cargas, escalado adaptativo y empleo de hardware de bajo consumo (ARM, FPGA). Métricas como el M-PUE permiten evaluar la relación entre energía consumida y servicio efectivo, ajustada al contexto operativo. En el contexto OTAN, la disponibilidad energética se considera una capacidad operacional (*operational energy*) y no un recurso meramente logístico. Por ello, la sostenibilidad energética se integra como requisito doctrinal y factor decisivo en la planificación y despliegue de capacidades TIC militares.

Asimismo, el uso de microrredes híbridas gestionadas, baterías de ciclo profundo, distribución inteligente de carga y priorización energética basada en criticidad funcional permite maximizar la autonomía en escenarios con acceso limitado a combustible o generación. Técnicas como apagado selectivo, estados de bajo consumo y despliegues escalonados de módulos contribuyen a mantener servicios esenciales sin comprometer la continuidad operativa.

Estos tres vectores –conectividad degradada, seguridad multinivel y sostenibilidad energética– definen el marco de requisitos sobre el que se construyen las estrategias de virtualización y computación distribuida que se analizan en las secciones siguientes.

2.2 Principios y tecnologías de virtualización en entornos de Defensa

La virtualización constituye uno de los pilares tecnológicos fundamentales sobre los que se sustenta la transformación digital de la defensa. Su propósito esencial es desacoplar la ejecución de los servicios lógicos de la infraestructura física, habilitando una utilización eficiente de los recursos, una mayor flexibilidad en el despliegue y un control más seguro, trazable y energéticamente optimizado de los activos críticos. En el ámbito militar, esta capacidad trasciende la mera optimización técnica: se convierte en un elemento doctrinal que condiciona la resiliencia operativa, la interoperabilidad multinacional y la soberanía tecnológica.

La madurez alcanzada por la virtualización en la última década permite articular infraestructuras distribuidas y federadas, coherentes con los modelos doctrinales basados en nodos estratégicos, modulares operacionales y capacidades tácticas *edge*. En este contexto, la virtualización actúa simultáneamente como mecanismo de consolidación, aislamiento, automatización y despliegue rápido, permitiendo adaptar cada CPD a su función operativa sin perder coherencia con el marco normativo común.

Actualmente, el ecosistema de virtualización en defensa se estructura en torno a cuatro aproximaciones principales: máquinas virtuales completas, contenedores, micro-VM y *unikernels*. Cada una proporciona diferentes grados de aislamiento, rendimiento, eficiencia energética y facilidad de certificación, conformando un conjunto de tecnologías complementarias que permiten optimizar la respuesta de cada nivel de despliegue.

Además, la virtualización moderna se concibe como un conjunto transversal de mecanismos de abstracción aplicables a distintos niveles: CPU, red, almacenamiento, sistema operativo o servicio. Este enfoque resulta especialmente valioso en entornos DDIL, donde la continuidad operativa depende de la capacidad del nodo para operar temporalmente de forma autónoma, mantener dominios segregados y soportar sincronización diferida.

2.2.1 Fundamentos técnicos y niveles de virtualización

La virtualización introduce una capa de abstracción entre el hardware físico y los servicios que se ejecutan sobre él, tal como se ilustra en la Figura 2-5. Este principio se materializa mediante hipervisores, motores de contenedores, funciones de red virtualizadas (NFV), sistemas de almacenamiento definido por software (SDS) y mecanismos de segmentación lógica avanzada.

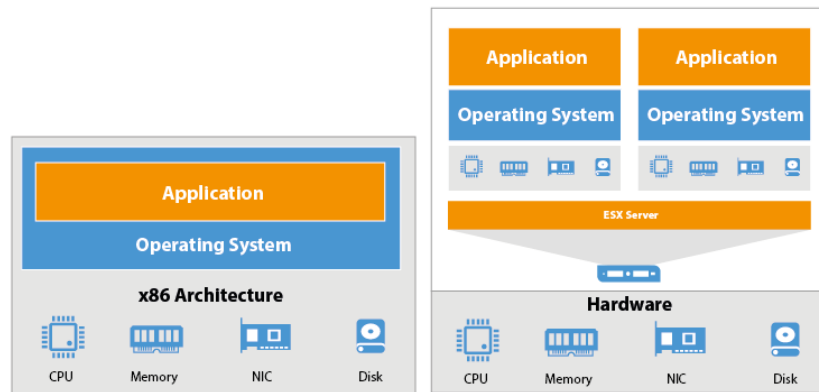


Figura 2-5: Diferencia entre arquitectura física y virtual [34].

Esta abstracción no se limita al servidor, sino que se extiende a la red y al almacenamiento, convergiendo en el paradigma de Infraestructura Definida por Software (SDI). Bajo este modelo, el CPD completo se gestiona como código, desacoplado del hardware físico. A continuación, la Tabla 2-2 detalla las tecnologías específicas que habilitan cada una de estas capas funcionales.

Tipo de virtualización	Tecnologías representativas	Casos de uso típicos
CPU	Intel VT-x, AMD-V, Xen, KVM, Hyper-V	Consolidación de servidores y aislamiento fuerte
Memoria	Balloon drivers, KSM, EPT, NUMA	Overcommit controlado, optimización <i>multi-tenant</i> y reducción de huella energética
Almacenamiento	LVM, ZFS, Ceph	Tolerancia a fallos y aprovisionamiento dinámico
Red	Open vSwitch, VXLAN, SR-IOV, Calico	SDN, segmentación por dominios, redes <i>overlay</i> en operaciones multinacionales
E/S	IOMMU, VFIO, DPDK	Aceleración criptográfica, uso compartido seguro de GPU/TPM y baja latencia en enlaces de misión
Sistema operativo	Docker, LXC, Podman, Kubernetes, OpenShift	Microservicios, despliegues rápidos, CI/CD, servicios desacoplados
Escritorios y aplicaciones	VDI, Citrix, Horizon	Puestos de mando virtualizados y simuladores
Datos	Denodo, Apache Drill, Teiid, Red Hat DV	Federación de fuentes y acceso seguro y unificado
FaaS	AWS Lambda, Knative, OpenFaaS	<i>Edge computing</i> y automatización táctica

Tabla 2-2: Niveles de virtualización y tecnologías representativas.

La combinación de estos mecanismos permite diseñar arquitecturas altamente flexibles, capaces de adaptarse a la misión y a la disponibilidad energética. Esta versatilidad resulta crítica para superar la rigidez de las infraestructuras heredadas (*legacy*), habilitando la redistribución dinámica de la capacidad de cómputo para asegurar los servicios más críticos ante situaciones de saturación o contingencia.

Sin embargo, en entornos militares, esta agilidad operativa no puede comprometer la integridad del sistema. Estos niveles de virtualización deben coexistir bajo requisitos estrictos de auditoría continua, particionado fuerte y control de acceso granular, tal como establecen las medidas de operación, protección y explotación del ENS y las guías técnicas asociadas. De este modo, la virtualización actúa como garante técnico de la soberanía del dato, permitiendo mantener la continuidad de la cadena de mando incluso sobre infraestructuras degradadas.

2.2.2 Hipervisores y máquinas virtuales

Las máquinas virtuales representan el modelo más consolidado y seguro de virtualización. A través de hipervisores de tipo 1 (*bare-metal*), como KVM, Xen o VMware ESXi, se crean entornos completamente aislados, cada uno con su propio sistema operativo y recursos virtuales dedicados. Esta robustez las convierte en la base de los CPD estratégicos, donde la disponibilidad y la segregación de dominios son prioritarias.

Su principal fortaleza reside en la compatibilidad con los marcos normativos. La Guía CCN-STIC-220 [6] detalla los controles para asegurar hipervisores y el aislamiento entre VMs, abordando medidas clave del Anexo II del ENS [5] tales como op.exp.5 (*Gestión de la capacidad*), op.acc.1 (*Control de acceso*) o [op.sep.1/2] (*Particionado y segregación de redes*). Esta base de cumplimiento es indispensable para la acreditación en categoría alta del ENS, garantizando a su vez la convergencia con las directivas de seguridad de la OTAN (como la AC/35-D/2004 [35]) y estándares internacionales (ISO/IEC 27001 [23]).

Ventajas:

- Aislamiento total entre cargas de distinta clasificación.
- Alta compatibilidad con normas y certificaciones de seguridad.
- Madurez tecnológica y soporte estable a largo plazo.

Limitaciones:

- Elevado consumo energético y sobrecarga de gestión.
- Escasa flexibilidad en entornos móviles o de campaña.
- Dependencia de infraestructuras fijas o semipermanentes.

2.2.3 Contenedores

Los contenedores representan un paradigma más ligero de virtualización, ejecutando aplicaciones en espacios aislados dentro del mismo sistema operativo. Comparten el *kernel* del anfitrión, lo que reduce drásticamente la huella de memoria y acelera los tiempos de despliegue. Tecnologías como Docker, LXC o Podman permiten ejecutar cientos de instancias por nodo, mientras que herramientas como Kubernetes u OpenShift facilitan su orquestación y gestión a gran escala.

En operaciones de defensa, los contenedores permiten desplegar servicios modulares en entornos operacionales o tácticos, favoreciendo la escalabilidad horizontal y la portabilidad entre dominios aliados. Sin embargo, su menor aislamiento —debido al *kernel* compartido, un riesgo explícitamente abordado en la Guía CCN-STIC-652A (Apdo. 4.2 Riesgos asociados) [36]— requiere políticas de seguridad reforzadas (como perfiles Seccomp/AppArmor, medida [op.pl.5] del ENS [5]) y auditoría continua, conforme a los requisitos FMN Spiral 5 para entornos operacionales.

Ventajas:

- Arranque rápido (1–3 segundos) y alta densidad de instancias.
- Portabilidad entre infraestructuras heterogéneas.
- Idóneos para microservicios, CI/CD y despliegues tácticos.

Limitaciones:

- Aislamiento más débil frente a VM tradicionales.
- Riesgo de vulnerabilidades en el *kernel* compartido.
- Complejidad en la gestión de secretos y autenticaciones.

2.2.4 Micro-VM y virtualización ligera

Las micro-VM constituyen un punto intermedio entre las máquinas virtuales y los contenedores. Utilizan hipervisores ultraligeros, como *Firecracker* o *Kata Containers*, capaces de lanzar entornos aislados en menos de medio segundo y con una huella mínima de memoria. Su nivel de aislamiento es comparable al de las VM, pero su consumo energético es sensiblemente menor.

Estas propiedades las hacen idóneas para CPD tácticos y nodos *edge*, donde la continuidad de servicio y la seguridad deben equilibrarse con limitaciones energéticas. Desde el punto de vista de la ciberseguridad, su ventaja radica en la reducción de la *Trusted Computing Base* (TCB) [37]: al emular solo los dispositivos esenciales, minimizan drásticamente la superficie de ataque respecto a una VM tradicional. Su adopción en defensa está en fase de validación dentro de programas OTAN y europeos de computación distribuida.

Ventajas:

- Aislamiento equiparable al de las VM tradicionales con menor TCB.
- Bajo consumo energético y arranque instantáneo.
- Integración transparente con orquestadores de contenedores.

Limitaciones:

- Menor madurez y falta de marcos normativos de acreditación específicos.
- Menor compatibilidad con sistemas operativos complejos.
- Ecosistema en evolución y documentación aún limitada.

2.2.5 Unikernels: virtualización especializada

Los *unikernels* representan la virtualización extrema: combinan el código de la aplicación con un núcleo mínimo del sistema operativo en una única imagen ejecutable. Eliminan componentes innecesarios, reduciendo la superficie de ataque y los tiempos de arranque. Estas propiedades los hacen especialmente adecuados para funciones críticas y dedicadas, como cifrado, filtrado o monitorización segura en tiempo real.

Aunque su adopción en defensa es aún incipiente, su potencial para sistemas embebidos, satelitales o de sensores tácticos es elevado, especialmente en misiones con alta exigencia de eficiencia energética y seguridad.

2.2.6 Comparativa y aplicabilidad en defensa

Para visualizar las diferencias estructurales que justifican los distintos niveles de eficiencia y sobrecarga (F_{virt}), la Figura 2-6 compara la pila tecnológica de cada solución. La altura de la pila representa la sobrecarga estructural (F_{virt}), que disminuye desde la VM tradicional hasta el *unikernel*, reflejando cómo la eliminación progresiva de capas intermedias (sistemas operativos invitados, hipervisores pesados) reduce el consumo de recursos y también su superficie de ataque.

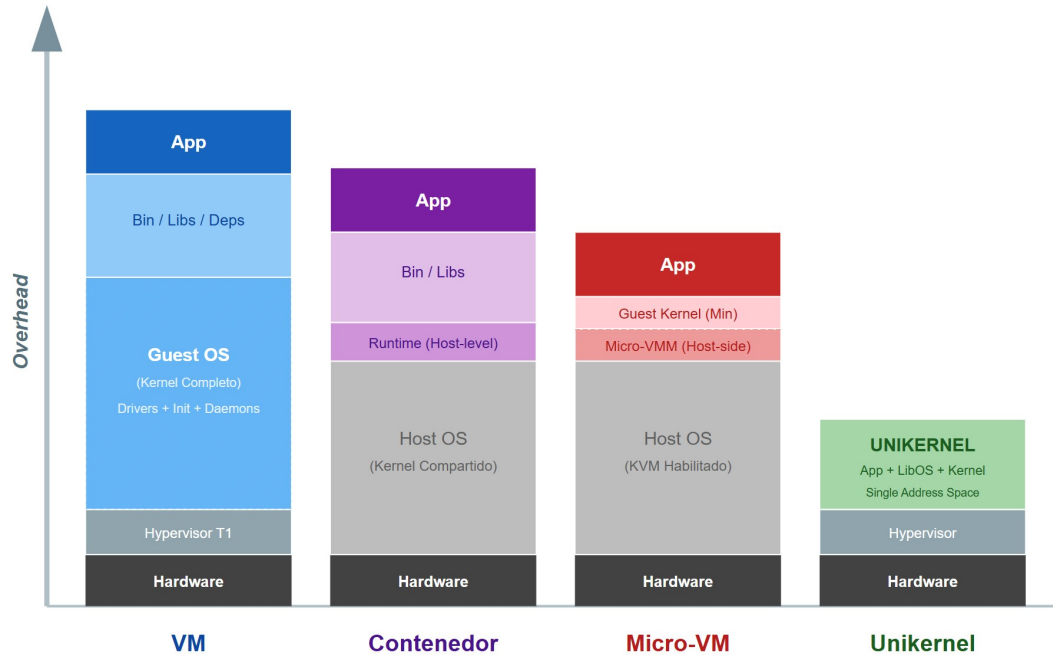


Figura 2-6: Comparativa de las pilas de virtualización y reducción de la sobrecarga. Fuente: Elaboración propia.

La Tabla 2-3 sintetiza las principales características de las tecnologías de virtualización analizadas. Es importante distinguir entre la **densidad de recursos** (capacidad de alojar instancias en reposo, donde el ahorro puede llegar al 60 %) y la **eficiencia en ejecución** (*overhead* de CPU/RAM activa), que será la base para el cálculo del M-PUE en el Capítulo 5.

Asimismo, se incorpora una valoración del nivel de madurez tecnológica mediante la escala *Technology Readiness Level* (TRL)¹. Este factor resulta determinante para evaluar la viabilidad de adopción inmediata en sistemas críticos de defensa frente a soluciones experimentales.

Criterio	VM	Contenedores	Micro-VM	Unikernels
Tiempo de arranque	30–60 s	1–3 s	<0.5 s	<1 s
Consumo energético relativo	1.0	0.6	0.4	0.3
Aislamiento y seguridad	Muy alto	Medio	Alto	Muy alto
Madurez (TRL est.)	Alta (TRL 9)	Alta (TRL 8-9)	Media (TRL 6-7)	Baja (TRL 4-5)
Compatibilidad ENS/CCN-STIC	Consolidada	Parcial	En estudio	No definida
Adecuación a entornos DDIL	Media	Alta	Muy alta	Alta
Uso predominante	CPD estratégicos	Nodos operacionales	Nodos tácticos	Funciones dedicadas

Tabla 2-3: Comparativa de tecnologías de virtualización y nivel TRL estimado en defensa.

¹El nivel de madurez tecnológica (TRL) se basa en la escala oficial definida por la Comisión Europea en los Anexos Generales del programa Horizon Europe (Work Programme 2023-2025), adoptada mediante Decisión C(2025) 2779 [38]: TRL 9 (Probado en entorno operativo real), TRL 7-8 (Validado/Cualificado en entorno relevante), TRL 5-6 (Validado/Demostrado en entorno relevante), TRL <5 (Desarrollo experimental).

2.2.7 Síntesis doctrinal

Las tecnologías de virtualización no deben considerarse excluyentes, sino complementarias dentro del ecosistema TIC de defensa. Las máquinas virtuales aportan estabilidad y acreditación formal; los contenedores, agilidad y escalabilidad; las micro-VM, equilibrio entre aislamiento y eficiencia; y los *unikernels*, máxima optimización y especialización.

En conjunto, estas tecnologías permiten diseñar arquitecturas federadas, seguras y sostenibles, capaces de mantener la continuidad del servicio en condiciones adversas. Este marco constituye la base tecnológica para desarrollar los modelos energéticos y metodológicos analizados en los capítulos siguientes.

2.3 Principios de eficiencia energética en infraestructuras virtualizadas

La eficiencia energética constituye un eje estratégico en el diseño y operación de los CPD de defensa. En entornos donde la disponibilidad eléctrica condiciona la continuidad de misión, optimizar el consumo adquiere un valor tanto técnico como doctrinal. Según el grupo de trabajo OTAN IST-208, el consumo asociado a sistemas eléctricos y de climatización en CPD desplegados puede representar entre el 50 % y 60 % del gasto energético total durante operaciones prolongadas.

La virtualización actúa como catalizador de eficiencia al permitir una utilización más racional de la infraestructura física. No obstante, su impacto real depende del grado de consolidación alcanzado, del equilibrio entre carga y consumo y del diseño de la arquitectura energética. En entornos militares, estos factores se integran con las restricciones de seguridad, movilidad y resiliencia impuestas por la doctrina operativa y por los marcos normativos nacionales y aliados.

2.3.1 Factores determinantes del consumo energético

El consumo total de un CPD virtualizado puede descomponerse, siguiendo el estándar industrial definido por The Green Grid [16], en dos grandes bloques: la energía consumida directamente por el equipamiento TI y la energía consumida por la infraestructura que le da soporte. Para un análisis más detallado en el contexto militar, este consumo se desglosa en:

- **Consumo informático:** energía requerida por los servidores físicos (CPU, memoria, almacenamiento local y GPU), equipos de red, almacenamiento externo y equipamiento suplementario como KVM o consolas de gestión.
- **Consumo de infraestructura:** energía destinada a los sistemas que soportan al equipamiento TI, incluyendo:
 - Entrega de potencia: SAI/UPS, PDU de sala, generadores, baterías y pérdidas en la distribución eléctrica externa al equipamiento TI.
 - Sistemas de refrigeración: *chillers*, torres, bombas, CRAH/CRAC o unidades DX.
 - Iluminación del CPD.
- **Pérdidas de conversión:** transformadores, convertidores o microrredes de campaña.
- **Sobrecarga virtual:** hipervisores, orquestadores o mecanismos de aislamiento lógico.

La contribución relativa de cada componente varía según el tipo de despliegue, como se muestra en la Tabla 2-4. En entornos estratégicos, el consumo auxiliar puede superar el 40 % del total, mientras que en despliegues tácticos predominan las pérdidas de conversión y la eficiencia de los servidores.

Componente	CPD estratégico	CPD operativo	CPD táctico
Consumo informático	45–55 %	55–65 %	65–75 %
Infraestructura (climatización, UPS)	35–45 %	25–35 %	10–20 %
Pérdidas eléctricas y conversión	5–8 %	7–10 %	10–15 %
Sobrecarga de virtualización	5–7 %	5–8 %	5–10 %

Tabla 2-4: Distribución estimada del consumo energético por tipo de CPD.

Optimizar el rendimiento energético no implica solo reducir consumo, sino mejorar la relación entre energía utilizada y servicio computacional efectivo. En este sentido, indicadores como el PUE de The Green Grid [16] constituyen la base para evaluar dicha relación.

2.3.2 Mecanismos de eficiencia en entornos virtualizados

La virtualización introduce varios mecanismos técnicos que permiten reducir el consumo energético global de los CPD, aunque con impactos distintos según el tipo de tecnología y el escenario operativo.

- **Consolidación dinámica de cargas.** Reagrupa máquinas virtuales o contenedores en menos nodos físicos durante baja demanda, permitiendo apagar o hibernar los restantes. En entornos estables puede reducir el consumo hasta un 30–40 %, mientras que en entornos DDIL requiere políticas predictivas para evitar pérdida de disponibilidad.
- **Escalado adaptativo.** Ajusta capacidad de cómputo según métricas de carga, temperatura o disponibilidad energética. Hipervisores y orquestadores (*Kubernetes*, *OpenShift*) implementan escalado automático que optimiza CPU y memoria en tiempo real, evitando desperdicio energético.
- **Apagado selectivo y *power capping*.** Desactiva componentes no críticos inactivos y limita el consumo máximo a nivel de servidor o rack, estabilizando microrredes tácticas o generadores portátiles.
- **Asignación energética consciente.** Mediante políticas *energy-aware scheduling*, los orquestadores seleccionan el nodo de ejecución considerando rendimiento térmico y eficiencia energética, fundamento de la orquestación sostenible en infraestructuras federadas.

2.3.3 Eficiencia por tecnología de virtualización

La eficiencia energética depende del equilibrio entre consolidación y sobrecarga introducida por la capa de virtualización. La Tabla 2-5 muestra valores medios observados, considerando el consumo relativo respecto a un entorno nativo sin virtualización. Este diferencial de eficiencia será formalizado en el Factor de Virtualización (F_{virt}) que se define en la métrica M-PUE (Sección 2.4).

Tecnología	Sobrecoste energético (%)	Densidad (instancias/nodo)	Escalabilidad
VM	15–25	10–15	Media
Contenedores	5–10	50–100	Alta
Micro-VM	8–12	30–60	Alta
<i>Unikernels</i>	3–8	80–120	Muy alta

Tabla 2-5: Sobrecoste y densidad energética media por tecnología de virtualización.

En entornos estratégicos, donde la energía es abundante pero la seguridad prioritaria, las VM siguen siendo preferentes. En cambio, los despliegues operacionales o tácticos –más limitados energéticamente– se benefician de contenedores, micro-VM o *unikernels*, que ofrecen mejor relación entre rendimiento, aislamiento y consumo.

2.3.4 Marco normativo y sostenibilidad operativa

La OTAN y la Unión Europea incorporan de forma creciente la sostenibilidad energética como un vector esencial de resiliencia, interoperabilidad y autonomía estratégica. Iniciativas como el *NATO Green Defence Framework* [39, 40] o el programa E2C [12] promueven arquitecturas distribuidas, eficientes y modulares, orientadas a reducir la huella logística en operaciones prolongadas y a garantizar la autosuficiencia energética de las infraestructuras TIC desplegadas.

En el ámbito nacional, esta tendencia se alinea con las políticas de eficiencia y sostenibilidad impulsadas por el Ministerio de Defensa y por los planes de transición ecológica en el sector público. En este contexto, la virtualización de infraestructuras críticas se perfila como el habilitador técnico necesario para conciliar la creciente demanda de potencia de cálculo con los exigentes objetivos de reducción de huella de carbono y costes operativos.

El *White Paper 49* de The Green Grid [16] refuerza este enfoque al establecer las mejores prácticas de medición para el *Power Usage Effectiveness* (PUE), destacando la importancia de la coherencia en los límites de medición (*measurement boundaries*), la trazabilidad temporal y la preferencia por métricas basadas en energía (kWh) frente a potencia (kW). Además, introduce el principio de *total energy accountability*, que recomienda contabilizar las pérdidas por transporte, conversión y almacenamiento cuando sea relevante para la comparabilidad de instalaciones. Estos principios metodológicos han sido adoptados en la definición de la métrica M-PUE, adaptándolos al contexto militar mediante la introducción de factores de corrección que reflejan la variabilidad operativa, ambiental y logística de los CPD de defensa.

Debe aclararse que el ENS tiene un alcance centrado exclusivamente en la ciberseguridad y la protección de la información —garantizando la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de los servicios y sistemas de información—. Aunque el ENS incluye medidas relacionadas con la continuidad del suministro eléctrico y la protección de las instalaciones, estas se contemplan desde la perspectiva de la seguridad, no de la eficiencia energética o el impacto ambiental. Por tanto, la evaluación energética se rige por marcos complementarios, como las normas de gestión energética (*ISO 50001*) [41], las estrategias de sostenibilidad TIC o las directrices de contratación pública verde, que pueden integrarse de forma coordinada con los requisitos de seguridad establecidos por el ENS y las guías CCN-STIC.

En consecuencia, la evaluación integral de las infraestructuras virtualizadas de defensa debe combinar tres dimensiones complementarias:

- **Métricas técnicas de eficiencia energética**, tales como el *PUE* y su extensión M-PUE.
- **Resiliencia y continuidad operativa**, garantizando la disponibilidad bajo condiciones degradadas.
- **Cumplimiento normativo**, asegurando la alineación con marcos de ciberseguridad y gobernanza.

Este enfoque unificado permite valorar el rendimiento de los CPD no solo por su consumo eléctrico, sino también por su sostenibilidad operativa, su trazabilidad normativa y su capacidad para mantener la misión bajo condiciones cambiantes. De esta forma, la eficiencia energética trasciende su dimensión técnica y se consolida como un criterio estratégico dentro del modelo de sostenibilidad y superioridad operativa de las Fuerzas Armadas.

2.4 Propuesta de métrica energética: M-PUE

El indicador PUE, desarrollado por The Green Grid, se ha consolidado como la referencia internacional para evaluar la eficiencia energética de los CPD. Se define como la relación entre el consumo energético total del CPD y la energía utilizada directamente por el equipamiento informático. En su formulación clásica se expresa como:

$$\text{PUE} = \frac{E_{total}}{E_{TI}} \quad (2.1)$$

donde E_{total} representa la energía total suministrada al CPD (medida en la acometida) y E_{TI} la consumida por servidores, redes y almacenamiento. Un valor ideal de PUE se aproxima a 1, lo que indica que la totalidad de la energía se destina al procesamiento útil.

The Green Grid [16] detalla tres niveles de precisión (Nivel 1 a Nivel 3) según la granularidad de las mediciones, destacando la necesidad de trazabilidad y consistencia temporal para comparar resultados.

Sin embargo, el PUE tradicional fue concebido para entornos civiles, estables y con infraestructura permanente. Su aplicabilidad a entornos militares –caracterizados por movilidad, fuentes híbridas, climatología variable y exigencias doctrinales– resulta limitada. Por ello, se propone una extensión del concepto: el M-PUE, que introduce factores de corrección operativos, ambientales y tecnológicos para representar fielmente la eficiencia de infraestructuras de defensa.

El M-PUE amplía el modelo original siguiendo las recomendaciones de trazabilidad y normalización expuestas en el *White Paper 49* [16], garantizando comparabilidad entre mediciones y niveles de precisión equivalentes a los *Measurement Levels* (Nivel 1-3) definidos en dicho estándar.

2.4.1 Limitaciones del PUE convencional en entornos de defensa

La aplicación del PUE clásico en el ámbito militar presenta varias limitaciones técnicas y doctrinales, algunas de ellas señaladas por el propio *White Paper 49* [16] para contextos no ideales:

- No considera la variabilidad de las fuentes energéticas (diésel, baterías, fotovoltaica o microrredes híbridas).
- Ignora las pérdidas derivadas de conversión, transporte o almacenamiento en sistemas desplegados.
- No incorpora la sobrecarga energética introducida por tecnologías de virtualización o consolidación dinámica. De hecho, se advierte que una optimización del TI (ej. virtualización) puede empeorar el PUE si la infraestructura (ej. refrigeración) no se ajusta proporcionalmente.
- No ajusta los resultados según condiciones ambientales extremas (temperatura, altitud, humedad), aunque el clima y la ubicación afectan drásticamente al PUE, dificultando la comparación.
- No define con claridad los límites de medición ni los requisitos de integridad de datos necesarios para una comparación fiable entre instalaciones.

Además, el *White Paper 49* [16] establece que el valor del PUE no puede ser inferior a 1.0, ya que toda instalación consume inevitablemente energía adicional a la destinada al equipamiento TI. Asimismo, el modelo no contempla la reutilización o cogeneración del calor residual –por ejemplo, para climatización o generación secundaria–, aspecto que debe evaluarse mediante métricas complementarias como el *Energy Reuse Effectiveness* (ERE).

En entornos estratégicos donde existe recuperación térmica (por ejemplo, reutilización del calor de servidores para apoyar sistemas HVAC), la eficiencia térmica no debe “mejorar” el PUE, sino reportarse de forma independiente mediante métricas complementarias como el ERE, conforme a lo indicado en el *White Paper 49* [16]. Aunque estos mecanismos son poco frecuentes en despliegues tácticos, sí resultan relevantes en CPD permanentes de defensa, donde podrían integrarse en futuras ampliaciones del modelo M-PUE.

Por otra parte, el propio *White Paper 49* [16] recuerda que las mediciones del PUE deben estar asociadas a fronteras de medida claramente definidas y a series temporales continuas, recomendando un muestreo máximo de 15 min y la utilización de valores energéticos (kWh) frente a potencias instantáneas (kW). Estos criterios son esenciales para garantizar trazabilidad y comparabilidad entre instalaciones, especialmente cuando se pretende establecer equivalencias con la métrica M-PUE.

En síntesis, estas carencias pueden generar evaluaciones sesgadas: un CPD táctico, eficiente dentro de su contexto operativo, podría parecer menos eficiente que un CPD fijo si no se normalizan sus condiciones de operación. La métrica M-PUE corrige esta distorsión al incorporar factores de ajuste derivados del entorno, la virtualización y la logística, ofreciendo una evaluación más representativa y auditable.

2.4.2 Definición formal del M-PUE

Las limitaciones del indicador PUE tradicional en escenarios no estacionarios —especialmente cuando existen microrredes aisladas, variaciones térmicas severas y sobrecargas asociadas a la virtualización— requieren una métrica capaz de capturar los efectos operativos propios de los CPD desplegados. Siguiendo los principios de *energy accountability* establecidos por The Green Grid [16], se propone la extensión M-PUE.

A diferencia del PUE convencional, el M-PUE incorpora factores de penalización que modelan las ineficiencias exógenas al equipamiento TI. Concretamente, se definen coeficientes para la degradación térmica ambiental (F_{amb}), las pérdidas por conversión en generadores tácticos (F_{gen}), la carga logística asociada al transporte de combustible en zona de operaciones (F_{log}) y la sobrecarga de virtualización (F_{virt}).

Para dotar al modelo de rigor técnico y evitar la arbitrariedad en la simulación, los rangos de penalización asignados a todos los factores (F_{virt} , F_{gen} , F_{amb} , F_{log}) se han derivado de la síntesis de estándares industriales y militares de referencia, tal como se detalla en la Tabla 2-6.

Factor	Rango Típico	Fuente de Referencia / Estándar
F_{amb}	1.0 – 1.4	ASHRAE TC 9.9 (Clases A3/A4): Define la degradación de eficiencia de refrigeración al operar fuera de la ventana recomendada (18 – 27°C) en despliegues sin suelo técnico.
F_{gen}	1.0 – 1.3	MIL-STD-810H / STANAG 4010: Basado en curvas de eficiencia de generadores tácticos diésel, que presentan pérdidas del 10–30 % por conversión AC/DC y operación a carga parcial.
F_{virt}	1.01 – 1.25	Benchmarks Industriales (SPECvirt / AWS): Agregación de estudios de rendimiento comparado entre KVM (overhead ≈ 20 %), Contenedores (Docker) y Micro-VMs (Firecracker ≈ 5 %).
F_{log}	1.0 – 1.5	DoD FBCF: Estimación del <i>Fully Burdened Cost of Fuel</i> . El rango abarca desde el suministro por red comercial estándar (1.0) hasta el coste energético de transportar combustible a zona de operaciones (1.5), incluyendo convoyes y protección de fuerza.

Tabla 2-6: Justificación técnica y fuentes de referencia para los rangos de penalización del M-PUE.

Es importante señalar que, para la aplicación del modelo, se adopta un criterio de diseño conservador (*worst-case scenario*). Esto implica seleccionar los valores superiores de los rangos de penalización documentados para garantizar la viabilidad operativa de la solución incluso en las condiciones más adversas. La formulación matemática resultante es:

$$M-PUE = \frac{E_{total}}{E_{TI}} \times (F_{gen} \times F_{amb} \times F_{log} \times F_{virt}) \quad (2.2)$$

Los cuatro coeficientes (F_i) corresponden a los factores de penalización desglosados en la Tabla 2-6. Cabe destacar que todos actúan como multiplicadores ≥ 1 , garantizando que el resultado nunca sea inferior a la unidad y manteniendo la coherencia física con el modelo estándar de The Green Grid.

2.4.3 M-PUE frente a métricas de sostenibilidad civil

El PUE, definido por The Green Grid [16] y estandarizado en ISO/IEC 30134-2 [42], constituye el indicador de referencia para evaluar la eficiencia energética de los CPD. Sin embargo, su ámbito de aplicación se limita a instalaciones fijas con condiciones de operación estables, lo que reduce su utilidad en escenarios desplegados o tácticos caracterizados por variabilidad energética, climatológica y logística.

En paralelo, la industria civil ha ampliado el marco de sostenibilidad mediante métricas complementarias:

- **Water Usage Effectiveness (WUE)**, ISO/IEC 30134-9 [43]: eficiencia en el uso de agua.
- **Carbon Usage Effectiveness (CUE)**, ISO/IEC 30134-8 [44]: huella de carbono asociada al consumo eléctrico.
- **Energy Reuse Factor (ERF)**, ISO/IEC 30134-6 [45]: capacidad de recuperación y reutilización de energía térmica.

Estas métricas son altamente pertinentes en CPD estratégicos (E1), donde la sostenibilidad ambiental constituye un objetivo prioritario. No obstante, en entornos operacionales y tácticos (E2-E3) presentan limitaciones al no considerar factores críticos como la disponibilidad y transporte del combustible, la estabilidad de las microrredes, la penalización térmica bajo condiciones extremas o el impacto directo de la virtualización sobre el consumo. Por este motivo, la métrica M-PUE propuesta en este trabajo extiende el PUE clásico incorporando factores propios del contexto militar como los comentados en el apartado anterior.

El M-PUE no sustituye a las métricas de sostenibilidad civil, sino que las complementa como indicador de sostenibilidad operativa y logística adaptado a escenarios DDIL. Su incorporación permite evaluar tecnologías no solo por su consumo energético, sino por su impacto sobre la autonomía, la resiliencia y la eficiencia logística del despliegue, dimensiones que resultan esenciales en los análisis doctrinales desarrollados en los capítulos siguientes.

2.4.4 Interpretación y clasificación operativa

En el ámbito de la infraestructura computacional de hiperescala, referentes industriales como Google han logrado estandarizar un PUE promedio de 1.09, acercándose al ideal teórico mediante tecnologías avanzadas de enfriamiento y gestión de cargas [46]. Sin embargo, la traslación directa de estas métricas al ámbito de la defensa resulta inviable. A diferencia de los entornos civiles estáticos, las operaciones tácticas priorizan la supervivencia, la movilidad y la continuidad del servicio sobre la optimización energética pura, lo que introduce penalizaciones térmicas inevitables.

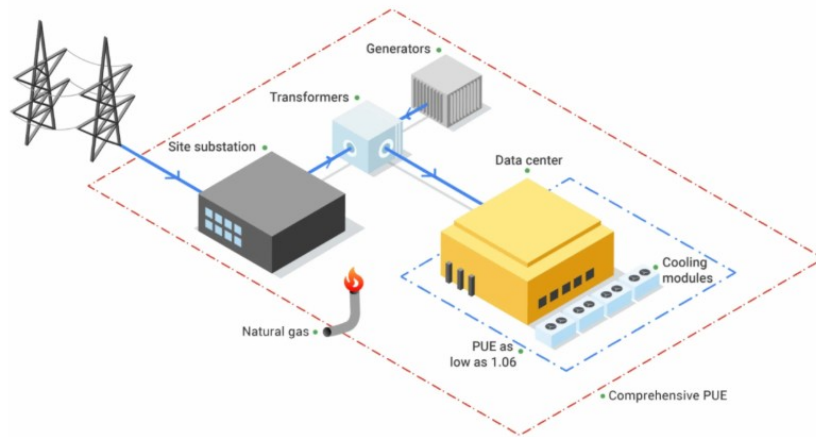


Figura 2-7: Medición de PUE en los CPD de Google. [46]

Consecuentemente, aunque el M-PUE mantiene la lógica direccional del PUE clásico (donde valores menores indican mayor eficiencia), su escala debe interpretarse bajo un marco adaptado a la realidad logística del teatro de operaciones. La Tabla 2-7 propone una clasificación calibrada que correlaciona el valor del indicador con las limitaciones físicas del entorno de despliegue.

Valor M-PUE	Clasificación	Tipo de entorno
1.0 – 1.3	Excelente	CPD estratégico fijo con control térmico estable y suministro energético continuo.
1.3 – 1.6	Bueno	CPD modular operacional con fuentes híbridas y variabilidad ambiental moderada.
1.6 – 2.0	Aceptable	Despliegue táctico con limitaciones energéticas o térmicas significativas.
> 2.0	Crítico	Operaciones en entornos extremos con alta penalización ambiental o baja calidad de energía.

Tabla 2-7: Clasificación orientativa del M-PUE según el entorno de operación.

Es importante notar que el objetivo del indicador no es obtener un valor absoluto óptimo, sino proporcionar una métrica proporcional al contexto. De acuerdo con las recomendaciones de The Green Grid [16], el M-PUE debe analizarse preferiblemente como una serie temporal (media móvil o análisis estacional) y no como un dato aislado, permitiendo así identificar tendencias de degradación o mejora operativa dentro de las restricciones de cada misión.

2.4.5 Ejemplo aplicado

Para ilustrar la aplicabilidad del modelo, se analiza un caso representativo de un módulo de computación militar desplegado en entorno operacional con recursos energéticos limitados. Los valores utilizados se inspiran en escenarios documentados por el grupo de trabajo OTAN IST-208 y en los principios de medición definidos por The Green Grid [16].

- Energía total suministrada: $E_{total} = 4.8 \text{ kWh}$
- Energía consumida por servidores y equipos TIC: $E_{TI} = 3.0 \text{ kWh}$
- Fuente energética: microred diésel-solar híbrida con pérdidas de conversión del 5 % $\rightarrow F_{ent} = 1.05$

- Condiciones ambientales adversas (45 °C, 80 % humedad relativa) $\rightarrow F_{amb} = 1.10$
- Virtualización basada en contenedores ligeros $\rightarrow F_{virt} = 1.10$
- Logística optimizada con almacenamiento local y autonomía parcial $\rightarrow F_{log} = 1.05$

Aplicando la ecuación general del modelo:

$$\text{M-PUE} = \frac{4.8}{3.0} \times 1.05 \times 1.10 \times 1.10 \times 1.05 \approx \mathbf{2.13}$$

El valor resultante (M-PUE ≈ 2.13) es coherente con un escenario operacional sometido a:

- penalización térmica elevada,
- pérdidas de microrred híbrida,
- overhead de virtualización ligera,
- y logística energética con transporte y almacenamiento.

A diferencia del PUE clásico:

$$\text{PUE} = \frac{4.8}{3.0} = 1.6$$

El M-PUE representa una métrica físicamente correcta (≥ 1.0), auditable e interpretable en términos operativos, evitando resultados imposibles como los que podrían aparecer al aplicar factores menores que 1.

2.4.6 Relevancia doctrinal y de interoperabilidad

El M-PUE puede integrarse como instrumento operativo en los marcos doctrinales OTAN y nacionales. En particular:

- Permite evaluar la viabilidad energética de nodos federados conforme a la doctrina *Federated Mission Networking* (FMN).
- Facilita comparaciones entre infraestructuras heterogéneas bajo criterios de sostenibilidad y eficiencia logística.
- Contribuye al cumplimiento del *Plan de Transición Energética del Ministerio de Defensa* y de las directrices CCN-STIC-220 en materia de gestión sostenible de infraestructuras TIC.
- Promueve la trazabilidad energética exigida por el ENS, alineando la eficiencia con la gobernanza normativa y la ciberseguridad.

De este modo, el M-PUE amplía la filosofía del PUE tradicional, incorporando factores operativos, ambientales y logísticos que reflejan la realidad de las infraestructuras militares. Proporciona un marco de medición verificable y comparable, conforme a las recomendaciones del *White Paper 49* [16], y adaptable a los marcos normativos nacionales y aliados.

Su aplicación permite evaluar la eficiencia de los CPD militares desde una perspectiva integral – técnica, doctrinal y sostenible –, consolidando la energía como un recurso táctico que puede auditarse, optimizarse y gobernarse con criterios objetivos.

2.5 Marco doctrinal y normativo: ENS, CCN-STIC y FMN Spiral 5

La virtualización y la gestión energética de las infraestructuras TIC en defensa no pueden analizarse de forma aislada del marco doctrinal y normativo que regula su diseño, acreditación y operación.

Por este motivo, toda arquitectura tecnológica en el ámbito militar debe garantizar simultáneamente tres principios fundamentales: **seguridad, interoperabilidad y sostenibilidad**.

Estos principios se materializan a través de tres pilares normativos complementarios:

- El **Esquema Nacional de Seguridad (ENS)**, que establece los requisitos mínimos de protección para los sistemas clasificados o críticos;
- Las **guías técnicas CCN-STIC**, que detallan su implementación técnica y los controles aplicables a entornos virtualizados e híbridos;
- La doctrina **Federated Mission Networking (FMN)** de la OTAN, actualmente en su Spiral 5, que define los estándares de interoperabilidad técnica y doctrinal entre aliados.

Sin perjuicio de la amplitud del conjunto normativo completo, en el contexto de este TFM se presenta una versión acotada orientada únicamente a los elementos con impacto directo en virtualización y computación distribuida. De este modo se evita introducir complejidad normativa no vinculada al ámbito técnico analizado, manteniendo un enfoque operativo y coherente con los objetivos del trabajo.

En conjunto, estos marcos configuran la arquitectura de gobernanza sobre la que se apoya la transformación digital de la defensa. Asimismo, legitiman la introducción de métricas de evaluación como el M-PUE, vinculando la eficiencia energética con la sostenibilidad operativa y el cumplimiento normativo.

2.5.1 El Esquema Nacional de Seguridad

El ENS, regulado por el Real Decreto 311/2022, define los principios y requisitos mínimos de seguridad aplicables a los sistemas de información del sector público y, por extensión, a los sistemas de defensa que gestionan información clasificada o sensible. Define tres categorías de impacto –Básico, Medio y Alto– en función del daño que una brecha de seguridad pueda ocasionar a la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de los activos gestionados.

En el ámbito de Defensa, la mayoría de los sistemas se clasifican como de nivel alto, lo que exige aplicar controles reforzados en materia de gestión de la configuración, segmentación de redes, autenticación y auditoría continua.

Bajo esta premisa, la virtualización se convierte en un habilitador del cumplimiento, permitiendo:

- **Aislar dominios de seguridad** mediante hipervisores o redes virtuales segregadas. Esta capacidad es crítica para cumplir con la medida [mp.com.4] (*Separación de flujos de información en la red*) del ENS, así como para implementar los controles de la guía CCN-STIC-220 respecto al aislamiento de la gestión del hipervisor.
- **Gestionar de forma centralizada las configuraciones** (*hardening*, parcheado), facilitando la aplicación de la medida [op.exp.3] (*Gestión de la configuración de seguridad*).
- **Implementar mecanismos automatizados de registro y trazabilidad** –elementos esenciales para las medidas [op.exp.8] (*Registro de la actividad*) y [op.mon.1] (*Detección de intrusión*)–, requisitos críticos en categoría alta para garantizar la auditoría forense.

El ENS incorpora además el principio de proporcionalidad, que permite adaptar los controles a las condiciones operativas (incluidos entornos desplegados o DDIL) sin degradar el nivel global de seguridad. Este principio es clave para la evaluación del ICOMP definida en el Capítulo 4.

Este principio resulta clave en entornos desplegados o tácticos, donde la continuidad operativa forma parte intrínseca de la seguridad de misión.

2.5.2 Guías técnicas del CCN-STIC

El Centro Criptológico Nacional (CCN) complementa al ENS mediante sus guías técnicas STIC, que concretan las medidas de seguridad para cada tipo de entorno tecnológico. Estas guías son de aplicación directa a los sistemas del Ministerio de Defensa y constituyen la referencia nacional en materia de acreditación de entornos virtualizados, contenedorizados o *cloud*.

Entre las más relevantes para este trabajo destacan:

- **CCN-STIC-220:** controles de seguridad en entornos de virtualización. Define los requisitos mínimos para hipervisores, aislamiento de cargas y segmentación de redes virtuales.
- **CCN-STIC-823:** seguridad en infraestructuras *cloud* híbridas y públicas. Regula la segregación de recursos, la gestión de identidades y el control de acceso privilegiado.
- **CCN-STIC-652A:** seguridad en entornos basados en contenedores. Establece medidas de refuerzo para orquestadores, imágenes y cadenas de suministro de software.

La aplicación coherente de estas guías garantiza la conformidad del modelo de virtualización con los requisitos nacionales de acreditación. La Tabla 2-8 sintetiza la relación entre guías y tecnologías.

Guía CCN-STIC	Ámbito de aplicación	Tecnologías afectadas
220	Entornos de virtualización tradicionales	Hipervisores tipo 1 y 2, máquinas virtuales
823	Infraestructuras <i>cloud</i> híbridas o federadas	Hipervisores, orquestadores
652A	Contenedores y microservicios	Docker, LXC, Kubernetes, OpenShift

Tabla 2-8: Correspondencia entre guías CCN-STIC y tecnologías de virtualización.

Estas directrices son de aplicación obligatoria en cualquier sistema clasificado o que gestione información sensible del Ministerio de Defensa. No obstante, la rápida evolución de las tecnologías – especialmente micro-VM y *unikernels*– plantea una brecha normativa: no existen normativa específicas para su acreditación y deben evaluarse mediante controles equivalentes (aislamiento, trazabilidad, micro-segmentación) extraídos de CCN-STIC-220 y 652A. Esta situación justifica el empleo de métricas como el ICOMP y del modelo M-PUE para comparar tecnologías con distintos niveles de madurez normativa.

De forma complementaria, la norma ISO/IEC 27017:2015 [47] proporciona controles específicos para entornos de computación en la nube, desarrollando medidas de seguridad sobre entornos multi-tenant, responsabilidades compartidas y protección contra alteraciones de configuración. Asimismo, la ISO/IEC 27018:2019 [48] extiende estas medidas a la protección de datos personales (PII) en nubes públicas o híbridas, ofreciendo garantías adicionales en términos de auditoría, segregación lógica y cifrado de información sensible.

2.5.3 Principios de arquitectura de seguridad: Alineamiento con Zero Trust

La evaluación de la conformidad normativa en entornos de defensa no puede limitarse a un listado estático de controles, sino que debe verificar la madurez de la arquitectura de seguridad. Para garantizar la validez en contextos multinivel y federados, cualquier modelo de evaluación debe alinearse conceptualmente con el marco internacional de referencia: la *Zero Trust Architecture* (ZTA) definida por el *National Institute of Standards and Technology* (SP 800-207) [49].

Este marco establece tres principios rectores que deben ser cuantificables:

- **Verificación explícita (Aislamiento):** La capacidad de segregar cargas de trabajo de forma robusta, un requisito crítico para la soberanía del dato y alineado con CCN-STIC-220.
- **Menor privilegio (Microsegmentación):** La posibilidad de aplicar controles granulares de tráfico «este-oeste» entre servicios virtualizados.
- **Asumir la brecha (Trazabilidad):** La integridad y verificabilidad de los registros de auditoría, en coherencia con las exigencias del ENS.

La integración de estos principios del NIST SP 800-207 con la normativa nacional ENS constituye la base teórica sobre la que se desarrollará el indicador de cumplimiento ICOMP descrito en el Capítulo 4, permitiendo cuantificar el grado de madurez de las arquitecturas analizadas.

2.5.4 Doctrina OTAN: Federated Mission Networking Spiral 5

La doctrina OTAN FMN define el conjunto de normas, estándares y procedimientos que garantizan la interoperabilidad técnica y doctrinal entre las naciones aliadas en operaciones conjuntas. Su desarrollo incremental en espirales incorpora progresivamente nuevas capacidades y requisitos de resiliencia.

Spiral 5, actualmente en despliegue, introduce un enfoque centrado en la resiliencia de servicios críticos en entornos DDIL. Entre sus avances más relevantes destacan:

- Integración de capacidades de *edge computing* y nodos tácticos virtualizados, respondiendo al principio FMN de *services at the edge* para reducir la dependencia del núcleo.
- Mecanismos de operación autónoma ante pérdida de conectividad (DDIL), materializando el principio FMN de *Resilience and Graceful Degradation* para asegurar la continuidad de misión.
- Políticas de interoperabilidad energética y sostenibilidad logística, como parte del principio FMN de *Efficient Use of Resources*.
- Requisitos de trazabilidad normativa en sistemas virtualizados multinivel, alineados con el principio FMN de *Assured Information Sharing* en entornos federados.

FMN Spiral 5 promueve un modelo de infraestructura federada, donde cada nación mantiene la soberanía de sus recursos, pero garantiza interoperabilidad mediante estándares comunes (STANAG 5524 [50], 4559 [51], etc.). En este escenario, la virtualización actúa como facilitador de interoperabilidad y aislamiento entre dominios, mientras que métricas como el M-PUE proporcionan una medida cuantitativa de eficiencia energética y sostenibilidad del conjunto federado.

2.5.5 Convergencia normativa y oportunidades

La articulación del ENS, las guías STIC y la doctrina FMN genera una arquitectura de gobernanza que integra el cumplimiento normativo, la implementación técnica y el contexto operativo multinacional, tal como se sintetiza en la Tabla 2-9.

Nivel normativo	Rol en la virtualización militar
FMN Spiral 5 (OTAN)	Interoperabilidad técnica y doctrinal aliados. Resiliencia en entornos DDIL e integración de <i>edge computing</i> .
ENS (RD 311/2022)	Principios y requisitos mínimos de seguridad para sistemas clasificados y proporcionalidad de controles.
Guías CCN-STIC	Aplicación técnica del ENS en virtualización, contenedores y <i>cloud</i> . Referencia para acreditación.

Tabla 2-9: Convergencia doctrinal y normativa.

El marco doctrinal y normativo constituye el esqueleto invisible que otorga legitimidad y coherencia a la virtualización en defensa. El ENS y las guías CCN-STIC proporcionan la base de acreditación nacional, mientras que la doctrina FMN Spiral 5 garantiza la interoperabilidad aliada y la sostenibilidad operativa. Su convergencia respalda la introducción de indicadores como el M-PUE, que amplían la evaluación tradicional de seguridad hacia un modelo integral de eficiencia energética, resiliencia y gobernanza tecnológica.

Este marco establece las condiciones necesarias para desarrollar, en el Capítulo 4, la metodología de evaluación y los modelos comparativos que permitirán validar empíricamente las estrategias de virtualización analizadas.

2.5.6 Virtualización como habilitador de Zero Trust y Soberanía del Dato

Los principios de seguridad perimetral clásica resultan insuficientes en despliegues tácticos, donde el perímetro físico es difuso y las amenazas pueden originarse dentro de la infraestructura. En este contexto, el modelo de ZTNA adopta un enfoque basado en la desconfianza por defecto: todo acceso debe ser autenticado, autorizado y registrado, sin asumir confianza inherente a ninguna zona de red.

El uso de ZTNA en este capítulo se realiza en un sentido estrictamente conceptual, sin pretender abordar una implementación completa, sino únicamente alinear sus principios de aislamiento, microsegmentación y trazabilidad con las exigencias del ENS y las guías CCN-STIC.

La virtualización actúa como habilitador tecnológico de este modelo al permitir la implementación de microsegmentación a nivel de software. Cada máquina virtual, micro-VM o contenedor puede configurarse como un dominio de confianza aislado, inspeccionando incluso el tráfico lateral entre cargas en el mismo nodo físico. Esta granularidad es crítica en entornos multinacionales federados (FMN), donde un mismo CPD puede alojar cargas con distinta clasificación –p. ej., SECRETO OTAN y RESERVADO– siempre que se implementen dominios segregados con aislamiento fuerte y trazabilidad verificable conforme al ENS y las guías CCN-STIC.

Esta arquitectura de seguridad distribuida y verificable garantiza la Soberanía del Dato, uno de los pilares estratégicos de las capacidades TIC de defensa, al asegurar que la ubicación física o lógica del dato no compromete su control, confidencialidad o trazabilidad.

2.6 Riesgos y barreras de implementación

El análisis realizado en este capítulo evidencia que, a pesar del elevado potencial de las estrategias de virtualización en defensa, su aplicación práctica conlleva una serie de riesgos y limitaciones que deben ser cuidadosamente considerados. Estos desafíos se agrupan en tres dimensiones principales: técnica, organizativa y normativa. Su análisis anticipado permite definir medidas de mitigación realistas y garantizar la viabilidad del modelo en escenarios reales, especialmente en entornos DDIL, complementando así el análisis normativo de la Sección 2.5.

2.6.1 Riesgos técnicos

Esta dimensión abarca los desafíos intrínsecos a la arquitectura y al despliegue tecnológico, donde la heterogeneidad de los sistemas y la hostilidad del entorno físico condicionan la viabilidad de la solución.

- **Dependencia de proveedores y soberanía tecnológica.** Una parte significativa de las soluciones de virtualización –hipervisores, micro-VM o plataformas de orquestación– presenta modelos de licencia privativos o componentes de código cerrado. Esto puede entrar en conflicto con los principios de soberanía tecnológica y auditabilidad exigidos en entornos clasificados.

- **Integración con infraestructuras heredadas.** La coexistencia de sistemas *legacy* con arquitecturas virtualizadas avanzadas introduce retos de compatibilidad y madurez que afectan a capas de virtualización, *middleware* y aplicaciones críticas.
- **Limitaciones para la validación en entornos reales.** La experimentación directa en CPD desplegados bajo condiciones DDIL es compleja debido a restricciones logísticas, de seguridad y disponibilidad de medios, lo que obliga a recurrir a simulaciones y modelos teóricos.
- **Riesgos de ciberseguridad emergente.** La combinación de múltiples tecnologías (hipervisores, contenedores, micro-VM) puede generar nuevas superficies de ataque y brechas entre capas si no se implementan políticas de seguridad homogéneas, segmentación reforzada y aislamiento verificable.
- **Observabilidad limitada en escenarios DDIL.** La degradación o intermitencia de los enlaces condiciona la telemetría continua, afectando la gestión dinámica de cargas, la auditoría de eventos y la respuesta a incidentes. Sin mecanismos *store-and-forward*, bitácoras firmadas y sincronización diferida, la trazabilidad se ve comprometida.

2.6.2 Riesgos organizativos

Más allá del hardware y el software, el factor humano y la cultura institucional juegan un papel determinante en la viabilidad operativa, pudiendo actuar como catalizadores o como frenos al cambio.

- **Capacitación técnica especializada.** La adopción de contenedores, micro-VM, orquestadores distribuidos y mecanismos de seguridad multinivel exige perfiles altamente cualificados; la falta de capacitación puede frenar la implantación.
- **Gestión del cambio y resistencia institucional.** La transición desde infraestructuras tradicionales hacia entornos virtualizados y adaptativos puede generar resistencia en estructuras jerárquicas donde prima la fiabilidad demostrada frente a la innovación.
- **Gobernanza y reparto de responsabilidades.** La operación distribuida a lo largo de niveles estratégico, operacional y táctico requiere roles y responsabilidades claramente definidos, para evitar solapamientos o vacíos en la cadena de mando técnica.

2.6.3 Riesgos normativos y de acreditación

Finalmente, el cumplimiento normativo representa el garante indispensable de la seguridad nacional, pero su rigidez actual plantea dificultades para certificar tecnologías disruptivas o arquitecturas altamente dinámicas.

- **Complejidad de la acreditación ENS en entornos distribuidos.** Aunque el ENS y las guías CCN-STIC cubren entornos virtualizados convencionales (CCN-STIC-220), híbridos (CCN-STIC-823) y contenedores (CCN-STIC-652A) [36], aún no existen marcos consolidados para certificar tecnologías emergentes como micro-VM o *unikernels*, lo que dificulta su implantación en sistemas de clasificación alta.
- **Verificación de configuraciones dinámicas.** Las reconfiguraciones frecuentes en entornos dinámicos dificultan una acreditación continua si no se dispone de registros firmados, sellos de tiempo y mecanismos de control basados en automatización del cumplimiento (*compliance-as-code*).
- **Interoperabilidad multinivel.** La coexistencia de dominios OTAN, UE, nacionales y clasificados requiere políticas armonizadas de identidad, cifrado, segmentación y auditoría. Cualquier desviación puede bloquear la federación de servicios o el intercambio seguro de información.

En consecuencia, la mitigación de estas barreras exige un enfoque progresivo, automatizado y verificable. Este debe combinar: estandarización de políticas alineadas con el ENS y FMN, despliegues piloto escalonados, capacitación del personal técnico, y la integración de acuerdos de nivel de servicio (SLA/SLO) que incorporen criterios energéticos, logísticos y de seguridad.

2.7 Síntesis de fundamentos técnicos y doctrinales

El presente capítulo ha establecido los fundamentos tecnológicos y doctrinales que sustentan la virtualización como elemento estructural de la transformación digital en defensa. A lo largo de sus secciones se ha mostrado cómo las infraestructuras militares evolucionan desde modelos centralizados hacia arquitecturas federadas, distribuidas y energéticamente sostenibles, guiadas por principios de seguridad, interoperabilidad y eficiencia.

2.7.1 Síntesis técnica

Desde el punto de vista tecnológico, la virtualización se consolida como la piedra angular de los CPD de defensa. La transición desde entornos monolíticos hacia arquitecturas distribuidas –basadas en hipervisores, contenedores, micro-VM y *unikernels*– permite alcanzar niveles superiores de flexibilidad, aislamiento y sostenibilidad logística.

Esta evolución ha dado lugar a un modelo jerárquico-federado donde la capacidad de cómputo se distribuye entre los niveles estratégico, modular operacional y táctico, garantizando la continuidad del servicio en escenarios DDIL. En este contexto, cada tecnología cumple un rol diferenciado:

- Las **máquinas virtuales (VM)** aseguran consolidación y cumplimiento normativo.
- Los **contenedores** aportan agilidad y densidad computacional en despliegues operacionales.
- Las **micro-VM** equilibran aislamiento y ligereza, adecuadas para nodos *edge* y escenarios tácticos.
- Los ***unikernels*** representan la virtualización extrema para funciones especializadas y sistemas embebidos.

En paralelo, se han identificado los mecanismos técnicos de eficiencia energética asociados a la virtualización: consolidación dinámica de cargas, apagado selectivo, *power capping* y planificación energética. Estos principios sustentan la métrica M-PUE, cuya formulación ampliada incorpora penalizaciones energéticas, logísticas y ambientales coherentes con los entornos militares heterogéneos.

2.7.2 Síntesis doctrinal y normativa

Desde la perspectiva doctrinal, el capítulo ha integrado los tres marcos que definen la gobernanza de las infraestructuras TIC en defensa:

- El **ENS**, que establece los principios de confidencialidad, integridad, disponibilidad y proporcionalidad.
- Las **guías CCN–STIC**, que desarrollan los controles técnicos aplicables a hipervisores, contenedores e infraestructuras híbridas.
- La doctrina **OTAN FMN Spiral 5**, que proporciona el marco de interoperabilidad y resiliencia multinacional en entornos DDIL.

La convergencia entre estos marcos crea una base de legitimidad y trazabilidad que convierte la virtualización en una herramienta no solo técnica, sino también de cumplimiento normativo. Permite integrar seguridad, sostenibilidad e interoperabilidad bajo una misma arquitectura de control, facilitando la acreditación tanto nacional como aliada.

Además, la introducción de métricas como el M-PUE responde a las recomendaciones OTAN y CCN-STIC de incorporar indicadores cuantitativos en la evaluación de infraestructuras críticas. Ello habilita un enfoque basado en evidencia que complementa los procesos de acreditación tradicionales. De este modo, los requisitos del ENS y las directrices OTAN dejan de ser restricciones para convertirse en vectores de innovación.

Para sintetizar la interacción entre los tres ejes fundamentales del estudio (doctrina, tecnología y dimensiones de evaluación), se propone el marco conceptual ilustrado en la Figura 2-8, que guía el análisis posterior.

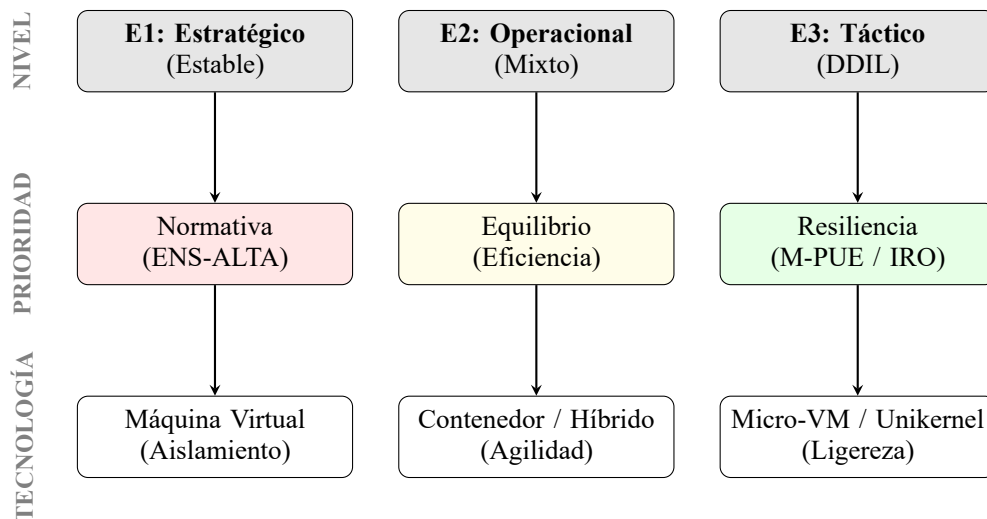


Figura 2-8: Marco conceptual: Relación entre el nivel de despliegue, la prioridad estratégica y la tecnología idónea.
Fuente: Elaboración propia.

2.7.3 Conclusiones parciales

De la revisión efectuada pueden extraerse las siguientes conclusiones parciales:

- La virtualización constituye un pilar estructural de la transformación digital en defensa, con impacto directo en la eficiencia operativa, la resiliencia y la sostenibilidad logística.
- La eficiencia energética debe entenderse como un componente operativo y doctrinal, no solo técnico, y evaluarse mediante métricas adaptadas como el M-PUE.
- El marco ENS-CCN-FMN proporciona la base de legitimidad, trazabilidad y gobernanza necesaria para la adopción segura de arquitecturas virtualizadas.
- La identificación de riesgos técnicos y barreras normativas confirma que la tecnología por sí sola no es suficiente, requiriendo un marco de decisión que pondere estas limitaciones frente a las ventajas operativas.
- Persisten vacíos normativos y metodológicos –especialmente en torno a las micro-VM y los *unikernels*– que requieren enfoques adaptativos y métricas flexibles de evaluación.

Conviene señalar que el presente capítulo no tiene por objeto realizar una comparación experimental directa ni un benchmarking cuantitativo exhaustivo entre tecnologías de virtualización, sino identificar, desde la literatura técnica, normativa y doctrinal, los factores críticos que condicionan su adopción en entornos de defensa. Esta delimitación justifica la necesidad de un marco metodológico propio que permita integrar eficiencia energética, resiliencia operativa y cumplimiento normativo, cuya definición y formalización se desarrollan en el Capítulo 4.

Estas conclusiones consolidan el marco conceptual sobre el que se desarrollará el Capítulo 3, dedicado al análisis comparativo del estado del arte en estrategias de virtualización y optimización energética de CPD en defensa. Dicho capítulo examinará las tendencias actuales, los avances en eficiencia y las oportunidades de integración de las métricas y doctrinas expuestas.

3 ESTADO DEL ARTE, TENDENCIAS Y ANÁLISIS COMPARATIVO

La digitalización de la defensa y la evolución de las operaciones multidominio han impulsado una transición decisiva hacia infraestructuras tecnológicas virtualizadas, distribuidas y energéticamente eficientes. En este escenario, la virtualización se consolida como el eje vertebrador de la transformación digital, permitiendo maximizar el rendimiento de los recursos disponibles y dotar de mayor flexibilidad y resiliencia a los sistemas de información y comunicaciones (CIS).

La madurez alcanzada por las arquitecturas *cloud*, *edge* y *fog computing* en el ámbito civil ha favorecido su progresiva incorporación en entornos militares. Sin embargo, las condiciones doctrinales, normativas y logísticas propias de la defensa exigen un enfoque diferenciado, en el que la eficiencia energética, la interoperabilidad aliada y la seguridad de la información actúan como principios rectores ineludibles.

El presente capítulo analiza de forma crítica el estado del arte y las tendencias actuales en materia de virtualización aplicada a infraestructuras de defensa. Su propósito es doble:

- a) Examinar las principales estrategias y tecnologías que sustentan la virtualización moderna, desde los modelos de despliegue en el *Compute Continuum* [52, 53] hasta la consolidación dinámica y la eficiencia energética;
- b) Identificar las limitaciones, la deuda técnica operativa y las oportunidades de mejora que condicionan su plena adopción en el ámbito militar.

La revisión integra resultados de proyectos internacionales, literatura científica, normativa OTAN y europea, así como programas de innovación tecnológica en defensa. El enfoque es esencialmente comparativo: se contrastan las soluciones y metodologías maduras del sector civil con sus adaptaciones doctrinales y operativas en el entorno militar.

El capítulo se estructura en cinco secciones: la Sección 3.1 analiza la integración de la virtualización en arquitecturas *fog/edge* y su impacto en la autonomía operativa; la Sección 3.2 revisa las estrategias de eficiencia energética; la Sección 3.3 resume las tendencias de gestión; la Sección 3.4 expone las limitaciones actuales con énfasis en la deuda técnica y la madurez (TRL); y la Sección 3.5 sintetiza la brecha metodológica existente y plantea oportunidades de mejora.

3.1 Virtualización y *edge computing* en el ámbito militar

La convergencia entre virtualización y *edge computing* representa uno de los pilares tecnológicos sobre los que se construyen las nuevas arquitecturas digitales de defensa. Su finalidad es acercar la capacidad de cómputo al punto donde se generan los datos, reduciendo la dependencia de los CPD estratégicos y garantizando la continuidad de servicio en entornos DDIL.

La virtualización en el *edge* militar permite desplegar servicios críticos sobre infraestructuras ligeras, modulares y tolerantes a la desconexión. De este modo, los sistemas pueden mantener su operatividad incluso en condiciones adversas, con autonomía funcional y capacidad de sincronización posterior con los niveles superiores de mando y control.

3.1.1 Evolución del paradigma *edge*: distinción entre *fog* y *edge*

El concepto de *edge computing* se originó en el ámbito civil para optimizar la latencia. Sin embargo, para una aplicación rigurosa en defensa, es crítico distinguir las capas funcionales según la arquitectura de referencia del NIST SP 500-325 [54]:

- **Cloud (Nivel Estratégico):** Capacidad masiva centralizada (CPD nacional). Prioriza la capacidad de cómputo sobre la latencia.
- **Fog Computing (Nivel Operacional):** Nodos de «niebla» que actúan como intermediarios de agregación (Puestos de Mando de Brigada). Aquí la virtualización requiere un equilibrio entre potencia de servidor y movilidad de contenedor.
- **Edge Computing (Nivel Táctico):** Computación en el extremo de la red, abarcando desde los *Edge Nodes* vehiculares hasta el *Far Edge* en sensores. Este nivel prioriza la autonomía operativa en entornos DDIL y el cumplimiento de restricciones SWaP (*Size, Weight and Power*) para procesar el dato en origen.

En los últimos años, tanto la OTAN como la Unión Europea han reconocido el valor de este *Compute Continuum* como parte esencial de la resiliencia digital. Iniciativas como la European Edge Computing Initiative (E2C) o la doctrina FMN Spiral 5 promueven la creación de infraestructuras federadas capaces de operar de forma descentralizada.

En este contexto, el estándar IEEE 2413 [55] propone una arquitectura de referencia orientada al Internet de las Cosas (IoT), basada en principios de modularidad y federación. Aunque concebida para entornos civiles, esta estructura resulta aplicable a despliegues tácticos donde convergen sensores, nodos de cómputo y actuadores distribuidos, como ocurre en operaciones ISR o C2 desplegado. Esta aproximación refuerza la necesidad de diseñar infraestructuras *edge* resilientes, capaces de operar con autonomía y reintegrarse posteriormente en mallas federadas bajo criterios de interoperabilidad OTAN-FMN.

Mientras que la literatura académica reciente se centra en la optimización de la latencia para aplicaciones 5G comerciales [56], este estudio prioriza la autonomía operativa bajo condiciones de denegación de servicio en entornos DDIL. La arquitectura propuesta no asume una conectividad «siempre disponible» con la nube central, sino que diseña el nodo táctico para operar en aislamiento prolongado, una restricción de diseño ausente en la mayoría de los modelos civiles de *edge computing*. Esta adaptación de los conceptos teóricos a la realidad operativa se sistematiza en la Tabla 3-1, que define las funciones críticas para cada escalón de mando.

Nivel de despliegue	Concepto NIST	Función y características principales
Estratégico	<i>Cloud</i>	Extensión del CPD central en bases logísticas o permanentes. Alta capacidad, cumplimiento ENS-ALTA y compatibilidad FMN Spiral 5.
Operacional	<i>Fog Node</i>	Nodos desplegados en el teatro de operaciones. Mantienen servicios esenciales y federan capacidades con los niveles superior e inferior.
Táctico	<i>Edge Node</i>	Módulos ultracompactos embebidos en plataformas móviles o sensores. Operación autónoma, bajo consumo y tolerancia DDIL.
Espacial / ISR	<i>Far Edge</i>	Procesamiento local en plataformas aéreas o satelitales para reducir latencia en la explotación de datos ISR.

Tabla 3-1: Modelos de despliegue de *edge computing* en entornos de defensa.

3.1.2 Arquitecturas virtualizadas y federación de nodos

Las arquitecturas de *edge* militar integran capas de virtualización ligera para ejecutar funciones de misión de forma segura sobre hardware heterogéneo. El principio doctrinal subyacente es el de federación controlada: cada nodo debe poder operar de forma independiente, pero con capacidad de reintegrarse en la malla federada una vez restablecida la conectividad.

Las iniciativas de modernización y marcos normativos aliados –como la arquitectura FMN Spiral 5, la aceleradora *NATO DIANA* [57] o el proyecto European Defence Cloud [18]– promueven la estandarización de este enfoque mediante el uso de hipervisores seguros, contenedores verificados y orquestadores tolerantes a fallos (*KubeEdge*, *Rancher Fleet*, *Lightkube*).

La Tabla 3-2 sintetiza las capacidades operativas y de seguridad de las distintas tecnologías, basándose en la arquitectura de aislamiento documentada en el paper de presentación de AWS Firecracker [37], las directrices de seguridad para contenedores de NIST SP 800-190 [58] y los modelos de despliegue de la CNCF [59].

Tecnología	Ventajas operativas	Desafíos
VM	Madurez y soporte normativo consolidado.	Baja densidad, mayor consumo y menor idoneidad para nodos móviles o energéticamente limitados. Tiempos de arranque lentos. Ideal para CPD estratégico.
Contenedores	Alta densidad y despliegue rápido. Ideal para servicios modulares.	Aislamiento débil (<i>kernel</i> compartido). Complejidad de acreditación.
Micro-VM	Aislamiento casi tan fuerte como VM, pero con la velocidad y eficiencia de contenedores. Integración transparente con orquestadores.	Ecosistema incipiente. Ausencia de normativa específica.
Unikernels	Consumo ultrarreducido y superficie de ataque mínima.	Dificultad de auditoría y trazabilidad, y compatibilidad limitada con sistemas convencionales.

Tabla 3-2: Análisis comparativo de tecnologías de virtualización para entornos *edge* militares.

3.1.3 Tendencias y líneas de convergencia

La revisión doctrinal y tecnológica permite identificar tres tendencias consolidadas en la evolución del *edge* militar:

- **Especialización funcional del *edge*:** evolución desde nodos genéricos hacia infraestructuras de misión optimizadas para tareas específicas –como inteligencia de señales, comunicaciones seguras o soporte logístico–, incorporando hardware acelerado (GPU, FPGA) y virtualización ligera.
- **Interoperabilidad federada:** desarrollo de arquitecturas multinivel donde los nodos comparten servicios mediante políticas STANAG y marcos FMN, con mecanismos de descubrimiento y federación segura.
- **Eficiencia energética contextualizada:** integración de métricas como el M-PUE para ajustar el consumo de energía a las condiciones de entorno y carga operativa, reforzando la sostenibilidad del sistema.

3.1.4 Retos actuales

A pesar de los avances tecnológicos, la implementación de capacidades *edge* virtualizadas en defensa enfrenta varios desafíos estructurales:

- **Madurez desigual de tecnologías:** la certificación ENS–ALTA o FMN aún no contempla micro-VM ni *unikernels*, lo que limita su acreditación formal.
- **Interoperabilidad multinacional:** la federación de nodos entre aliados requiere políticas comunes de identidad, sincronización y trazabilidad de servicios.
- **Sostenibilidad energética:** la autonomía de los nodos tácticos depende de la optimización del consumo y la gestión eficiente de microrredes híbridas.

En conjunto, la virtualización en el *edge* militar se configura como una capacidad estratégica orientada a la autonomía y la resiliencia operativa. Las tecnologías ligeras –contenedores, micro-VM y *unikernels*– ofrecen una base sólida para el despliegue rápido y seguro de servicios críticos, aunque su integración plena exige progresos en estandarización, acreditación y eficiencia energética. Este último aspecto constituye el eje central de la siguiente sección.

3.2 Estrategias de eficiencia energética y consolidación dinámica

La eficiencia energética en infraestructuras virtualizadas de defensa se ha convertido en un factor estratégico que trasciende el ámbito técnico. En los despliegues militares, donde la energía puede provenir de microrredes híbridas, generadores portátiles o fuentes renovables intermitentes, la optimización del consumo influye directamente en la autonomía operativa y la sostenibilidad logística. El equilibrio entre rendimiento, seguridad y eficiencia constituye un elemento clave para garantizar la continuidad de las operaciones en entornos DDIL o de alta exigencia ambiental.

La virtualización, al concentrar múltiples servicios en recursos físicos limitados, ofrece oportunidades de ahorro energético significativas. Sin embargo, también introduce desafíos en la gestión térmica, el dimensionamiento de cargas y la priorización de servicios críticos. Las estrategias actuales buscan un punto de equilibrio entre consolidación, disponibilidad y consumo, mediante políticas adaptativas y modelos de planificación eficientes.

Esta sección analiza las principales líneas de trabajo en materia de eficiencia energética en entornos virtualizados, desde la consolidación dinámica de cargas hasta la gestión de potencia y la federación energética multinivel.

3.2.1 Consolidación dinámica de cargas

La consolidación dinámica consiste en reagrupar instancias virtuales o contenedores sobre un número reducido de nodos físicos durante periodos de baja demanda, permitiendo apagar o hibernar los equipos inactivos. Adquiere especial relevancia en defensa por su capacidad de reducir el consumo logístico y mejorar la autonomía de los módulos desplegados.

El proceso se apoya en técnicas de migración en caliente, monitorización continua y políticas de umbral que determinan cuándo consolidar o distribuir las cargas. No obstante, en entornos militares debe garantizarse que la consolidación no comprometa la disponibilidad inmediata ante variaciones imprevistas de carga o contingencias de misión. Para instrumentar este equilibrio, existen diferentes estrategias operativas cuyas implicaciones tácticas se detallan en la Tabla 3-3.

En el ámbito civil, prototipos como GreenCloudSim, OpenDC o las plataformas de simulación del programa OTAN IST-208 han demostrado reducciones de consumo de hasta un 40 % sin afectar la disponibilidad del servicio. Su aplicación en defensa requiere equilibrar el ahorro energético con los requisitos de disponibilidad, redundancia y seguridad de la información clasificada.

Consolidación	Mecanismo técnico	Consideraciones para defensa
Reactiva	Migración en caliente de VM o contenedores cuando la carga baja del umbral predefinido.	Ahorro energético moderado (20–30 %), riesgo de latencia ante picos súbitos de carga.
Predictiva	Reubicación anticipada basada en patrones históricos de carga o demanda estimada.	Alta eficiencia (>35 %), requiere telemetría fiable y capacidad de monitorización local.
Cooperativa	Coordinación entre nodos federados mediante políticas comunes de orquestación.	Ideal para despliegues multinodo; exige sincronización segura y canal de control resiliente.

Tabla 3-3: Principales estrategias de consolidación y aplicabilidad en defensa.

A diferencia de los modelos civiles de eficiencia energética –como los enfoques de The Green IT orientados principalmente a la reducción de OPEX en centros de datos estables [60]–, en entornos militares la optimización no responde a criterios económicos, sino tácticos. La energía condiciona directamente la supervivencia del nodo: apagar o hibernar servidores implica evaluar su impacto en la disponibilidad inmediata ante una contingencia operativa.

Asimismo, la literatura científica y los estándares industriales recientes sobre consolidación y eficiencia energética –p. ej., la visión de sostenibilidad en hiperescala de Buyya et al. [61], los esquemas de programación de tareas eficientes en costes de Kumar y Karri. [62], las estrategias de optimización de costes del marco *Well-Architected* de AWS [63] o los informes globales de Donnellan et al. (Uptime Institute) [64]– se centran exclusivamente en modelos de centros de datos con conectividad permanente, priorizando la reducción de OPEX y la estabilidad térmica. Este TFM adopta por tanto un enfoque diferenciado, orientado a la autonomía operativa y a la sostenibilidad en despliegues tácticos, donde la energía no es un coste, sino un recurso de supervivencia.

3.2.2 Escalado adaptativo y planificación energética consciente

El escalado adaptativo (*elastic scaling*) permite ajustar los recursos asignados a cada instancia en función de la carga, la temperatura o la disponibilidad energética del entorno. A nivel operativo, los orquestadores –como OpenStack, OpenNebula o Kubernetes– aplican políticas de escalado vertical (variación de CPU y memoria) y horizontal (creación o eliminación de instancias) para mantener el equilibrio entre rendimiento y consumo.

En entornos tácticos, esta elasticidad debe vincularse al estado de la microrred o del generador local. Por ejemplo, un nodo *edge* puede reducir su frecuencia de reloj o suspender contenedores secundarios cuando el nivel de batería desciende por debajo de un umbral crítico. Este principio de planificación energética consciente se apoya en métricas contextuales como el M-PUE, que se introducirá en el Capítulo 4. Para sistematizar estas capacidades, la Tabla 3-4 resume las principales modalidades de escalado y su aportación específica a la defensa.

Escalado	Aplicación típica	Ventajas en defensa
Vertical	Ajuste de núcleos y memoria por instancia.	Control preciso del consumo, bajo impacto en la latencia.
Horizontal	Creación o eliminación de instancias según la carga.	Mejora la continuidad del servicio en entornos DDIL mediante réplicas locales.
Energético	Activación condicionada por disponibilidad eléctrica, térmica o estado de la microrred.	Optimiza la autonomía en microrredes tácticas; integrable con métricas M-PUE.

Tabla 3-4: Tipos de escalado adaptativo aplicables a entornos virtualizados de defensa.

3.2.3 Gestión de potencia y control térmico

La limitación de potencia (*power capping*) y la gestión térmica se consideran mecanismos complementarios para mejorar la eficiencia energética. Su objetivo es restringir el consumo máximo de un servidor o clúster, evitando picos que puedan comprometer la estabilidad eléctrica o la capacidad de refrigeración del sistema.

Los estándares IPMI 2.0 [65], Redfish [66] y las soluciones de DCIM proporcionan interfaces de gestión remota que permiten regular parámetros como la potencia suministrada, la frecuencia de operación o las políticas de ventilación y refrigeración.

En entornos militares o desplegados, estas capacidades deben integrarse en sistemas de gestión remota tolerantes a desconexiones y capaces de operar de forma autónoma ante la pérdida de enlace con el nivel estratégico. Una tendencia creciente es vincular estos parámetros energéticos con el planificador del orquestador, de modo que las decisiones de encendido, apagado o migración de cargas se coordinen según la prioridad del servicio y la energía disponible.

3.2.4 Consolidación energética federada

En operaciones multinacionales o de coalición, la eficiencia energética no puede abordarse de manera aislada. Los programas OTAN FMN, European Defence Cloud y E2C promueven la federación de recursos energéticos y computacionales bajo políticas comunes de interoperabilidad y sostenibilidad. En este contexto, la consolidación dinámica puede extenderse a escala federada, permitiendo la redistribución de cargas entre CPD estratégicos y nodos tácticos en función del coste energético instantáneo o la disponibilidad eléctrica local. Este modelo colaborativo se articula en tres niveles de coordinación, detallados en la Tabla 3-5, que abarcan desde el ámbito nacional hasta el despliegue en zona de operaciones.

Nivel de federación	Objetivo principal	Mecanismos asociados
Nacional	Coordinación entre CPD estratégicos y operativos.	SDN, balanceo inter-CPD, métricas M-PUE.
Multinacional	Coordinación de recursos entre aliados FMN.	Políticas STANAG, federación de orquestadores, intercambio seguro de telemetría.
Misión	Redistribución táctica durante operaciones conjuntas.	Planificadores adaptativos y migración inter-nodo bajo enlace satelital o radioenlace.

Tabla 3-5: Escenarios de consolidación energética federada en el marco OTAN/UE.

3.2.5 Tendencias emergentes y líneas de investigación

La literatura técnica y los programas de innovación en defensa evidencian una evolución hacia enfoques más holísticos de eficiencia energética, basados en la integración de métricas, sostenibilidad y resiliencia operativa.

- **Integración de métricas combinadas:** unificación de indicadores energéticos, térmicos y de disponibilidad, conjugando métricas de eficiencia (PUE, M-PUE) con parámetros de fiabilidad como el *Mean Time Between Failures* (MTBF) dentro de un marco común de evaluación.
- **Gestión energética distribuida:** coordinación entre nodos federados mediante políticas comunes de consumo y priorización de carga, especialmente en operaciones conjuntas.
- **Diseño modular y sostenible:** incorporación de componentes reutilizables y configuraciones energéticamente optimizadas para CPD desplegables.

Estas tendencias apuntan hacia infraestructuras militares más eficientes, sostenibles y adaptables, sin comprometer la seguridad ni la disponibilidad operativa. En los CPD estratégicos ya se aplican principios avanzados de sostenibilidad, evaluando no solo el PUE, sino también la Eficacia del Uso del Agua (WUE) [67] y obteniendo certificaciones como LEED [68]. El reto actual es trasladar estos enfoques al ámbito táctico, integrándolos en el factor logístico (F_{log}) de la métrica M-PUE.

3.3 Tendencias y aproximaciones en la gestión y evolución tecnológica

La virtualización ha dejado de ser una tecnología aislada para convertirse en un elemento central de las infraestructuras digitales modernas. En el ámbito de la defensa, esta transformación se traduce en una convergencia entre virtualización, eficiencia operativa y sostenibilidad energética, impulsada por la necesidad de disponer de entornos más flexibles, seguros y autónomos.

A medida que las arquitecturas distribuidas evolucionan, los mecanismos de gestión de recursos también se sofistican. La evolución de los modelos de administración —desde el control manual hasta la orquestación— refleja una tendencia global hacia entornos capaces de adaptarse dinámicamente a las condiciones operativas, de red o de energía. Esta sección examina dichas tendencias, destacando los avances tecnológicos que, sin sustituir los principios clásicos de virtualización, amplían su alcance funcional y estratégico.

3.3.1 Evolución de la gestión de recursos virtualizados

Los sistemas virtualizados han pasado de un modelo estático y jerárquico, basado en configuraciones predefinidas, a entornos dinámicos gestionados por políticas de orquestación. En el sector civil, la automatización basada en herramientas como OpenStack, Kubernetes o Ansible ha permitido escalar servicios en función de la carga y la demanda energética. En defensa, esta evolución se adapta a la necesidad de resiliencia y control, priorizando la trazabilidad, la seguridad y la independencia operativa. Este proceso de maduración tecnológica se sistematiza en la Tabla 3-6, que describe el tránsito desde la administración manual hacia la autonomía adaptativa.

Etapa evolutiva	Tecnologías representativas	Características principales
Administración manual	Scripts, herramientas básicas de virtualización (KVM, Xen).	Control directo y predecible, pero alta carga de gestión y limitada escalabilidad.
Orquestación automatizada	OpenStack, Kubernetes, Terraform, Ansible.	Consolidación y despliegue dinámico con supervisión centralizada; requiere conectividad estable.
Orquestación resiliente	KubeEdge, Lightkube, Rancher Fleet.	Soporta operación local en entornos DDIL y federación segura de nodos <i>edge</i> .
Gestión adaptativa emergente	Planificadores energéticamente conscientes, optimización contextual.	Ajuste de recursos según métricas ambientales y energéticas sin intervención humana.

Tabla 3-6: Evolución de la gestión de recursos virtualizados.

En entornos militares, la transición hacia modelos de orquestación más resilientes se centra en tres ejes: la reducción de la dependencia del enlace con el nivel estratégico, la capacidad de operación autónoma en el borde y la integración de métricas energéticas en las políticas de planificación. Estos principios orientan la evolución hacia sistemas capaces de mantener el equilibrio entre disponibilidad, seguridad y sostenibilidad, incluso bajo condiciones de red degradada.

3.3.2 Gestión basada en métricas energéticas y de servicio

El desarrollo de métricas como el M-PUE ha permitido vincular directamente la eficiencia energética con la planificación operativa de los recursos virtualizados. Esta aproximación constituye un cambio conceptual relevante: la energía deja de ser un parámetro externo y pasa a integrarse como un factor de decisión dentro del ciclo de orquestación.

Las políticas de planificación energética consciente permiten que cada nodo –ya sea un CPD estratégico o un módulo táctico– ajuste su carga, refrigeración y frecuencia de operación según el nivel de energía disponible o las prioridades de misión. De este modo, la infraestructura virtualizada se comporta de forma más sostenible y previsiblemente eficiente. Para instrumentalizar estas políticas, la Tabla 3-7 resume las principales métricas empleadas y su impacto operativo específico.

Tipo de métrica	Aplicación operativa	Beneficio en entornos de defensa
PUE	Relación entre energía total y energía de TI en CPD fijos.	Evaluación de eficiencia estructural y <i>benchmarking</i> con el sector civil.
M-PUE	Métrica adaptada a microrredes y entornos tácticos.	Permite decisiones energéticas contextualizadas y comparables entre despliegues.
MTBF / MTTR	Indicadores de fiabilidad y recuperación del servicio.	Correlacionan disponibilidad operativa con consumo y redundancia.
CEE / EUE (Energy Use Effectiveness)	Métricas emergentes orientadas a sostenibilidad global.	Facilitan la trazabilidad energética y la planificación logística.

Tabla 3-7: Métricas aplicadas en infraestructuras virtualizadas.

La tendencia actual se orienta hacia la combinación de indicadores múltiples que integran eficiencia, disponibilidad y sostenibilidad, aportando una visión holística del rendimiento operativo. Este enfoque se alinea con los objetivos de la OTAN y la UE en materia de infraestructuras verdes y digitalización sostenible, y refuerza la idea de que la gestión energética es una dimensión estratégica de la virtualización.

3.3.3 Hacia una gestión autónoma supervisada

Aunque el presente trabajo no profundiza en modelos de automatización avanzada o inteligencia artificial, la literatura reciente y los programas de innovación en defensa apuntan hacia una evolución natural: la incorporación progresiva de mecanismos de gestión autónoma supervisada. Estos modelos no sustituyen la intervención humana, sino que la complementan con sistemas capaces de ejecutar decisiones limitadas y verificables en función de parámetros operativos predefinidos.

Proyectos como *NATO IST-208* o el European Defence Cloud exploran esta línea de desarrollo, donde los planificadores virtuales pueden adaptar recursos de forma predictiva según la carga, el consumo energético o las condiciones del entorno. Aunque aún se encuentran en fases experimentales, estos enfoques anticipan una futura convergencia entre virtualización, sostenibilidad y automatización verificable.

En este sentido, el reto doctrinal no reside únicamente en la madurez tecnológica, sino en la creación de marcos normativos y metodológicos que garanticen la trazabilidad, la certificación y el control humano de las decisiones automatizadas.

La gestión y evolución tecnológica de los entornos virtualizados en defensa avanza hacia un modelo más flexible, energético y normativamente integrable. El equilibrio entre orquestación automatizada, control humano y sostenibilidad operativa define la línea de progreso inmediato del sector. Estas tendencias, junto con los retos técnicos y normativos identificados, contextualizan la evolución hacia infraestructuras virtualizadas más resilientes y sostenibles.

3.4 Limitaciones y retos actuales

A pesar de los avances tecnológicos y doctrinales descritos en las secciones anteriores, la adopción plena de la virtualización en infraestructuras de defensa sigue condicionada por un conjunto de limitaciones estructurales. Estas limitaciones abarcan no solo aspectos técnicos, sino también factores normativos, operativos, energéticos y organizativos, que determinan la madurez real de las arquitecturas virtualizadas en el entorno militar.

El análisis de estas restricciones permite identificar los márgenes de mejora y los ámbitos en los que las capacidades actuales aún no satisfacen las exigencias de interoperabilidad, seguridad y sostenibilidad establecidas por los marcos ENS, CCN-STIC y FMN Spiral 5.

3.4.1 Limitaciones tecnológicas

Las tecnologías de virtualización más recientes –micro-VM, *unikernels* y entornos basados en contenedores– presentan ventajas claras en eficiencia y ligereza, pero su adopción se ve frenada por un nivel TRL insuficiente para sistemas críticos.

Mientras que los hipervisores clásicos (KVM, Xen, VMware ESXi) se sitúan en un TRL 9 con respaldo normativo consolidado, las soluciones ligeras oscilan frecuentemente en niveles de TRL 5-7, careciendo aún del soporte industrial a largo plazo y las herramientas de auditoría necesarias para la capacidad operativa plena. Esta situación las enfrenta al conocido «Valle de la Muerte» de la adquisición en defensa: la dificultad de pasar del prototipo validado en laboratorio (TRL 6) al sistema de combate desplegado con soporte logístico (TRL 9).

Además, la coexistencia de sistemas heredados con nuevos entornos virtualizados introduce complejidad en la gestión, dificultando la interoperabilidad entre plataformas y niveles de clasificación. Estas barreras se desglosan en la Tabla 3-8, donde se relaciona cada área tecnológica con su impacto operativo directo.

Área tecnológica	Limitación actual	Impacto operativo en defensa
Micro-VM y <i>unikernels</i>	Falta de certificación ENS–ALTA y guías CCN–STIC específicas.	Dificultad para acreditar su uso en dominios clasificados o federados.
Contenedores y orquestadores	Riesgos derivados del <i>kernel</i> compartido y cadena de suministro de imágenes.	Posible propagación lateral de vulnerabilidades entre dominios virtualizados.
Interoperabilidad y orquestación	Orquestadores diseñados para entornos civiles con alta conectividad.	Requieren adaptación para operación DDIL y replicación asíncrona.
Telemetría y sensorización	Falta de estándares unificados en nodos tácticos y microrredes.	Dificulta la aplicación de políticas de consolidación y optimización.

Tabla 3-8: Principales limitaciones tecnológicas en la virtualización aplicada a defensa.

En conjunto, la brecha tecnológica reside en la falta de integración entre innovación y certificación: las herramientas existen, pero su acreditación y trazabilidad no alcanzan todavía los niveles exigidos por la doctrina de seguridad nacional y aliada.

3.4.2 Retos normativos y doctrinales

El marco normativo constituye uno de los factores más determinantes en la adopción de la virtualización en defensa. Aunque el ENS y las guías CCN-STIC ofrecen un marco robusto, su alcance aún no cubre por completo las nuevas tipologías de virtualización ligera, ni define métricas energéticas o de sostenibilidad aplicables a entornos tácticos.

Además, surge un reto geopolítico crítico: el riesgo de *Vendor Lock-in* en soluciones de virtualización propietarias. La dependencia de proveedores no europeos en el núcleo de la infraestructura virtualizada puede comprometer la Soberanía Digital y la capacidad de auditoría profunda del código, un objetivo prioritario de la Brújula Estratégica de la UE.

Asimismo, la doctrina OTAN FMN Spiral 5 ha avanzado notablemente en interoperabilidad y federación de servicios, pero carece todavía de un modelo formal de evaluación de eficiencia operativa o energética, limitando la comparación entre aliados. Con el fin de ofrecer una visión integrada de estos desafíos, la Tabla 3-9 sintetiza los principales vacíos y conflictos detectados.

Dominio normativo	Vacío o conflicto identificado	Consecuencia práctica
ENS	No contempla explícitamente tecnologías ligeras ni marcos de eficiencia energética.	Inseguridad jurídica en su despliegue operativo y en auditorías de conformidad.
Guías CCN-STIC	Cobertura parcial de micro-VM, contenedores y telemetría energética.	Falta de criterios homogéneos para acreditación y supervisión.
FMN Spiral 5	Foco técnico en interoperabilidad, sin incorporar indicadores de eficiencia.	Dificultad para evaluar la sostenibilidad y resiliencia energética en coaliciones.
STANAG	Normas centradas en red y seguridad de datos.	Necesidad de actualización para soportar arquitecturas distribuidas y <i>edge</i> .
Soberanía	Dependencia de hipervisores propietarios de código cerrado.	Riesgo de pérdida de control en la cadena de suministro y dificultad de certificación de alto nivel.

Tabla 3-9: Principales vacíos normativos y doctrinales en la virtualización de defensa.

En síntesis, el marco normativo actual es sólido y garantiza un alto nivel de seguridad en entornos convencionales, pero su ritmo de actualización es inferior al de la evolución tecnológica, lo que genera un desfase que limita la innovación certificada en entornos distribuidos y tácticos.

3.4.3 Limitaciones operativas: la deuda técnica operativa

La operación y el mantenimiento de infraestructuras virtualizadas en defensa requieren una transformación organizativa paralela a la tecnológica. Las restricciones derivadas de la disponibilidad de personal especializado, la logística de mantenimiento y la dependencia de conectividad afectan directamente a la sostenibilidad de los despliegues.

Un factor crítico a menudo ignorado es la «Deuda Técnica Operativa». La necesidad de mantener operativos sistemas de armas y C2 legados, diseñados hace décadas sobre arquitecturas monolíticas, obliga a utilizar técnicas de virtualización pesada (contenedores de sistema o VM) para encapsularlos, impidiendo aprovechar la eficiencia de otras arquitecturas. Esta deuda técnica penaliza el rendimiento global y el consumo energético del CPD táctico.

- **Formación y cualificación técnica:** la adopción de orquestadores, virtualización ligera y gestión energética demanda perfiles técnicos específicos aún escasos en las unidades operativas.
- **Mantenimiento en despliegues prolongados:** la estandarización de hardware y software mejora la interoperabilidad, pero complica la reposición y el soporte técnico en entornos remotos.

- **Gestión de ciclo de vida:** la actualización y el parcheo deben realizarse sin degradar la disponibilidad de servicios críticos, especialmente bajo condiciones DDIL.
- **Dependencia de conectividad:** los sistemas centralizados de gestión y telemetría deben complementarse con mecanismos locales que permitan continuidad operativa ante pérdida de enlace.

Estas limitaciones refuerzan la necesidad de modelos de gestión descentralizados, basados en nodos autónomos pero federados, y de programas de formación continuada en virtualización segura y sostenibilidad digital.

3.4.4 Limitaciones energéticas y de sostenibilidad

El consumo energético y la eficiencia operacional continúan siendo factores críticos en la adopción de la virtualización militar, especialmente en nodos *edge* y despliegues tácticos. Aunque las métricas adaptativas –como el M-PUE– permiten una evaluación contextual, su implementación práctica depende de la disponibilidad de sensores, datos fiables y políticas comunes entre aliados.

- **Variabilidad del suministro:** los entornos tácticos dependen de microrredes híbridas (solar, diésel, baterías) que obligan a priorizar servicios esenciales y ajustar la carga computacional.
- **Gestión térmica y ambiental:** las condiciones extremas (temperatura, humedad, polvo) afectan tanto al rendimiento como al consumo energético de los equipos.
- **Falta de estandarización de métricas:** no existe todavía una referencia doctrinal común para el cálculo y validación de indicadores energéticos operativos.
- **Equilibrio entre eficiencia y resiliencia:** las políticas de ahorro energético deben diseñarse sin comprometer la redundancia y la disponibilidad de servicios críticos.

La sostenibilidad energética se consolida así como un vector estratégico dentro de la defensa digital, vinculando la eficiencia técnica con la autonomía operativa y la reducción del impacto logístico.

3.4.5 Síntesis y proyección

Las limitaciones identificadas evidencian la existencia de un conjunto de brechas estructurales que trascienden la mera cuestión técnica. La Tabla 3-10 sintetiza los principales ámbitos de mejora detectados y su impacto relativo.

Dominio	Brecha principal identificada	Impacto estimado
Tecnológico	Madurez insuficiente (TRL) de tecnologías ligeras y sensorización energética deficiente.	Alto
Normativo	Falta de actualización del ENS y riesgos de Soberanía Digital.	Alto
Operativo-logístico	Deuda técnica de sistemas legados y dependencia de conectividad.	Medio-Alto
Energético	Carencia de métricas estandarizadas y políticas conjuntas de sostenibilidad.	Alto

Tabla 3-10: Síntesis de brechas estructurales en la virtualización de defensa.

En conjunto, la madurez tecnológica, la sostenibilidad energética y la armonización normativa conforman los tres pilares sobre los que debe evolucionar la virtualización de defensa en los próximos años. El reconocimiento de estas limitaciones sirve de base para definir las líneas de mejora metodológica y las oportunidades de innovación que se desarrollan en la siguiente sección.

3.5 Brecha metodológica y oportunidad de innovación

El análisis conjunto de las secciones anteriores pone de manifiesto una brecha significativa entre la madurez tecnológica alcanzada por la virtualización en defensa y la ausencia de un marco metodológico homogéneo que permita evaluarla, acreditarla y optimizarla de forma sistemática. Esta brecha no responde únicamente a factores técnicos, sino también a la falta de procedimientos normalizados que integren criterios de seguridad, eficiencia energética y sostenibilidad operativa bajo un mismo enfoque de evaluación.

El desarrollo de metodologías adaptadas a la singularidad de los entornos militares, caracterizados por la movilidad, la heterogeneidad de plataformas y la operación en condiciones DDIL, constituye por tanto una necesidad estructural. La virtualización se ha convertido en un elemento transversal que afecta simultáneamente al diseño, la gestión y la acreditación de los CPD distribuidos, lo que exige disponer de mecanismos de evaluación comparables, trazables y auditables.

3.5.1 Identificación de la brecha metodológica

A nivel internacional, la mayoría de los marcos de referencia existentes –como ISO/IEC 30134 [42, 44, 43], EN 50600 [69] o las métricas de eficiencia definadas por The Green Grid [16]– están orientados a infraestructuras civiles. Estos modelos se centran en el rendimiento energético o la disponibilidad de los sistemas, pero no contemplan factores tácticos, condiciones de conectividad limitada ni requisitos de acreditación multinivel.

En el ámbito militar, las doctrinas OTAN y los estándares nacionales (ENS, CCN–STIC) abordan la seguridad y la interoperabilidad, pero carecen de un marco metodológico que relacione estas dimensiones con el rendimiento técnico y energético de las plataformas virtualizadas.

El resultado es una fragmentación evaluativa: un CPD puede tener un PUE excelente, pero ser normativamente inseguro (incumpliendo CCN-STIC-220 [6]); o puede ser perfectamente seguro (ENS-ALTA), pero logísticamente insostenible en un despliegue DDIL.

La Tabla 3-11 resume los principales vacíos detectados:

Dominio de evaluación	Situación actual	Brecha metodológica identificada
Seguridad y acreditación	Regulada por ENS y guías CCN–STIC.	Ausencia de integración con métricas de rendimiento y sostenibilidad.
Eficiencia energética	Regida por ISO/IEC 30134 y The Green Grid.	No adaptada a condiciones operativas ni a entornos DDIL.
Interoperabilidad aliada	Establecida en doctrina FMN Spiral 5 y STANAG.	No incorpora variables de eficiencia, consumo o sostenibilidad de misión.
Virtualización distribuida	Evaluada mediante indicadores técnicos locales.	Falta de metodología unificada para comparar despliegues estratégicos, operativos y tácticos.

Tabla 3-11: Vacíos metodológicos en la evaluación de infraestructuras virtualizadas de defensa.

3.5.2 Oportunidades de innovación y líneas de mejora

El cierre de esta brecha metodológica abre un amplio campo de innovación en materia de defensa digital. La consolidación de un marco unificado permitiría no solo medir con precisión la eficiencia y la seguridad de las infraestructuras virtualizadas, sino también optimizar su diseño y su operación conforme a criterios objetivos y reproducibles.

Se identifican cuatro líneas prioritarias de mejora:

- **Integración de métricas técnicas y normativas:** desarrollo de un marco de evaluación que combine indicadores de seguridad (ENS–CCN–STIC), interoperabilidad (FMN–STANAG) y eficiencia energética (M–PUE), proporcionando una visión completa del rendimiento del sistema.
- **Adaptación de las métricas a escenarios operativos:** incorporación de factores de corrección que reflejen las condiciones ambientales, la disponibilidad de energía y la conectividad de cada nivel de despliegue (estratégico, operativo o táctico).
- **Estandarización de la telemetría energética y operacional:** definición de parámetros mínimos y protocolos de intercambio de datos que permitan comparar el rendimiento de los CPD y nodos virtualizados entre unidades o aliados.
- **Acreditación unificada de infraestructuras virtualizadas:** establecimiento de un procedimiento de certificación que valore de forma conjunta la seguridad, eficiencia y sostenibilidad, reduciendo duplicidades en los procesos de auditoría.

Estas oportunidades de innovación no requieren el desarrollo de nuevas tecnologías disruptivas, sino la articulación de una metodología de evaluación integral que combine principios técnicos, doctrinales y normativos. Su aplicación permitiría medir con rigor la madurez digital de una infraestructura de defensa y orientar las inversiones hacia soluciones verdaderamente sostenibles y resilientes.

A continuación, la Tabla 3-12 sintetiza de forma explícita cómo cada vacío identificado en el estado del arte se traduce en un requisito cubierto por los componentes del marco IGEO propuesto.

Limitación del Estado del Arte	Impacto en Defensa	Solución Propuesta (TFM)
Métricas energéticas civiles (PUE)	Ignoran la logística de combustible y el entorno hostil.	M-PUE: Incorpora factores F_{log} y F_{amb} para penalizar el coste real en zona de operaciones.
Evaluación normativa estanca	Seguridad y eficiencia se tratan como silos separados.	IGEO: Integra cumplimiento (ICOMP) y eficiencia en un único índice de decisión.
Modelos de decisión binarios	No consideran la degradación progresiva del servicio.	Modelo Multiescala: Asigna tecnologías según la prioridad táctica (E1/E2/E3).
Validación de tecnologías ligeras	Incertidumbre sobre el uso de micro-VM y <i>unikernels</i> .	Análisis ICOMP: Cuantifica el grado de aislamiento real para validar su uso en entornos tácticos.

Tabla 3-12: Relación entre las limitaciones del estado del arte y las soluciones metodológicas aportadas.

En conclusión, el análisis realizado en este capítulo demuestra que la virtualización en defensa carece de un marco metodológico integrador. Mientras la literatura civil optimiza el PUE (coste económico) y la doctrina militar prioriza la seguridad, no existe un modelo previo que cuantifique la «penalización operativa» de aplicar seguridad estricta en entornos energéticamente hostiles.

Cubrir este vacío constituye el punto de partida del marco IGEO propuesto en el siguiente capítulo, que se presenta como una respuesta sistemática para evaluar, de forma simultánea, la eficiencia, la resiliencia y la interoperabilidad de la infraestructura.

4 METODOLOGÍA INTEGRADA Y MARCO DE EVALUACIÓN PARA ENTORNOS VIRTUALIZADOS DE DEFENSA

Este capítulo desarrolla el núcleo metodológico del Trabajo Fin de Máster. Tras haber caracterizado en los capítulos precedentes los fundamentos técnicos, operativos y doctrinales que condicionan la virtualización de CPD en defensa, se presenta aquí un marco integrado de evaluación orientado a entornos militares modernos. Su finalidad es proporcionar una herramienta rigurosa, sistemática y adaptativa que permita analizar y comparar arquitecturas virtualizadas bajo condiciones reales de operación, incluyendo escenarios DDIL, restricciones energéticas y exigencias normativas.

A diferencia de los enfoques civiles o exclusivamente técnicos, el método propuesto combina tres dimensiones críticas y mutuamente dependientes: **eficiencia energética, resiliencia y continuidad de los servicios virtualizados**, y **cumplimiento doctrinal y normativo**. El capítulo articula esta aproximación mediante una estructura que integra fundamentos, principios, arquitectura conceptual, métricas e ilustración aplicada.

En primer lugar, se expone la finalidad estratégica del método y su función dentro de un ciclo continuo de evaluación. A continuación, se presentan los principios doctrinales, operativos y energéticos que sustentan la metodología. Sobre esta base se describe la estructura conceptual del modelo, diseñada para operar en los niveles estratégico, operativo y táctico. Posteriormente se introducen las métricas e indicadores que permiten evaluar de forma cuantitativa el rendimiento, la eficiencia y el cumplimiento normativo. Finalmente, se aplican estos elementos en una serie de escenarios representativos en condiciones DDIL, como paso previo al análisis detallado del Capítulo 5.

El resultado es un marco metodológico **coherente, trazable y aplicable**, alineado con las prácticas de ingeniería de sistemas, la doctrina OTAN FMN y la normativa española de seguridad. Este capítulo define, en suma, *cómo evaluar* la virtualización en defensa de manera integrada, reproducible y válida para la toma de decisiones en los distintos niveles de mando.

4.1 Fundamentación y propósito estratégico del método

La transformación digital en defensa ha situado a los CPD en el núcleo funcional de las operaciones contemporáneas. En este contexto, la virtualización adquiere un carácter decididamente estratégico: no sólo debe optimizar recursos, sino garantizar continuidad de servicio, autonomía operativa y cumplimiento normativo en entornos caracterizados por restricciones energéticas severas, variabilidad ambiental y condiciones DDIL.

Esta realidad introduce una tensión estructural que se manifiesta en tres dominios estrechamente vinculados: el energético, el operativo y el normativo-doctrinal.

- **Dimensión energética:** Responde a la escasez de recursos y la complejidad logística de su suministro. Los despliegues avanzados dependen de microrredes híbridas o generadores, cuya estabilidad resulta crítica para garantizar la continuidad del procesamiento.
- **Dimensión operativa:** Los servicios virtualizados deben mantener su funcionalidad ante degradaciones de red, latencias elevadas o desconexiones parciales, asegurando en todo momento la autonomía local.
- **Dimensión normativa:** Incluso en entornos degradados, es imprescindible cumplir con los principios del ENS, las guías CCN-STIC y las directrices FMN, que imponen requisitos de trazabilidad e integridad del servicio.

De esta combinación de tensiones surge la necesidad de un **marco metodológico integrado** capaz de evaluar y comparar estrategias de virtualización de manera coherente en los tres niveles doctrinales —estratégico, operativo y táctico—. Los enfoques tradicionales suelen centrarse únicamente en la eficiencia de cómputo o en el cumplimiento normativo, descuidando la interacción entre estos dominios; otros modelos, más orientados al ámbito civil, obvian la criticidad del comportamiento bajo DDIL o la dependencia logística del suministro energético. En consecuencia, en defensa requiere un método específico que articule una evaluación sistemática y reproducible de las arquitecturas virtualizadas de sus CPD.

Esta propuesta se ilustra en la Figura 4-1, donde se visualiza la tensión entre la prioridad normativa (ICOMP) y la restricción energética (M-PUE) en los tres niveles doctrinales. Como se observa en el esquema, el marco IGEO adapta la tecnología (VM, Híbrido, Micro-VM) según la presión inversa de las bandas superior e inferior, garantizando la viabilidad operativa en el borde táctico.

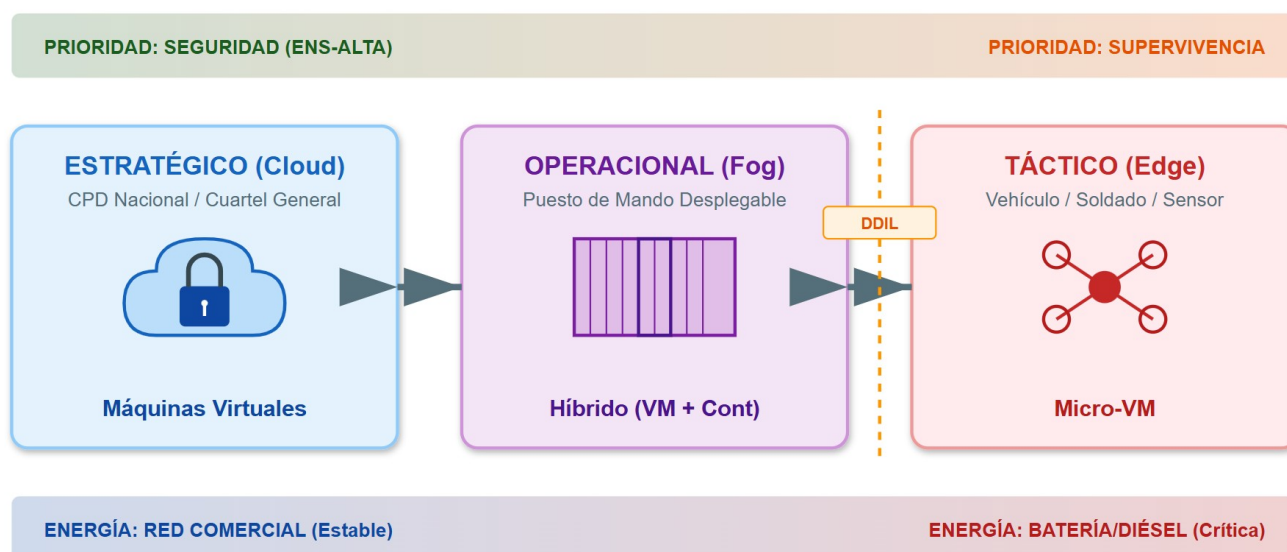


Figura 4-1: Estructura conceptual del continuo de computación en Defensa. Fuente: Elaboración propia.

El propósito de la metodología presentada en este capítulo es precisamente cubrir esa brecha. Su función es doble. En primer lugar, actúa como herramienta de evaluación, proporcionando un conjunto estructurado de criterios y métricas que permiten valorar el rendimiento energético, operativo y normativo de un CPD virtualizado, independientemente de su escala o ubicación en la cadena de mando. En segundo lugar, opera como guía de diseño, ofreciendo un proceso formal que ayuda a configurar arquitecturas más eficientes, resilientes y acreditables, sin prescribir tecnologías concretas. La metodología mantiene una estricta neutralidad tecnológica para evaluar, en condiciones homogéneas, hipervisores de tipo 1, contenedores, micro-VM o *unikernels*.

Este enfoque se apoya en varios principios que vertebran su aplicación. La integración multiescala garantiza que los resultados sean comparables entre los niveles estratégico, operativo y táctico, respetando las diferencias funcionales entre CPD permanentes, módulos avanzados y nodos ligeros. La adaptabilidad contextual permite ajustar la evaluación a las condiciones energéticas, ambientales y de conectividad propias de cada entorno, evitando marcos rígidos que pierden validez en despliegues reales. La trazabilidad normativa asegura la alineación continua con los controles ENS y CCN-STIC, lo que facilita auditorías y procesos de acreditación. La sostenibilidad operativa, por su parte, sitúa la eficiencia energética como un requisito táctico, no como un objetivo accesorio: un diseño energéticamente eficiente incrementa la autonomía, agiliza la maniobra y reduce la carga logística. Por último, la neutralidad tecnológica permite comparar configuraciones dispares mediante criterios comunes, evitando sesgos derivados de la adopción exclusiva de un paradigma de virtualización.

En conjunto, esta sección establece el fundamento conceptual del método y su razón de ser operativa. La defensa moderna exige mecanismos evaluativos que reflejen simultáneamente las realidades energéticas, normativas y operativas de los CPD. El marco metodológico que se desarrolla a continuación responde a esa necesidad mediante una estructura cohesionada que integra principios, arquitectura conceptual y métricas cuantitativas. A partir de esta base, el capítulo avanza hacia la definición precisa de los elementos que conforman el método y su articulación práctica en escenarios característicos del entorno militar.

4.2 Principios doctrinales, operativos y energéticos del marco

El método propuesto se apoya en un conjunto de principios que garantizan su coherencia, su validez en los distintos niveles doctrinales y su aplicabilidad en entornos caracterizados por limitaciones energéticas, variabilidad operativa y exigencias normativas estrictas. Estos principios no se plantean como requisitos aislados, sino como dimensiones interdependientes que configuran el comportamiento global del marco metodológico. Su reagrupación en tres bloques –doctrinales, operativos y energéticos-logísticos– permite articular una base sólida y consistente sobre la que evaluar las estrategias de virtualización en los CPD de defensa.

En el primer bloque, los **principios doctrinales** aseguran la alineación del método con los marcos de referencia nacionales e internacionales que regulan la seguridad, la interoperabilidad y la gestión de sistemas de información en defensa. Incluyen el respeto a los principios del ENS, la aplicación de las guías CCN-STIC relevantes y la adopción de las directrices OTAN FMN, especialmente en materia de interoperabilidad multinacional y operación en red. Este bloque obliga a que cualquier evaluación o recomendación derivada del método mantenga trazabilidad normativa, auditabilidad y compatibilidad con los procesos formales de acreditación.

El segundo bloque recoge los **principios operativos**, orientados a garantizar que las estrategias de virtualización respondan a la realidad dinámica de los despliegues militares. Este grupo integra la capacidad de autonomía local, la resiliencia frente a condiciones DDIL y la adaptabilidad contextual de las configuraciones virtualizadas. El método incorpora estos aspectos mediante la priorización de arquitecturas y políticas de gestión capaces de mantener servicios esenciales –autenticación, mensajería, DNS, C2– aun cuando la conectividad sea intermitente o el entorno experimente degradaciones severas. En consonancia con la estructura jerárquica de las operaciones militares, este bloque se articula para ser aplicable en los niveles estratégico, operativo y táctico, manteniendo coherencia conceptual entre ellos.

Finalmente, los **principios energéticos y logísticos** definen la relación entre la virtualización y el consumo eléctrico, integrando la sostenibilidad operativa como eje central del método. Este grupo reconoce que la eficiencia energética no es un objetivo secundario, sino un requisito táctico que condiciona la autonomía, la maniobrabilidad y la carga logística asociada a los despliegues. La virtualización debe contribuir a la reducción del consumo total, la optimización de la densidad de carga útil y la disminución de la dependencia del reabastecimiento energético. Asimismo, estos principios fomentan la modularidad y escalabilidad del despliegue, permitiendo adaptar la huella energética a las necesidades operativas reales.

La Tabla 4-1 sintetiza los tres bloques de principios y su correspondencia con los marcos doctrinales y las funciones que desempeñan dentro del método. Su función es ofrecer una visión unificada de los fundamentos que estructuran el marco, facilitando su lectura transversal y asegurando su alineación con la doctrina vigente.

Bloque de principios	Referencia doctrinal / normativa	Propósito dentro del método
Principios doctrinales	ENS (RD 311/2022), CCN-STIC, FMN Spiral 5	Asegurar trazabilidad normativa, integridad del servicio, auditabilidad continua y compatibilidad con procesos de acreditación y marcos de interoperabilidad aliados.
Principios operativos	FMN-DDIL, doctrina conjunta de operaciones, guías de despliegue modular	Garantizar continuidad de servicios esenciales, autonomía local, resiliencia ante degradaciones y adaptabilidad a niveles estratégico, operativo y táctico.
Principios energéticos y logísticos	NATO IST-208, <i>Green Defence Framework</i> , prácticas de eficiencia modular	Optimizar la sostenibilidad energética, reducir la carga logística, mejorar la densidad de carga útil y promover modularidad y escalabilidad del despliegue virtualizado.

Tabla 4-1: Principios doctrinales, operativos y energéticos del marco metodológico.

Este conjunto de principios constituye la base estructural del marco metodológico. Su integración permite que la evaluación de las estrategias de virtualización mantenga un equilibrio adecuado entre innovación técnica, sostenibilidad operativa y cumplimiento regulatorio. A partir de esta fundamentación, el capítulo avanza hacia la definición de la **estructura conceptual del método**, donde se articulan los planos técnico, operativo y normativo que conforman su arquitectura general.

4.3 Estructura conceptual del método

La eficacia del marco metodológico propuesto depende de su capacidad para integrar, de forma coherente, los distintos planos que intervienen en la gestión de infraestructuras virtualizadas en defensa. Para ello, el método se articula en torno a una estructura conceptual basada en tres planos funcionales que permiten descomponer la complejidad del entorno sin perder trazabilidad, coherencia ni alineamiento doctrinal. Estos planos actúan como perspectivas complementarias de un mismo proceso de evaluación continua, garantizando que el análisis responda tanto a los requisitos de rendimiento como a las exigencias de seguridad, interoperabilidad y sostenibilidad energética.

El **plano técnico** constituye la base empírica del método y proporciona la información necesaria para comprender el comportamiento real de la infraestructura virtualizada. En este nivel se identifican los recursos disponibles, se clasifican las tecnologías empleadas –hipervisores de tipo 1, máquinas virtuales, contenedores, micro-VM o *unikernels*– y se recopilan datos de telemetría energética y operativa procedentes del CPD o del módulo desplegable. La descripción de los sistemas sigue una aproximación estructurada compatible con ISO/IEC 42010 [70], de manera que los componentes, sus dependencias y los flujos energéticos puedan modelarse de forma abstracta y verificable. Este plano permite alimentar el método con datos completos, trazables y compatibles con la auditoría continua exigida por el ENS.

El **plano operativo** transforma la información técnica en conocimiento orientado a la toma de decisiones. Opera como un nivel intermedio que interpreta métricas, valora configuraciones alternativas y determina la idoneidad de cada estrategia de virtualización en función del contexto doctrinal (estratégico, operativo o táctico) y de las condiciones energéticas o ambientales del despliegue. Este plano integra la lógica de operación en condiciones DDIL, priorizando arquitecturas capaces de sostener servicios críticos –como autenticación, resolución de nombres, mensajería o funciones C2– aun en ausencia de conectividad estable. Asimismo, incorpora criterios de consolidación dinámica, replicación adaptativa y redistribución de cargas, evaluando su impacto en la eficiencia energética, la continuidad del servicio y la sostenibilidad logística.

Finalmente, el **plano normativo** proporciona el marco de control que legitima y verifica el proceso metodológico. Recoge los requisitos aplicables del ENS, las guías CCN-STIC de referencia y las directrices OTAN FMN en materia de interoperabilidad, disponibilidad y gobernanza de la información. Este plano no actúa como un simple listado de controles: constituye la capa que garantiza que todas las decisiones y estrategias propuestas sean trazables, auditables y compatibles con los procesos de acreditación que rigen los sistemas de información de defensa. Incluye mecanismos de registro, validación documental y verificación del cumplimiento, asegurando que el modelo responda a la estructura regulatoria en la que deben operar los CPD militares.

La interacción entre estos tres planos se articula mediante un **ciclo continuo de evaluación** que estructura el funcionamiento del método. El proceso comienza con la medición técnica del comportamiento de la infraestructura, continúa con la interpretación operativa de los datos y culmina con la verificación normativa del grado de cumplimiento y la generación de evidencias auditables. Los resultados de este ciclo realimentan el sistema, actualizando umbrales, ajustando políticas y refinando configuraciones en un proceso iterativo que favorece la mejora continua y la adaptación del diseño a las necesidades cambiantes del entorno.

Esta estructura conceptual dota al método de claridad, modularidad y coherencia doctrinal. La separación funcional entre planos no implica compartimentos estancos, sino un reparto natural de responsabilidades que permite evaluar infraestructuras virtualizadas desde una perspectiva integral. De este modo, el modelo es aplicable tanto al análisis diagnóstico de CPD existentes como al diseño de nuevas arquitecturas más eficientes, resilientes y acreditables. Sobre esta base, la siguiente sección desarrolla las **métricas e indicadores** que operacionalizan el método y permiten cuantificar su aplicación en escenarios reales y condiciones DDIL.

4.4 Métricas e indicadores

El valor del método propuesto depende de la capacidad de traducir los principios técnicos, operativos y normativos en un conjunto de indicadores cuantificables que permitan evaluar, de forma objetiva, el rendimiento de las infraestructuras virtualizadas. En el ámbito de la defensa, donde las decisiones deben sustentarse en datos auditables y compatibles con los procesos de acreditación, la definición de un sistema métrico sólido es esencial para comparar configuraciones, identificar oportunidades de mejora y apoyar decisiones de diseño, despliegue y acreditación para orientar la modernización del CPD.

Las métricas aquí presentadas se conciben con la flexibilidad suficiente para aplicarse tanto en CPD estratégicos permanentes como en módulos desplegables y nodos tácticos bajo condiciones DDIL.

El modelo metriza tres dimensiones fundamentales: la eficiencia energética, a través del M-PUE; la resiliencia operativa, mediante indicadores derivados de la ingeniería de alta disponibilidad; y la madurez normativa y arquitectónica, evaluada según la capacidad del entorno para implementar aislamiento, microsegmentación y trazabilidad conforme a las guías ENS y CCN-STIC. Estas dimensiones no actúan de manera independiente: representan los tres vectores que condicionan la sostenibilidad, continuidad y legitimación de cualquier infraestructura virtualizada en defensa. El método ofrece una visión integrada del equilibrio entre estos elementos, evitando optimizaciones parciales que puedan comprometer la operación o la seguridad.

4.4.1 Métricas energéticas: la métrica M-PUE

El componente energético se evalúa mediante la métrica M-PUE, una extensión del PUE tradicional adaptada a las condiciones operativas y logísticas de los entornos militares. A diferencia del PUE convencional, que evalúa la eficiencia en centros de datos fijos y climatizados, el M-PUE integra factores que representan la estabilidad de la fuente energética, la influencia del entorno físico y la eficiencia de la tecnología de virtualización empleada.

Para la definición de los coeficientes de penalización (F_{gen} , F_{amb} , F_{log} , F_{virt}), se ha adoptado sistemáticamente un enfoque de *diseño del peor caso* (*worst-case design*). Se seleccionan los valores superiores de los rangos documentados en estándares internacionales de climatización –concretamente las directrices de la **ASHRAE** (*American Society of Heating, Refrigerating and Air-Conditioning Engineers*) para equipamiento Clase A4– [71], para garantizar que el modelo resultante sea robusto incluso en las condiciones más adversas, evitando falsos positivos de eficiencia.

$$M-PUE = \frac{E_{total}}{E_{TI}} \times (F_{gen} \times F_{amb} \times F_{log} \times F_{virt}) \quad (4.1)$$

donde los componentes del modelo se definen como:

- E_{total} : Energía total suministrada al módulo o CPD (medida en acometida o generador).
- E_{TI} : Energía estrictamente consumida por los sistemas de cómputo, red y almacenamiento.
- F_{gen} (Factor de Generación): Estabilidad y rendimiento de la fuente energética (microrred híbrida, diésel, solar). Penaliza las pérdidas por conversión AC/DC e ineficiencias en microrredes híbridas o generadores tácticos (≥ 1.0).
- F_{amb} (Factor Ambiental): Penalización por condiciones térmicas o ambientales adversas que obligan a un sobreesfuerzo de los sistemas de climatización.
- F_{virt} (Factor de Virtualización): Eficiencia relativa según la tecnología de virtualización. Representa el *overhead* computacional introducido por la capa de software (VM, contenedores, micro-VM), siendo siempre ≥ 1.0 .
- F_{log} (Factor Logístico): Impacto logístico del transporte y reposición energética en zona de operaciones.

Las penalizaciones F_{gen} , F_{amb} , F_{log} y F_{virt} no se asignan de manera arbitraria: derivan de umbrales documentados en ASHRAE TC 9.9 [71], el White Paper 49 de The Green Grid [16] o MIL-STD-1472 [72] que condicionan la operación en modo degradado. Cada penalización representa la traslación cuantitativa de un requisito operativo o ambiental a un coeficiente multiplicativo que ajusta el M-PUE a condiciones reales de despliegue.

Para garantizar trazabilidad y comparabilidad, se adoptan los niveles L1–L3 del White Paper 49 de The Green Grid [16]. Su adaptación al entorno militar se resume en la Tabla 4-2, que diferencia la granularidad de instrumentación en función del tipo de despliegue.

Aspecto	L1 (Básico)	L2 (Intermedio)	L3 (Avanzado)
Punto de medición principal (E_{total})	Acometida general o salida del generador táctico.	Acometida con submedición parcial de climatización y distribución.	Submedición completa de HVAC, UPS y auxiliares con reconciliación energética.
Punto de medición TI (E_{TI})	Salida de UPS o cuadro TI.	PDU de fila o rack.	Medida en toma individual por servidor o dispositivo.
Intervalo de muestreo	≤ 15 min (instrumentación portátil).	≤ 15 min (agregación automática parcial).	≤ 15 min (telemetría continua BMS/DCIM).
Ámbito recomendado	Nodos tácticos.	CPD operativo.	CPD estratégico.

Tabla 4-2: Niveles L1–L3 para el cálculo del M-PUE en entornos de defensa.

4.4.2 Métricas operativas y de resiliencia

La resiliencia operativa se fundamenta en los principios de **Alta Disponibilidad (HA)**, que permiten cuantificar de forma objetiva la fiabilidad y la capacidad de recuperación de un sistema. En un entorno DDIL, la resiliencia no se define sólo por la ausencia de fallos, sino por la rapidez con la que el sistema recupera su funcionalidad tras una degradación o pérdida temporal de recursos.

El indicador central es la **Disponibilidad Efectiva (A_{ef})**, definida mediante las métricas estándar de ingeniería de sistemas:

$$A_{ef} = \frac{MTBF}{MTBF + MTTR} \quad (4.2)$$

donde el **Tiempo Medio entre Fallos (MTBF)** cuantifica la fiabilidad del sistema, y el **Tiempo Medio de Reparación (MTTR)** refleja la capacidad de recuperación. En entornos virtualizados, el MTTR se reduce significativamente gracias a técnicas como la migración en caliente o el relanzamiento automático de instancias, lo que incrementa la resiliencia en comparación con infraestructuras físicas tradicionales.

Sobre esta base, el **Índice de Resiliencia Operativa (IRO)** se formula como:

$$IRO = A_{ef} \times \max\left(0, 1 - \frac{L_{med}}{L_{max}}\right) \quad (4.3)$$

Este indicador integra la disponibilidad efectiva con la calidad del servicio. Las variables de red se definen como:

- L_{med} (Latencia Media): Retardo promedio medido en el enlace de misión durante el ciclo de evaluación.
- L_{max} (Latencia Máxima Tolerable): Umbral de latencia a partir del cual el servicio crítico (ej. C2 o voz) se considera degradado funcionalmente.

Nota: Se introduce la función $\max(0, \dots)$ para acotar el índice a 0 en casos teóricos de saturación donde la latencia medida supere el umbral máximo tolerable ($L_{med} > L_{max}$), evitando resultados negativos sin sentido físico.

El IRO ofrece así una medida sintética y directamente auditable del comportamiento del sistema bajo condiciones DDIL.

4.4.3 Métricas normativas y de arquitectura de seguridad

La evaluación normativa del entorno no se limita al cumplimiento de controles, sino que considera la madurez arquitectónica necesaria para sostener operaciones seguras en el marco del ENS, las guías CCN-STIC y la doctrina OTAN FMN. Esta aproximación se concreta en el ICOMP, basado en tres ejes que representan componentes estructurales de una arquitectura de seguridad moderna, alineada con los principios ZTNA:

- **Grado de Aislamiento (GA):** mide la robustez del aislamiento entre cargas de trabajo, elemento central para la soberanía del dato y alineado con CCN-STIC-220.
- **Capacidad de Microsegmentación (CM):** evalúa la posibilidad de aplicar controles granulares de tráfico «este-oeste» entre servicios virtualizados, pilar fundamental de las arquitecturas ZTNA.
- **Nivel de Trazabilidad (NT):** valora la integridad, completitud y verificabilidad de los registros de auditoría, en coherencia con las exigencias del ENS (RD 311/2022).

El índice se calcula mediante una suma ponderada de estos factores:

$$ICOMP = w_{GA} \times GA + w_{CM} \times CM + w_{NT} \times NT \quad (4.4)$$

Donde los componentes se definen como:

- w_{GA}, w_{CM}, w_{NT} : Coeficientes de ponderación interna que permiten ajustar el modelo al perfil de seguridad (por defecto se asumen equiprobables: $1/3$).
- GA, CM, NT : Variables de estado normalizadas en el rango $[0, 1]$ que evalúan la madurez de la implementación técnica de cada medida.

4.4.4 Integración de métricas: el Índice Global de Eficiencia Operativa

El método sintetiza las tres dimensiones anteriores mediante el IGEO, definido como:

$$IGEO = w_E \cdot \left(\frac{1}{M-PUE} \right) + w_O \cdot IRO + w_N \cdot ICOMP \quad (4.5)$$

Donde los coeficientes de ponderación estratégica (w_E, w_O, w_N) cumplen la condición de cierre $\sum w_i = 1$. Esta normalización es necesaria para acotar el valor del índice IGEO entre 0 y 1, facilitando su interpretación doctrinal como un porcentaje de idoneidad operativa. Los pesos representan la prioridad del Mando:

- w_E : Peso asignado a la **Eficiencia Energética** y sostenibilidad logística.
- w_O : Peso asignado a la **Resiliencia Operativa** y continuidad del servicio.
- w_N : Peso asignado al **Cumplimiento Normativo** y seguridad doctrinal.

4.4.5 Justificación de las ponderaciones: Postura ante el riesgo e intención del mando

Los coeficientes de ponderación (w_E, w_O, w_N) no son valores estáticos; constituyen la traducción matemática de la «Postura ante el Riesgo» y de la «Intención del Mando» para una operación específica. Su ajuste permite que el IGEO refleje la realidad táctica y estratégica del despliegue:

- **Escenario estratégico (territorio nacional):** Se adopta una «alta aversión al riesgo». El Mando prioriza la trazabilidad y la seguridad jurídica sobre la eficiencia inmediata.
Configuración típica: $w_N = 0.5$ (Normativa dominante), $w_E = 0.3$, $w_O = 0.2$.
- **Escenario operacional (base desplegada):** Se busca un equilibrio sostenido. La eficiencia logística cobra importancia para reducir la huella, pero sin comprometer la seguridad de la información de coalición.
Configuración típica: $w_O = 0.4$, $w_E = 0.4$, $w_N = 0.2$.
- **Escenario táctico (edge, DDIL):** El Mando asume un riesgo controlado para garantizar la supervivencia de la misión («Mission Command»). La prioridad absoluta es la autonomía energética y la continuidad del servicio.
Configuración típica: $w_O = 0.5$ (Resiliencia crítica), $w_E = 0.4$, $w_N = 0.1$.

Este enfoque convierte el IGEO en un sistema de soporte a la decisión flexible, capaz de modelar matemáticamente el «trade-off» inherente a la conducción de operaciones militares.

4.4.6 Algoritmo de decisión estratégica y condiciones de contorno

La integración de las métricas en el índice IGEO permite formalizar la toma de decisiones. Sin embargo, para garantizar que la solución seleccionada sea viable y segura, el algoritmo incorpora «Condiciones de Contorno» (*Constraints*) basadas en la madurez tecnológica (TRL). No basta con que una tecnología sea eficiente; primero debe ser lo suficientemente madura para el nivel de criticidad del sistema.

Para facilitar la comprensión global del modelo, la Figura 4-2 ilustra el flujo completo de procesamiento.

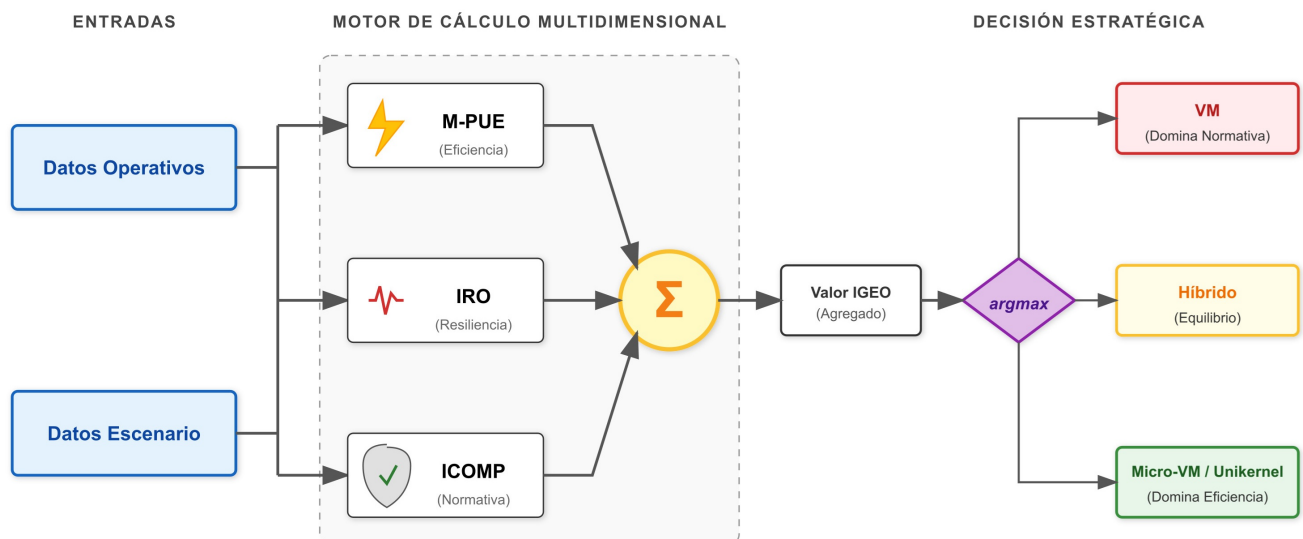


Figura 4-2: Arquitectura funcional del método IGEO. Fuente: Elaboración propia.

El estado final se determina mediante la siguiente función de optimización con restricciones:

$$T_{opt} = \underset{t \in \mathcal{T}}{\operatorname{argmax}}(IGEO(t)) \quad \text{sujeto a: } TRL(t) \geq TRL_{req} \quad (4.6)$$

Donde T_{opt} representa la tecnología óptima seleccionada del conjunto de candidatos $\mathcal{T} = \{\text{VM}, \text{Contenedor}, \text{Micro-VM}/\text{Unikernel}\}$. La restricción de TRL actúa como un «Veto Tecnológico»:

- **En Nivel estratégico (E1):** Se exige $TRL \geq 9$. Esto suele filtrar tecnologías experimentales como los *unikernels*, favoreciendo a las VM por su robustez normativa, independientemente de su menor eficiencia energética.
- **En Nivel táctico (E3):** Se acepta $TRL \geq 6 - 7$. Esto habilita el uso de Micro-VMs y Contenedores ligeros, permitiendo que su superior eficiencia energética M-PUE domine la función de selección.

Una vez superado el umbral de madurez, el motor de cálculo determina la tecnología ganadora según las prioridades del IGEO, generando tres zonas de decisión claras:

- **Selección de VM (Dominio Normativo):** Se activa cuando el escenario prioriza la seguridad ($w_N \geq 0.5$). Matemáticamente, la máquina virtual maximiza el índice gracias a su componente de cumplimiento ($ICOMP \approx 1.0$), siendo la opción obligada para CPD estratégicos donde la trazabilidad prima sobre el consumo.
- **Selección Híbrida/Contenedor (Equilibrio):** Se activa como solución de compromiso cuando ningún factor domina por sí solo. Maximiza el índice en escenarios operacionales que requieren agilidad de despliegue sin renunciar a una base de seguridad moderada.
- **Selección de micro-VM / *unikernel* (Prioridad Eficiencia):** Se activa en escenarios tácticos donde la suma de pesos operativos y energéticos ($w_O + w_E$) es dominante.
 - El **micro-VM** se selecciona como estándar general por su equilibrio entre ligereza y capacidad de aislamiento verificable.
 - El ***unikernel*** queda reservado para funciones específicas de nicho (sensores, sistemas embebidos o tiempo real) donde la restricción energética es crítica y se acepta una menor trazabilidad normativa a cambio de máxima supervivencia operativa.

Este algoritmo asegura que la recomendación estratégica no sea solo eficiente numéricamente, sino «doctrinalmente viable», evitando el despliegue de soluciones inmaduras en nodos críticos.

El método propuesto no pretende predecir valores absolutos de consumo o disponibilidad, sino comparar configuraciones de forma homogénea bajo supuestos controlados, permitiendo identificar tendencias relativas y compromisos estratégicos.

4.5 Ejemplo ilustrativo de aplicación del método

Con el fin de reforzar la trazabilidad y reproducibilidad del marco, este apartado presenta un ejemplo numérico completo de aplicación del método IGEO. Se detallan los valores de entrada, los coeficientes empleados y el cálculo paso a paso de cada métrica. Este ejemplo no pretende representar un despliegue real clasificado, sino ilustrar de forma transparente el funcionamiento interno del modelo matemático.

El modelado analítico y los cálculos presentados en este capítulo y en los escenarios posteriores se han implementado mediante una herramienta de hoja de cálculo parametrizada. Esto permite reproducir los resultados variando los coeficientes de penalización definidos en las tablas de referencia, garantizando la consistencia aritmética del análisis.

Datos de entrada

Se considera un CPD operativo con las siguientes condiciones:

- Energía total suministrada: $E_{total} = 5.2$ kWh
- Energía TI consumida: $E_{TI} = 3.6$ kWh
- Fuente energética: red local estable ($F_{gen} = 1.01$)
- Condiciones ambientales: templadas ($F_{amb} = 1.00$)
- Tecnología: contenedores ($F_{virt} = 1.12$)
- Penalización logística: $F_{log} = 1.03$
- MTBF = 410 h, MTTR = 18 h
- Latencia media $L_{med} = 42$ ms, latencia máxima tolerable $L_{max} = 120$ ms
- Madurez normativa (ENS/CCN-STIC): $GA = 0.82$, $CM = 0.78$, $NT = 0.91$
- Ponderaciones: $w_E = 0.4$, $w_O = 0.4$, $w_N = 0.2$

Cálculo paso a paso

1) Cálculo del M-PUE

$$M-PUE = \frac{5.2}{3.6} \times 1.01 \times 1.00 \times 1.03 \times 1.12 \approx 1.68$$

2) Cálculo del IRO

$$A_{ef} = \frac{410}{410 + 18} \approx 0.958$$

$$IRO = A_{ef} \times \left(1 - \frac{L_{med}}{L_{max}}\right) = 0.958 \times \left(1 - \frac{42}{120}\right) \approx 0.62$$

3) Cálculo del ICOMP

$$ICOMP = w_{GA} \cdot GA + w_{CM} \times CM + w_{NT} \times NT$$

Con ponderaciones uniformes ($w_{GA} = w_{CM} = w_{NT} = 1/3$):

$$ICOMP = 0.82 \times \frac{1}{3} + 0.78 \times \frac{1}{3} + 0.91 \times \frac{1}{3} \approx 0.84$$

4) Cálculo del IGEO

$$IGEO = w_E \times \frac{1}{M-PUE} + w_O \times IRO + w_N \times ICOMP$$

$$IGEO = 0.4 \times \left(\frac{1}{1.68}\right) + 0.4 \times 0.62 + 0.2 \times 0.84$$

$$IGEO = 0.238 + 0.248 + 0.168 \approx 0.65$$

El ejemplo muestra cómo el método permite obtener una valoración integrada del comportamiento de un CPD operativo con parámetros heterogéneos. Esta demostración numérica sirve como referencia para interpretar los escenarios desarrollados en el Capítulo 5.

4.6 Validación conceptual del método en escenarios doctrinales representativos

La validez de un marco metodológico orientado a la evaluación de infraestructuras virtualizadas en defensa depende de su capacidad para aplicarse de forma coherente a lo largo de todo el espectro de operaciones. Con el fin de demostrar la aplicabilidad práctica del método, esta sección presenta tres escenarios teóricos que cubren desde la estabilidad del nivel estratégico hasta las condiciones extremas del borde táctico.

El objetivo es contrastar el comportamiento del sistema métrico (M-PUE, IRO, IGEO). Los escenarios presentados en esta sección de validación utilizan parámetros nominales estándar para verificar la coherencia aritmética del método. El análisis de estrés bajo condiciones de «peor caso» (*worst-case*), con parámetros endurecidos, se reserva para el análisis estratégico del Capítulo 5.

4.6.1 Caso A: Nodo táctico desplegable (Entorno DDIL)

El primer escenario representa un nodo táctico integrado en un vehículo de mando, caracterizado por recursos energéticos reducidos, logística compleja y enlaces intermitentes. Es el caso de uso principal para validar la sensibilidad del modelo ante condiciones adversas.

Condiciones iniciales:

- Energía total disponible: $E_{total} = 2.4$ kWh
- Energía de TI consumida: $E_{TI} = 1.5$ kWh (PUE Base ≈ 1.6)
- Fuente: microrred híbrida diésel-solar (inestable) $\rightarrow F_{gen} = 1.05$
- Condiciones ambientales: 42°C, alta humedad $\rightarrow F_{amb} = 1.10$
- Logística táctica: transporte a zona hostil $\rightarrow F_{log} = 1.50$
- Tecnología: Contenedores y micro-VM (ligera) $\rightarrow F_{virt} = 1.08$ (8 % overhead)

Evaluación del M-PUE: Aplicando la fórmula multiplicativa definida:

$$M-PUE = \frac{2.4}{1.5} \times 1.05 \times 1.10 \times 1.50 \times 1.08 \approx \mathbf{2.99}$$

Este valor (**2.99**) refleja el coste real de operar en táctico: por cada unidad de energía computacional útil, se requieren casi 3 unidades de esfuerzo logístico y energético global.

Resultado integrado (IGEO): Con ponderaciones tácticas ($w_E = 0.4$, $w_O = 0.4$, $w_N = 0.2$) y métricas operativas ($A_{ef} = 0.94$, $IRO = 0.81$, $ICOMP = 0.87$):

$$IGEO = 0.4 \times \left(\frac{1}{2.99} \right) + 0.4 \times 0.81 + 0.2 \times 0.87 \approx 0.13 + 0.32 + 0.17 \approx \mathbf{0.62}$$

El índice desciende a 0.62, evidenciando cómo la carga logística penaliza severamente la viabilidad del nodo, salvado únicamente por su alta resiliencia operativa.

4.6.2 Caso B: CPD operativo avanzado (Entorno Mixto)

El segundo escenario se sitúa en una base avanzada (Forward Operating Base), actuando como enlace entre el nivel estratégico y el táctico. Presenta estabilidad moderada pero mantiene dependencia logística.

Condiciones iniciales:

- Energía total: $E_{total} = 5.0$ kWh
- Energía TI: $E_{TI} = 4.0$ kWh (PUE Base = 1.25)
- Fuente: red eléctrica local con apoyo solar $\rightarrow F_{gen} = 1.02$
- Condiciones ambientales: templadas $\rightarrow F_{amb} = 1.00$
- Logística operacional: convoyes regulares $\rightarrow F_{log} = 1.10$
- Tecnología: Hipervisor tipo 1 + Contenedores $\rightarrow F_{virt} = 1.15$ (15 % overhead mixto)

Evaluación del M-PUE:

$$M-PUE = \frac{5.0}{4.0} \times 1.02 \times 1.00 \times 1.10 \times 1.15 \approx \mathbf{1.61}$$

Resultado integrado (IGEO): Con ponderaciones equilibradas ($w_E = 0.4$, $w_O = 0.4$, $w_N = 0.2$) y métricas ($IRO = 0.88$, $ICOMP = 0.93$):

$$IGEO = 0.4 \times \left(\frac{1}{1.61} \right) + 0.4 \times 0.88 + 0.2 \times 0.93 \approx 0.248 + 0.352 + 0.186 \approx \mathbf{0.79}$$

El CPD muestra un perfil de excelencia operativa, situándose en un punto intermedio de eficiencia.

4.6.3 Caso C: CPD estratégico fijo (Línea Base)

El tercer escenario corresponde a un CPD permanente en territorio nacional. Actúa como referencia base para el estudio, representando un entorno sin restricciones logísticas de combate ($F_{log} = 1.0$) ni ambientales.

Condiciones iniciales:

- Energía total: $E_{total} = 15.0$ kWh
- Energía TI: $E_{TI} = 12.0$ kWh
- Fuente: Red estable + UPS $\rightarrow F_{gen} = 1.00$
- Tecnología: Máquinas Virtuales (VM) robustas $\rightarrow F_{virt} = 1.25$ (25 % overhead por seguridad)
- Logística: Red de suministro nacional $\rightarrow F_{log} = 1.00$

Evaluación del M-PUE:

$$M-PUE = \frac{15.0}{12.0} \times 1.00 \times 1.00 \times 1.00 \times 1.25 \approx \mathbf{1.56}$$

Nótese que, aunque el PUE físico es excelente (1.25), la sobrecarga de seguridad de las VMs eleva el M-PUE final a 1.56.

Resultado integrado (IGEO): Con prioridad normativa ($w_E = 0.3$, $w_O = 0.2$, $w_N = 0.5$) y métricas altas ($IRO = 0.92$, $ICOMP = 0.96$):

$$IGEO = 0.3 \times \left(\frac{1}{1.56} \right) + 0.2 \times 0.92 + 0.5 \times 0.96 \approx \mathbf{0.86}$$

El entorno alcanza la puntuación más alta (0.86), demostrando que en el nivel estratégico la inversión en seguridad se compensa con la alta puntuación normativa.

4.6.4 Comparativa general y análisis transversal

La Tabla 4-3 resume los valores recalculados, mostrando la progresión coherente entre niveles doctrinales.

Escenario	M-PUE	IRO	ICOMP	IGEO
CPD táctico (Caso A)	2.99	0.81	0.87	0.62
CPD operativo (Caso B)	1.61	0.88	0.93	0.79
CPD estratégico (Caso C)	1.56	0.92	0.96	0.86

Tabla 4-3: Comparativa de resultados obtenidos en los escenarios analizados.

En conjunto, estos escenarios validan la sensibilidad del modelo: el M-PUE escala desde 1.56 en territorio nacional hasta casi 3.0 en el borde táctico, capturando cuantitativamente el coste logístico de la operación.

La presente validación confirma la coherencia interna y la consistencia aritmética del marco propuesto; no obstante, el contraste empírico de los coeficientes energéticos, ambientales y operativos en entornos físicos reales queda fuera del alcance de este trabajo y se identifica explícitamente como una línea futura de investigación en la Sección 6.3.

4.7 Síntesis metodológica y proyección del marco

El presente capítulo ha definido un método integral para evaluar infraestructuras virtualizadas en defensa, articulado en torno a una estructura conceptual coherente y un sistema de métricas capaz de caracterizar, con precisión y trazabilidad, la eficiencia energética, la resiliencia operativa y el cumplimiento normativo de un CPD. La integración de los planos técnico, operativo y normativo permite abordar de manera simultánea las dimensiones medibles del entorno, las decisiones adaptativas necesarias para sostener servicios críticos y las exigencias doctrinales que condicionan la operación en todos los niveles de mando.

La aplicación conceptual del método a escenarios tácticos, operativos y estratégicos demuestra su versatilidad y evidencia que puede emplearse tanto para evaluar configuraciones existentes como para orientar diseños prospectivos. Los resultados obtenidos reflejan que la madurez de una infraestructura virtualizada depende del equilibrio entre consumo energético, continuidad del servicio y capacidad de cumplir con los requisitos de seguridad y auditoría establecidos por el ENS, las guías CCN-STIC y la doctrina OTAN FMN. Este equilibrio constituye el eje central del proceso y permite identificar con claridad las oportunidades de mejora en cada entorno analizado.

El método se concibe como un instrumento reproducible, auditable y compatible con procesos formales de acreditación, capaz de adaptarse a módulos ligeros, CPD avanzados y entornos estratégicos permanentes. Su valor radica en proporcionar un marco objetivo para la toma de decisiones en condiciones DDIL y para la modernización progresiva de la infraestructura digital de defensa.

Sobre esta base, el siguiente capítulo emplea el sistema de métricas y los escenarios aquí desarrollados para analizar los resultados de manera comparada y formular recomendaciones concretas de optimización energética, sostenibilidad operativa y alineamiento doctrinal. Mientras que el Capítulo 4 ha establecido *cómo evaluar*, el Capítulo 5 se centra en *cómo interpretar los resultados* y en el papel que desempeñan en la transformación digital de los CPD militares.

5 RESULTADOS Y ANÁLISIS DE ESCENARIOS

La estructura del capítulo responde a esta lógica analítica: la Sección 5.1 establece el planteamiento metodológico y la justificación del modelado; la Sección 5.2 define los parámetros de entrada, los perfiles tecnológicos y traduce los escenarios doctrinales (E1, E2, E3) en las ponderaciones estratégicas del IGEO; la Sección 5.3 presenta los datos obtenidos. Las secciones 5.5, 5.6 y 5.7 desarrollan el análisis estratégico integrado, evaluando el conflicto (*trade-off*) entre M-PUE, IRO e ICOMP para cada uno de los tres niveles doctrinales. Finalmente, la Sección 5.8 presenta la discusión de resultados y valida la hipótesis metodológica.

5.1 Planteamiento metodológico del análisis

La validación del marco propuesto se desarrolla mediante un **modelado analítico paramétrico** orientado a proyectar el comportamiento teórico de los CPD de defensa en sus tres niveles doctrinales. Dado que el despliegue físico de infraestructuras en zona de operaciones conlleva restricciones de seguridad y logística que exceden el alcance de este trabajo, se adopta una metodología de *Tabletop Analysis*, un enfoque ampliamente utilizado en estudios doctrinales cuando la experimentación directa no es viable.

Esta técnica consiste en una evaluación sistemática de escenarios sobre el papel, donde se somete al modelo a distintas variables de estrés para verificar su coherencia lógica y cuantitativa. En ingeniería de sistemas críticos, permite validar la viabilidad del diseño y anticipar cuellos de botella antes de incurrir en los costes y riesgos de un despliegue físico real.

Posteriormente, este método aplica las fórmulas del modelo IGEO sobre un conjunto de parámetros seleccionados a partir de estándares industriales y normativas de referencia en entornos militares (ASHRAE, MIL-STD, STANAG), permitiendo identificar diferencias estructurales entre arquitecturas sin necesidad de instrumentación física.

5.1.1 Objetivos del análisis

El propósito principal del estudio es comparar el comportamiento de diversas tecnologías de virtualización frente a variaciones en la carga de trabajo, la disponibilidad energética y las condiciones de conectividad. De manera específica, el análisis se orienta a:

- Cuantificar la mejora energética derivada del uso de tecnologías ligeras de virtualización.
- Evaluar la influencia del nivel doctrinal de despliegue sobre la estabilidad del servicio y el consumo.
- Analizar la relación entre eficiencia, resiliencia y conformidad normativa, identificando posibles compromisos entre dimensiones.

- Verificar la aplicabilidad del método definido en el Capítulo 4 a entornos operativos reales o modelados.

Estos objetivos permiten contrastar el método tanto como instrumento analítico como herramienta de apoyo a la decisión.

5.1.2 Dimensiones analíticas

El análisis se articula en torno a tres dimensiones complementarias que, consideradas en conjunto, permiten una evaluación integral del comportamiento de cada tecnología:

- **Dimensión energética:** análisis del indicador M-PUE y del consumo relativo frente a la máquina virtual como caso base.
- **Dimensión operativa:** estudio del impacto sobre la disponibilidad de servicio (*Service Level Agreement*, SLA) y el tiempo medio de recuperación (*Mean Time To Recovery*, MTTR).
- **Dimensión normativa:** evaluación del grado de conformidad con los requisitos ENS y las guías CCN-STIC aplicables a entornos virtualizados.

La combinación de estas dimensiones permite obtener indicadores compuestos y observar patrones de compromiso entre sostenibilidad, continuidad y seguridad.

5.1.3 Hipótesis de trabajo

El modelo parte de un conjunto de hipótesis que permiten aislar las variables críticas:

- **Cargas normalizadas.** Se asume una carga equivalente al 100 % de la capacidad nominal para evaluar el comportamiento energético en condiciones de máxima exigencia.
- **Determinismo paramétrico.** Los valores de penalización (F_{gen} , F_{amb}) se tratan como constantes derivadas de especificaciones técnicas, de modo que el cálculo es determinista; la media de N iteraciones se emplea únicamente para homogenizar el flujo computacional.
- **Escenarios doctrinales.** Se definen tres perfiles operativos (E1, E2, E3) cuyas prioridades (w_E , w_O , w_N) actúan como filtros de decisión estratégica.

Estas hipótesis permiten aislar los efectos de la tecnología, del entorno y de la escala doctrinal, facilitando la comparación sistemática.

5.1.4 Métricas empleadas

Las métricas seleccionadas se alinean con los componentes del marco metodológico y garantizan la comparabilidad entre tecnologías:

- **M-PUE:** relación entre el consumo total y el consumo de TI, ajustada a entornos desplegados.
- **Consumo relativo (%)**: porcentaje de energía consumida frente al caso base.
- **SLA (%)**: porcentaje medio de disponibilidad de servicio.
- **MTTR (min)**: tiempo medio de recuperación ante fallo o degradación.
- **Índice de conformidad normativa (ICOMP)**: ratio ponderado de cumplimiento ENS-ALTA y CCN-STIC.

La ponderación de cada métrica depende del nivel doctrinal, priorizando la eficiencia en el entorno táctico, el equilibrio en el operacional y la conformidad en el estratégico.

5.1.5 Justificación y limitaciones del modelo

La validación mediante modelado analítico, en lugar de simulación estocástica o testbed físico, se justifica por la naturaleza doctrinal del estudio. El objetivo no es medir métricas concretas de hardware, sino validar la coherencia interna del marco IGEO y cuantificar los órdenes de magnitud que diferencian a las tecnologías de virtualización en escenarios contrastados.

El uso de parámetros derivados de literatura técnica consolidada (como el *overhead* documentado de hipervisores KVM o micro-VM basadas en Firecracker) proporciona una proyección de referencia trazable y consistente, suficiente para sustentar decisiones de planificación tecnológica del Mando.

5.2 Parámetros de configuración y escenarios de prueba

El análisis comparativo se ejecuta sobre un modelo analítico multiescala diseñado para proyectar el comportamiento de un CPD de defensa en sus tres niveles doctrinales. El objetivo es establecer un marco de prueba coherente con la metodología del Capítulo 4, definiendo sistemáticamente los factores que intervienen en la evaluación.

El modelo representa un CPD heterogéneo capaz de ejecutar simultáneamente las cuatro tecnologías analizadas, alojando cargas de misión representativas (C2, ISR, logística). Los supuestos doctrinales siguen los marcos de referencia del ENS para la evaluación de aislamiento y trazabilidad, y los de FMN Spiral 5 para la interoperabilidad y resiliencia federada.

5.2.1 Fuentes de referencia para la parametrización

Los parámetros de entrada del modelo se han extraído de estándares y guías técnicas reconocidas. Cabe matizar que los valores asignados a los coeficientes de penalización del modelo (F_{gen} , F_{amb} , F_{log} y F_{virt}) no deben interpretarse como constantes universales, sino como rangos representativos derivados de la literatura técnica, estándares industriales y la experiencia operativa documentada. Este enfoque de «arbitrariedad controlada» permite modelar el comportamiento del sistema sin depender de mediciones físicas específicas de un único fabricante. En consonancia con esta premisa, la Tabla 5-1 detalla las magnitudes seleccionadas y el respaldo documental que valida su uso en este análisis.

Parámetro	Valor típico	Fuente de referencia / Justificación
F_{amb} (E3)	1.4	ASHRAE TC 9.9: Degradación de eficiencia (COP) en operación a 45°C, clases térmicas A3/A4.
F_{gen} (E3)	1.3	MIL-STD / STANAG: Pérdidas por conversión AC/DC y variabilidad en generadores tácticos móviles.
F_{log}	1.0 – 1.5	DoD FBCF: Estimación del <i>Fully Burdened Cost of Fuel</i> [73], reflejando el coste logístico. Se estandariza: E1 (1.0), E2 (1.1), E3 (1.5).
F_{virt} (VM)	1.25	Literatura técnica: <i>Overhead</i> de ejecución consolidado en hipervisores tipo 1 (KVM/ESXi) por emulación y doble <i>kernel</i> .
F_{virt} (Contenedor)	1.10	NIST SP 800-190 / Docker: Sobrecarga ligera asociada a <i>namespaces</i> .
F_{virt} (Micro-VM)	1.05	Firecracker (AWS): <i>Overhead</i> <5 % frente a bare-metal según mediciones publicadas y benchmarks industriales.
F_{virt} (Unikernel)	1.01	Research (MirageOS/Unikraft): Ejecución en espacio de direcciones único sin cambios de contexto (ring transition).
ICOMP	0.0–1.0	ENS / FNM: Capacidad de aplicar controles de aislamiento y trazabilidad.

Tabla 5-1: Justificación técnica de los valores empleados en el modelado analítico.

5.2.2 Perfiles tecnológicos y parametrización detallada

A partir de las fuentes de referencia anteriores, se definen los perfiles específicos. Nota sobre la eficiencia: Mientras que en el Capítulo 2 se indicaba un ahorro de recursos en reposo de hasta el 60 % para tecnologías ligeras, el modelo de cálculo utiliza factores F_{virt} conservadores (1.05 a 1.25). Esto se debe a que el M-PUE evalúa la *sobrecarga energética activa* durante la ejecución, no la densidad de almacenamiento, garantizando así que no se sobreestime la autonomía en el planeamiento logístico. Bajo este criterio de prudencia, la Tabla 5-2 establece la relación operativa entre la tecnología empleada, su factor de penalización y el nivel de aislamiento asociado.

Tecnología	F_{virt}	Aislamiento	Detalle Técnico
VM	1.25	ALTA	Sobrecarga por gestión completa de hardware y <i>kernel</i> . Cumple CCN-STIC-220.
Contenedor	1.10	MEDIA	Coste de namespaces. Aislamiento parcial (<i>kernel</i> compartido).
Micro-VM	1.05	MEDIA-ALTA	Optimización VirtIO y arranque rápido. Equilibrio seguridad/eficiencia.
Unikernel	1.01	BAJA	Ejecución en espacio único (Library OS). Rendimiento nativo y trazabilidad limitada.

Tabla 5-2: Perfiles tecnológicos y factores de penalización empleados en el modelo.

Por otro lado, los parámetros ambientales, energéticos y logísticos (F_{amb} , F_{gen} , F_{log}) se modelan en función de la severidad del escenario. La Tabla 5-3 sistematiza los valores numéricos exactos aplicados en la simulación para los tres niveles de severidad (E1, E2 y E3), abarcando desde la eficiencia base del hardware hasta el coste logístico.

Parámetro	E1	E2	E3	Contexto Operativo
PUE_{base}	1.20	1.25	1.50	Eficiencia nativa del hardware TI (antes de penalizaciones).
F_{gen}	1.0	1.1	1.3	Red comercial vs. generador híbrido vs. generador táctico.
F_{amb}	1.0	1.2	1.4	CPD climatizado vs. contenedor ISO vs. <i>shelter</i> desplegado.
F_{log}	1.0	1.1	1.5	Red nacional vs. logística operacional vs. zona hostil.
E_{total} (Índice)	100	85	75	Disponibilidad energética normalizada (E1=100) para el cálculo base.

Tabla 5-3: Parámetros base, energéticos y logísticos aplicados por escenario.

5.2.3 Escenarios doctrinales y traducción estratégica

El análisis se organiza en torno a tres escenarios doctrinales (E1, E2, E3). Para contextualizar su interconexión física y lógica, la Figura 5-1 ilustra la topología de red y los medios de transmisión que condicionan los factores F_{log} y F_{gen} en cada nivel.

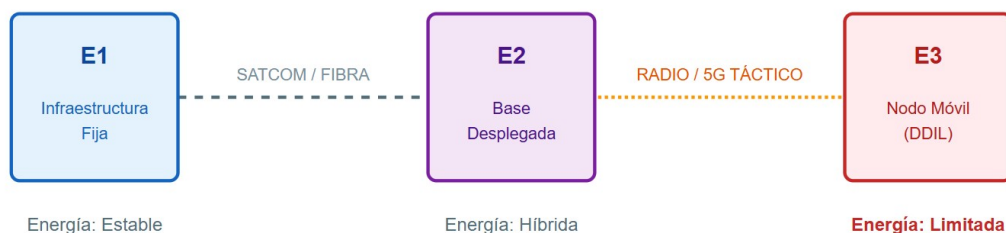


Figura 5-1: Arquitectura de referencia y topología física de escenarios (E1, E2, E3). Fuente: Elaboración propia.

Sus prioridades operativas se traducen matemáticamente en los pesos del algoritmo IGEO, asignando mayor relevancia a la seguridad, la eficiencia o la resiliencia en función del escenario doctrinal asociado al escalón de mando. Esta configuración, detallada en la Tabla 5-4, constituye la base paramétrica sobre la que se ejecuta la simulación.

Escenario	w_E	w_O	w_N	Justificación Doctrinal
E1 - Estratégico	0.3	0.2	0.5	Cumplimiento: Trazabilidad y seguridad (ENS-ALTA).
E2 - Operacional	0.4	0.4	0.2	Equilibrio: Continuidad y eficiencia (Bases desplegadas).
E3 - Táctico	0.4	0.5	0.1	Supervivencia: Resiliencia en DDIL y autonomía energética.

Tabla 5-4: Definición de escenarios doctrinales y sus correspondientes ponderaciones estratégicas en el IGEO.

5.3 Resultados del modelado

La proyección de los resultados sobre los tres escenarios doctrinales (E1, E2, E3) y las cuatro tecnologías de virtualización genera un conjunto de datos estructurado en torno a las tres dimensiones: eficiencia energética (M-PUE), resiliencia operativa (IRO) y conformidad normativa (ICOMP). Las tablas siguientes recogen los resultados obtenidos, que constituyen la base cuantitativa para el análisis doctrinal desarrollado en las secciones posteriores.

La Tabla 5-5 presenta los resultados de la dimensión energética, expresados en términos de M-PUE recalculado con los factores logísticos realistas (F_{log}). Se observa cómo la degradación del entorno (E3) eleva el índice general drásticamente, situando a las tecnologías pesadas en rangos de inviabilidad.

Tecnología	M-PUE (E1)	M-PUE (E2)	M-PUE (E3)
VM	1.50	2.27	5.12
Contenedor	1.32	1.99	4.50
Micro-VM	1.26	1.90	4.30
Unikernel	1.21	1.83	4.14

Tabla 5-5: Resultados consolidados del M-PUE.

La proyección gráfica de estos datos permite visualizar la divergencia no lineal del rendimiento.

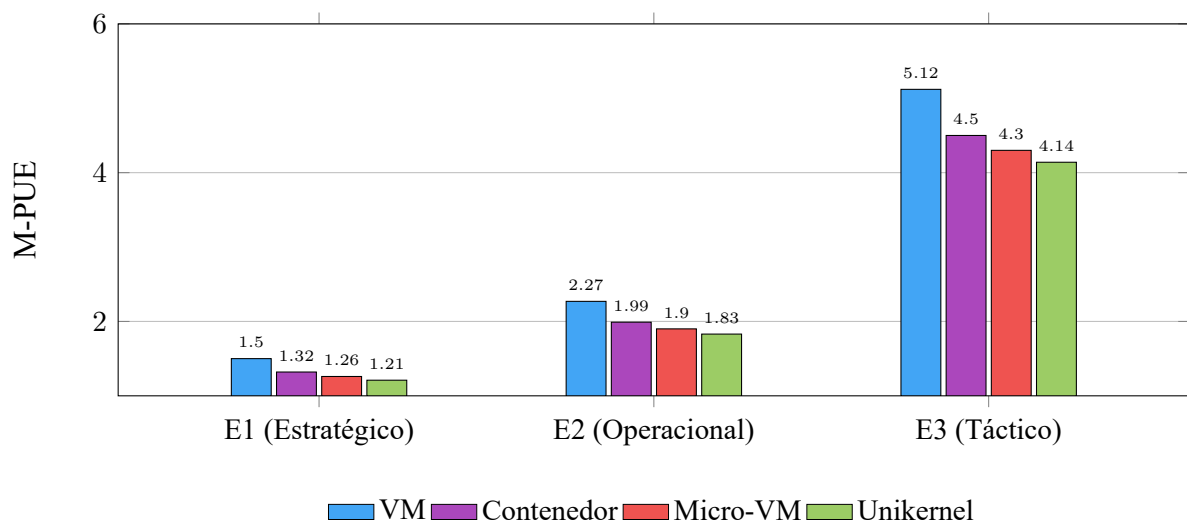


Figura 5-2: Evolución del M-PUE por escenario. Fuente: Elaboración propia.

Aunque una diferencia de 0.4 puntos en el M-PUE podría parecer marginal en entornos civiles, en el ámbito logístico-militar representa una reducción de la demanda de combustible superior al 15 %. Mientras que en el escenario estratégico (E1) las diferencias son asumibles, el impacto combinado de la logística y la generación en E3 actúa como un multiplicador de ineficiencia, haciendo que la virtualización tradicional se dispare por encima de 5.0, mientras que las tecnologías de aislamiento ligero logran contener el impacto relativo.

Por otro lado, la Tabla 5-6 recoge los indicadores de resiliencia operativa, incluyendo el SLA medio y el MTTR.

Tecnología	SLA (E1/E2/E3) (%)	MTTR (min)	Comentario operativo
VM	99.2 / 97.8 / 95.0	22	Aislamiento fuerte, recuperación lenta.
Contenedor	98.8 / 97.5 / 94.5	18	Agilidad alta, aislamiento limitado.
Micro-VM	98.5 / 97.2 / 94.2	14	Buen compromiso seguridad/rendimiento.
Unikernel	97.5 / 96.0 / 93.5	10	Máxima rapidez, trazabilidad reducida.

Tabla 5-6: Indicadores de resiliencia operativa (IRO): SLA medio y MTTR.

Finalmente, la Tabla 5-7 sintetiza el **ICOMP** como medida del grado relativo de conformidad normativa en cada tecnología.

Tecnología	ICOMP	Nivel ENS	Justificación Técnica
VM	1.00	ALTA	Aislamiento Físico. GA máximo y NT elevado
Micro-VM	0.95	ALTA	Aislamiento por hardware (KVM). Superficie de ataque mínima y alta seguridad.
Contenedor	0.80	MEDIA/ALTA	Aislamiento débil por software (Namespaces). Riesgo de fuga por <i>kernel</i> compartido. Alcanzar nivel alto requiere <i>hardening</i> estricto (SELinux, SCC) y orquestadores complejos, aumentando la carga operativa.
Unikernel	0.50	N/A	Inviabile para certificación. Trazabilidad nula e imposibilidad de instalar agentes de auditoría.

Tabla 5-7: Comparativa de conformidad normativa.

Es importante matizar la puntuación de los contenedores (ICOMP 0.80). Si bien plataformas avanzadas como Red Hat OpenShift permiten alcanzar niveles de seguridad aptos para entornos clasificados (mediante perfiles SELinux, namespaces de usuario y auditoría estricta), este aislamiento es lógico (software) y depende de una configuración perfecta.

A diferencia de la Micro-VM, que cuenta con una barrera de aislamiento por hardware (instrucciones VT-x del procesador) desde su concepción, el contenedor parte de un modelo de *kernel* compartido. Esto implica que, para igualar la seguridad de una VM, el contenedor exige una «penalización operativa» en forma de complejidad de gestión y bastionado. Por tanto, en escenarios tácticos con soporte limitado, la Micro-VM ofrece una relación seguridad/simplicidad superior.

5.4 Análisis de sensibilidad del M-PUE

Con el fin de verificar la robustez del modelo propuesto, se ha ejecutado un análisis de sensibilidad orientado a cuantificar el impacto de las variaciones ambientales severas sobre el M-PUE. Esta evaluación permite determinar si las conclusiones obtenidas en los escenarios doctrinales (E1–E3) se mantienen estables ante fluctuaciones en el factor F_{amb} .

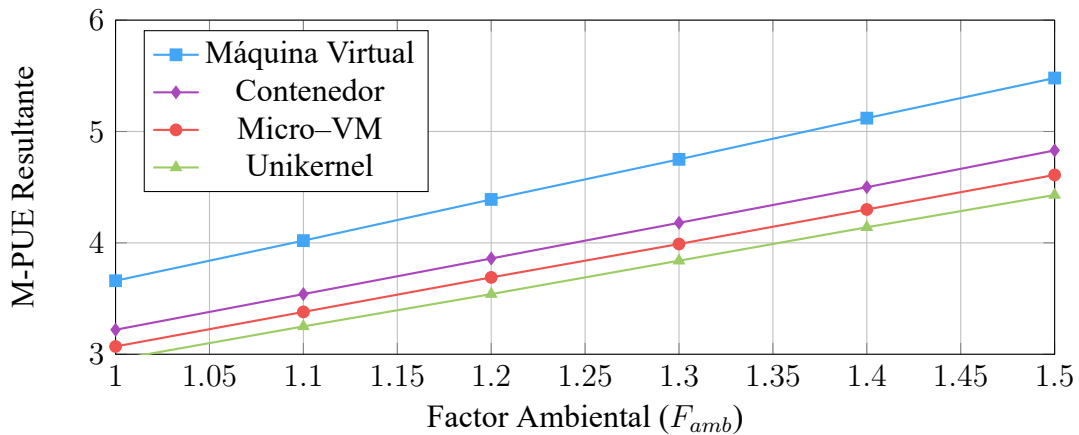


Figura 5-3: Sensibilidad del M-PUE ante la degradación ambiental en el escenario táctico (E3). Fuente: Elaboración propia.

La tendencia mostrada en la Figura 5-3 revela una dinámica no lineal crítica para la toma de decisiones. Antes de detallar el comportamiento por tecnología, es necesario definir un umbral límite identificado en este estudio: la «zona de insostenibilidad logística». Esta frontera se establece operativamente a partir de un valor M-PUE >2.0 , punto en el cual el coste energético de mantener la infraestructura supera el beneficio operativo, comprometiendo la autonomía de los generadores tácticos y exigiendo una cadena de suministro de combustible difícil de sostener en combate.

En el escenario táctico (E3), el efecto multiplicador de la logística ($F_{log} = 1.5$) hace que todas las tecnologías operen en regímenes de alto consumo, pero la diferencia de pendiente es crucial:

- Las **VM** sufren una degradación acelerada, disparando su M-PUE por encima de 5.0. Esto las sitúa muy profundamente en la «zona de insostenibilidad logística», invalidando su uso en operaciones prolongadas sin red eléctrica estable.
- Las **micro-VM** amortiguan este efecto, manteniendo un comportamiento significativamente más bajo (M-PUE ≈ 4.30), lo que supone un ahorro de combustible vital en la cadena logística.
- Los **unikernels** presentan la menor sensibilidad, actuando como la opción más robusta termodinámicamente, aunque limitados por su madurez normativa.

Este comportamiento valida la robustez del M-PUE para discriminar tecnologías no solo por su consumo base, sino por su comportamiento bajo estrés logístico.

Del análisis de sensibilidad se desprenden tres conclusiones doctrinales:

- **El entorno y la logística actúan como multiplicadores de ineficiencia.** En el E3, el *overhead* del software deja de ser un coste marginal para convertirse en un riesgo logístico mayor.
- **La diferencia tecnológica ahorra combustible real.** La brecha de eficiencia entre una VM y una micro-VM en este escenario equivale a reducir casi una unidad completa de energía por cada unidad de cómputo, lo que impacta directamente en el número de convoyes de suministro necesarios.
- **Inviabilidad de arquitecturas pesadas.** Para escenarios extremos, las arquitecturas pesadas (VM) quedan técnicamente invalidadas por consumo excesivo.

5.5 Análisis del escenario estratégico (E1)

El escenario estratégico (E1) se corresponde con centros permanentes, infraestructuras críticas y sistemas que manejan información clasificada o de alta sensibilidad. Se caracteriza por condiciones estables en energía y climatización ($F_{gen} = 1.0$, $F_{amb} = 1.0$) y conexión a red comercial ($F_{log} = 1.0$). En este contexto, el criterio dominante de decisión es el cumplimiento normativo y la trazabilidad completa, aspectos recogidos en el **ICOMP** definido en el Capítulo 4.

5.5.1 Eficiencia energética en CPD estables

Las condiciones favorables del entorno implican que las diferencias en eficiencia energética entre tecnologías, expresadas mediante el M-PUE (Eq. 4.1), no constituyen el principal factor de priorización para el Mando. Aun así, los resultados de la Tabla 5-5 muestran que las micro-VM (M-PUE = 1.26) y los *unikernels* (M-PUE = 1.21) ofrecen mejoras respecto a la máquina virtual tradicional (M-PUE = 1.50). Estas diferencias son relevantes desde la perspectiva de optimización del CPD, pero E1 concede un peso reducido a la dimensión energética ($w_E = 0.30$) según la Tabla 5-4.

5.5.2 Resiliencia operativa y estabilidad del servicio

La resiliencia operativa (**IRO**), definida mediante la Eq. 4.3, se mantiene elevada en todas las tecnologías debido a la estabilidad estructural del entorno estratégico. Aunque los valores de **MTTR** (Tabla 5-6) varían –siendo más altos en máquinas virtuales (22 min) y más bajos en *unikernels* (10 min)–, la elevada disponibilidad del entorno garantiza un SLA superior al 97.5 % en todos los casos. Esta combinación se traduce en un IRO elevado, al minimizar tanto la indisponibilidad como la penalización por latencia relativa ($1 - L_{med}/L_{max}$), que en E1 mantiene valores prácticamente óptimos.

5.5.3 Conformidad normativa y requisitos de trazabilidad

El componente crítico en E1 es el **ICOMP**, cuyo cálculo integra el **Grado de Aislamiento (GA)**, la **Capacidad de Microsegmentación (CM)** y el **Nivel de Trazabilidad (NT)**. Según los resultados de la Tabla 5-7, las **máquinas virtuales tradicionales** son la única tecnología que obtiene un ICOMP completo: su aislamiento basado en virtualización hardware proporciona el GA máximo, su compatibilidad con políticas de segmentación avanzada garantiza un CM elevado y su madurez operacional asegura el NT requerido por ENS-ALTA y por la guía CCN-STIC-220. Por el contrario, los contenedores presentan limitaciones inherentes al *kernel* compartido, las micro-VM se encuentran en proceso de consolidación normativa y los *unikernels* carecen de mecanismos de auditoría suficientemente maduros para entornos clasificados.

5.5.4 Decisión estratégica para E1

En el nivel estratégico, la ponderación del IGEO prioriza de forma explícita la dimensión normativa ($w_N = 0.50$), por encima de la energética y la operativa. En consecuencia, aunque existan alternativas con mejor eficiencia (micro-VM, *unikernels*), la tecnología que satisface de manera más coherente los requisitos doctrinales de E1 es la **máquina virtual tradicional**. Su alineamiento pleno con el ENS, su capacidad de auditoría, su integración con CCN-STIC-220 y su madurez probada en CPD de defensa la convierten en la opción óptima para servicios estratégicos. De manera consistente con el marco IGEO, el escenario E1 confirma que la **seguridad y la trazabilidad normativa priman sobre la eficiencia**, y que la selección tecnológica debe responder al equilibrio doctrinal propio de cada nivel de mando.

En síntesis, el escenario E1 confirma que la dimensión normativa domina la decisión estratégica, y que la eficiencia energética tiene un impacto marginal en la priorización. El IGEO actúa aquí como mecanismo de verificación de madurez y cumplimiento.

5.6 Análisis del escenario operacional (E2)

El escenario operacional (E2) representa el nivel intermedio de la doctrina, caracterizado por condiciones variables de conectividad, carga y disponibilidad energética. Es el escenario típico de bases desplegadas, nodos regionales o centros móviles en los que conviven servicios de mando y control, funciones logísticas y capacidades de integración con aliados. Frente a la estabilidad del nivel estratégico y la presión extrema del nivel táctico, E2 exige alcanzar un **equilibrio** entre eficiencia, resiliencia y cumplimiento normativo, lo que lo convierte en el escenario más complejo desde la perspectiva del IGEO.

5.6.1 Eficiencia energética y dinámica de carga

Los valores energéticos y ambientales de E2 incorporan un factor logístico moderado ($F_{log} = 1.1$) y ambiental ($F_{amb} = 1.2$), propio de una base desplegada con suministro regular pero no ilimitado. Según los resultados de la Tabla 5-5, esto eleva el M-PUE de las **máquinas virtuales** a 2.27, cruzando el umbral de 2.0 y señalando una ineficiencia notable. Sin embargo, las **micro-VM** (1.90) y **contenedores** (1.99) logran mantenerse por debajo de este límite crítico. A diferencia del entorno estable de E1, estas diferencias se acumulan a lo largo de ciclos operativos prolongados, afectando a la autonomía energética y a la capacidad de consolidación. Por este motivo, E2 asigna un peso significativo a la métrica energética del IGEO ($w_E = 0.40$).

5.6.2 Resiliencia operativa ante variabilidad de red

La resiliencia operativa en E2 se ve condicionada por la intermitencia de los enlaces y por la probabilidad de fallos asociados a equipos expuestos, por lo que el **IRO** adquiere un papel central. De acuerdo con los resultados de la Tabla 5-6, los **contenedores** y las **micro-VM** presentan **MTTR** inferiores a las máquinas virtuales (18 y 14 minutos, respectivamente, frente a 22 minutos en VM). Esta diferencia tiene un impacto directo en el IRO, puesto que un MTTR menor reduce la indisponibilidad en la ecuación (Eq. 4.3) y facilita una recuperación más rápida ante fallos. Asimismo, la estabilidad relativa del SLA en E2 (entre 97.0 % y 97.5 %) mantiene la penalización por latencia dentro de márgenes aceptables, consolidando un perfil de resiliencia intermedio entre E1 y E3. Dado este comportamiento, E2 asigna al componente operativo un peso equivalente al energético en el IGEO ($w_O = 0.40$).

5.6.3 Conformidad normativa en entornos mixtos

En el escenario operacional, el cumplimiento normativo (ICOMP) mantiene una importancia significativa, aunque subordinada a los requisitos energéticos y operativos. La Tabla 5-7 muestra que las **máquinas virtuales** continúan ofreciendo el máximo nivel de conformidad, con valores completos en **GA** (aislamiento), **CM** (microsegmentación) y **NT** (trazabilidad). Los **contenedores**, si bien presentan un nivel de cumplimiento parcial (ICOMP = 0.80), mantienen un **CM** elevado gracias a su integración nativa con políticas de segmentación, pero un **GA** más débil debido al *kernel* compartido. Las **micro-VM**, por su parte, ofrecen un compromiso especialmente adecuado para este escenario: proporcionan un **GA** mayor que el de los contenedores y un **NT** reforzable mediante medidas compensatorias, manteniendo además ventajas operativas. Esto sitúa al componente normativo en una posición intermedia dentro del IGEO de E2 ($w_N = 0.20$), reflejando la necesidad de cumplir sin sacrificar la disponibilidad del servicio.

5.6.4 Decisión operativa para E2

El escenario operacional evidencia la inexistencia de un ganador claro entre tecnologías. Las VM destacan por su ICOMP elevado, pero penalizan la eficiencia energética y la resiliencia. Los contenedores proporcionan una excelente eficiencia y un MTTR competitivo, pero su GA limitado restringe su empleo en cargas clasificadas. Las micro-VM ofrecen el mejor equilibrio general, combinando un M-PUE moderado, un MTTR reducido y un nivel de aislamiento superior al de los contenedores.

En consecuencia, la decisión estratégica en E2 se alinea con el principio fundamental del marco IGEO: **asignar cada tipo de carga a la tecnología que maximiza su utilidad marginal en función del equilibrio doctrinal**. Así, las cargas ENS-ALTA / FMN-SECRET deberían priorizar VM o micro-VM (predominio de w_N), mientras que cargas logísticas o aplicaciones ENS-MEDIA pueden desplegarse eficientemente en contenedores (predominio de w_E). El escenario operacional confirma que la clave no es seleccionar una única tecnología, sino **adoptar una política de virtualización híbrida** guiada por el IGEO para optimizar el rendimiento del CPD bajo condiciones mixtas.

En síntesis, el E2 valida la necesidad de un enfoque híbrido: aunque ninguna tecnología maximiza todas las dimensiones simultáneamente, el IGEO permite identificar la combinación óptima según la carga de trabajo.

5.7 Análisis del escenario táctico (E3)

El escenario táctico (E3) representa el nivel doctrinal más exigente desde la perspectiva energética, logística y operativa. Se caracteriza por entornos DDIL en los que la disponibilidad de energía es limitada, la climatología es adversa y la conectividad con escalones superiores es intermitente. Consecuentemente, la prioridad estratégica recae en la **resiliencia operativa (IRO)** y en la **eficiencia energética (M-PUE)**, siendo el cumplimiento normativo importante pero subordinado a la continuidad de la misión.

5.7.1 Eficiencia energética como factor crítico

El impacto combinado de la logística de zona hostil ($F_{log} = 1.5$) y la generación táctica ($F_{gen} = 1.3$) es determinante. Como muestra la Tabla 5-5, el M-PUE de las máquinas virtuales se dispara a 5,12. Este valor confirma que, por cada unidad de energía computacional, se gastan más de 4 unidades en la cadena de suministro y conversión, haciendo inviable el despliegue masivo de VMs. Las **micro-VM** (4.30), aunque también impactadas, ofrecen un ahorro relativo que, escalado a nivel de misión, resulta crítico para la autonomía del nodo. En consecuencia, la dimensión energética del IGEO adquiere un peso elevado en este escenario ($w_E = 0.40$).

5.7.2 Resiliencia operativa bajo condiciones adversas

La resiliencia operativa (**IRO**), definida mediante la Eq. 4.3, es especialmente sensible a las variaciones del **MTTR** en entornos DDIL. Los resultados de la Tabla 5-6 muestran que las **micro-VM** y los **unikernels** reducen el MTTR hasta 14 y 10 minutos, respectivamente, frente a los 22 minutos de las máquinas virtuales. Esta diferencia impacta directamente en la disponibilidad efectiva A_{ef} y, por extensión, en el IRO, al disminuir la proporción de tiempo fuera de servicio. Además, la latencia relativa (L_{med}/L_{max}) se mantiene dentro de límites aceptables incluso bajo estrés energético, permitiendo que tecnologías ligeras sostengan mejor el servicio ante fallos recurrentes. Dado el carácter crítico de la continuidad operativa en E3, la dimensión operativa es la más relevante dentro de la ponderación del IGEO ($w_O = 0.50$).

5.7.3 Conformidad normativa en un entorno degradado

El escenario táctico no elimina la necesidad de seguridad, pero exige una interpretación adaptativa del cumplimiento normativo. De acuerdo con la Tabla 5-7, los **unikernels** presentan un ICOMP reducido debido a un **Nivel de Trazabilidad (NT)** insuficiente y a la ausencia de mecanismos formales de auditoría. Los **contenedores** ofrecen ventajas en despliegue y eficiencia, pero su **Grado de Aislamiento (GA)** limitado, producto del *kernel* compartido, implica riesgos en entornos donde conviven cargas de distintos dominios.

En cambio, las **micro-VM** proporcionan un equilibrio adecuado: su aislamiento basado en micro-hipervisores incrementa el GA, permiten aplicar microsegmentación y pueden reforzar el NT mediante medidas compensatorias. Aunque las máquinas virtuales ofrecen la máxima conformidad normativa, su elevado coste energético y operativo las vuelve inadecuadas para despliegues prolongados en E3. El IGEO refleja esta realidad asignando un peso reducido a la dimensión normativa ($w_N = 0.10$).

Por otro lado, los **unikernels** presentan un ICOMP reducido (0.50). Esto genera una paradoja operativa: aunque son la opción energéticamente óptima, su falta de trazabilidad los invalida para procesar información clasificada, relegándolos a sistemas de baja criticidad. Esta conclusión es especialmente relevante porque valida la utilidad del marco metodológico propuesto: si solo se hubieran considerado criterios de eficiencia energética (M-PUE), el *unikernel* habría aparecido como la solución ideal, ignorando su inviabilidad normativa (ICOMP) y exponiendo al sistema a riesgos de seguridad inaceptables.

5.7.4 Decisión operativa para E3

La integración de las tres dimensiones del análisis confirma que el entorno táctico exige tecnologías ligeras, resilientes y energéticamente sostenibles. Las VM quedan descartadas por inviabilidad logística, mientras que los **unikernels** deben restringirse a funciones embebidas o roles unidominio debido a su bajo NT. Los **contenedores** son válidos para cargas no clasificadas o de bajo riesgo, pero presentan limitaciones de aislamiento que los hacen insuficientes para servicios tácticos críticos. En este contexto, la **micro-VM** emerge como la tecnología óptima para la mayor parte de los despliegues tácticos: combina un M-PUE moderado, un MTTR reducido, un GA adecuado y un NT reforzable. Bajo las ponderaciones establecidas en la Tabla 5-4, las micro-VM maximizan el IGEO en E3, confirmando su idoneidad como base tecnológica para nodos tácticos, sensores avanzados y capacidades ISR distribuidas. En suma, el escenario táctico valida la hipótesis general del trabajo: la tecnología óptima depende del contexto doctrinal, y en E3 la sostenibilidad y la resiliencia prevalecen como criterios decisivos.

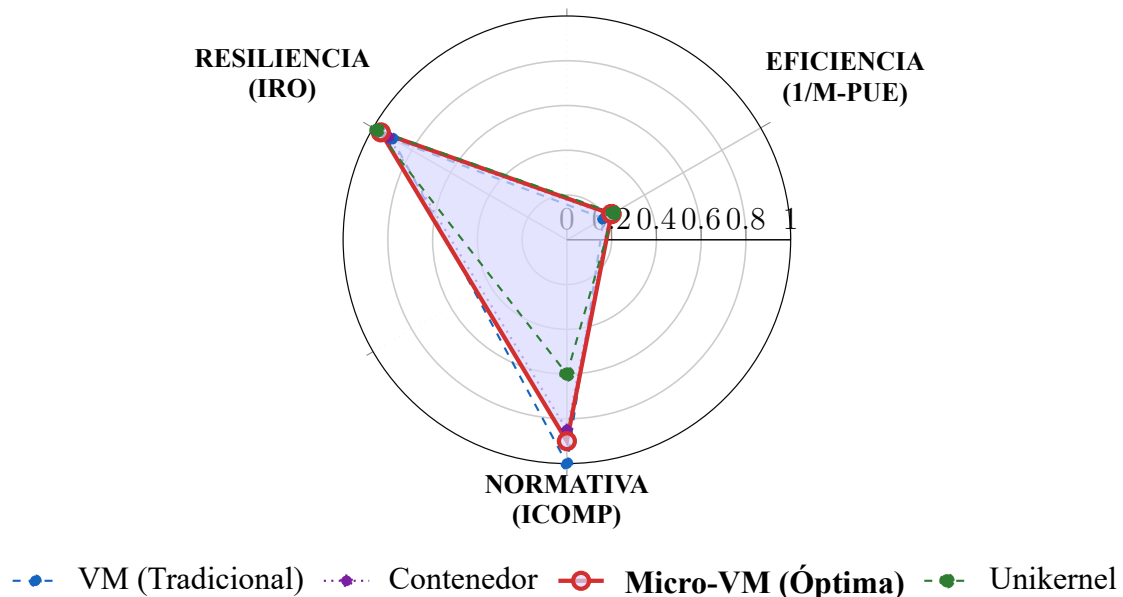


Figura 5-4: Perfil de competencia tecnológica en escenario táctico (E3). Fuente: Elaboración propia.

El diagrama de la Figura 5-4 evidencia la superioridad estratégica de micro-VM (Área Azul Sólida), que mantiene un perfil de cobertura equilibrado frente a las asimetrías críticas de la VM (déficit severo de eficiencia) y del *unikernel*, cuyo perfil asimétrico refleja una marcada especialización técnica pero también su inviabilidad normativa en el estado actual.

En síntesis, E3 demuestra que la sostenibilidad logística es la variable dominante, y que solo tecnologías ligeras mantienen un perfil operativo viable para misiones sostenidas.

5.8 Discusión y síntesis de hallazgos

El análisis integrado de los tres escenarios doctrinales confirma que la selección tecnológica en entornos de defensa no puede abordarse desde criterios puramente técnicos, sino desde una lógica estratégica que equilibre eficiencia energética, resiliencia operativa y cumplimiento normativo. La aplicación del marco metodológico definido en el Capítulo 4 –junto con las métricas M-PUE, IRO e ICOMP y su integración en el índice compuesto IGEO– demuestra que cada tecnología optimiza dimensiones distintas y que dichas diferencias se acentúan en función del nivel de mando y de las condiciones operativas.

5.8.1 Comparación transversal de las tecnologías

Los resultados muestran patrones consistentes en los tres escenarios: (1) Las **VM** continúan siendo la referencia para entornos donde la trazabilidad y el aislamiento son críticos, manteniendo los valores más altos de ICOMP gracias a su GA basado en hardware y a su NT elevado. Sin embargo, su ineficiencia en E3 las descarta para operaciones tácticas. (2) Los **contenedores** presentan una mejora energética significativa y MTTR moderados, lo que favorece un IRO competitivo en condiciones estables o semiestables. (3) Las **micro-VM** combinan características de contenedores y máquinas virtuales: menor consumo, MTTR reducido y un GA superior al de los contenedores, lo que las convierte en una alternativa versátil para despliegues mixtos y tácticos. (4) Los **unikernels** son los más eficientes y rápidos, pero presentan limitaciones importantes en NT y GA, restringiendo su aplicabilidad a funciones no clasificadas o embebidas.

5.8.2 Justificación de la selección de micro-VM frente a unikernels

Aunque los datos del análisis (Tabla 5-5) otorgan al *unikernel* la máxima puntuación en eficiencia energética ($M-PUE \approx 4.14$ en E3) y velocidad de recuperación, su adopción como estándar doctrinal se ve penalizada por su baja madurez normativa ($ICOMP = 0.60$).

La arquitectura monolítica del *unikernel* dificulta la inyección de agentes de seguridad y la generación de trazas de auditoría conformes al ENS. Por el contrario, la micro-VM ofrece un perfil de rendimiento cuasi-idéntico pero manteniendo la capacidad de aislamiento y gobernanza de un sistema operativo completo. Esta característica la convierte en el «óptimo sistémico»: maximiza la operatividad sin comprometer la acreditación de seguridad, resolviendo el compromiso estratégico del escenario táctico mejor que cualquier otra alternativa.

5.8.3 Impacto diferenciado de las métricas en cada escenario

La comparación a través de escenarios revela cómo la ponderación de las métricas –según la lógica del IGEO– modifica la valoración global de las tecnologías:

- En el **escenario estratégico (E1)**, la dimensión normativa domina ($w_N = 0.50$). La VM supera con claridad al resto al maximizar el ICOMP.
- En el **escenario operacional (E2)**, el equilibrio entre eficiencia ($w_E = 0.40$) y resiliencia ($w_O = 0.40$) desplaza la preferencia hacia soluciones híbridas.
- En el **escenario táctico (E3)**, la resiliencia y la sostenibilidad energética adquieren máxima prioridad. El alto coste logístico del combustible penaliza severamente a las arquitecturas pesadas, posicionando a las micro-VM como la opción dominante.

5.8.4 Interpretación estratégica de los resultados

Los hallazgos evidencian una tensión estructural entre seguridad, eficiencia y resiliencia. Ninguna tecnología alcanza simultáneamente el máximo rendimiento en las tres dimensiones, y esta tensión se intensifica a medida que el entorno operativo se degrada. En escenarios estables, los requisitos normativos son determinantes; en escenarios semiestables, la eficiencia y la continuidad del servicio adquieren prioridad equilibrada; y en escenarios degradados, la sostenibilidad energética y la recuperación rápida de servicios se convierten en factores decisivos. Esta dinámica confirma la necesidad de adoptar una política de virtualización multinivel, en la que cada tecnología se asigna en función del tipo de carga, la clasificación del dato, la exposición al entorno y las prioridades de misión.

5.8.5 Proyección hacia arquitecturas híbridas de defensa

La convergencia de resultados en los tres escenarios sugiere que las infraestructuras de defensa evolucionarán hacia modelos híbridos capaces de integrar máquinas virtuales para servicios críticos, contenedores para capacidades ágiles y micro-VM para nodos desplegados y servicios de borde. Esta proyección valida el modelo de *Continuum de Computación* descrito en el Capítulo 3, demostrando que la arquitectura ideal no es monolítica, sino un continuo federado donde los recursos se distribuyen estratégicamente según la disponibilidad energética y las necesidades de la misión. La aplicación flexible de estas tecnologías, guiada por un modelo de decisión como el IGEO, permite adaptar el diseño del despliegue en función de las condiciones operativas y doctrinales previstas, favoreciendo además la interoperabilidad con marcos aliados donde la modularidad y la soberanía del dato son elementos esenciales.

5.8.6 Validación metodológica del marco IGEO

La comparación cruzada entre los escenarios E1, E2 y E3 valida la hipótesis central del trabajo: no existe una tecnología universalmente superior, sino una **tecnología óptima para cada contexto doctrinal**. El conflicto entre eficiencia (M-PUE), resiliencia (IRO) y seguridad (ICOMP) es cuantificable y relevante desde la perspectiva operativa. El IGEO permite visualizar este conflicto mediante ponderaciones ajustables y métricas homogéneas, proporcionando una herramienta sólida para fundamentar decisiones de Mando. El análisis realizado demuestra que el IGEO no solo organiza las métricas, sino que **estructura la toma de decisiones estratégicas**, justificando de forma transparente los *trade-offs* necesarios en cada nivel de despliegue y completando el ciclo metodológico iniciado en el Capítulo 4.

5.8.7 Implicaciones para la práctica y la política de defensa

Los resultados obtenidos permiten derivar un conjunto de implicaciones prácticas tanto para el diseño y operación de centros de proceso de datos como para la formulación de políticas tecnológicas en el ámbito de defensa:

- **Decisiones de inversión:** el modelo IGEO evidencia que la adopción selectiva de micro-VM en nodos tácticos maximiza la autonomía energética y reduce la dependencia logística, mientras que los entornos estratégicos deben mantener hipervisores tradicionales para garantizar trazabilidad y cumplimiento ENS-ALTA.
- **Criterios de rediseño de CPD:** los resultados sugieren que la arquitectura óptima es híbrida, combinando máquinas virtuales para dominios clasificados, contenedores para servicios ágiles y micro-VM para capacidades expedicionarias en escenarios DDIL.
- **Orquestación y telemetría:** la sensibilidad operativa observada en E3 indica que los sistemas de orquestación deben integrar métricas térmicas y energéticas en tiempo real, priorizando cargas según su impacto logístico y su criticidad.

- **Adaptación doctrinal:** los hallazgos refuerzan la necesidad de actualizar guías CCN-STIC y requisitos ENS para contemplar tecnologías ligeras de aislamiento reforzado, garantizando trazabilidad suficiente en despliegues tácticos.
- **Interoperabilidad aliada:** la adopción progresiva de micro-VM alinea las capacidades nacionales con los requisitos de resiliencia y modularidad definidos en FMN Spiral 5, facilitando la integración federada en operaciones multinacionales.

En conjunto, los resultados de este capítulo permiten validar de manera integral los cuatro Objetivos Específicos (OE-1 a OE-4), demostrando que el marco IGEO es capaz de caracterizar, comparar y priorizar tecnologías de virtualización en función de su idoneidad doctrinal en los niveles estratégico, operacional y táctico.

6 CONCLUSIONES, APORTACIONES Y LÍNEAS FUTURAS

Este capítulo presenta la síntesis final del trabajo y completa el ciclo metodológico iniciado en los capítulos anteriores. A partir de los resultados obtenidos mediante el modelado analítico multiescala realizado, se evalúa la validez del marco definido y se verifica el cumplimiento de los objetivos y la hipótesis planteados. El análisis integrado de las métricas M-PUE, IRO e ICOMP, así como su consolidación en el índice compuesto IGEO, permite fundamentar de forma cuantitativa y doctrinalmente alineada las conclusiones del estudio.

6.1 Conclusiones estratégicas y validación de la hipótesis

El análisis comparativo desarrollado valida la hipótesis central de este Trabajo Fin de Máster: **no existe una tecnología de virtualización universalmente óptima en defensa**, sino una tecnología adecuada para cada contexto doctrinal. El análisis paramétrico multiescala demuestra que el rendimiento relativo de las tecnologías analizadas (máquinas virtuales, contenedores, micro-VM y *unikernels*) depende directamente de las prioridades estratégicas del escenario, expresadas mediante las ponderaciones del IGEO. Estos resultados evidencian un conflicto estructural entre las dimensiones fundamentales del marco metodológico: la eficiencia energética (M-PUE), la resiliencia operativa (IRO) y la conformidad normativa (ICOMP).

Ninguna tecnología maximiza simultáneamente estas tres métricas, evidenciando la imposibilidad de una solución de «talla única» (*one-size-fits-all*) en el ámbito militar. Este hallazgo valida la necesidad del modelo IGEO como orquestador de la diversidad tecnológica. Este *trade-off*, cuantificado en los escenarios proyectados, se manifiesta de forma consistente:

- **Escenario estratégico (E1).** Con una clara priorización del cumplimiento normativo ($w_N = 0.50$), la máquina virtual tradicional es la opción óptima. Su aislamiento basado en hardware y su madurez normativa (ICOMP completo) garantizan la trazabilidad y seguridad requeridas por ENS-ALTA, superando la ventaja energética o de MTTR de otras tecnologías, que en este entorno estable ($F_{log} = 1.0$) resulta marginal.
- **Escenario Operacional (E2).** Bajo una ponderación equilibrada entre eficiencia y resiliencia ($w_E = 0.40$, $w_O = 0.40$), se confirma la necesidad de un modelo híbrido de virtualización. El impacto del factor logístico intermedio ($F_{log} = 1.1$) empieza a penalizar a las arquitecturas pesadas. Las VM siguen siendo esenciales para cargas ENS-ALTA, mientras que contenedores y micro-VM ofrecen un mejor equilibrio para cargas ENS-MEDIA y servicios ágiles, maximizando la eficiencia logística sin comprometer la continuidad del servicio.

- **Escenario Táctico (E3).** En condiciones DDIL, el análisis reveló que la carga logística extrema ($F_{log} = 1.5$) sitúa a la virtualización tradicional en una zona de «inviabilidad logística» (M-PUE >5.0). Las micro-VM emergen como la opción superior no solo por eficiencia, sino por pura supervivencia operativa. Su capacidad para reducir drásticamente el consumo de combustible y el tiempo de recuperación (MTTR) las convierte en la solución más viable para nodos tácticos. Por su parte, los *unikernels*, pese a ofrecer una eficiencia teórica marginalmente superior, quedan relegados por el «Veto Normativo»: su déficit de auditabilidad (ICOMP 0.50) impide su despliegue generalizado en sistemas de mando, resolviendo la paradoja de eficiencia a favor de la micro-VM como solución de compromiso.

La coherencia entre estos resultados permite afirmar que los **objetivos específicos del trabajo (OE-1 a OE-5)** quedan plenamente cumplidos: se identifican las limitaciones normativas de cada tecnología, se caracterizan sus perfiles operativos, se formula una métrica energética adaptada a entornos desplegados (M-PUE), se define un modelo de resiliencia (IRO) y se integra el conjunto en un marco compuesto (IGEO) capaz de estructurar decisiones de mando basadas en prioridades doctrinales. El modelado analítico, pese a sus restricciones, proporciona una validación consistente del método y demuestra que el IGEO es una herramienta eficaz para racionalizar la selección tecnológica en arquitecturas de defensa.

En conjunto, la evidencia obtenida consolida un principio fundamental: la virtualización en defensa debe abordarse desde una lógica estratégica dependiente del nivel de despliegue, y no como una decisión tecnológica uniforme. La articulación del análisis mediante el IGEO permite visualizar los compromisos necesarios entre seguridad, eficiencia y resiliencia, garantizando que las decisiones tecnológicas se alineen de manera explícita con las prioridades doctrinales y operativas de cada escalón del mando.

Finalmente, aunque el análisis identifica tecnologías óptimas por nivel, la arquitectura objetivo no debe ser estanca. La visión final es un ecosistema federado donde las Máquinas Virtuales (E1) actúan como repositorios persistentes y seguros, mientras que las micro-VM (E3) operan como elementos de maniobra ágil, interconectados bajo una política de seguridad común que garantice la coherencia del dato en todo el teatro de operaciones.

6.2 Aportaciones metodológicas y doctrinales

El trabajo no se limita a evaluar tecnologías de virtualización, sino que desarrolla un marco integral de análisis y decisión específicamente orientado a infraestructuras de defensa. Las aportaciones generadas abarcan tres niveles complementarios: métrico, metodológico y doctrinal, y permiten abordar la virtualización desde una perspectiva alineada con las prioridades estratégicas identificadas en el Capítulo 1.

6.2.1 Aportación 1: Formalización de la métrica M-PUE

La primera contribución original es la definición del **M-PUE**, concebido para evaluar la eficiencia energética de infraestructuras virtualizadas bajo condiciones operativas donde la disponibilidad energética, el entorno ambiental y la eficiencia de la virtualización tienen un impacto estratégico. El M-PUE extiende el PUE convencional incorporando tres factores doctrinales críticos: el factor ambiental (F_{amb}), el factor de disponibilidad energética (F_{gen}) y, crucialmente, el factor logístico (F_{log}). Esta formulación permite medir la sostenibilidad real de tecnologías como VM, contenedores y micro-VM bajo condiciones estables, mixtas o DDIL, visibilizando el coste oculto del transporte de energía en zona de operaciones. Su aplicación en los escenarios doctrinales confirma su utilidad para cuantificar la viabilidad de despliegues tácticos y para comparar tecnologías de forma homogénea. Esta métrica cubre el vacío doctrinal identificado en el Capítulo 1 respecto a la ausencia de indicadores energéticos adaptados a entornos desplegados.

6.2.2 Aportación 2: El IGEO como herramienta de decisión

La segunda contribución central es la formulación del **IGEO**, que integra en un único marco las tres dimensiones críticas en defensa: eficiencia energética (M-PUE), resiliencia operativa (IRO) y conformidad normativa (ICOMP). El IGEO incorpora ponderaciones dinámicas (w_E, w_O, w_N) que reflejan las prioridades estratégicas asignadas por el mando en cada nivel doctrinal (E1, E2, E3). Su relevancia no radica únicamente en la estructura matemática del índice, sino en su función como mecanismo doctrinal de apoyo a la decisión. Los resultados del Capítulo 5 demuestran que el IGEO selecciona de manera coherente la tecnología que maximiza la utilidad estratégica en cada escenario: VM en E1, arquitecturas híbridas en E2 y micro-VM en E3. Con ello, el IGEO se consolida como un instrumento que permite justificar de forma transparente los *trade-offs* entre seguridad, resiliencia y sostenibilidad.

6.2.3 Aportación 3: Marco de adopción progresiva para la Defensa

La tercera aportación es la definición de un **modelo de adopción estratégica** que traduce los resultados del análisis en un itinerario aplicable a organizaciones de defensa. Este marco plantea una transición hacia una arquitectura de virtualización híbrida y multinivel mediante tres fases: (1) **validación en entornos controlados** mediante un *testbed* que permita evaluar M-PUE, IRO e ICOMP; (2) **piloto operacional** en infraestructuras ENS-MEDIA/ALTA para verificar el comportamiento en carga real y su alineamiento con CCN-STIC; y (3) **federación OTAN-UE** orientada a la interoperabilidad FMN y a la soberanía del dato. Este modelo facilita la transición desde un enfoque centrado en máquinas virtuales hacia un ecosistema más flexible que integra contenedores y micro-VM en función del nivel doctrinal y la criticidad de la carga. Esta aportación da cumplimiento directo al **OE-6**, al proporcionar un itinerario de adopción verificable y alineado con ENS y FMN.

6.3 Limitaciones y líneas futuras de investigación

El trabajo se ha basado en un **modelado analítico paramétrico** como mecanismo principal de validación. Esta aproximación ha permitido integrar factores energéticos, operativos y normativos de forma homogénea, pero conlleva limitaciones metodológicas inherentes a la simulación teórica:

- **Ausencia de validación empírica en DDIL.** Variables críticas como la degradación real del enlace o la disipación térmica en microrredes móviles se han modelado mediante coeficientes (F_{amb}, F_{gen}), sin una validación física en un *testbed* real. Esta limitación se aborda directamente en la propuesta de la línea futura **L1**.
- **Dependencia de la parametrización.** La precisión del índice IGEO depende de la exactitud de los datos de entrada. La falta de integración automática con orquestadores reales impide actualmente un ajuste dinámico de los pesos (w_i) durante la operación, una brecha que motiva la línea de investigación **L2**.
- **Contextualidad de las ponderaciones estratégicas.** Los valores de ponderación empleados en el índice IGEO (w_E, w_O, w_N) dependen del juicio experto y de la priorización doctrinal de la misión, lo que introduce un componente inevitablemente contextual. No obstante, esta característica no constituye una debilidad del modelo, sino una condición inherente a los procesos de planificación en defensa, donde la toma de decisiones técnicas se encuentra subordinada a criterios operativos y estratégicos definidos por el mando.

Más allá de las restricciones metodológicas del estudio, el análisis revela también barreras estructurales para la adopción real de estas arquitecturas en Defensa:

- **Factor humano y doctrina de empleo.** La transición desde sistemas monolíticos hacia arquitecturas distribuidas basadas en micro-VM y orquestadores dinámicos eleva significativamente la complejidad técnica del nodo táctico. Esto impone una limitación organizativa crítica: la necesidad de capacitar a operadores especialistas en zona de operaciones o, alternativamente, garantizar enlaces de soporte remoto (*reach-back*) robustos. Esta dependencia tecnológica podría friccionar con la doctrina de «simplicidad en el borde», que prioriza sistemas mantenibles por personal generalista bajo estrés de combate.
- **Madurez de la cadena de suministro software.** A diferencia de los hipervisores comerciales consolidados (certificados bajo Common Criteria con niveles EAL+ [74]), el ecosistema de *unikernels* y micro-VMs carece aún de una base industrial equivalente. La falta de proveedores que garanticen soporte a largo plazo (LTS) introduce riesgos de mantenibilidad en los ciclos de vida de los sistemas de defensa, que suelen extenderse entre 10 y 15 años, generando incertidumbre sobre la gestión de la obsolescencia y la aplicación de parches de seguridad.

De estas limitaciones, tanto técnicas como estructurales, se derivan varias líneas futuras de investigación que permitirían consolidar el marco propuesto y evolucionarlo hacia aplicaciones operativas y doctrinales más amplias. Esta visión prospectiva se estructura en la hoja de ruta de la Figura 6-1 y se desglosa en los siguientes puntos:

- L1: Validación experimental del M-PUE en entornos reales.** Se propone desarrollar un *testbed* físico compuesto por nodos virtualizados con tecnologías VM, contenedores, micro-VM y *unikernels*, alimentados mediante microrredes híbridas. Esta infraestructura permitiría validar experimentalmente la sensibilidad del M-PUE a los factores operativos y extender la métrica incorporando el indicador WUE (*Water Usage Effectiveness*) —crítico en zonas de operaciones áridas—, contribuyendo a la línea doctrinal de *Defensa Verde Digital* impulsada por el Plan de Acción Climática de la Alianza [75].
- L2: Integración del IGEO en sistemas de planeamiento de misión.** Una línea de alto impacto consiste en incorporar el algoritmo IGEO como módulo de apoyo a la decisión en las fases de generación de fuerza. Esto permitiría automatizar el proceso de selección de la configuración de despliegue óptima antes de la misión, asegurando que cada unidad salga a zona de operaciones con la arquitectura (VM/Contenedor/Micro-VM) que mejor se ajuste a su perfil logístico y de seguridad previsto.
- L3: Desarrollo de nodos tácticos basados en micro-VM y federación SDN.** El escenario E3 revela el potencial de las micro-VM como base para nodos de borde. Una línea futura es diseñar un prototipo táctico que integre micro-VM con políticas *Zero Trust*. Esta federación debe apoyarse en redes definidas por software (SDN) y soluciones de orquestación Multi-Site, que permitan extender las políticas de seguridad y los segmentos de red desde el núcleo hasta el borde, garantizando la continuidad del servicio.
- L4: Contribución a la estandarización.** Dada la ausencia de métricas energéticas adaptadas al ámbito militar, se propone someter el modelo M-PUE y el marco IGEO a valoración técnica en los grupos de trabajo de la OTAN Science and Technology Organization [76]. Esta vía permitiría contrastar la metodología con expertos aliados y contribuir al desarrollo futuro de criterios interoperables de sostenibilidad.
- L5: Evolución de la seguridad mediante Computación Confidencial.** Investigar la integración de tecnologías de aislamiento por hardware (como Intel SGX [77] o AMD SEV [78]) en contenedores y micro-VM. Esto permitiría elevar su puntuación ICOMP al proteger la memoria en uso (*data-in-use*), mitigando las vulnerabilidades del kernel compartido y facilitando su acreditación para niveles de clasificación superiores en entornos tácticos.

L6: Investigación en mecanismos de auditoría externa y trazabilidad para *unikernels*. Si bien los *unikernels* demostraron la máxima eficiencia teórica (M-PUE), su adopción está bloqueada porque su arquitectura cerrada impide instalar los agentes de seguridad que exige el ENS (bajo ICOMP). Se propone investigar técnicas de auditoría que permitan monitorizar su ejecución y generar evidencias forenses desde fuera. Esto solucionaría su déficit normativo, habilitando su uso en sensores tácticos y drones donde la eficiencia energética es vital.



Figura 6-1: Hoja de ruta y proyección de líneas futuras (L1–L6). Fuente: Elaboración propia.

En conjunto, estas líneas futuras permiten evolucionar el marco metodológico desde una validación teórica hacia una capacidad plenamente integrada en infraestructuras reales, reforzando su aplicación en arquitecturas tácticas, operacionales y estratégicas y ampliando su impacto doctrinal en el ámbito de la Defensa.

En síntesis, este Trabajo Fin de Máster aporta una contribución original al proponer un marco metodológico que conecta la ingeniería de sistemas (M-PUE) con la decisión doctrinal (IGEO). El estudio demuestra que la virtualización, abordada desde esta perspectiva integral, se convierte en una capacidad estratégica esencial para una Defensa más resiliente, auditable y energéticamente sostenible. El trabajo concluye con una visión clara: avanzar hacia una infraestructura digital militar resiliente, auditable y energéticamente sostenible, en la que la eficiencia operativa y la ciberseguridad converjan bajo un mismo marco de gobernanza técnica y doctrinal, reforzando la autonomía, la sostenibilidad y la excelencia estratégica de las Fuerzas Armadas en el contexto de la defensa del siglo XXI.

7 BIBLIOGRAFÍA

- [1] “Denied, Disrupted, Intermittent, and Limited Impact (DDIL),” Tech. Rep. NISTIR 8286D-upd1, National Institute of Standards and Technology (NIST), 2024. [En línea]. Disponible en: https://csrc.nist.gov/glossary/term/denied_disrupted_intermittent_and_limited_impact [Consultado: 11-nov-2025].
- [2] K. Galvin, H. Jense, T. van den Berg, J. M. Pullen, C. Blais, and M. Dechand, “Advancing modelling and simulation in NATO Federated Mission Networking,” tech. rep., NATO Science and Technology Organization, Modelling and Simulation Group (STO-MP-MSG-207), 2023. [En línea]. Disponible en: <https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-207/MP-MSG-207-07.pdf> [Consultado: 15-oct-2025].
- [3] “Allies enhance NATO’s digital posture,” 2025. [En línea]. Disponible en: https://www.nato.int/cps/en/natohq/news_237092.htm [Consultado: 16-oct-2025].
- [4] “NATO Digital Backbone & NATO Digital Backbone Reference Architecture (DBRA),” tech report, North Atlantic Treaty Organization (NATO), 2024. [En línea]. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/12/pdf/241213-DBRA.pdf [Consultado: 16-oct-2025].
- [5] “Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.” núm. 106, 4 de mayo de 2022, pp. 62782–62867, 2022. [En línea]. Disponible en: <https://www.boe.es/buscar/act.php?id=B0E-A-2022-7191> [Consultado: 15-oct-2025].
- [6] “Guía de Seguridad de las TIC CCN-STIC-220: Arquitecturas Virtuales. Seguridad en entornos de virtualización,” 2020. [En línea]. Disponible en: <https://www.ccn-cert.cni.es/es/guias-de-acceso-publico-ccn-stic/5192-ccn-stic-220-arquitecturas-virtuales/file> [Consultado: 15-oct-2025].
- [7] “Guía de Seguridad de las TIC CCN-STIC-823: Seguridad en entornos Cloud,” 2019. [En línea]. Disponible en: <https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file?format=html> [Consultado: 15-oct-2025].
- [8] “Ist-208 research symposium: Energy and logistics in tactical ict,” sto meeting proceedings, NATO Science and Technology Organization, 2024. Presented at NATO STO IST-208 Symposium. Restricted distribution; not available online.
- [9] S. Rostami, D. G. Down, and G. Karakostas, “Linearized data center workload and cooling management,” *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 3502–3514, 2024. [En línea]. Disponible en: <https://ieeexplore.ieee.org/document/10520293> [Consultado: 17-oct-2025].

- [10] P. Arroba, J. L. Risco-Martín, J. M. Moya, and J. L. Ayala, “Efficient energy consumption in hybrid cloud environment using adaptive vm consolidation,” *Scientific Reports*, 2024. [En línea]. Disponible en: <https://www.nature.com/articles/s41598-024-72459-z> [Consultado: 15-oct-2025].
- [11] H. R. Naji and R. Esmaeili, “Reduction of energy consumption in cloud data centers with proper placement of virtual machines,” *The Journal of Supercomputing*, vol. 81, no. 17, pp. 1590–1620, 2025. [En línea]. Disponible en: <https://doi.org/10.1007/s11227-025-08072-2> [Consultado: 15-oct-2025].
- [12] European Commission and European Alliance for Industrial Data, Edge and Cloud, “European industrial technology roadmap for the next generation cloud-edge offering,” tech. rep., European Commission, 2021. [En línea]. Disponible en: <https://digital-strategy.ec.europa.eu/en/library/today-commission-receives-industry-technology-roadmap-cloud-and-edge> [Consultado: 02-dic-2025].
- [13] “Boletín de observación tecnológica en defensa n.º 83,” boletín de observación tecnológica, Ministerio de Defensa, 2024. [En línea]. Disponible en: <https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/bot-83.pdf> [Consultado: 11-nov-2025].
- [14] European External Action Service (EEAS), “A strategic compass for security and defence,” 2022. [En línea]. Disponible en: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf [Consultado: 12-dic-2025].
- [15] “Plan Industrial y Tecnológico para la Seguridad y la Defensa,” informe, Gobierno de España, 2025. [En línea]. Disponible en: <https://www.lamoncloa.gob.es/consejodeministros/resumenes/Documents/2025/230425-plan-industrial-y-tecnologico-para-la-seguridad-y-la-defensa.pdf> [Consultado: 11-nov-2025].
- [16] “PUE: A comprehensive examination of the metric,” tech. rep., The Green Grid, 2012. [En línea]. Disponible en: https://datacenters.lbl.gov/sites/default/files/WP49-PUE%20A%20Comprehensive%20Examination%20of%20the%20Metric_v6.pdf [Consultado: 20-oct-2025].
- [17] M. Duranton and et al., “Hipec vision 2023: High performance embedded architecture and compilation,” tech. rep., HiPEAC Network of Excellence (European Commission), 2021. [En línea]. Disponible en: <https://www.hipec.net/vision/2023/> [Consultado: 12-dic-2025].
- [18] “European Defence Operational Collaborative Cloud (EDOCC),” 2022. [En línea]. Disponible en: https://defence-industry-space.ec.europa.eu/document/download/ade27d7c-f9b6-49a0-b2fb-f621d6abe897_en [Consultado: 21-nov-2025].
- [19] Ministerio de Defensa, España, “Numant-IA: Centro de Capacidades Tecnológicas Avanzadas.” Nota de prensa, 2025. [En línea]. Disponible en: <https://www.defensa.gob.es/gabinete/notasPrensa/2025/09/DGC-250903-visita-proyecto-numant-ia.html> [Consultado: 21-nov-2025].
- [20] “ANSI/TIA-942-C — Telecommunications Infrastructure Standard for Data Centers,” 2024. [En línea]. Disponible en: <https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/> [Consultado: 18-oct-2025].
- [21] “UNE-EN 1047-2:2019 — unidades de almacenamiento de seguridad. clasificación y métodos de ensayo de resistencia al fuego. parte 2: Cámaras y contenedores ignífugos,” 2019. [En línea]. Disponible en: <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0061739> [Consultado: 18-oct-2025].
- [22] “ANSI/BICSI 002-2024 — Data Center Design and Implementation Best Practices,” 2024. [En línea]. Disponible en: <https://www.bicsi.org/standards/available-standards-store/single-purchase/ansi-bicsi-002-the-standard-for-data-center-design> [Consultado: 18-oct-2025].

- [23] “ISO/IEC 27001:2022 — information security, cybersecurity and privacy protection — information security management systems — requirements,” 2022. [En línea]. Disponible en: <https://www.iso.org/standard/82875.html> [Consultado: 10-oct-2025].
- [24] “ISO/IEC 18598:2016 — information technology — automated infrastructure management (aim) systems — requirements, data exchange and applications,” 2016. [En línea]. Disponible en: <https://www.iso.org/standard/62987.html> [Consultado: 02-nov-2025].
- [25] Department of Defense (DoD), *MIL-STD-188-125-1: High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions. Part 1: Fixed Facilities*. United States Department of Defense, 2005. [En línea]. Disponible en: https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=204459 [Consultado: 12-dic-2025].
- [26] “Electromagnetic compatibility (EMC) — Part 1: General — Section 1: Application and interpretation of fundamental definitions and terms,” Informe técnico IEC TR 61000-1-1, International Electrotechnical Commission, 1992. [En línea]. Disponible en: <https://webstore.iec.ch/publication/4134> [Consultado: 30-oct-2025].
- [27] “ISO/IEC 11801-1:2017 — information technology — generic cabling for customer premises — part 1: General requirements,” 2017. [En línea]. Disponible en: <https://www.iso.org/standard/66182.html> [Consultado: 30-oct-2025].
- [28] “Centro de datos Alcalá de Henares,” ficha técnica, Telefónica, 2012. [En línea]. Disponible en: <https://www.movistar.es/estaticos/grandesempresas/pdf/CdG-ALCALA-DE-HENARES.pdf> [Consultado: 5-nov-2025].
- [29] “Mobile data centers from cancom.” [En línea]. Disponible en: <https://physical-infrastructure.cancom.com/mobile-data-centers-from-cancom/> [Consultado: 6-nov-2025].
- [30] “MIL-STD-810H — department of defense test method standard: Environmental engineering considerations and laboratory tests,” 2019. [En línea]. Disponible en: https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=35978 [Consultado: 16-nov-2025].
- [31] “MIL-STD-461G — Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” 2015. [En línea]. Disponible en: https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=35789 [Consultado: 11-nov-2025].
- [32] “HPE Edgeline EL8000 Converged Edge System.” [En línea]. Disponible en: <https://buy.hpe.com/us/en/compute/edgeline-systems/edgeline-systems/edgeline-converged-edge-systems/hpe-edgeline-el8000-converged-edge-system/p/1011622898> [Consultado: 8-nov-2025].
- [33] “Mission Partner Environments,” s.f. [En línea]. Disponible en: <https://www.gdit.com/mission-partner-environments/> [Consultado: 8-nov-2025].
- [34] “Servidores físicos vs. máquinas virtuales,” 2023. [En línea]. Disponible en: <https://www.veeam.com/blog/es/why-virtual-machine-backups-different.html> [Consultado: 8-nov-2025].
- [35] North Atlantic Council, “Ac/35-d/2004-rev4: Primary directive on cis security,” tech. rep., North Atlantic Treaty Organization (NATO), 2024. [En línea]. Disponible en: https://www.nbu.cz/download/pravni-predpisy---nato/AC_35-D_2004-REV4_ENG_NHQD339286.pdf [Consultado: 10-oct-2025].
- [36] “Guía de seguridad de las tic ccn-stic-652a: Seguridad en contenedores,” 2020. [En línea]. Disponible en: <https://www.ccn-cert.cni.es/es/guias-de-acceso-publico-ccn-stic/5189-ccn-stic-652a-seguridad-en-contenedores/file.html> [Consultado: 15-oct-2025].
- [37] A. Agache, M. Brooker, A. Florescu, A. Iordache, A. Liguori, R. Neugebauer, P. Piwonka, and D.-M. Popa, “Firecracker: Lightweight virtualization for serverless applications,” (Santa Clara, CA, USA), February 2020. [En línea]. Disponible en: <https://www.usenix.org/system/files/nsdi20-paper-agache.pdf> [Consultado: 23-nov-2025].

- [38] European Commission, “Horizon Europe Work Programme 2023-2025: 13. General Annexes.” European Commission Decision C(2025) 2779, 2025. [En línea]. Disponible en: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-13-general-annexes_horizon-2023-2024_en.pdf [Consultado: 12-dic-2025].
- [39] North Atlantic Treaty Organization (NATO), “Green defence framework.” Adopted by the North Atlantic Council, 2014. [En línea]. Disponible en: https://natolibguides.info/ld.php?content_id=25285072 [Consultado: 12-nov-2025].
- [40] “NATO Green Defence: From the 2014 green defence framework to the 2021 climate change and security action plan,” in *Climate Change and Security*, Springer International Publishing, 2023. [En línea]. Disponible en: https://link.springer.com/chapter/10.1007/978-94-024-2186-6_2#citeas [Consultado: 12-nov-2025].
- [41] International Organization for Standardization (ISO), “ISO 50001:2018: Energy management systems – requirements with guidance for use,” 2018. [En línea]. Disponible en: <https://www.iso.org/standard/69426.html> [Consultado: 05-dic-2025].
- [42] “ISO/IEC 30134-2:2016 — information technology — data centres — key performance indicators. part 2: Power usage effectiveness (pue),” 2016. [En línea]. Disponible en: <https://www.iso.org/standard/63451.html> [Consultado: 11-nov-2025].
- [43] “ISO/IEC 30134-2:2022 — information technology — data centres — key performance indicators. part 9: Water usage effectiveness (wue),” 2022. [En línea]. Disponible en: <https://www.iso.org/es/contents/data/standard/07/76/77692.html> [Consultado: 11-nov-2025].
- [44] “ISO/IEC 30134-8:2022 — information technology — data centres — key performance indicators. part 8: Carbon usage effectiveness (cue),” 2022. [En línea]. Disponible en: <https://www.iso.org/es/contents/data/standard/07/76/77691.html> [Consultado: 12-nov-2025].
- [45] “ISO/IEC 30134-6:2021 — information technology — data centres — key performance indicators. part 6: Energy reuse factor (erf),” 2021. [En línea]. Disponible en: <https://www.iso.org/standard/71717.html> [Consultado: 11-nov-2025].
- [46] “Data centers efficiency: How we do it — scale with speed and sustainability,” 2025. [En línea]. Disponible en: <https://datacenters.google/efficiency/> [Consultado: 11-nov-2025].
- [47] “ISO/IEC 27017:2015 — code of practice for information security controls based on ISO/IEC 27002 for cloud services,” 2015. [En línea]. Disponible en: <https://www.iso.org/standard/43757.html> [Consultado: 4-nov-2025].
- [48] “ISO/IEC 27018:2019 — code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors,” 2019. [En línea]. Disponible en: <https://www.iso.org/standard/76559.html> [Consultado: 4-nov-2025].
- [49] National Institute of Standards and Technology (NIST), “Zero trust architecture (nist sp 800-207),” tech. rep., U.S. Department of Commerce, 2020. [En línea]. Disponible en: <https://doi.org/10.6028/NIST.SP.800-207> [Consultado: 2-nov-2025].
- [50] NATO Standardization Office (NSO), “STANAG 5524 Ed.5,” standardization agreement, 2025. [En línea]. Disponible en: <https://nso.nato.int/nso/nsdd/main/standards?search=5524> [Consultado: 04-dic-2025].
- [51] NATO Standardization Office (NSO), “STANAG 4559 Ed.4: Nato standard isr library interface and services,” standardization agreement, North Atlantic Treaty Organization, 2018. [En línea]. Disponible en: <https://nso.nato.int/nso/nsdd/main/standards?search=5524> [Consultado: 04-dic-2025].

- [52] European Commission, “Cloud computing | shaping europe’s digital future,” 2025. [En línea]. Disponible en: <https://digital-strategy.ec.europa.eu/en/policies/cloud-computing> [Consultado: 12-dic-2025].
- [53] S. Dustdar, P. K. Donta, and V. Casamayor Pujol, “On distributed computing continuum systems,” *IEEE Transactions on Parallel and Distributed Systems*, 2022. [En línea]. Disponible en: <https://ieeexplore.ieee.org/document/9681207> [Consultado: 12-dic-2025].
- [54] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. Gurer, and C. Mahmoudi, “Nist sp 500-325: Fog computing conceptual model,” tech. rep., National Institute of Standards and Technology (NIST), 2018. [En línea]. Disponible en: <https://doi.org/10.6028/NIST.SP.500-325> [Consultado: 12-dic-2025].
- [55] “IEEE Standard for an Architectural Framework for the Internet of Things (IoT),” 2019. [En línea]. Disponible en: <https://standards.ieee.org/standard/2413-2019.html> [Consultado: 4-nov-2025].
- [56] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, “A survey on Mobile Edge Computing: The communication perspective,” *IEEE Communications Surveys and Tutorials*, 2017. [En línea]. Disponible en: <https://ieeexplore.ieee.org/document/8016573> [Consultado: 03-nov-2025].
- [57] North Atlantic Treaty Organization (NATO), “NATO DIANA: Defence innovation accelerator for the north atlantic – strategic direction and challenges,” 2023. [En línea]. Disponible en: <https://www.diana.nato.int> [Consultado: 04-dic-2025].
- [58] National Institute of Standards and Technology (NIST), “Application container security guide (nist sp 800-190),” tech. rep., U.S. Department of Commerce, 2017. [En línea]. Disponible en: <https://doi.org/10.6028/NIST.SP.800-190> [Consultado: 4-nov-2025].
- [59] CNCF Security Special Interest Group, “Cloud Native Security Whitepaper,” tech. rep., Cloud Native Computing Foundation, 2020.
- [60] K. Bilal, S. U. R. Malik, O. Khalid, A. Hameed, E. Alvarez, V. Wijaysekara, R. Irfan, S. Shrestha, D. Dwivedy, M. Ali, U. S. Khan, A. Abbas, N. Jalil, and S. U. Khan, “A taxonomy and survey on Green Data Center Networks,” *Future Generation Computer Systems*, 2013. [En línea]. Disponible en: https://www.academia.edu/4528052/A_taxonomy_and_survey_on_Green_Data_Center_Networks [Consultado: 21-nov-2025].
- [61] R. Buyya, S. Ilager, and P. Arroba, “Energy-efficiency and sustainability in new generation cloud computing: A vision and directions for integrated management of data centre resources and workloads,” *Software: Practice and Experience*, vol. 54, no. 1, pp. 24–38, 2024. [En línea]. Disponible en: <https://onlinelibrary.wiley.com/doi/10.1002/spe.3248> [Consultado: 05-dic-2025].
- [62] M. S. Kumar and G. R. Karri, “EEOA: Cost and Energy Efficient Task Scheduling in a Cloud-Fog Framework,” *Sensors*, vol. 23, no. 5, p. 2445, 2023. [En línea]. Disponible en: <https://doi.org/10.3390/s23052445> [Consultado: 12-nov-2025].
- [63] Amazon Web Services, *Cost Optimization Pillar - AWS Well-Architected Framework*. Amazon Web Services, Inc., 2024. [En línea]. Disponible en: <https://docs.aws.amazon.com/wellarchitected/latest/cost-optimization-pillar/wellarchitected-cost-optimization-pillar.pdf> [Consultado: 05-dic-2025].
- [64] Uptime Institute, “Global data center survey 2024,” industry report, Uptime Institute, 2024. [En línea]. Disponible en: <https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2024.GlobalDataCenterSurvey.Report.pdf> [Consultado: 05-dic-2025].
- [65] Intel Corporation, Hewlett-Packard, NEC, Dell, *Intelligent Platform Management Interface Specification Second Generation v2.0*, 2013. [En línea]. Disponible en: <https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/ipmi-second-gen-interface-spec-v2-rev1-1.pdf> [Consultado: 30-nov-2025].

- [66] “Dsp0266 — redfish scalable platforms management api specification,” 2024. [En línea]. Disponible en: https://www.dmtf.org/standards/published_documents/DSP0266_1.21.0.pdf [Consultado: 10-nov-2025].
- [67] “Water usage effectiveness (wue): A green grid data center sustainability metric,” tech. rep., The Green Grid, 2011. [En línea]. Disponible en: <https://airatwork.com/wp-content/uploads/The-Green-Grid-White-Paper-35-WUE-Usage-Guidelines.pdf> [Consultado: 9-nov-2025].
- [68] U.S. Green Building Council (USGBC), *LEED v4.1: Building Design and Construction (BD+C) – Data Centers Rating System*. U.S. Green Building Council, 2024. [En línea]. Disponible en: <https://www.usgbc.org/leed/v41#bdc> [Consultado: 01-dic-2025].
- [69] Asociación Española de Normalización (UNE), “UNE-EN 50600-1: Tecnología de la información. infraestructuras e instalaciones de centros de datos. parte 1: Conceptos generales,” tech. rep., UNE / CENELEC, 2019. [En línea]. Disponible en: <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0062011> [Consultado: 03-nov-2025].
- [70] ISO/IEC/IEEE, “ISO/IEC/IEEE 42010:2022: Systems and software engineering – architecture description,” tech. rep., International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) / Institute of Electrical and Electronics Engineers (IEEE), 2022. [En línea]. Disponible en: <https://www.iso.org/standard/74393.html> [Consultado: 15-nov-2025].
- [71] “Data center power equipment thermal guidelines and best practices,” tech. rep., ASHRAE Technical Committee 9.9, 2016. [En línea]. Disponible en: https://www.ashrae.org/file%20library/technical%20resources/bookstore/ashrae_tc0909_power_white_paper_22_june_2016_revised.pdf [Consultado: 12-nov-2025].
- [72] “MIL-STD-1472H — Department of Defense Design Criteria Standard: Human Engineering,” 2020. [En línea]. Disponible en: https://quicksearch.dla.mil/qsdcdetails.aspx?ident_number=36903 [Consultado: 12-nov-2025].
- [73] U.S. Government Accountability Office, “Defense management: Overarching organizational framework needed to guide and oversee energy reduction efforts for military operations,” report to congressional committees, U.S. Government Accountability Office. [En línea]. Disponible en: <https://www.gao.gov/products/gao-08-426> [Consultado: 13-dic-2025].
- [74] Common Criteria Recognition Arrangement, “Common Criteria Certified Products List,” 2025. [En línea]. Disponible en: <https://www.commoncriteriaportal.org/products/index.cfm> [Consultado: 12-dic-2025].
- [75] North Atlantic Treaty Organization, “NATO Climate Change and Security Action Plan.” Official Text, 2021. [En línea]. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_185174.htm [Consultado: 12-dic-2025].
- [76] NATO Science and Technology Organization, “Science & technology organization: Empowering the alliance’s technological edge.” NATO STO Website, 2025. [En línea]. Disponible en: <https://www.sto.nato.int/> [Consultado: 12-dic-2025].
- [77] Intel Corporation, *Intel® 64 and IA-32 Architectures Software Developer’s Manual. Volume 3D: System Programming Guide, Part 4 (Intel® SGX)*, 2024. [En línea]. Disponible en: <https://www.intel.com/content/www/us/en/developer/articles/technical/intel-sdm.html> [Consultado: 15-nov-2025].
- [78] Advanced Micro Devices (AMD), *Secure Encrypted Virtualization API Specification*, 2020. [En línea]. Disponible en: <https://www.amd.com/en/developer/sev.html> [Consultado: 15-nov-2025].

- [79] “AAP-06 NATO Glossary of Terms and Definitions (English and French),” NATO terminology publication, NATO Standardization Office, 2025. [En línea]. Disponible en: https://oos-data.army.cz/aap6/AAP-06%20NATOTerm_2025_04_24.pdf [Consultado: 22-oct-2025].
- [80] “Allied joint publication-01: Allied joint doctrine. edition f, version 1 with UK national elements,” NATO Terminology Publication, NATO Standardization Office, 2022. [En línea]. Disponible en: https://assets.publishing.service.gov.uk/media/659ea238e96df5000df843f3/AJP_01_EdF_with_UK_elements.pdf [Consultado: 22-oct-2025].
- [81] “PDC-00 glosario de términos militares y de defensa 2020,” informe técnico, Estado Mayor de la Defensa, 2020. [En línea]. Disponible en: <https://elconfidencialdigital.opennemas.com/media/elconfidencialdigital/files/2020/07/15/GLOSARIO%202020.pdf> [Consultado: 15-oct-2025].
- [82] “ISO/IEC/IEEE 14764:2022 — software engineering — software life cycle processes — maintenance,” 2022. [En línea]. Disponible en: <https://www.iso.org/standard/81692.html> [Consultado: 12-dic-2025].
- [83] European Commission, “EUDIS: Eu defence innovation scheme – fostering defence innovation in europe,” 2024. [En línea]. Disponible en: <https://eudis.europa.eu> [Consultado: 10-dic-2025].