



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Implantación de un modelo de Nube en el Ministerio de Defensa

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Arturo Blesa Solano

DIRECTORES: Fernando Suárez Lorenzo

Luis Modesto Álvarez Sabucedo

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Implantación de un modelo de Nube en el Ministerio de Defensa

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

Universida_deVigo

RESUMEN

Derivado de la Estrategia de Explotación de la Nube en el Ministerio de Defensa (MDEF) se le asigna al Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) la responsabilidad de definir un marco tecnológico para su implementación, recibiendo los roles de impulsor de la propia estrategia y gestor de una infraestructura inteligente. La mencionada estrategia expresa, por tanto, una clara intención de evolucionar hacia un modelo de nube en el seno del MDEF.

Se pretende definir una solución técnica para lograr este objetivo, fundamentada en marcos de referencia para la adopción de nube y buenas prácticas arquitectónicas orientadas a su construcción y explotación. Para ello se han tenido en cuenta los condicionantes de seguridad inherentes al MDEF, así como la situación real de la infraestructura presente a evolucionar.

El marco tecnológico que concreta la solución aborda diferentes aspectos como son diseño, arquitectura, operación y seguridad apostando, en definitiva, por un escenario en el que los servicios se repartan dentro de una nube híbrida compuesta por dos entornos:

- Nube privada: un entorno sobre instalaciones propiedad del MDEF que permita otorgar servicios en la nube dentro de la organización.
- Nube pública: un entorno virtual desplegado sobre infraestructuras comerciales en el que, además, se puedan canalizar servicios de entidades externas al MDEF.

Las líneas de actuación incorporadas en el trabajo realizado aspiran a servir como guía para la evolución de una infraestructura tradicional hacia una infraestructura inteligente, para cumplir con el objetivo de ofrecer una mejora continua en la provisión de los servicios.

PALABRAS CLAVE

ESTRATEGIA, NUBE, SOLUCIÓN, HÍBRIDA, MEJORA

AGRADECIMIENTOS

A mi mujer Alba y a mis hijos Jorge y Alejandro, por su inagotable paciencia y apoyo durante el tiempo dedicado a cursar este máster, muy especialmente a la hora de elaborar este trabajo.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	5
1 Introducción y objetivos	7
1.1 Introducción	7
1.2 Propósito	8
1.3 Objetivos	8
1.4 Organización de la memoria	9
2 Estado del arte	11
2.1 Conceptos presentes en el MDEF	11
2.1.1 El CESTIC	11
2.1.2 La I3D	12
2.1.3 Los Ámbitos del MDEF.....	12
2.2 La Estrategia de Explotación de la Nube en el MDEF	12
2.3 Posibles modelos de nube	13
2.3.1 Nube Privada	14
2.3.2 Nube Pública.....	14
2.3.3 Nube Híbrida	15
2.4 Aspectos de seguridad en el MDEF	15
2.4.1 El Esquema Nacional de Seguridad.....	15
2.4.2 La Baja y la Alta Clasificación.....	16
2.4.3 Los Dominios de Seguridad.....	16
3 Desarrollo del TFM	19
3.1 Diseño de la Nube MDEF	19
3.1.1 Aspectos generales.....	19
3.1.2 Capas de computación en la nube: Fog y Edge Computing	20
3.1.3 Situación final deseada	21
3.2 Arquitectura de la Nube MDEF	23
3.2.1 Marco de referencia	23
3.2.2 Pilares de la Arquitectura.....	24
3.2.3 Arquitectura de la Nube Privada.....	26
3.2.4 Arquitectura de la Golden Copy	28
3.2.5 Arquitectura de la Nube Pública.....	30
3.2.6 Arquitectura de la Nube Híbrida.....	33

3.2.7 Arquitectura de la Nube de Combate.....	36
3.3 Operación de la Nube MDEF.....	39
3.3.1 Estructura de Operación	39
3.3.2 Atribución de roles y responsabilidades de Operación.....	43
3.3.3 Modelo de Operación	45
3.3.4 Racionalización y control del gasto de Operación	50
3.4 Seguridad de la Nube MDEF	55
3.4.1 Enfoque de Seguridad Confianza Cero (Zero Trust).....	55
3.4.2 Herramientas de Seguridad.....	56
3.4.3 Gestión de Identidades.....	58
3.4.4 Identidad Híbrida	60
3.4.5 Autenticación y Acceso	62
3.4.6 Protección de los Servicios	66
3.4.7 Características de la Golden Copy.....	69
4 Resultados / Validación / Prueba.....	73
4.1 Planteamiento de un supuesto práctico	73
4.1.1 Punto de partida	73
4.1.2 Plan de migración	73
4.1.3 Estrategias de migración.....	74
4.2 Desarrollo del supuesto práctico	76
4.2.1 Casos a considerar	76
4.2.2 Servicios a considerar	77
4.2.3 Análisis y resultados	77
5 Conclusiones y líneas futuras	81
5.1 Conclusiones	81
5.1.1 Sobre aspectos generales	81
5.1.2 Sobre la Nube Privada	82
5.1.3 Sobre la Nube Pública	83
5.1.4 Sobre la Nube Híbrida	84
5.1.5 Sobre la Nube de Combate	85
5.2 Líneas futuras	85
6 Bibliografía.....	87
Anexo I: Abreviaturas y Acrónimos.....	91
Anexo II: Cálculo y análisis de resultados sobre un supuesto práctico de migración de servicios a la Nube MDEF	93

ÍNDICE DE FIGURAS

Figura 1-1 Ideograma de evolución de la I3D al modelo de nube (tomada de [1]).	8
Figura 2-1 Esquema de Nube Privada del MDEF (tomada de [1]).	14
Figura 2-2 Esquema de Nube Pública del MDEF (tomada de [1]).	14
Figura 2-3 Esquema de Nube Híbrida del MDEF (tomada de [1]).	15
Figura 3-1 Representación de la transición a la Nube MDEF (elaboración propia).	22
Figura 3-2 Capas de computación: <i>Cloud Computing (Core)</i> , <i>Fog</i> y <i>Edge Computing</i> (elaboración propia).	23
Figura 3-3 Buenas prácticas arquitectónicas de los principales proveedores de nube (tomada de [11]).	23
Figura 3-4 Pilares de la arquitectura de la Nube MDEF (tomada de [12]).	24
Figura 3-5 Esquema de regiones, zonas de disponibilidad y CPD (tomada de [13]).	26
Figura 3-6 Implementación con Redundancia (tomada de [13]).	27
Figura 3-7 Valoración de una Implementación con Redundancia (tomada de [13]).	28
Figura 3-8 Implementación con Redundancia y con Copia de Seguridad (tomada de [13]).	29
Figura 3-9 Valoración de una Implementación con Redundancia y con Copia de Seguridad (tomada de [13]).	29
Figura 3-10 Modelo de responsabilidad compartida para el aprovisionamiento de servicios desde nube pública (tomada de [1]).	30
Figura 3-11 Modelo de <i>Microsoft Azure</i> para la <i>Landing Zone</i> (tomada de [14]).	33
Figura 3-12 Detalle de arquitectura de nube híbrida (nube privada más nubes públicas) (elaboración propia).	33
Figura 3-13 Escenario de Hibridación (movimiento de cargas de nube privada hacia nube pública) (elaboración propia).	34
Figura 3-14 Escenario de Deshibridación (movimiento de cargas de nube pública hacia nube privada) (elaboración propia).	35
Figura 3-15 Escenario de cambio parcial entre diferentes proveedores (movimiento de cargas de nube pública hacia otra nube pública) (elaboración propia).	35
Figura 3-16 Escenario de cambio total entre diferentes proveedores (movimiento de cargas de nube pública hacia otra nube pública) (elaboración propia).	35
Figura 3-17 Representación de Capas “ <i>Edge to Cloud</i> ” (tomada de [21]).	37
Figura 3-18 Materialización de las Capas “ <i>Fog</i> y <i>Edge</i> ” sobre la base de dispositivos “ <i>Snow</i> ” (tomada de [21]).	37
Figura 3-19 Detalle de un rack “ <i>Outpost</i> ” que conforma la parte de nube privada “ <i>on-premise</i> ” del esquema “ <i>Edge to Cloud</i> ” (tomada de [21]).	38
Figura 3-20 Estructura de Operación de la Nube MDEF, partiendo del modelo de responsabilidad compartida para el aprovisionamiento de servicios desde nube pública (tomada de [1]), y completado con la parte de nube privada e infraestructura tradicional.	39
Figura 3-21 Comparativa entre virtualización tradicional y basada en contenedores (tomada de [23]).	40

Figura 3-22 Modelo de provisión de servicios en la Nube MDEF en relación con sus características y usuarios de destino (tomada de [1]).	41
Figura 3-23 Modelo de Operación de servicios en la Nube MDEF (tomada de [1]).	45
Figura 3-24 Representación de la asignación de recursos a un Inquilino (tomada de [24]).	46
Figura 3-25 Representación del nivel de aislamiento de recursos entre Inquilinos (tomada de [24]).	47
Figura 3-26 Representación del modelo de Inquilino Único (tomada de [24]).	47
Figura 3-27 Representación del modelo de Multi Inquilino (tomada de [24]).	48
Figura 3-28 Representación del modelo de Inquilino Mixto con partición vertical (tomada de [24]).	48
Figura 3-29 Representación del modelo de Inquilino Mixto con partición horizontal (tomada de [24]).	49
Figura 3-30 Representación del problema de “vecino ruidoso” en un modelo de Inquilino Mixto (tomada de [25]).	49
Figura 3-31 Comparativa de la diferente naturaleza de los gastos <i>CapEx</i> y <i>OpEx</i> (tomada de [26]).	51
Figura 3-32 Representación del servicio de <i>Microsoft Cost Management</i> para los recursos de nube pública junto con sus funcionalidades asociadas (tomada de [12]).	52
Figura 3-33 Marco de buenas prácticas <i>FinOps</i> (tomada de [28]).	54
Figura 3-34 Modelo de referencia del concepto de seguridad Confianza Cero (<i>Zero Trust</i>) (tomada de [22]).	56
Figura 3-35 Ideograma de la solución de identidad híbrida (según <i>Microsoft</i>) (tomada de [30]).	61
Figura 3-36 Esquema de funcionamiento para la implementación de la solución de identidad híbrida (según <i>Microsoft</i>) (tomada de [31]).	62
Figura 3-37 Elementos a evaluar para el acceso a los servicios bajo la solución de identidad híbrida (según <i>Microsoft</i>) (tomada de [30]).	63
Figura 3-38 Métodos de autenticación recomendados para el acceso a los servicios bajo la solución de identidad híbrida (según <i>Microsoft</i>) (tomada de [32]).	64
Figura 3-39 Implementación de <i>CBA</i> como método de autenticación (según <i>Microsoft</i>) (tomada de [36]).	66
Figura 3-40 Valoración de <i>CBA</i> como método de autenticación (según <i>Microsoft</i>) (tomada de [36]).	66
Figura 3-41 Modos básicos de funcionamiento de <i>CASB</i> (tomada de [37]).	67
Figura 3-42 Características de los distintos modos básicos de funcionamiento de <i>CASB</i> (tomada de [37]).	68
Figura 3-43 Relación de guías CCN-STIC-800 aplicables a <i>Microsoft Azure</i> (tomada de [40]).	69
Figura 3-44 Relación de guías CCN-STIC-800 aplicables a <i>AWS</i> (tomada de [40]).	69
Figura 3-45 Réplica de datos para la <i>Golden Copy</i> mediante <i>GRS</i> (según <i>Microsoft</i>) (tomada de [43]).	71
Figura 4-1 Diagrama de decisión de las <i>6Rs</i> para migración de servicios a nube (según <i>AWS</i>) (tomada de [50]).	75

ÍNDICE DE TABLAS

Tabla 3-1 Criterios básicos para decidir operar un servicio en Nube MDEF desde nube privada o nube pública.	42
Tabla 3-2 Criterios básicos para decidir el modelo de provisión de un servicio en Nube MDEF desde nube pública.	43
Tabla 3-3 Resumen de roles y responsabilidades junto con su atribución para la Operación de la Nube MDEF (tomada de [1]).	44
Tabla 4-1 Representación de ejes de medida y posibles casos a considerar para un supuesto práctico de migración de servicios a la Nube MDEF.	77
Tabla 4-2 Acciones resultantes obtenidas sobre una muestra de 66 servicios de la I3D para un supuesto práctico de migración de servicios a la Nube MDEF.	79
Tabla 4-3 Representación gráfica de las acciones resultantes obtenidas sobre una muestra de 66 servicios de la I3D para un supuesto práctico de migración de servicios a la Nube MDEF.	80

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

La Infraestructura Integral de Información para la Defensa (I3D), constituye una infraestructura tecnológica, bajo una autoridad operativa única que, mediante la convergencia de los sistemas de información y telecomunicaciones y los servicios que éstos proporcionan, debe optimizar el uso de los mismos y facilitar a los organismos y usuarios el acceso eficaz a los recursos de información del MDEF, desde cualquiera que sea su situación, en todo momento, y de forma segura.

Bajo la premisa de un empleo óptimo y eficiente de la infraestructura, se plantea el empleo de tecnologías de nube pública, en la que la infraestructura asociada a los sistemas y tecnologías de la información y las comunicaciones (CIS/TIC) sea propiedad de un proveedor comercial, pueda ser escalada dinámicamente, y albergue la demanda real de los usuarios ajustándose a la necesidad que en cada periodo se considere. De este modo, la tecnología de nube podría proporcionar flexibilidad para optimizar los costes derivados de los CIS/TIC y permitir a las organizaciones adaptarse a las prioridades cambiantes. De hecho, son muchas las organizaciones de todo tipo que están realizando la transición a servicios en la nube con el fin de aprovechar la amplia gama de beneficios que ofrecen.

Las arquitecturas en la nube requieren enfoques diferentes a los modelos tradicionales de infraestructuras basadas en recursos exclusivamente locales, principalmente en lo que se refiere a implementación de controles de seguridad y gestión de riesgos. Teniendo muy presentes los factores de seguridad y mitigación de riesgos mediante controles y procedimientos adecuados, como pilares inherentes a las actividades de Defensa, el MDEF tiene la posibilidad de disfrutar de los grandes beneficios que ofrece el concepto de nube.

Derivado de las consideraciones anteriores, el MDEF ha promulgado su propia Estrategia de Explotación de la Nube [1] por medio de la cual se faculta al Director del CESTIC para dictar, en el ámbito de sus competencias, las disposiciones oportunas para su aplicación. El desarrollo de esta estrategia, por medio de la aplicación de la tecnología de nube, va a conllevar de forma inevitable una evolución de la I3D, debiéndose abordar de manera integral, de modo que se contemplen diferentes aspectos tanto técnicos como organizativos.

Debe tenerse en cuenta que se parte de una situación establecida en la que se cuenta con una infraestructura, en producción, ya existente. La infraestructura CIS/TIC adquirida por el MDEF fue dimensionada para soportar la demanda máxima esperada, independientemente de la frecuencia con la que este hecho ocurra, por lo que cabe la posibilidad de un aprovechamiento ineficiente de parte de los recursos CIS/TIC del MDEF.

La organización y optimización, desde el inicio, de los Dominios de Seguridad de Baja y Alta Clasificación es crucial para el éxito futuro de esta implantación. Ambas infraestructuras se encuentran diferenciadas y requieren un tratamiento particularizado para cada caso, en cuanto a tecnología de nube se refiere.

En resumen, y de forma gráfica, el siguiente modelo contenido en la Estrategia de Explotación de la Nube [1] representa el esquema objetivo al que se debe tender a la hora de implantar un modelo de nube en el MDEF.

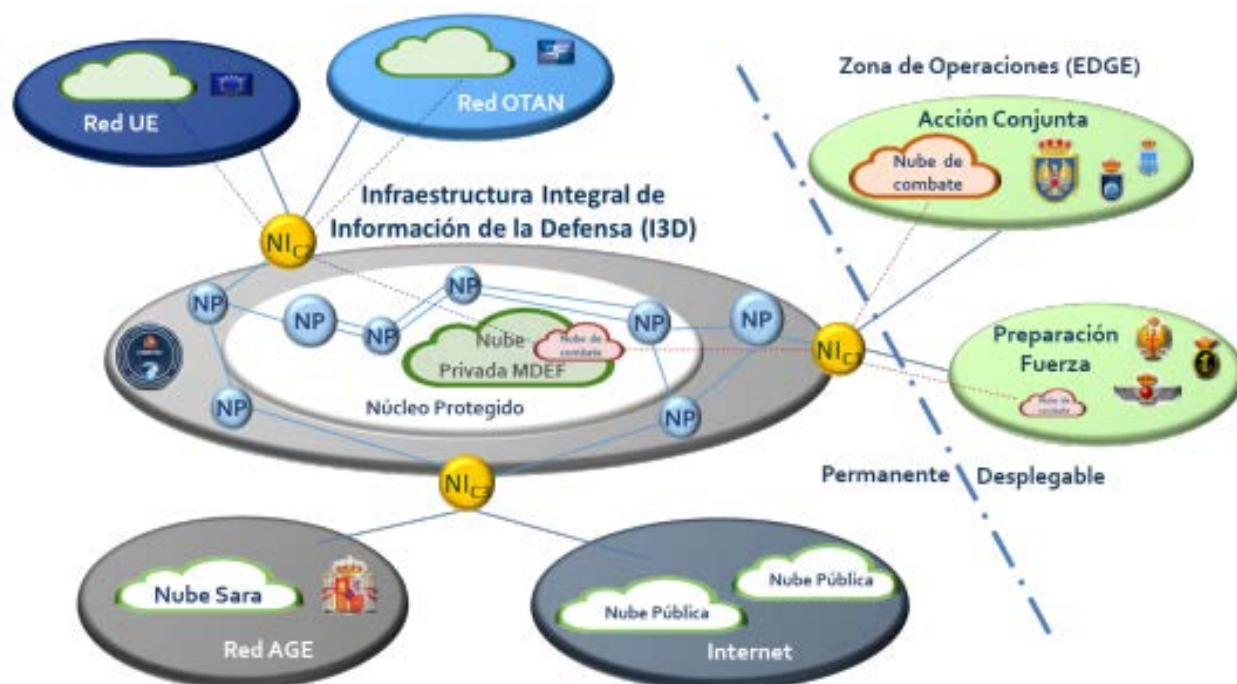


Figura 1-1 Ideograma de evolución de la I3D al modelo de nube (tomada de [1]).

1.2 Propósito

El propósito del presente trabajo es impulsar y evolucionar la I3D a un modelo de Nube, por medio del desarrollo de la Estrategia de Explotación de la Nube en el MDEF [1], y materializándolo sobre la base de marcos de referencia para la adopción de nube, buenas prácticas arquitectónicas orientadas a su construcción y explotación, y los propios recursos reales existentes en el MDEF.

1.3 Objetivos

Una vez establecido el propósito de este trabajo, es posible identificar una serie de Objetivos Parciales (OP) con el fin de permitir alcanzar dicho propósito:

- OP 1. Establecer las directrices técnicas para ofrecer una solución integral para el MDEF, basada en nube, dentro del marco fijado por el documento [1] y por la situación real de la infraestructura presente de la I3D a evolucionar.
- OP 2. Detallar los aspectos de diseño, arquitectura, operación y seguridad necesarios para desplegar un modelo de nube en el MDEF, tanto en su vertiente permanente como desplegable.
- OP 3. Identificar los principios básicos y criterios a seguir para llevar a cabo la migración de aquellos servicios y sistemas que pretendan hacer uso de recursos de nube del MDEF, como parte de la transición de la I3D a un modelo de nube.

1.4 Organización de la memoria

Con la finalidad de alcanzar los Objetivos Parciales anteriormente descritos, la organización por Capítulos (Cap) que se seguirá en el desarrollo del presente trabajo será la siguiente:

- Cap 1. Introducción, definición de la finalidad a alcanzar y organización por objetivos del presente trabajo.
- Cap 2. Exploración del entorno y la casuística específica del MDEF, en cuanto a normativa y características de los clientes y servicios a proporcionar, se refiere.
- Cap 3. Descripción detallada de la solución tecnológica propuesta, abordando la necesidad de establecer un modelo de nube capaz de ofrecer cobertura a los Dominios de Seguridad nacionales de Baja y Alta Clasificación.
- Cap 4. Ejercicio práctico correspondiente a un proceso de migración de servicios existentes en el MDEF, sobre la solución de nube planteada.
- Cap 5. Análisis de resultados, como consecuencia del trabajo realizado, identificando aquellos aspectos en los que se podría mejorar y ampliar la solución planteada.
- Cap 6. Compendio bibliográfico de las diferentes referencias sobre las que se ha apoyado el presente trabajo.

2 ESTADO DEL ARTE

2.1 Conceptos presentes en el MDEF

De cara a poder desarrollar de manera adecuada el presente trabajo, conviene describir la situación actual existente en el MDEF, respecto a diferentes aspectos organizativos y conceptuales que condicionan y deben guiar la consecución de los objetivos planteados:

2.1.1 *El CESTIC*

El CESTIC es el órgano directivo al que le corresponde la planificación, desarrollo, programación y gestión de las políticas relativas a los CIS/TIC, la transformación digital, la gestión de los datos, la información y el conocimiento y la seguridad de la información, así como la supervisión y dirección de su ejecución. Asimismo, le corresponde la provisión segura de los servicios de la I3D y de las actuaciones de ciberseguridad para la protección de esta infraestructura y de la información que procesa y gestiona.

También es responsable de la definición de la estrategia tecnológica sobre los CIS/TIC, la transformación digital y la seguridad de la información y en estas materias, en colaboración con la Dirección General de Armamento y Material (DGAM), del impulso de un modelo de innovación y del apoyo a la industria nacional de la Defensa para su participación en proyectos a nivel nacional e internacional [2].

Entre sus cometidos están el desarrollar e impulsar programas, proyectos y actuaciones para el despliegue de servicios digitales, capacidades e infraestructuras, que contribuyan a acelerar el proceso de transformación digital en el seno del MDEF.

Los roles otorgados al CESTIC en el marco del proceso de implantación de un modelo de nube, son, entre otros, los de:

- Gestor de Servicios basados en la nube: con el propósito de gestionar los servicios de producción propia o proporcionados por los proveedores externos, supervisando su comportamiento y evolución, en beneficio del MDEF.
- Proveedor de Servicios basados en la nube: con el objetivo de convertirse en el proveedor de servicios basados en la nube para el MDEF. Se significa que el CESTIC, de igual modo, puede comportarse como consumidor de servicios basados en la nube, respecto a un proveedor externo, para el cumplimiento de sus cometidos.

Consecuentemente CESTIC se constituye en una organización impulsora de la implantación de la nube, lo cual conduce a la evolución de una infraestructura tradicional, basada antiguos centros de

procesamiento de datos (CPD), hacia una infraestructura CIS/TIC, gestionada inteligentemente, basada en la nube. En dicha nube, la asignación de recursos es flexible, relativamente oculta y multi-ubicada, a diferencia de la infraestructura tradicional, donde los recursos están asignados de manera rígida.

2.1.2 La I3D

La I3D es una infraestructura tecnológica bajo la autoridad operativa única del Director del CESTIC que, mediante la convergencia de los sistemas de información y telecomunicaciones y los servicios que éstos proporcionan, debe ser capaz de optimizar el uso de los mismos y facilitar a los organismos y usuarios el acceso eficaz a los recursos de información de la Defensa, desde cualquiera que sea su situación geográfica y, en todo momento, de forma segura [2].

Se trata de una red privada de nivel estatal destinada a la provision de servicios específicos de Defensa y Seguridad Nacional y que, por tanto, debe contar con los más altos estándares de calidad, disponibilidad, redundancia, seguridad y resiliencia.

2.1.3 Los Ámbitos del MDEF

A efectos del presente trabajo, los Ámbitos con los que cuenta el MDEF son el Ejército de Tierra, la Armada, el Ejército del Aire y del Espacio, el Estado Mayor de la Defensa (EMAD), la Secretaría de Estado de Defensa (SEDEF), la Subsecretaría de Defensa (SUBDEF) y la Secretaría General de Política de Defensa (SEGENPOL). En un momento dado, por motivos de especificidad en el cumplimiento y desarrollo de sus misiones y cometidos, también podrían considerarse como Ámbitos separados la Unidad Militar de Emergencias (UME) y otros organismos autónomos pertenecientes al MDEF [3].

La importancia de identificar estos Ámbitos radica en el hecho de ser considerados como los clientes que van a beneficiarse de la implantación de un modelo de nube en el MDEF.

2.2 La Estrategia de Explotación de la Nube en el MDEF

Es el documento [1], que establece el marco estratégico para el desarrollo y aprovechamiento de la tecnología de nube como una capacidad propia de la I3D. Sobre el mismo debe pivotar la solución a proponer para poder alcanzar la implantación de un modelo de nube en el MDEF.

El documento destaca lo siguiente:

- El MDEF entiende la nube como una tecnología que puede explotarse en diferentes modalidades (privada, pública, híbrida), sin priorizar ninguna.
- Se aprecia la necesidad de realizar evaluaciones y establecer criterios que guíen la adopción de esta tecnología.
- Es preciso revisar las arquitecturas y fijar normas para su correcto gobierno y operación.
- Se debe crear un Grupo de Trabajo Permanente (GTP) para impulsar su implantación y empleo.

De la lectura del documento se puede extraer como consecuencia principal el hecho de que, debido al carácter transversal de esta tecnología, su adopción afecta a todos los ámbitos de la I3D: telecomunicaciones, infraestructuras, arquitecturas, aplicaciones, seguridad, operación, normativa, gobierno, inversiones, personal, etc. El mayor impacto es el concerniente al desarrollo, despliegue y puesta a disposición de servicios y aplicaciones, que constituye la utilidad más relevante de la nube.

En consecuencia, es preciso conseguir un alineamiento entre los actores, estrategias y estructuras de gobierno CIS/TIC afectadas, complementar la estrategia con una perspectiva de mayor detalle, y establecer un marco de actuación preciso para la misión del GTP. Dicho marco de actuación es el que se aspira a concretar de la mano de documentos como el presente trabajo, persiguiendo el hecho de “aterrizar” la estrategia en forma de una propuesta tecnológicamente viable.

Se sabe de antemano, en base a ejemplos comerciales, que la tecnología de nube proporciona capacidades constituidas por un conjunto de recursos, servicios y paradigmas tecnológicos, que pueden ser accedidos remotamente, aislando al consumidor de la infraestructura subyacente empleada por el proveedor. Sin embargo, la adopción de la nube en el MDEF no puede tratarse como un mero proceso de implantación tecnológica. Para maximizar los beneficios y reducir los riesgos de una posible migración a la nube, se requiere adoptar una perspectiva transformacional:

- Desplegando la capacidad de forma progresiva, y en armonía con la base tecnológica existente, o base legada, que tendrá que converger progresivamente hacia la nube.
- Evolucionando la arquitectura de las aplicaciones y facilitando la producción y consumo de servicios en nube.
- Actualizando los procesos de desarrollo y despliegue, para poder provechar las ventajas que ofrecen los paradigmas de explotación inherentes a la nube.
- Permitiendo la explotación autónoma, pero supervisada, de la capacidad por parte de los Ámbitos del MDEF.
- Armonizando, con sus particularidades, los procesos que intervienen en el ciclo de vida de los servicios.
- Avanzando hacia una gestión centralizada y global de la capacidad CIS/TIC de la I3D y sus inversiones correspondientes.
- Promoviendo una adecuada gestión del cambio, entre la comunidad CIS/TIC del MDEF, con especial foco en la formación del personal técnico.

2.3 Posibles modelos de nube

Los beneficios que puede proporcionar al MDEF la adopción de la nube, y las expectativas que éstos pueden generar, deben fundamentarse exclusivamente en el análisis riguroso de sus características y necesidades, alejándose de argumentos preconcebidos e interesados de los proveedores de servicios en nube.

En concreto, son especialmente discutibles los siguientes argumentos comerciales, de rabiosa actualidad, los cuales pueden llegar a tener un gran impacto en la misión del MDEF y en su realidad organizacional:

- *“La nube pública es más eficiente en costes que el modelo on-premise”.*
- *“La adopción de la nube pública implica una reducción sensible de los tiempos de despliegue de nuevos servicios”.*
- *“La nube pública permite reducir significativamente el personal dedicado a la operación de infraestructuras”.*
- *“La nube pública es más segura”.*

El MDEF debe mantenerse especialmente atento a aquellos organismos e instituciones que, por su grado de madurez en la adopción de la nube, ya disponen de lecciones aprendidas sobre sus ventajas e inconvenientes. Los que aún se encuentran en fase de adopción deben constituir únicamente una referencia informativa. Esta postura va a ser la que permita optar por el modelo de nube que mejor se adecúe a las necesidades del MDEF, siendo conscientes de que las soluciones adoptadas por otras entidades estatales pueden ser perfectamente válidas [4], pero no aptas para el propio MDEF.

En este sentido, la experiencia y pasos que se están dando respecto a la adopción de capacidades de nube pública por organismos como la OTAN [5], o el *US Army* [6], deben valorarse basándose en un estudio detallado del caso de uso, de modo que permitan determinar si su aplicación es trasladable al caso nacional del MDEF.

En línea con lo estipulado en el documento [1], se definen las siguientes tipologías principales como esquemas de partida para llevar a cabo la evolución de la I3D hacia un modelo basado en nube.

2.3.1 Nube Privada

Modelo que se implementa en las propias instalaciones del MDEF y que cuenta con un alto nivel de características de la nube, como alta automatización, escalabilidad y elasticidad. No obstante, dentro de lo que se puede considerar como entorno privado propio, se pueden establecer distintos modos de despliegue. Los despliegues que se contemplan en nube privada son los siguientes:

- Nube Privada Interna (*Internal Private Cloud*), constituye el concepto de nube privada más tradicional, empleando equipamiento de la propia organización en propiedad o alquiler.
- Nube Privada Virtual (*Virtual Private Cloud - VPC*), hace referencia a un conjunto de recursos computacionales, que pueden ser ajustados bajo demanda, y pertenecen a un proveedor externo. Una nube privada virtual ofrece la posibilidad de utilizar las ventajas de una red virtualizada, al mismo tiempo que aprovecha las ventajas de una nube, como el autoservicio, la escalabilidad y la elasticidad.

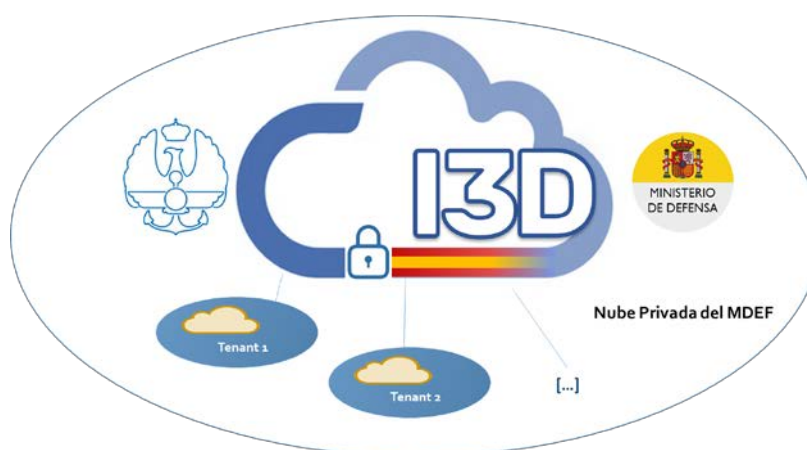


Figura 2-1 Esquema de Nube Privada del MDEF (tomada de [1]).

2.3.2 Nube Pública

Modelo en el que los recursos son propiedad de entidades ajenas al MDEF, fundamentalmente proveedores de dimensión global, que proporcionan sus servicios a través de Internet. Para que el MDEF pueda utilizar estos servicios dichos proveedores deben contar, según se define en [1], con la certificación de conformidad con el Esquema Nacional de Seguridad [7] de categoría Alta.

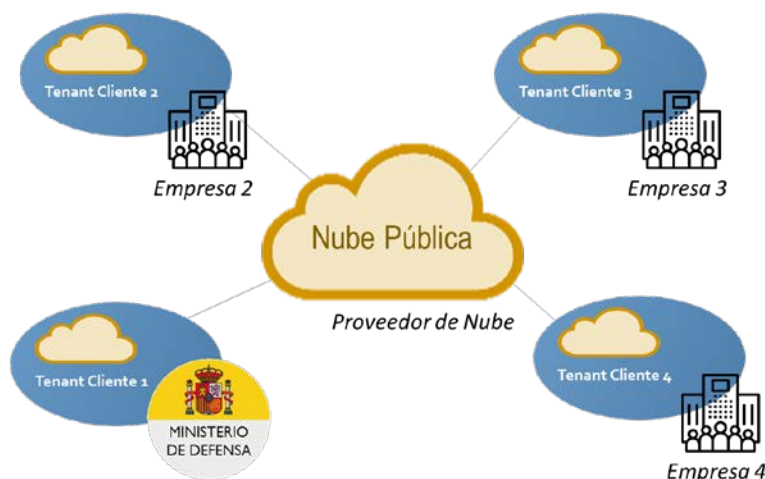


Figura 2-2 Esquema de Nube Pública del MDEF (tomada de [1]).

2.3.3 Nube Híbrida

Modelo que utiliza una combinación de servicios de nube pública y de nube privada, orquestado entre ambas plataformas. De este modo, aquellos servicios cuyos requisitos lo permitan, pueden desplegarse en una nube pública, mientras que aquellos otros considerados críticos o que manejen información sensible serán alojados en una nube privada. Al igual que en el caso anterior, para que el MDEF utilice estos servicios los proveedores deben contar, según se define en [1], con la certificación de conformidad con el Esquema Nacional de Seguridad [7] de categoría Alta.

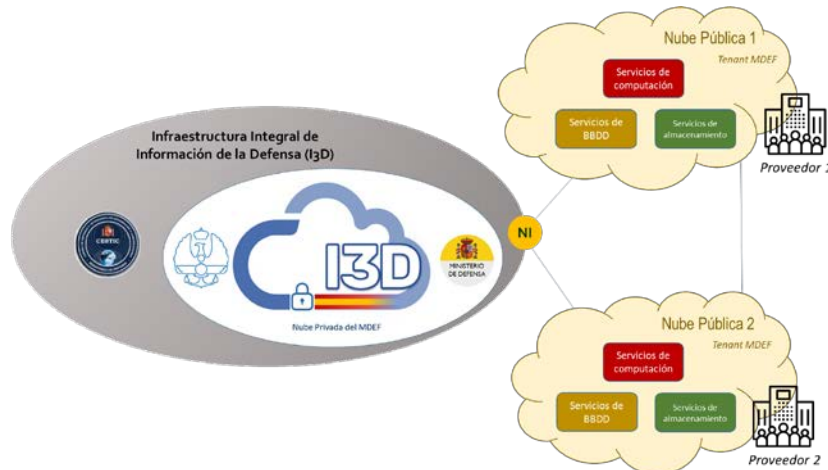


Figura 2-3 Esquema de Nube Híbrida del MDEF (tomada de [1]).

2.4 Aspectos de seguridad en el MDEF

Tal y como se viene anticipando, el factor seguridad resulta crucial para el MDEF a la hora de determinar el modelo y la solución tecnológica adoptar para la implantación de un modelo de nube. Por ello, resulta procedente exponer de forma somera aquellos conceptos y normativas de seguridad, que van a actuar como condicionantes a tener en cuenta en el desarrollo del presente trabajo.

2.4.1 El Esquema Nacional de Seguridad

La normativa que regula el Esquema Nacional de Seguridad [7], determina al mismo como un sistema de protección de las redes y sistemas de información de las administraciones públicas españolas, entre las que se incluiría la I3D, así como de las infraestructuras críticas. El objetivo del Esquema Nacional de Seguridad es garantizar la seguridad de las redes y sistemas de información, y promover la cooperación entre las diferentes entidades que forman parte de este.

Está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos, que se gestionen en el ejercicio de sus competencias.

Establece las obligaciones y responsabilidades de las entidades que forman parte del Esquema Nacional de Seguridad, así como las medidas y procedimientos necesarios para garantizar la seguridad de las redes y sistemas de información. También establece las normas para la detección y gestión de incidentes de seguridad, y para la notificación de estos incidentes a las autoridades competentes.

La normativa de la referencia [7] actualiza y sustituye al anterior Real Decreto 3/2010, por el que se regulaba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, basándose en la directiva de seguridad de las redes y sistemas de información de la Unión Europea (UE), y en la normativa española sobre seguridad de las TIC. Asimismo, se enmarca en el contexto actual de amenazas cibernéticas, cada vez más complejas y sofisticadas, que ponen en riesgo la seguridad de las redes y sistemas de información en España.

La evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

2.4.2 La Baja y la Alta Clasificación

La normativa relativa a clasificación de la información existente en el MDEF [8] establece que la información puede discriminarse en dos categorías:

- Información No Clasificada: se divide, a su vez, en dos subcategorías según su “ámbito de distribución” y también es conocida por información “calificada”:
 - Información de Uso Público.
 - Información de Uso Oficial.
- Información Clasificada: se divide, a su vez, en varios “grados de clasificación”:
 - Difusión Limitada.
 - Confidencial.
 - Reservado.
 - Secreto.

Por otro lado y, en cuanto a la infraestructura utilizada para gestionar la información, ésta también puede discriminarse según el tipo y grado de clasificación de la información que maneja:

- Infraestructuras para Baja Clasificación: estas infraestructuras están acreditadas según el Esquema Nacional de Seguridad y están destinadas a gestionar:
 - Información No Clasificada: tanto información de Uso Público como de Uso Oficial.
 - Información Clasificada: únicamente en el grado de Difusión Limitada, o sus equivalentes extranjeros.
- Infraestructuras para Alta Clasificación: estas infraestructuras están acreditadas según el Esquema Nacional de Seguridad, junto con la normativa especial aplicable, y están destinadas a gestionar información clasificada hasta el grado Reservado, o sus equivalentes extranjeros.

2.4.3 Los Dominios de Seguridad

Los Dominios de Seguridad son segmentaciones de las infraestructuras CIS/TIC de la I3D, realizadas según la clasificación de seguridad de la información que gestionan. Los Dominios de Seguridad establecidos en la I3D son los siguientes:

- DS0: Dominio de Seguridad No Clasificado.
- DS1: Dominio de Seguridad Reservado Nacional.
- DS2: Dominio de Seguridad *NATO Secret*, correspondiente a OTAN.
- DS3: Dominio de Seguridad *EU Secret*, correspondiente a UE.

Los Dominios de Seguridad en la I3D quedan agrupados en:

- Dominios de Baja Clasificación de la I3D (I3D-BC), que agrupan las infraestructuras para Baja Clasificación: DS0.
- Dominios de Alta Clasificación de la I3D (I3D-AC), que agrupan las infraestructuras para Alta Clasificación: DS1, DS2 y DS3.

El Dominio de Seguridad DS0 incluye la información de Uso Público y de Uso Oficial. También puede incorporar una discriminación temática condicionada por la infraestructura tradicional que se denomina “dominio de uso”. Los dominios de uso existentes son:

- USOP: Uso Público.
- USOF: Uso Oficial.
- WAN PG: Red de Propósito General (antiguo).

En cuanto a los Dominios de Seguridad DS1, DS2 y DS3, el único sobre el cual se van a poder tomar decisiones concernientes a diseño, arquitectura y operación, por motivos de soberanía va a ser el DS1 por el hecho de ser un Dominio de Seguridad para empleo exclusivamente nacional. En los casos concernientes al DS2 y DS3, las respectivas autoridades de OTAN y UE serán las que determinen las decisiones a adoptar, siendo el MDEF un consumidor de servicios, o cliente si se prefiere, a imagen y semejanza de los Ámbitos en el caso nacional.

En resumen, y derivado de los motivos expuestos, la propuesta de solución a desarrollar en el presente trabajo va a versar sobre la implantación de un modelo de nube para el MDEF que cubra las necesidades nacionales, es decir:

- Baja Clasificación en su totalidad, habida cuenta de que el escenario final debe ser el de poder gestionar información de Uso Público, Uso Oficial y Difusión Limitada. Corresponderá al DS0.
- Alta Clasificación en su vertiente nacional, habida cuenta de que el escenario final debe ser el de poder manejar de información clasificada nacional hasta el grado de Reservado. Corresponderá al DS1.

Para el manejo de información perteneciente a OTAN y UE quedarán emplazados, respectivamente, los DS2 y DS3, cuyo desarrollo correrá a cargo de las propias organizaciones pertinentes.

3 DESARROLLO DEL TFM

3.1 Diseño de la Nube MDEF

3.1.1 Aspectos generales

La implantación de un modelo de nube en el MDEF, en adelante la Nube MDEF, se articulará en una red de servidores y aplicaciones con capacidad para prestar servicios propios de la I3D de forma descentralizada. Los servicios mencionados deberán poder ser accedidos desde ubicaciones previstas por el MDEF, incluyendo su Ámbitos, mediante capacidades de la infraestructura de telecomunicaciones proporcionada por la I3D.

Esta red de servidores, inicialmente implantada en diferentes emplazamientos físicos del MDEF, sobre dos CPD independientes, se ha visto superada por el concepto actual de aprovisionamiento de servicios basados en la nube, que podemos encontrar habitualmente como servicio comercial. Además, han surgido otras necesidades, como la de disponer de una computación más extendida con pequeños CPD adicionales a los dos principales, con capacidades especializadas más cercanas a los destinatarios de esta demanda, situados en bases y buques militares, que serán tratados como una parte más de la arquitectura, dentro de las capas *Fog* y *Edge Computing*, que se desarrollarán en el presente trabajo.

En conclusión, el documento de Arquitectura Global CIS/TIC [9], efectivamente, describe un despliegue de infraestructuras de información en dos CPD, pero simplemente para establecer una redundancia de servicios, y no una provisión de éstos mediante un modelo de nube propiamente dicho.

Evolucionando lo anterior, la Nube MDEF se considerará al conjunto de capacidades siguientes:

- Nube Privada: servicios desplegados por CESTIC en una infraestructura propietaria de nube, para uso propio interno o para los Ámbitos destinatarios de la demanda. Ofrecerá características similares a la nube pública, pero con un nivel de control y seguridad superior y auditable.
- Nube Pública: servicios desplegados sobre infraestructura pública de nube, perteneciente a proveedores comerciales, pudiendo ser una solución multi-proveedor, pero contando siempre con la certificación de conformidad con el Esquema Nacional de Seguridad de categoría Alta.
- Nube Híbrida: compuesta por el conjunto de nube privada y nube pública.
- Nubes de Terceros: servicios desplegados sobre nubes de otras organizaciones no comerciales pertenecientes a la Administración General del Estado (AGE), de modo que CESTIC pueda ser capaz de interactuar con dichos servicios desplegados por terceros (ej: AGE con Nube SARA).

La Nube MDEF pretende tratar a la infraestructura CIS/TIC, explotada por los diversos Ámbitos, como un bien compartido accesible y accedido a través de un conjunto de servicios discriminados de acuerdo a los diversos Dominios de Seguridad existentes.

Los modelos de provisión de nube, que esencialmente establecen el uso de recursos exclusivamente propios (nube privada), exclusivamente ajenos (nube pública) o combinados (nube híbrida), quedarán condicionados por los Ámbitos a los que sirven (destinatarios), la naturaleza de los servicios prestados de acuerdo con su Catálogo de Servicios, y el Dominio de Seguridad donde la información ha de ser manipulada en función del nivel de clasificación.

En el caso del dominio DS0 se pretende disponer de una nube híbrida en la que se ponga a disposición de los Ámbitos, sistemas de información, o servicios específicos, así como los esenciales requeridos para el soporte de los primeros, conformando un Catálogo de Servicios estandarizado. Tales servicios catalogados serán prestados en diversas modalidades que se agruparán en Infraestructura como Servicio (*IaaS*), Plataforma como Servicio (*PaaS*) y *Software* como Servicio (*SaaS*).

En el caso del dominio DS1 se contempla un escenario similar al anterior, pero en el que, por restricciones relativas a seguridad, la prestación de los servicios se lleve a cabo única y exclusivamente desde una nube privada, la cual surgiría evolucionando la infraestructura actual.

En cuanto al despliegue de servicios, el mismo estará sometido al principio de Preferencia en Nube (*Cloud First*)¹, recogido en el documento de la referencia [1], migrándose los existentes cuando sea posible e incorporándose los nuevos al paradigma de nube, por presuponerse que su arquitectura va a estar preparada para ello.

Por último, y con objeto de abordar el diseño de la Nube MDEF de forma realista, no debe perderse de vista el aspecto de la infraestructura legada, entendida como aquella que se ubica en CPD propiedad del CESTIC y que se encuentra actualmente en producción proporcionando servicios. Dicha infraestructura debe ser objeto de evolución a una infraestructura propietaria de nube, constituyendo la nube privada.

3.1.2 Capas de computación en la nube: *Fog* y *Edge Computing*

Dentro de los múltiples casos de uso de la Nube MDEF, deben contemplarse supuestos de empleo que requieran capacidades especializadas más cercanas a los destinatarios finales de los servicios. De esta manera se da cobertura a la necesidad recogida en el documento de la referencia [1], en el cual se distingue entre un tipo de trabajo basado en ubicaciones “permanentes” en contraposición a un segundo tipo de trabajo sujeto a ubicaciones “desplegables”.

Por este motivo, además del *Core* (núcleo) de este diseño basado en la nube, hay que considerar dentro del alcance del propio diseño las capas de *Fog* y *Edge Computing* (computación intermedia y en el extremo).

Este hecho se debe a razones operativas, derivadas de las propias misiones y cometidos de los Ámbitos, las cuales pueden requerir una disponibilidad y una sensibilidad a la latencia, que hagan necesario acercar los datos a la ubicación de explotación.

Fog y *Edge Computing* se conciben como muy similares y próximos, si bien su principal diferencia reside en la forma en que manejan los datos cerca de esa ubicación de explotación.

¹ Preferencia en Nube (*Cloud First*): al igual que otros organismos como la OTAN, debe impulsarse la aproximación en la que prime la provisión de servicios CIS/TIC mediante tecnologías de nube respecto al modelo tradicional de servicios CIS/TIC, aprovechando los beneficios que ésta aporta.

Esta aproximación no indica que todos los servicios deban siempre ser provistos mediante tecnología de nube; se precisa una evaluación de los requisitos de los servicios, basada en criterios técnicos, para decidir la idoneidad de una tecnología u otra. Adicionalmente, y en línea con lo marcado en el ámbito de aplicación de la estrategia [1], también se tendrán en cuenta aspectos como su potencial beneficio y utilidad para las operaciones militares.

Como consecuencia de la introducción estos conceptos en el presente trabajo, a continuación, se realiza una breve descripción de ambos:

Edge Computing o Computación en el Extremo:

- Ubicación: el procesamiento de datos se realiza en el borde de la red, cerca de los dispositivos o sensores que generan y consumen estos datos.
- Propósito: diseñado para tareas de procesamiento sencillas y en tiempo real.
- Ejemplo: una plataforma con sensores que monitorizan diferentes aspectos de la misma. El *Edge Computing* realiza el procesamiento en el mismo lugar donde se generan y consumen los datos.
- Ventajas:
 - Latencia reducida: al procesar datos localmente, se evita la demora de envío a la nube.
 - Menor carga en la red: sólo se envían los datos relevantes a la nube.
- Desventajas:
 - Capacidad limitada: la capacidad de cómputo en el borde es menor que en la nube.
 - Escalabilidad: puede presentar limitaciones para grandes volúmenes de datos.

Fog Computing o Computación Intermedia:

- Ubicación: el procesamiento se realiza sobre infraestructura de cómputo cercana a las fuentes de datos, como pequeños nodos, que albergan redes de usuario o centros de datos.
- Propósito: utilizado para operaciones más complejas o grupos de datos que requieren algoritmos sofisticados.
- Ejemplo: en una plataforma inteligente, los sensores, cámaras de vigilancia y otros dispositivos generan datos constantemente. El *Fog Computing* permite fusionar y procesar estos datos cerca de su origen.
- Ventajas:
 - Mayor capacidad de cómputo: permite realizar tareas más complejas.
 - Menor congestión de red: reduce la carga en la red principal.
- Desventajas:
 - Mayor coste: requiere infraestructura adicional a la de los dispositivos y sensores.
 - Mayor complejidad: configurar y administrar múltiples nodos implica una carga de complejidad adicional.

En resumen, el *Edge Computing* pone el énfasis en el procesamiento local y rápido, mientras que el *Fog Computing* amplía esta idea situando recursos de computación en una ubicación intermedia entre la nube y el extremo final, de cara a abordar operaciones más complejas y descentralizadas.

Esta aproximación se alinea con el concepto de OTAN denominado Nube de Combate (*Combat Cloud*) [10], cuya aplicación es preceptiva por motivos de interoperabilidad, para todos aquellos países que como España son miembros de la Alianza.

3.1.3 Situación final deseada

A la vista de los conceptos y condicionantes presentados, se concluye que la situación final deseada es un escenario compuesto que combine las capacidades y las bondades que proporciona una solución de nube híbrida, pudiéndose determinar en función de una serie de criterios establecidos el mejor de los entornos, público o privado, que sea óptimo para cada uno de los servicios.

Para alcanzar esta situación final debe abordarse un proceso de transición, articulado en las siguientes fases:

- Fase 1: migración de los CPD existentes a una nueva infraestructura virtualizada, como solución de nube privada, que pueda tener extensión de forma ágil y sencilla hacia los diferentes proveedores de nube, por medio de una plataforma de movilidad de cargas de trabajo.
- Fase 2: establecimiento de una *Golden Copy*², tanto para los Dominios de Seguridad DS0 como DS1, en nubes de otras organizaciones pertenecientes a la AGE y sin fines comerciales (Nubes de Terceros). Las copias de seguridad se realizarían sobre una infraestructura ubicada a no menos de 300 km de la región en la que se ubican los CPD.
- Fase 3: determinación de los posibles proveedores comerciales de nube pública, susceptibles de ser contratados para alojar cargas de trabajo, pertenecientes exclusivamente al Dominio de Seguridad DS0.
- Fase 4: valoración de los servicios susceptibles de ser migrados a nube, en base a una serie de criterios claramente definidos y vinculados a aspectos tales como beneficio, valor, complejidad y riesgo.

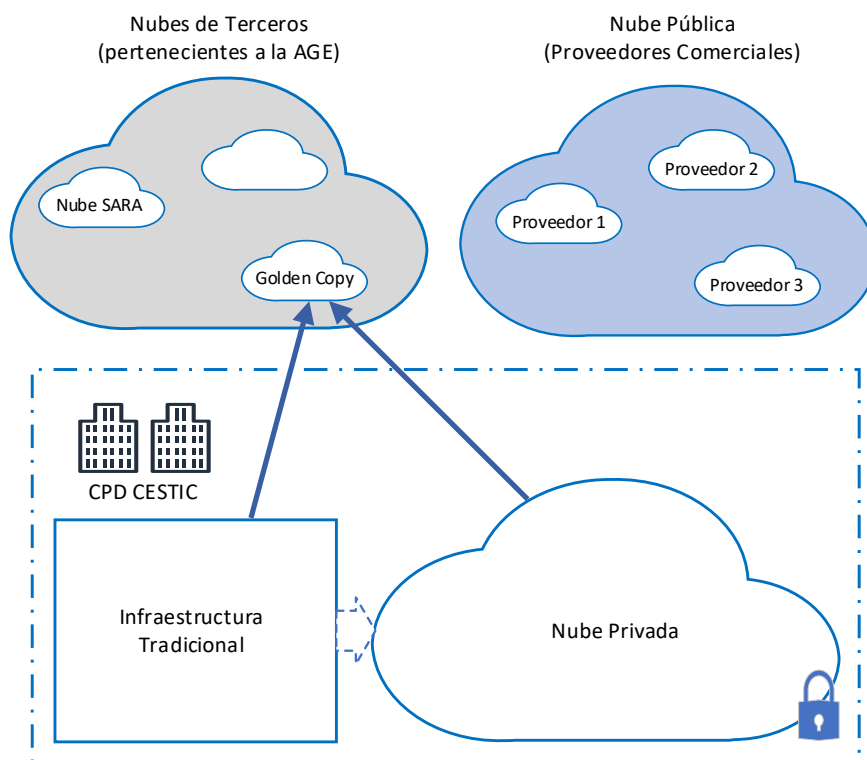


Figura 3-1 Representación de la transición a la Nube MDEF (elaboración propia).

Es preciso mencionar que, con anterioridad a este proceso de transición del entorno tradicional al de nube, ya existen casos en el MDEF de servicios que se encuentran en nube pública, migrados a esta por motivos puntuales, pero no alineados con el modelo de nube híbrida que se propone en el presente trabajo. Se tratan, fundamentalmente, de servicios relativos a entornos y plataformas de enseñanza.

El esquema anterior se completaría mediante las capas de computación de *Fog y Edge Computing*, que representarían la Nube de Combate, la cual desde un punto de vista operativo obedecería a propósitos mucho más tácticos, materializando la extensión de la Nube MDEF a Zonas de Operaciones en el exterior y Fuerza en preparación.

² *Golden Copy*: copia íntegra e inmutable de los datos críticos del MDEF para garantizar el nivel mínimo de funcionamiento y la rápida reanudación de los servicios críticos en caso de un desastre. Esta copia íntegra e inmutable complementaría a las copias de seguridad, y procedimientos ya existentes, ejecutados de manera local.

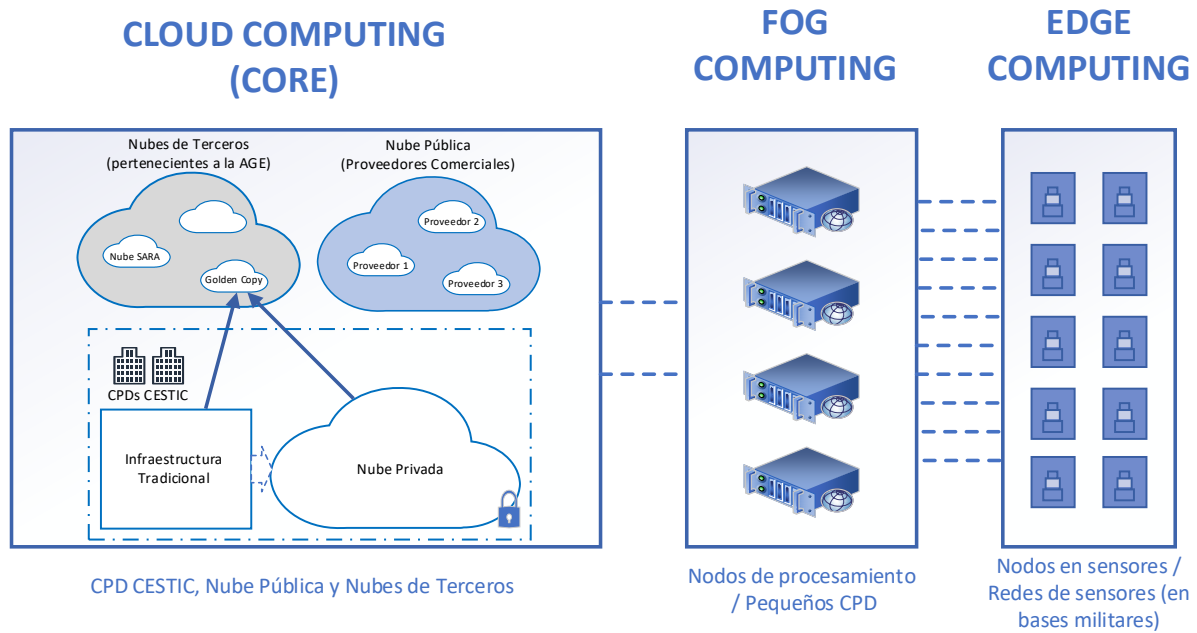


Figura 3-2 Capas de computación: *Cloud Computing (Core), Fog y Edge Computing* (elaboración propia).

3.2 Arquitectura de la Nube MDEF

3.2.1 Marco de referencia

Como punto de partida para asentar la Arquitectura de la Nube MDEF se van a considerar aquellos marcos de referencia para la adopción de nube, y buenas prácticas arquitectónicas orientadas a su construcción y explotación, creados para arquitectos, desarrolladores y propietarios de soluciones, con el fin de mejorar la calidad y seguridad de sus cargas de trabajo. En dichos documentos se contemplan una serie de aspectos que componen los pilares fundamentales sobre los que esta arquitectura debe descansar, y que son los siguientes:

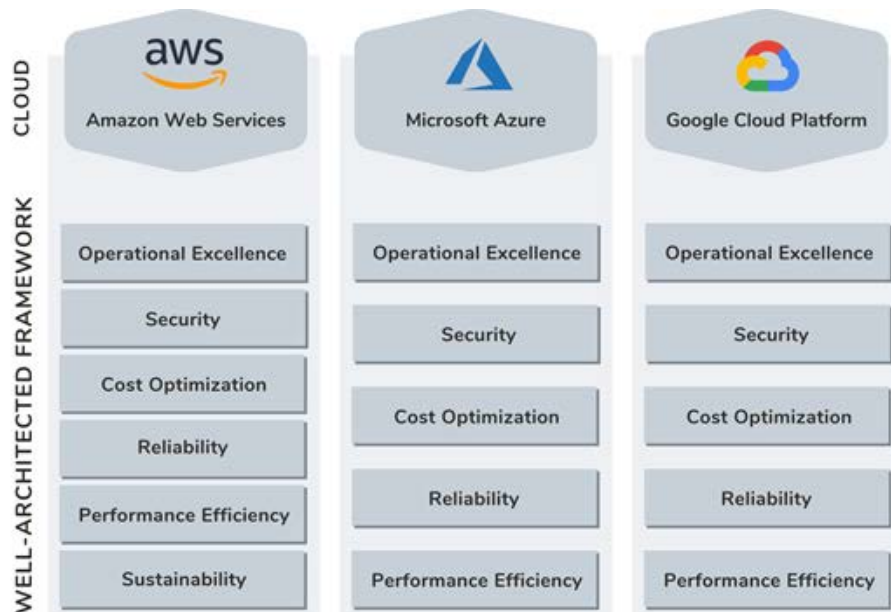


Figura 3-3 Buenas prácticas arquitectónicas de los principales proveedores de nube (tomada de [11]).

En una primera aproximación puede apreciarse que dichos pilares básicos son muy similares, cuando no iguales, entre los principales proveedores comerciales de nube pública. Por este motivo, para la realización del presente trabajo, se va a optar por considerar únicamente uno de ellos de forma consistente, a la hora de sustentar la arquitectura de la Nube MDEF.

En particular, se va a tomar como referencia principal el estándar de *Microsoft Azure Well-Architected Framework* [12] por el hecho de existir un “Protocolo general de actuación entre el Ministerio de Defensa y *Microsoft Ibérica S.R.L.*”, vigente desde junio de 2024, motivo por el cual se presupone que la colaboración entre ambas partes puede mantenerse activa a corto y medio plazo.

3.2.2 Pilares de la Arquitectura

Partiendo, por tanto, del documento de la referencia [12], se definen 5 pilares conectados, tal y como se muestran en la figura siguiente, y que se detallan a continuación. Dichos pilares deben impregnar la Arquitectura a adoptar para la Nube MDEF, y tenerse presentes en todo momento:



Figura 3-4 Pilares de la arquitectura de la Nube MDEF (tomada de [12]).

- *Cost Optimization* u Optimización de Costes:

Objetivo: acelerar el tiempo de aprovisionamiento de los servicios evitando soluciones complejas de elevado coste.

La observancia de este principio permite establecer una presupuestación de los distintos servicios que proporcionan los diferentes proveedores de nube pública, pudiéndose hacer estimaciones de costes a futuro con herramientas de cálculo de precios y de coste real de la propiedad.

Además, una vez ya desplegados los servicios en nube pública, se dispone de mecanismos y herramientas que permiten la optimización de los recursos utilizados para estos servicios (*FinOps*)³, y el escalado tanto vertical, ampliando los recursos necesarios, como horizontal, ampliando el número de servicios.

³ *FinOps*: disciplina que combina principios de administración financiera con ingeniería y operaciones en la nube para proporcionar a las organizaciones una mejor comprensión de su gasto en la nube. También les ayuda a tomar decisiones fundamentadas sobre cómo asignar y administrar sus costes de nube. El objetivo de *FinOps* no es ahorrar dinero, sino maximizar los ingresos o el valor empresarial a través de la nube. De este modo contribuye a controlar el gasto en la nube al tiempo que mantienen el nivel de rendimiento, fiabilidad y seguridad necesario, para respaldar las operaciones de una organización.

- *Security* o Seguridad.

Objetivo: proteger, detectar y responder a las amenazas en todo el entorno de nube pública, por medio de la creación de cargas de trabajo que utilicen principios de seguridad basados en el marco de Confianza Cero (*Zero Trust*)⁴.

Por norma general, los proveedores comerciales de nube habilitan diferentes servicios que contribuyen de por sí a alcanzar el propósito de este pilar, tales como administración continua, protección de las cargas de trabajo e identificación y mitigación de las amenazas sobre dichas cargas de trabajo.

Sin embargo, en lo que respecta a las cargas de trabajo depositadas en nube pública, la protección y segmentación de las aplicaciones para aplicar configuraciones de seguridad, son responsabilidades no delegables en el proveedor comercial de nube.

- *Reliability* o Fiabilidad.

Objetivo: dotar de resiliencia a las aplicaciones mediante respuesta ante fallos, ofreciendo una alta fiabilidad.

Para mejorar la fiabilidad se hará uso de una adecuada configuración de zonas de disponibilidad, complementando la misma con la realización de pruebas periódicas que permitan validar umbrales, objetivos y supuestos críticos, además de pruebas de carga para comprobar la escalabilidad y el rendimiento bajo carga.

Es preciso contar con arquitecturas de aplicaciones resilientes en las que los objetivos de confiabilidad estén correcta y precisamente definidos, para recuperarse adecuadamente de posibles fallos.

Por norma general, los proveedores comerciales de nube disponen de cuadros de mando capaces de ofrecer una vista consolidada de los datos y métricas, así como del estado de los servicios.

- *Operational Excellence* o Excelencia Operacional.

Objetivo: desplegar un entorno de aplicación sostenible, con objeto de poder crear y mantener cargas de trabajo, fácilmente automatizables y monitorizables.

Se utilizará metodología *DevOps*⁵, para crear y probar cargas de trabajo tanto en la fase de desarrollo como en la de producción, para conseguir la homogeneización y alineamiento entre el desarrollo y las operaciones. Con carácter general, será posible aprovechar flujos ya definidos por los diferentes proveedores comerciales de nube.

- *Performance Efficiency* o Eficiencia en el Rendimiento.

Objetivo: ayudar a diseñar y administrar cargas de trabajo que se puedan escalar, vertical u horizontalmente, de acuerdo con los cambios de carga, diseñando sistemas eficientes, y optimizando los recursos.

⁴ Confianza Cero (*Zero Trust*): marco de seguridad que supone que hay incumplimientos y comprueba cada solicitud como si la seguridad ya estuviese comprometida. Independientemente del origen de la solicitud o de los recursos a los que se acceda, la Confianza Cero implica desconfiar y comprobar siempre.

⁵ *DevOps*: combinación de los términos ingleses *development* (desarrollo) y *operations* (operaciones), con objeto de designar la unión de personas, procesos y tecnología para ofrecer valor a los clientes de forma constante. Permite que los roles que antes estaban aislados (desarrollo, operaciones, ingeniería de la calidad y seguridad) se coordinen y colaboren para producir productos mejores y más confiables. Al adoptar una cultura de *DevOps*, junto con sus prácticas y herramientas correspondientes, los equipos adquieren la capacidad de responder mejor a las necesidades de los clientes, aumentar la confianza en las aplicaciones que crean, y alcanzar los objetivos de la organización en menos tiempo.

Considerando cada servicio como un conjunto, junto con sus aplicativos de soporte y la latencia entre capas, se va a conseguir asegurar que todos los servicios puedan escalar para admitir cargas y que ningún componente del mismo constituya un cuello de botella.

A partir de la monitorización de los servicios, y de sus registros, se van a poder identificar tendencias, analizar patrones y proporcionar información diversa para adoptar criterios. Los registros también se podrán aprovechar para comprender mejor el rendimiento del servicio y cómo se utiliza. Además, con una adecuada monitorización se podrán supervisar los datos, incluidas las solicitudes, las respuestas, las tasas de error, las excepciones y el rendimiento de la carga.

3.2.3 Arquitectura de la Nube Privada

Tal y como se ha comentado, en relación con el documento de Arquitectura Global CIS/TIC [9], se dispone de una infraestructura legada ubicada en dos CPD ejerciendo roles de principal y alternativo, sin ningún tipo de orientación a la provisión de servicios basándose en un modelo en nube.

El objetivo es, partiendo de esa infraestructura disponible en el MDEF, cambiar este enfoque y establecer una configuración que permita implementar una solución realista y adecuada en términos de fiabilidad, rendimiento y coste. Para ello, tomando como referencia el estándar de *Microsoft Azure Well-Architected Framework* [12], en su aspecto de recomendaciones para el uso de zonas de disponibilidad y regiones [13], se considera para el caso planteado establecer una solución Activo-Activo entre ambos CPD que asegure la operatividad deseada.

En dicha referencia se definen las zonas de disponibilidad como grupos separados de CPD, o un único CPD independiente, dentro de una región. Las zonas de disponibilidad se encuentran lo suficientemente cerca como para tener conexiones de baja latencia con otras zonas de disponibilidad, estando conectadas por una red de alto rendimiento con una latencia de ida y vuelta de menos de 2 ms.

Sin embargo, las zonas de disponibilidad también deben estar lo suficientemente separadas para reducir la probabilidad de que más de una se vea afectada de manera simultánea por interrupciones locales o climatológicas. De igual modo, las zonas de disponibilidad deben contar con una infraestructura de suministro eléctrico, de refrigeración y de red independientes. Están diseñadas de forma en que, cuando una zona experimente alguna interrupción, las zonas restantes puedan seguir ofreciendo servicios regionales, capacidad y alta disponibilidad.

En el diagrama siguiente, a modo de ejemplo, se muestran varias regiones de *Microsoft Azure*. En el mismo se aprecia que una misma región puede contar con más de una zona de disponibilidad (regiones 1 y 2), y estas a su vez tener uno o más CPD.



Figura 3-5 Esquema de regiones, zonas de disponibilidad y CPD (tomada de [13]).

Para el caso específico del MDEF, se va a contar con una única región en la que existirán dos zonas de disponibilidad cada una de las cuales tendrá un único CPD.

El nivel de aplicación se distribuye entre ambas zonas de disponibilidad, contándose con la figura de un equilibrador de carga, capaz de dispersar las solicitudes en todas las instancias de cada zona de disponibilidad. Si una de las zonas de disponibilidad experimenta una interrupción, el equilibrador de carga va a dirigir el tráfico a las instancias de la otra.

El nivel de almacenamiento también se distribuye entre ambas zonas de disponibilidad, de modo que las copias de los datos de la aplicación se efectúen por medio de réplica síncrona. Cuando el nivel de aplicación realiza un cambio en los datos, el servicio de almacenamiento escribe el cambio en ambas zonas de disponibilidad y la transacción sólo se considera completa cuando se completan todos estos cambios. Este proceso garantiza que cada zona de disponibilidad siempre tenga una copia actualizada de los datos. Si una zona de disponibilidad experimenta una interrupción, se puede usar la otra zona de disponibilidad para acceder a los mismos datos.

Este enfoque con redundancia de zona aumenta la resistencia ante problemas como interrupciones en alguno de los CPD, sin embargo, dado que los datos se replican de forma síncrona, la aplicación tiene que esperar a que los datos se escriban en los distintos CPD de ambas zonas de disponibilidad.

Para la mayoría de las aplicaciones, la latencia introducida en la comunicación entre zonas es insignificante. No obstante, para algunas cargas de trabajo muy sensibles a la latencia, la réplica síncrona entre zonas de disponibilidad puede llegar a afectar al rendimiento de esas aplicaciones.

Particularmente, para el caso del MDEF, esta circunstancia se ve solventada por el hecho de contar con ambos CPD en diferentes partes de una misma área metropolitana, estando separados por una distancia inferior a los 100 km. La capacidad de comunicaciones entre ambas zonas de disponibilidad, o por añadidura entre ambos CPD, se basa en transmisión mediante fibra óptica y tecnología *DWDM*⁶, permitiendo garantizar una latencia adecuada para no afectar al rendimiento.

Ambos CPD se establecerían, por tanto, en una configuración con redundancia Activo-Activo, mediante réplica síncrona, conformando una region con dos zonas de disponibilidad. La representación de esta implementación con redundancia, junto con los criterios de valoración más destacados para su adopción, son los siguientes:

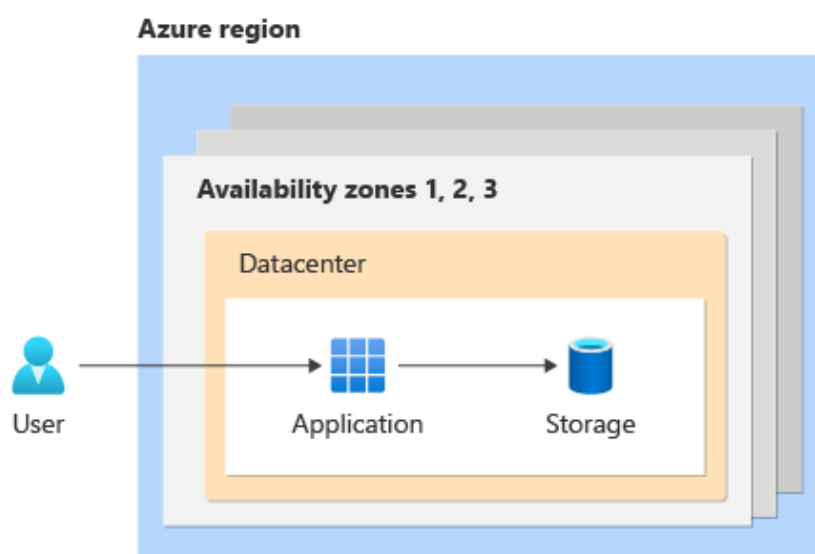


Figura 3-6 Implementación con Redundancia (tomada de [13]).

⁶ *DWDM (Dense Wavelength Division Multiplexing)*: técnica de transmisión en la que varias señales portadoras se transmiten por una única fibra óptica utilizando distintas longitudes de onda de un haz láser para cada una de ellas.

Fundamento	Impacto
Confiabilidad	Alta confiabilidad. Los servicios son resistentes a una interrupción de un centro de datos o una zona de disponibilidad. Los datos se replican sincrónicamente entre zonas de disponibilidad y sin retraso.
Optimización de costos	Costo moderado. En función de los servicios que use, puede incurrir en algunos costos de niveles de servicio más altos para habilitar la redundancia de zona.
Eficiencia del rendimiento	<i>Para la mayoría de las cargas de trabajo: rendimiento aceptable.</i> Es probable que este enfoque proporcione un rendimiento satisfactorio. <i>Para cargas de trabajo muy sensibles a la latencia: bajo rendimiento.</i> Algunos componentes pueden ser sensibles a la latencia debido al tráfico entre zonas o al tiempo de replicación de datos.
Excelencia operativa	Alta eficiencia operativa. Normalmente, solo debe administrar una sola instancia lógica de cada recurso. Para la mayoría de los servicios, durante una interrupción de zona de disponibilidad, la conmutación por error es responsabilidad de Microsoft y se produce automáticamente.

Figura 3-7 Valoración de una Implementación con Redundancia (tomada de [13]).

La valoración general, expresada en [13], por *Microsoft* para esta implementación es la siguiente:

“Para muchas cargas de trabajo de producción, una implementación con redundancia de zona proporciona el mejor equilibrio entre las ventajas y desventajas. Puede ampliar este enfoque con la copia de seguridad de datos asíncrona en otra región. Si no tiene claro qué enfoque seleccionar, comience con este tipo de implementación.”

3.2.4 Arquitectura de la Golden Copy

Como *Golden Copy* se define la copia de datos íntegra e inmutable que se puede utilizar como fuente confiable para una recuperación de datos ante un eventual desastre. El objetivo que se pretende alcanzar con esta *Golden Copy* es el de tener una salvaguarda que permita unas condiciones mínimas de recuperación, ante la ausencia de un tercer CPD de respaldo. Debe destacarse que, por razones de disponibilidad de recursos, actualmente no se considera viable poder disponer de más de dos CPD para la I3D, motivo por el cual se considerará esta solución basada en *Golden Copy* como la elegida para agregar una capa adicional de protección.

Tal y como se ha adelantado en la valoración de la implementación expresada en el punto anterior, y profundizando en el estándar de referencia [12], para establecer esta *Golden Copy* se va a evolucionar la implementación añadiendo una copia de seguridad como mecanismo de redundancia.

Esta *Golden Copy*, por tanto, se materializará en forma de copias de seguridad periódicas de la infraestructura y los datos en una región secundaria. Este enfoque proporciona un mecanismo de mitigación ante un incidente o desastre que afectase a toda la región principal.

Las condiciones mínimas con las que deberá contar esta *Golden Copy* son:

- Ubicación geográfica capaz de mitigar riesgos (desastres naturales o eventos adversos).
- Personal cualificado, mínimo o subcontratado, para su gestión y mantenimiento.
- Conexión segura y asíncrona a la I3D, mediante red de transporte, para proteger la confidencialidad y la integridad de los datos. Se busca aislamiento y protección frente a ataques, como puede ser *ransomware*.

Al implementar este enfoque, deben valorarse cuidadosamente los parámetros siguientes:

- *RTO (Recovery Time Objective)*, o Tiempo Objetivo de Recuperación, es el tiempo máximo que un sistema, aplicación o proceso puede estar inactivo tras un incidente o desastre antes de que afecte gravemente a la organización.

- RPO (*Recovery Point Objective*), o Punto Objetivo de Recuperación, representa la cantidad de datos e información que una organización puede aceptar como pérdida ante un incidente o desastre, de modo que le permita seguir operando con normalidad tras el mismo.

La representación de esta implementación con redundancia y con copia de seguridad, junto con los criterios de valoración más destacados para su adopción, son los siguientes:

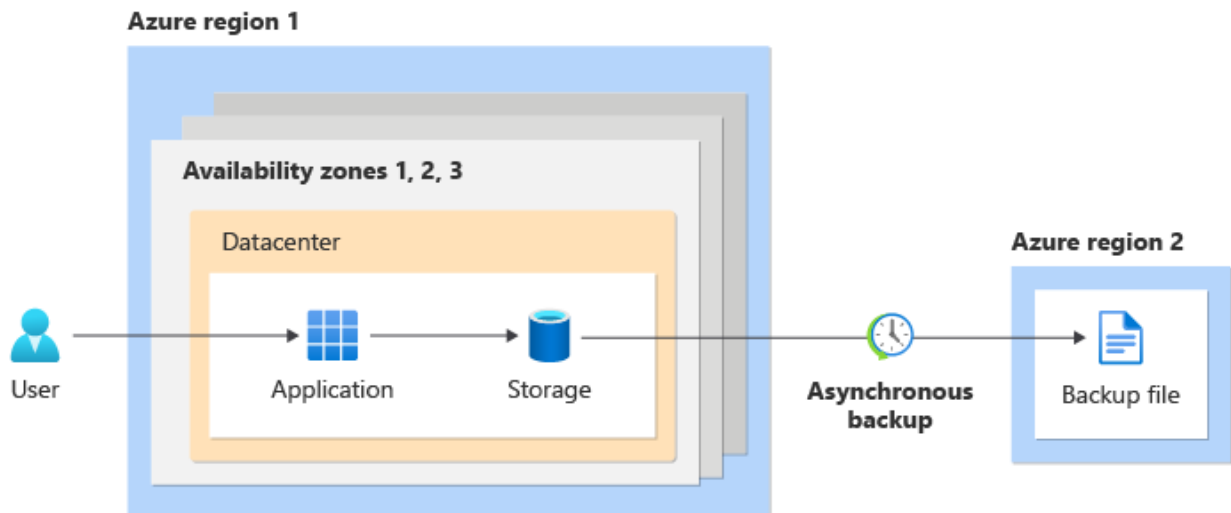


Figura 3-8 Implementación con Redundancia y con Copia de Seguridad (tomada de [13]).

Fundamento	Impacto
Confiabilidad	Confiabilidad muy alta. Los servicios son resistentes a una interrupción de un centro de datos o una zona de disponibilidad. Para la mayoría de los servicios, los datos se replican entre zonas automáticamente y sin retraso. Los datos se copian de seguridad de forma asincrónica en una región separada geográficamente. Esta copia de seguridad reduce el efecto de una interrupción de la región completa al minimizar la pérdida de datos. Después de una interrupción completa de la región, puede restaurar manualmente las operaciones en otra región. Sin embargo, los procesos de recuperación pueden ser complejos y pueden tardar tiempo en restaurarse manualmente en la otra región.
Optimización de costos	Costo moderado. Normalmente, agregar una copia de seguridad a otra región cuesta un poco más que la implementación de redundancia de zona.
Eficiencia del rendimiento	<i>Para la mayoría de las cargas de trabajo: rendimiento aceptable.</i> Es probable que este enfoque proporcione un rendimiento satisfactorio. <i>Para cargas de trabajo muy sensibles a la latencia: bajo rendimiento.</i> Algunos componentes pueden ser sensibles a la latencia debido al tráfico entre zonas o al tiempo de replicación de datos.
Excelencia operativa	<i>Durante una interrupción de zona de disponibilidad: alta eficiencia operativa.</i> La conmutación por error es responsabilidad de Microsoft y se produce automáticamente. <i>Durante una interrupción regional: baja eficiencia operativa.</i> La conmutación por error es su responsabilidad y podría requerir operaciones manuales y reimplementaciones.

Figura 3-9 Valoración de una Implementación con Redundancia y con Copia de Seguridad (tomada de [13]).

La valoración general, expresada en [13], por *Microsoft* para esta implementación es la siguiente:

“Este enfoque suele proporcionar un buen equilibrio para todos los problemas arquitectónicos. Si no está seguro de qué enfoque usar, comience con este tipo de implementación.”

3.2.5 Arquitectura de la Nube Pública

La arquitectura de nube pública a implantar, con independencia del proveedor seleccionado, pudiéndose dar una solución de múltiples proveedores de nube pública, propiedad de distintos proveedores comerciales, estaría basada en una solución de infraestructura de virtualización sobre nube pública como extensión de la solución implantada en la nube privada, a modo de un nuevo Centro de Datos definido por *Software (SDDC)*⁷, adicional a los dos CPD ya existentes.

En la nube pública existiría una serie de modelos para el aprovisionamiento de servicios de diferente complejidad y que se clasificarían en tres tipologías diferentes (*IaaS*, *PaaS* y *SaaS*), en línea con lo marcado en el documento de la referencia [1].

Dependiendo de la tipología del modelo, la responsabilidad de cada una de las capas quedaría determinada de la siguiente forma, de forma compartida entre el proveedor de servicios de nube pública y el propio CESTIC:

Modelo de Servicio		Componentes		Responsable		
SAAS PAAS IAAS		Gobernanza		Cliente		
		Aplicaciones		Cliente	Cliente	Proveedor
		Datos				
		Ejecución	Sistema Operativo			
		Gestión de Identidad	Middleware	Proveedor		
		Red	Almacenamiento			
		Servidores	Virtualización			
		Físico		Red	Hipervisor	Proveedor de servicios
Centro de Datos						

Figura 3-10 Modelo de responsabilidad compartida para el aprovisionamiento de servicios desde nube pública (tomada de [1]).

Dentro de la tipología de servicios que se ofertan por los proveedores comerciales de nube, inicialmente se identifican los siguientes servicios de *Core* (núcleo), como mínimo, necesarios:

- Portal (de la nube): interfaz sencilla para la gestión, administración y mantenimiento de los recursos y servicios en la nube.
- Servicio de Virtualización (en la nube): servicio que proporciona la infraestructura virtual en la nube pública para el despliegue de máquinas virtuales a semejanza de cómo se encuentra el Dominio de Seguridad DS0 en la nube privada, pero con la ventaja de que la gestión y el mantenimiento de esta infraestructura es llevada a cabo por el proveedor.

⁷ Centro de Datos definido por *Software (SDDC)*: consiste en un CPD en el que la infraestructura se virtualiza mediante la abstracción, la creación de grupos de recursos y la automatización. La infraestructura definida por *software* permite aprovisionar y gestionar con facilidad la infraestructura física empleando plantillas definidas por *software* y distintas *API* para definir y automatizar la configuración de la infraestructura y las operaciones del ciclo de vida.

Nótese que tal y como se concretó anteriormente, la situación final deseada únicamente contempla la posibilidad de alojar en nube pública cargas de trabajo pertenecientes al Dominio de Seguridad DS0.

- Servicio de Interconexión (entre nube privada y nube pública): servicio que permite la interconexión de un entorno en nube pública y los entornos existentes en infraestructuras pertenecientes a CPD del MDEF. Por lo general, este servicio va a exigir que los entornos presentes en los CPD del MDEF cuenten como base con una solución de virtualización. Este aspecto deberá ser tenido en cuenta a la hora de valorar la posible migración de un servicio a la nube, bien sea en su vertiente pública o privada.
- Servicios de Monitorización (en la nube): conjunto de servicios en la nube que permiten la monitorización del estado de los servicios, tales como disponibilidad, consumos, etc., y la detección de eventos e incidencias.

A su vez, se considera altamente recomendable adoptar un enfoque basado en *IaC*, para posibilitar el aprovisionamiento y respaldo de la infraestructura de computación a través de código, obviando la ejecución de procesos y configuraciones manuales. Cualquier entorno de aplicaciones requiere muchos componentes de infraestructura, como sistemas operativos, conexiones de bases de datos y almacenamiento. Los desarrolladores deben configurar, actualizar y mantener periódicamente la infraestructura para desarrollar, probar e implementar aplicaciones. La administración manual de la infraestructura lleva mucho tiempo y es propensa a errores, especialmente cuando se administran aplicaciones a escala.

La *IaC* permite automatizar la administración de la infraestructura para que los desarrolladores puedan centrarse en crear y mejorar las aplicaciones en lugar de administrar los entornos. En particular, su uso va a aportar ventajas a la hora de automatizar la gestión de la infraestructura en cuanto a la creación de entornos y ejecución de pruebas e implementaciones, y su posterior eliminación, de forma ágil y sin dependencias.

Durante el proceso de implantación de la arquitectura de nube pública se requiere definir una base sólida y de referencia sobre la cual poder desplegar los productos y servicios, de forma controlada y ordenada, además de segura. Esta base de referencia, siguiendo la línea marcada por el estándar de referencia de *Microsoft Azure* [12] en su apartado de plataforma de adopción de nube [14], se denomina *Landing Zone*. Nos referiremos a ella como una estructura diseñada para crear y gestionar cargas de trabajo en la nube pública de manera segura, eficiente y escalable.

De este modo, la *Landing Zone* va a constituir la base de definición para recoger y cumplir con los requisitos de seguridad, rendimiento, gobernabilidad y cumplimiento normativo del MDEF en cuestión. No llevar a cabo una definición adecuada de esta *Landing Zone*, puede conllevar en un futuro problemas graves en cuanto a la gobernanza y la calidad de los servicios que se ofrezcan desde la nube pública, así como riesgos asociados a la seguridad.

El diseño de la *Landing Zone* que se defina deberá estar guiado por los siguientes principios:

- Garantizar la seguridad desde el principio, en todas las cuentas, redes, y servicios, e integrarla en todas los Ámbitos y actividades del CESTIC.
- Asegurar la gobernanza, la supervisión de la seguridad y el cumplimiento normativo requerido al MDEF.
- Aprovisionar todas las capacidades funcionales y de seguridad de la nube utilizando *IaC*, para minimizar los riesgos derivados de la falta de automatización.

Para un posible caso de solución “multi-nube” sería necesario realizar esta definición para cada proveedor de nube pública sobre el que se fuese a desplegar algún servicio, estableciéndose un diseño de *Landing Zone* diferenciado por proveedor.

Una vez concluido el diseño de la *Landing Zone* éste debe validarse, normalmente por el propio proveedor de nube pública, para garantizar que se cumplen los requisitos mínimos necesarios antes de llevar a cabo su implantación.

El diseño de la *Landing Zone* deberá dar cobertura, al menos, a todos y cada uno de los elementos y capacidades siguientes:

- Automatización: se definirán los mecanismos usados para el despliegue de la *IaC*.
- Regiones: se identificará la región, o regiones, sobre la que se desplegarán los servicios.
- Facturación: se recogerán las herramientas que permitirán realizar el control de costes, en línea con los procedimientos y mecanismos *FinOps*. Se deberá habilitar el alertado preventivo para detectar desviaciones anómalas.
- Recursos: se identificarán la estructura y la estrategia de cuentas, ámbitos, proyectos y entornos.
- Red: se mostrará cómo se estructura la red y cómo se enruta cada flujo de tráfico. Entre otros componentes se incluirán:
 - Conectividad entre la nube pública y la infraestructura de telecomunicaciones del CESTIC
 - Modelo de red de acceso e interacción con la nube. Se propone la topología *Hub & Spoke*⁸.
 - Diseño de Nubes Privadas Virtuales (*Virtual Private Cloud - VPC*)⁹, como medida de refuerzo de seguridad en el entorno de nube pública.
 - Comunicación con los servicios de nube pública y entre las *VPC*.
- Gestión de Identidades y Accesos (*Identity and Access Management - IAM*): se indicarán las recomendaciones y configuraciones a realizar para la gestión de credenciales, la federación de *IAM* y las vinculaciones de roles a grupos. En particular se analizará la necesidad de integración de los *IAM*, con el Directorio Activo del dominio MDEF.ES que se implante en la nube privada. El objetivo último sería contar con una identidad de usuario única (híbrida) en el DS0, al estar integrado tanto en el entorno de nube pública como de nube privada.
- Monitorización: se definirá el almacenamiento y la recopilación de registros para su análisis y alertas.
- *Backup*, disponibilidad y Recuperación ante Desastres (*Disaster Recovery - DR*): se recogerán las políticas de *backup* por defecto y las opciones de disponibilidad y *DR* implantadas en los servicios que forman el *Core* (núcleo) de la *Landing Zone*.

En definitiva, una *Landing Zone* va a constituir un entorno basado en los principios clave de diseño para la implantación de los servicios en nube. Estos principios van a posibilitar la migración, actualización y despliegue de servicios en nube a gran escala. Una arquitectura basada en *Landing Zones* es escalable y modular, por lo que va permitir al MDEF adaptarse a las diferentes necesidades que con vistas a futuro se vayan produciendo.

⁸ Topología *Hub & Spoke*: topología de tipo radial en la que todos los nodos están conectados a un concentrador central, para el intercambio de datos y la comunicación. Es una forma sencilla y rentable de enrutar y administrar datos en una red, con el concentrador central que sirve como mediador para todas las comunicaciones, lo que facilita la configuración de los ajustes de seguridad y el monitoreo del tráfico. La topología radial es muy apreciada por su simplicidad, escalabilidad y capacidades de seguridad mejoradas, lo que la convierte en una opción valiosa para las organizaciones.

⁹ Nube Privada Virtual (*Virtual Private Cloud - VPC*): es una modalidad de nube que permite a una organización establecer su propio entorno informático, a modo de nube privada en una infraestructura de nube pública compartida. Permite a la organización definir y controlar una red virtual que está lógicamente aislada de todos los demás inquilinos de la nube pública, creando así un espacio privado y seguro en la nube pública.

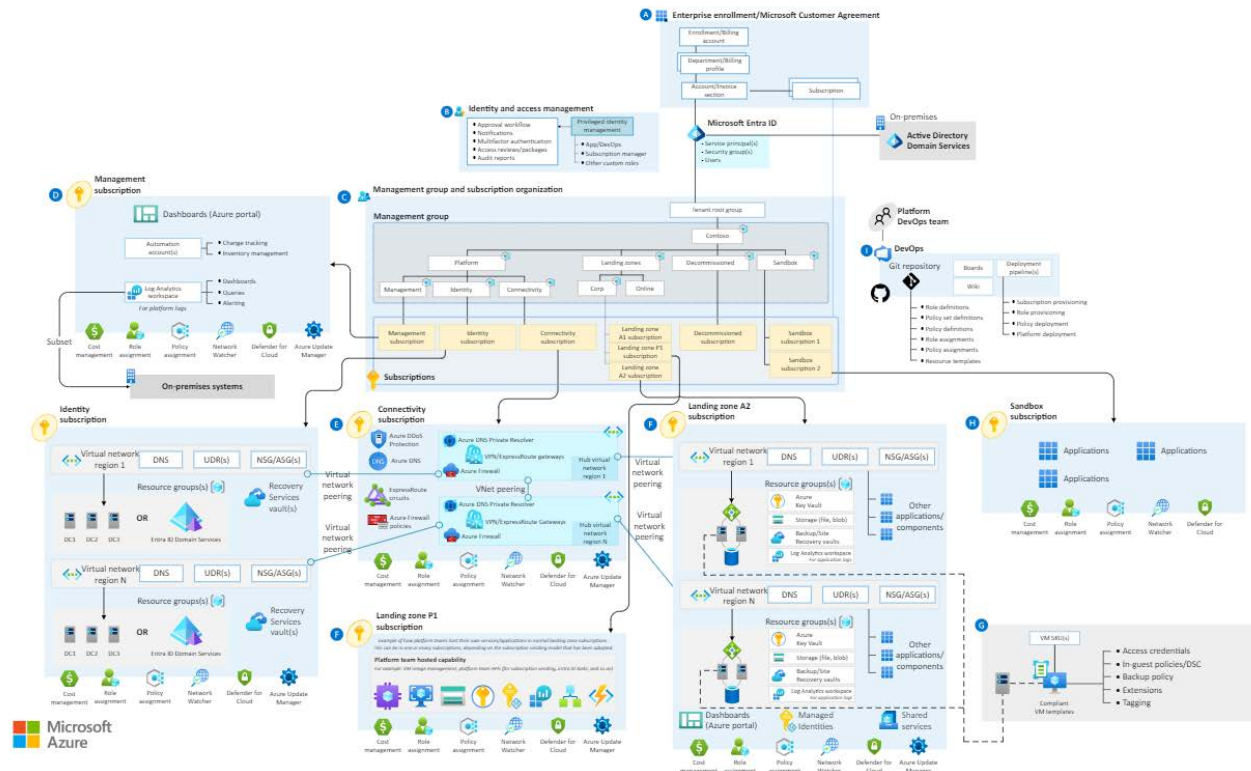


Figura 3-11 Modelo de Microsoft Azure para la Landing Zone (tomada de [14]).

3.2.6 Arquitectura de la Nube Híbrida

Como solución definitiva y completa se propone una arquitectura de nube híbrida, resultado de la combinación de las arquitecturas de nube privada y pública expuestas, interconectadas a través de una línea de comunicación privada, permitiendo la integración de ambas y desplegando los servicios de forma indistinta, atendiendo a una serie de criterios que definan un marco de valoración para decidir entre el alojamiento de dichos servicios en nube pública o privada.

De forma esquemática se recoge el esquema de la solución para la arquitectura de la nube híbrida que conformaría la Nube MDEF en su vertiente permanente:

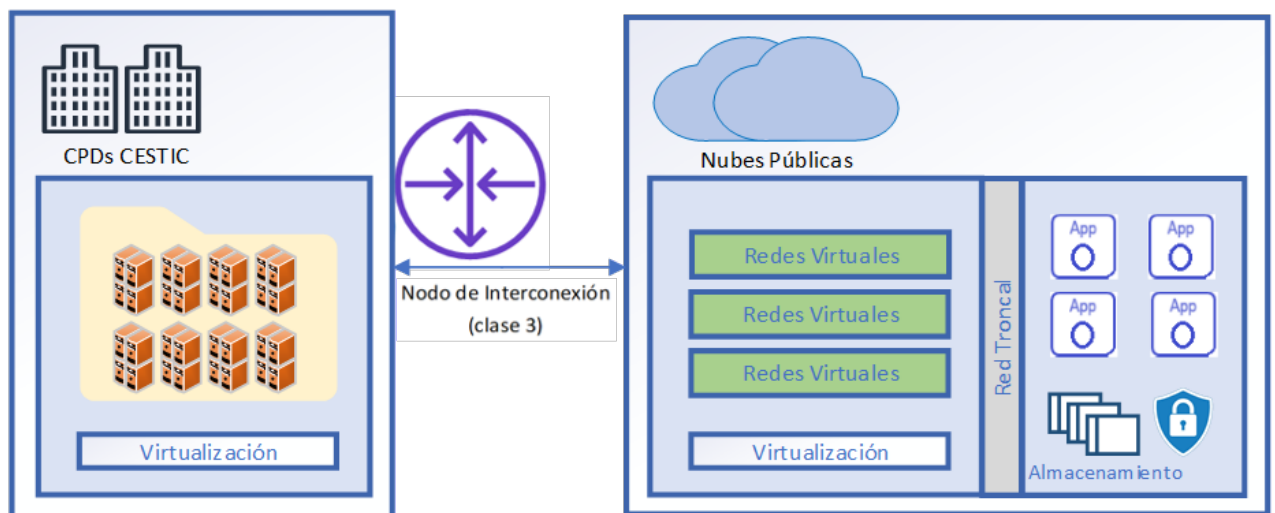


Figura 3-12 Detalle de arquitectura de nube híbrida (nube privada más nubes públicas) (elaboración propia).

La integración de ambas arquitecturas, considerándose que la solución de nube pública puede atender a una solución multi-proveedor, se deberá realizar a través de puntos de acceso dedicados desde el Dominio de Seguridad DS0 a los proveedores finales, teniendo como resultado final la solución de arquitectura de nube híbrida.

La comunicación desde el DS0 a la nube pública se llevará a cabo a través de una línea dedicada, externa a la infraestructura de Internet, y haciendo uso de un Nodo de Interconexión Clase 3, cuya definición y cometidos vienen recogidos en virtud del documento de la referencia [9], el cual constituye el escaño superior respecto a modelos de arquitectura a seguir en todos aquellos desarrollos CIS/TIC del MDEF. En base a ella, dicho nodo deberá ser capaz de proporcionar la interconexión con las redes de la AGE externas al MDEF y con redes privadas tales como Internet. Además, debe constituir el único punto de interconexión de la infraestructura CIS/TIC del MDEF con redes externas.

Para una mayor resiliencia y robustez de esta comunicación del DS0 a la nube pública, se propone proporcionar acceso por separado desde las ubicaciones físicas de ambos CPD del MDEF, reforzando así la posibilidad de seguir operando ante posibles situaciones de contingencia producidas por desastres.

Es crucial tener en cuenta el hecho de que la arquitectura deseable a nivel de nube pública, dentro de esta solución híbrida, es una arquitectura multi-nube que se apoye sobre de diferentes proveedores. Y es que si bien durante la elaboración del presente trabajo se está tomando como referencia general el estándar de *Microsoft Azure Well-Architected Framework* [12], debe ser imperativo que el MDEF pueda evitar al máximo una dependencia específica de un proveedor concreto, máxime cuando se traten de proveedores comerciales no nacionales.

La arquitectura híbrida planteada permite tanto la posibilidad de evolucionar de forma ágil servicios residentes en la nube privada hacia la nube pública, como su deshibridación, entendiendo como tal la migración de servicios cuyas cargas de trabajo se estén ejecutando en nube pública a la nube privada soportada por la infraestructura de CPD propietaria del MDEF. Este tipo de procesos son especialmente relevantes ante posibles contingencias tales como cambio de proveedores, finalización de relación con un proveedor, recuperación ante desastres, decisión estratégica, etc.

La solución comercial de virtualización que se adopte a nivel de nube privada, así como la propuesta de extensión de esta solución hacia la nube pública, para los diferentes proveedores de nube, debe ser capaz de facilitar este tipo de movimientos de carga en ambos sentidos en función de las necesidades de cada momento. En este sentido, la ejecución de los movimientos de carga entre nube privada y nube pública, se verán facilitados por el hecho de que la solución de virtualización que se adopte sea la misma tanto en origen como en destino.

A tenor de lo expuesto, las figuras siguientes ilustran de modo general algunos de los escenarios básicos de hibridación/deshibridación que podrían llegar a darse, expresando en fondo blanco la nube privada del MDEF y en fondo azul la nube pública de un proveedor de servicios determinado:

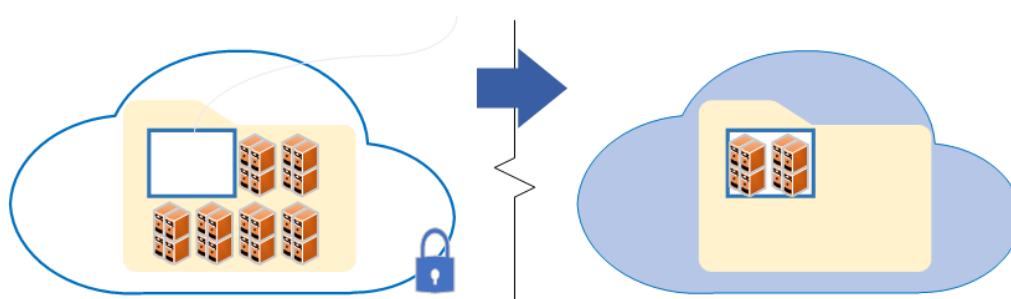


Figura 3-13 Escenario de Hibridación (movimiento de cargas de nube privada hacia nube pública) (elaboración propia).

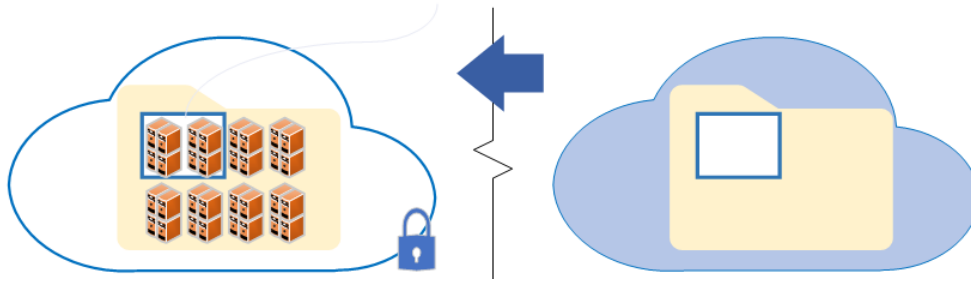


Figura 3-14 Escenario de Deshibridación (movimiento de cargas de nube pública hacia nube privada) (elaboración propia).

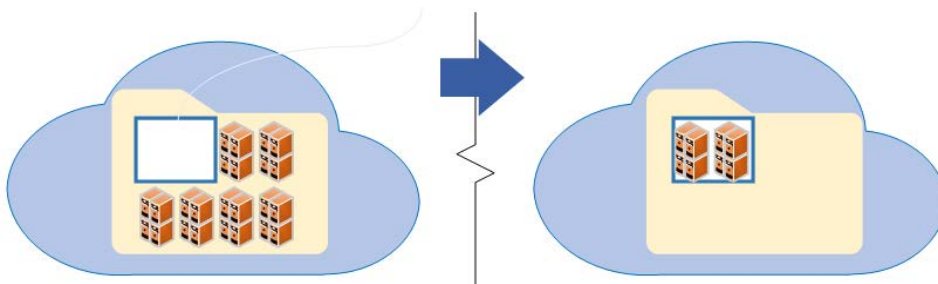


Figura 3-15 Escenario de cambio parcial entre diferentes proveedores (movimiento de cargas de nube pública hacia otra nube pública) (elaboración propia).

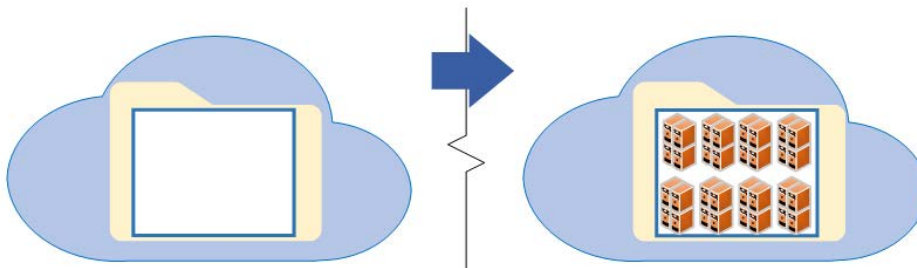


Figura 3-16 Escenario de cambio total entre diferentes proveedores (movimiento de cargas de nube pública hacia otra nube pública) (elaboración propia).

De forma general para los procesos de hibridación/deshibridación, con independencia del proveedor que se considere, pueden establecerse los siguientes pasos a seguir:

- Evaluación de servicios: realizar un inventario detallado de los servicios y recursos existentes que van a participar en el proceso.
- Planificación y diseño: desarrollar un plan detallado por fases, considerando requisitos de operación, arquitectura del servicio y aspectos de seguridad, entre otras consideraciones.
- Migración de servicios: trasladar los servicios seleccionados entre entornos, procurando minimizar o evitar interrupciones en la provisión del servicio durante este proceso.
- Integración de entornos: establecer conexiones seguras entre los entornos.
- Pruebas y validación: garantizar el correcto funcionamiento de los servicios trasladados.
- Optimización y monitorización: asegurar un rendimiento óptimo en el entorno final e implementar herramientas de monitoreo para observar dicho rendimiento.

Hay que mencionar que los diferentes escenarios representados anteriormente consideran que los servicios desplegados en nube pública se encuentran disponibles en la solución de virtualización existente para cada proveedor. Con la finalidad de facilitar posibles procesos de

hibridación/deshibridación, que impliquen movimientos de cargas “en caliente” [15], es preceptivo adoptar para la nube privada del MDEF soluciones comerciales de virtualización que se encuentren ampliamente extendidas entre los principales proveedores. En el caso de uso de servicios nativos de un proveedor, la deshibridación de este servicio, o cambio a otro proveedor, contará con una complejidad adicional a cualquier movimiento de este servicio. Por este motivo deberá evaluarse previamente la potencial complejidad de movimiento que genera la utilización de servicios nativos de cualquier proveedor comercial, con respecto a los beneficios sustanciales que pueden suponer económicamente.

3.2.7 Arquitectura de la Nube de Combate

Con objeto de abordar una solución de Arquitectura para la Nube MDEF, en su vertiente desplegable, es preciso acudir al concepto de Nube de Combate¹⁰. Para desarrollar este novedoso concepto y su arquitectura asociada, tomaremos como referencia el documento [16], el cual incluye la Nube de Combate como un elemento clave para impulsar la transformación digital de la Fuerza para combatir en el Multidominio¹¹, capacitándola para planear y ejecutar Operaciones Multidominio¹².

En los últimos años se está produciendo un cambio de paradigma en las operaciones militares, desarrollando un nuevo concepto de operación de la Fuerza en el Multidominio, en el que el combate colaborativo se eleva a su máximo nivel [17]. De este modo, el foco ya no está en las capacidades individuales de cada plataforma, sino en el empleo conjunto de todas las capacidades disponibles.

Para ello, hay muchas formas de conectar las plataformas y unidades, pero la forma óptima es el modelo de arquitectura de nube, siempre que sea en concepto de Nube de Combate. Este concepto permite compartir en tiempo real la información, de manera que otorgue a la Fuerza una clara ventaja táctica, disponiendo de la información necesaria en el lugar y tiempo que se necesite, para poder tomar decisiones de forma rápida y permitiendo una máxima hiperconectividad entre sensores [18].

Precisamente esta hiperconectividad y resiliencia inteligente es necesaria para asegurar el rendimiento y la protección en el intercambio de información, incluso en escenarios tecnológicamente degradados, utilizando todos los esquemas de comunicaciones disponibles. El objetivo es alcanzar la superioridad de la información para compartirla de forma efectiva en servicios consumibles por todos los activos conectados, en cualquier dominio, y ejercer un Mando y Control más avanzado y conjunto.

Ante la tarea de plantear una arquitectura tecnológica exitosa para dar soporte a esta nueva forma de llevar a cabo operaciones militares, se ha considerado tomar como referencia para el presente trabajo las enseñanzas y lecciones aprendidas de la participación de proveedores comerciales de nube pública en el conflicto de Ucrania, cuyo caso paradigmático es *Amazon Web Services (AWS)* [19]:

“AWS made one of the biggest contributions to Ukraine’s victory by providing the Ukrainian government with access and resources for migrating to the cloud and securing critical information. Literally saved our digital infrastructure, [by enabling] state registries and critical databases to migrate to the AWS cloud.”

Mykhailo Fédorov, Viceprimer Ministro y Ministro de Transformación Digital de Ucrania.

¹⁰ Nube de Combate (*Combat Cloud*): solución tecnológicamente avanzada para las capacidades militares que habilita su empleo, especialmente el Mando y Control, en el Multidominio, y que permite mediante la captura, procesamiento y distribución de datos, incluidos los que proporcionan sensores y sistemas, e intercambio de información, así como la prestación de servicios, que cada usuario, plataforma o nodo autorizado contribuya y reciba información esencial a tiempo para que sea capaz de utilizarla para la toma de decisiones y la ejecución de operaciones militares dentro de un espacio de batalla.

¹¹ Multidominio (*Multidomain - MD*): entorno de actuación muy complejo, que engloba a todos los ámbitos de operación, con una gran interdependencia e interacción entre todos ellos, bien sean físicos: Tierra, Mar, Aire y Espacio, o no físicos: Cognitivo y Ciberespacial.

¹² Operaciones Multidominio (*Multidomain Operations - MDO*): operaciones realizadas por la Fuerza que, por su agilidad y complejidad, necesitan de una adecuada interoperabilidad y conectividad que posibiliten un control distribuido de los medios para permitir la integración de todas sus capacidades y así poder producir efectos en y desde cualquiera de los ámbitos de operación.

La cita recogida deriva del hecho de poder salvar un volumen de 10 *Petabytes* (PB) de información de las instituciones ucranianas de ser totalmente eliminada [20], como parte de la estrategia rusa de bloquear el país haciendo colapsar la administración estatal, banca, universidades, etc., por medio de la destrucción física de los CPD que albergaban toda la información necesaria para el funcionamiento de estas instituciones.

Para llevar a cabo esta tarea de rescate de la información y su migración a la nube de AWS, se planteó un esquema de funcionamiento en capas [21], capaz de dar soporte a la situación de conectividad planteada en la situación final deseada para el Concepto de la Nube MDEF.

De este modo se establece un vínculo que transita desde el *Cloud Computing* hasta el *Edge Computing*, pasando por una capa intermedia de *Fog Computing*, capaz de proporcionar, sin solución de continuidad, una arquitectura de nube capaz de ser explotada tanto en su vertiente permanente como en su vertiente desplegable.



Figura 3-17 Representación de Capas “Edge to Cloud” (tomada de [21]).

Este producto comercial, diseñado específicamente “*ad-hoc*” para su empleo en el conflicto de Ucrania, no supone una solución directamente trasladable al caso de la Nube MDEF, pero sí muestra el hecho de que estado del arte actual ya permite ofrecer soluciones tecnológicamente maduras para desplegar sobre el terreno un número significativo de nodos capaz de conformar una auténtica Nube de Combate.

Estos nodos, tal y como los plantea AWS, estarían sustentados sobre sus dispositivos de la familia “*Snow*”, con capacidad de dar cobertura a las capas *Fog* y *Edge* de la Nube de Combate, en función de sus capacidades, y contando con un adecuado grado de ruggedización acorde a las condiciones tácticas de su empleo previsto.



Figura 3-18 Materialización de las Capas “Fog y Edge” sobre la base de dispositivos “Snow” (tomada de [21]).

En cualquier caso, debe tenerse presente que esta aproximación comercial concreta debe tomarse únicamente como una referencia de posible implementación de estas capas *Fog* y *Edge Computing*. De hecho, las capas 2 y 3 del esquema “*Edge to Cloud*” presentado deberían ser cubiertas precisadamente por las capacidades ya descritas de nube privada y nube pública, respectivamente, soportadas por los CPD del MDEF y por los proveedores comerciales de nube pública.

La tarea quedaría concretada, por tanto, en desarrollar unos nodos similares a los presentados por AWS, normalmente basados en tecnología de Infraestructura Hiperconvergente (*HCI*)¹³ que permitiese optimizar las especificaciones de peso y volumen, y con posibilidad de ser integrados en plataformas y organizaciones operativas altamente móviles, capaces de extender los servicios de la Nube MDEF hasta cualquier punto de una Zona de Operaciones. Estos nodos deberían, necesariamente, poder interoperar con la vertiente permanente de la Nube MDEF, de igual modo que los “*Snow*” son capaces de interoperar con los “*Outpost*” y los recursos de nube de AWS.



Figura 3-19 Detalle de un rack “*Outpost*” que conforma la parte de nube privada “*on-premise*” del esquema “*Edge to Cloud*” (tomada de [21]).

La configuración de los diferentes tipos de nodos surgirá como resultado de las propias restricciones de las plataformas que los integran y de sus requerimientos de movilidad que, de hecho, son resultado del Ámbito en el que operan y del propósito al que sirven, tal y como se define en [16]:

- Nodos de alta movilidad (capa 0): cuyas plataformas integradoras se encuentran en la Zona de Operaciones más a vanguardia. Estos nodos tendrán mayor número de sensores, efectores y usuarios conectados, mientras que la capacidad de cómputo será reducida, el tipo de datos que usarán será más táctico, de validez efímera y consumo rápido.
- Nodos semi-desplegables (capa 1): como pueden ser puestos tácticos avanzados. Dispondrán de mayor capacidad de proceso que los anteriores y tendrán asociados un menor número de sensores y efectores.
- Nodos fijos (Nube MDEF permanente - capas 2 y 3): ubicados en localizaciones estratégicas y entornos seguros del territorio nacional. Estos nodos tendrán gran capacidad de cómputo y acceso a bases de datos con información de inteligencia permanente.

¹³ Infraestructura Hiperconvergente (*Hiperconverged Infrastructure - HCI*): es un sistema integrado que combina virtualización, computación, conectividad de red y almacenamiento en una sola plataforma. Al hacerlo, se reduce la complejidad y los costes, al tiempo que se facilita una mayor escalabilidad, flexibilidad y agilidad para gestionar y explotar los recursos.

3.3 Operación de la Nube MDEF

3.3.1 Estructura de Operación

Cuando hablamos de Operación de la Nube MDEF nos estamos refiriendo a todas aquellas tareas relativas a la administración y el mantenimiento de la plataforma, que sirven para garantizar la disponibilidad de los servicios y su ejecución de forma óptima y eficiente.

En el caso de la Nube MDEF, y considerando la arquitectura planteada de un escenario híbrido basado en una infraestructura de dos CPD (infraestructura tradicional¹⁴ y nube privada) más nube pública (proveedores comerciales), podríamos diferenciar dos tipos de operaciones en función del entorno en el que nos encontremos:

- Operaciones en nube privada e infraestructura tradicional.
- Operaciones en nube pública (con un único proveedor o multi-proveedor).

Tal y como se ha visto, atendiendo al modelo de responsabilidad compartida promulgado según el documento de la referencia [1], que se adopta en nube pública, la principal diferencia que nos encontramos en cuanto a la operación sobre infraestructura tradicional y nube privada es que las tareas y responsabilidades relativas a los servicios desplegados en estos entornos recaerán de forma íntegra sobre los Equipos de Operaciones del CESTIC.

En conclusión, y como punto de partida, la estructura de Operación de la Nube MDEF vendrá definida por el modelo de responsabilidad compartida ya presentado a la hora de definir la Arquitectura de la Nube MDEF, completado con la parte de nube privada e infraestructura tradicional:

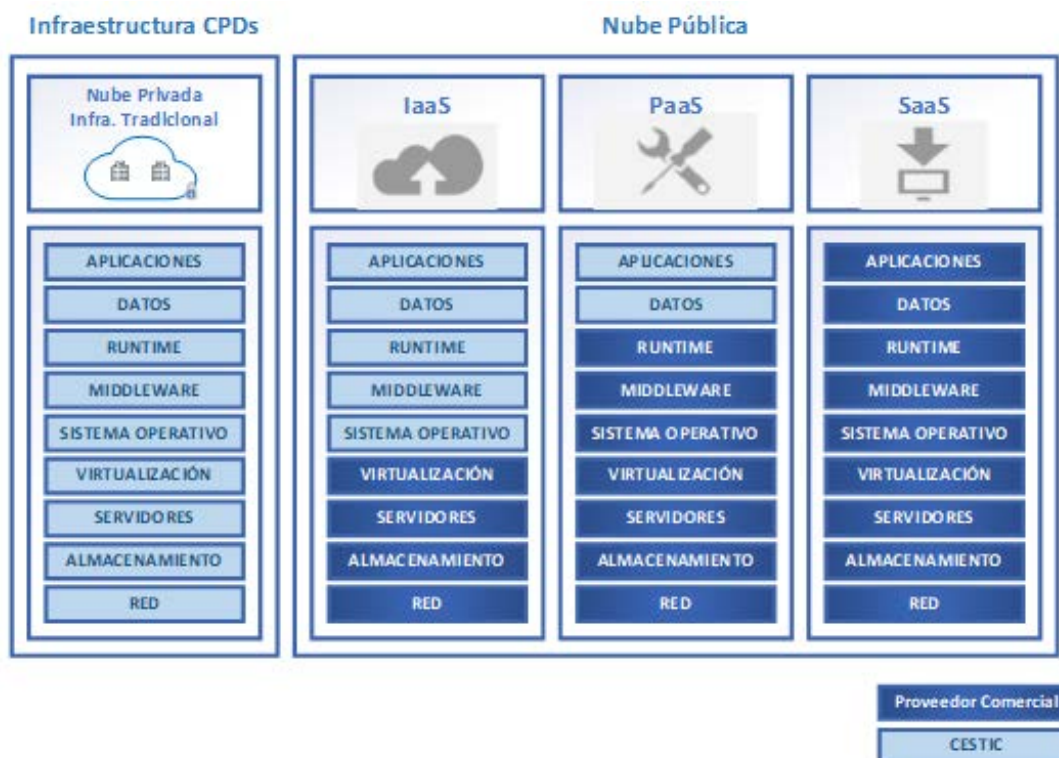


Figura 3-20 Estructura de Operación de la Nube MDEF, partiendo del modelo de responsabilidad compartida para el aprovisionamiento de servicios desde nube pública (tomada de [1]), y completado con la parte de nube privada e infraestructura tradicional.

¹⁴ Infraestructura tradicional: en este contexto nos referimos a infraestructura tradicional como la relativa a aquellos sistemas y servicios que por diversos motivos (economía, obsolescencia, complejidad, etc.) no son susceptibles de ser migrados a un entorno de nube, ya sea privada o pública. En cualquier caso, y bajo una perspectiva de operación, estos sistemas y servicios van a seguir siendo atendidos y provisionados, hasta su retirada, desde los dos CPD existentes.

Aparte de completar los aspectos mencionados, para ofrecer una estructura de operación completa, se ha suprimido un importante componente de los mencionados en el modelo de responsabilidad compartida: la Gestión de la Identidad.

Esta decisión se sustenta sobre la base de considerar este componente como una “piedra angular” para abordar el aspecto de Seguridad de la Nube MDEF conforme a un nuevo paradigma de seguridad conocido como Confianza Cero (*Zero Trust*), el cual no se había desarrollado en el momento de publicación de la Estrategia de Explotación de la Nube [1]. Dicho paradigma de seguridad ha sido promulgado para el MDEF sobre la base de la Estrategia de implantación del concepto de seguridad Confianza Cero (*Zero Trust*) [22], por lo que queda equiparado al mismo nivel normativo y con una fecha posterior, motivo por el cual se considera adecuado introducir este cambio¹⁵.

A su vez, desde una perspectiva de operación, es necesario considerar que uno de los principales problemas identificados lo constituye la velocidad en la configuración y provisión de servicios, así como el tiempo necesario para realizar despliegues. Otro grave inconveniente se produce por la falta de correspondencia entre los entornos preproductivos y de producción, lo cual dificulta verificar si el comportamiento de una determinada aplicación se corresponde con el previsto y planificado antes de su despliegue en producción.

Como respuesta a estos inconvenientes, la tecnología de nube permite provisionar y retirar dinámicamente entornos, reduciendo enormemente los tiempos de provisión y permitiendo la disponibilidad de éstos en modo “autoservicio” para aquellos usuarios que lo requieran. Para ello se ha previsto el uso de la *IaC*, de forma que los entornos preproductivos ya no requieran configuraciones *hardware* físicas, sino que sean provisionados mediante ficheros de definición procesables, tratándose como código fuente de lenguajes de programación. El empleo de la *IaC* contribuye a la aplicación del enfoque de desarrollo *DevOps*, o *DevSecOps* (*Development - Security - Operations*) en el MDEF, agilizando el proceso de desarrollo de *software*, simplificando su despliegue, e integrando los cambios en el código tan pronto como sea posible, con la frecuencia necesaria, y de una forma segura.

Por su parte, los contenedores son paquetes de *software* estándar que agrupan el código de una aplicación con las bibliotecas y los archivos de configuración asociados, junto con las dependencias necesarias para que la aplicación se ejecute. Se utilizan de manera análoga a la tecnología de virtualización, pero con la ventaja de ser más ligeros, *Megabytes* (MB) frente a *Gigabytes* (GB), y portables, debido a que utilizan el sistema operativo de su máquina anfitriona o *host* en lugar de integrar uno propio. Al no incluir un sistema operativo completo, los contenedores requieren de recursos computacionales mínimos y son rápidos y fáciles de instalar, habilitando que su despliegue se puede llevar a cabo en cuestión de segundos. Por ello, en el caso de los contenedores no es necesario el despliegue de un hipervisor para emular un sistema operativo completo.

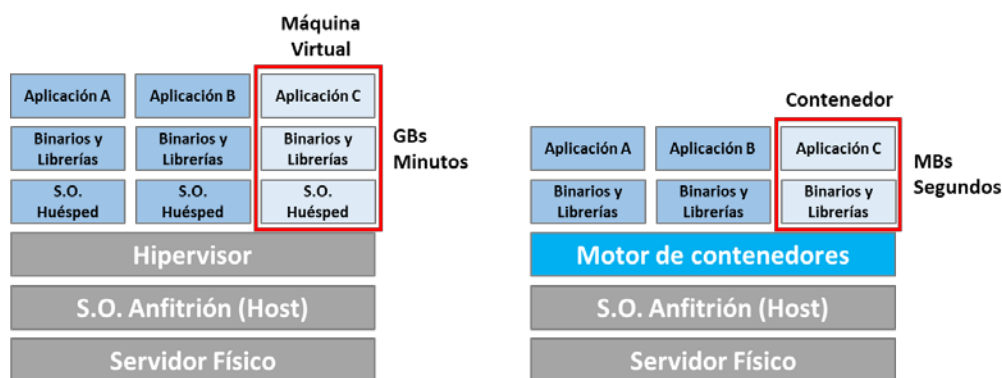


Figura 3-21 Comparativa entre virtualización tradicional y basada en contenedores (tomada de [23]).

¹⁵ Todo el componente de “Gestión de Identidad” se desarrollará, por tanto, en el apartado “3.4 Seguridad de la Nube MDEF”, quedando fuera del alcance de la Operación de la Nube MDEF. En cualquier caso, y dada su importancia, no será un componente que se obvie, sino que por el contrario será desarrollado de forma particular.

De esta forma, los contenedores, al actuar como una unidad estándar de implementación *software*, permiten aislar las aplicaciones, garantizando la consistencia del *software* entre los entornos preproductivos y de producción, y permitiendo que éstas se ejecuten idénticamente en cada uno de ellos, con una reducción al mínimo de los fallos posibles y una maximización de su portabilidad.

Todos estos aspectos, de nuevo, han sido desarrollados por una estrategia para el MDEF posterior a la correspondiente de nube, en este caso la Estrategia de Desarrollo de *Software* en el MDEF [23], la cual marca, entre sus Objetivos Generales:

“Aplicar el enfoque DevSecOps, como modelo obligatorio para el ciclo de vida del software en el MDEF. Este paradigma implica la automatización y estandarización de los trabajos, tales como: despliegue continuo (CD), integración continua (CI), controles de calidad y seguridad, instrumentos de gobierno y administración de la infraestructura como código (IaC).”

“Implantar la utilización de tecnología de contenerización y de nube, como elementos habilitadores e impulsores de los nuevos enfoques de desarrollo de software. En el caso de los contenedores, éstos se establecen como obligación para nuevos desarrollos, sólo sujeto a excepciones por razones técnicas o de relación coste-beneficio. En el caso de la nube, deberá evaluarse qué desarrollos son aptos para su empleo en función de los criterios que se determinen (sensibilidad de los datos, tiempo de respuesta, acreditación, etc.).”

En definitiva, deberán contemplarse los aspectos *DevSecOps* y la contenerización en la estructura de Operación de la Nube MDEF, de modo que el empleo de estos nuevos paradigmas en su conjunto, *DevSecOps*, contenerización y nube, permitan la provisión de entornos de desarrollo en modo servicio (*as a Service*). Uniendo todo ello a las ya mencionadas modalidades de provisión de servicios (*IaaS*, *PaaS*, *SaaS*), previstas en el modelo de responsabilidad compartida de la referencia [1], se establecería el siguiente modelo de provisión de servicios a la hora de operar en la Nube MDEF:

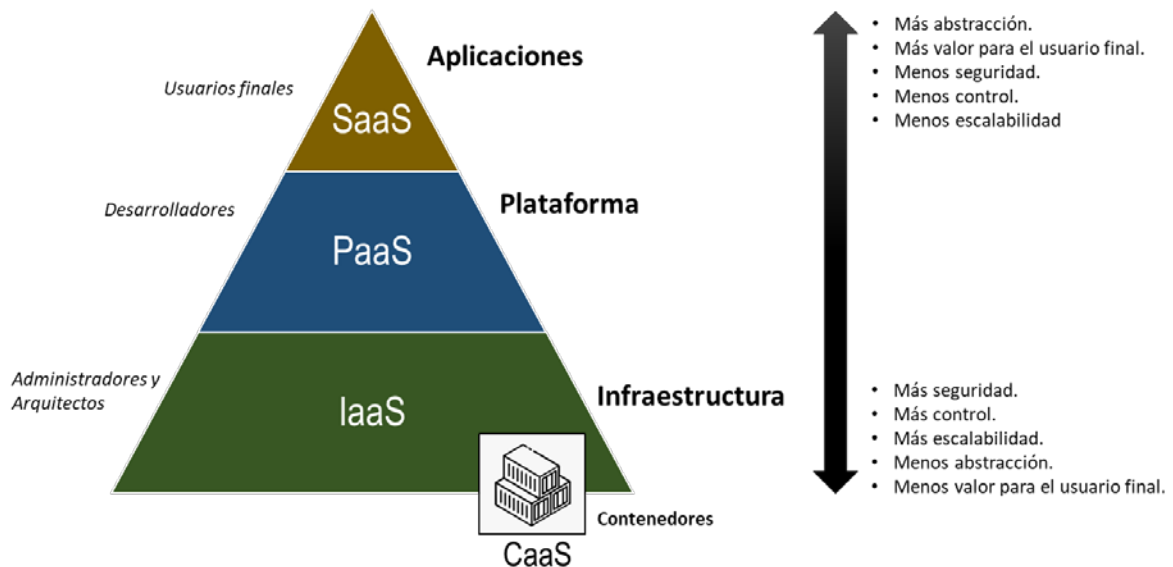


Figura 3-22 Modelo de provisión de servicios en la Nube MDEF en relación con sus características y usuarios de destino (tomada de [1]).

- **Infraestructura como Servicio (*IaaS*):** en este modelo se van a entregar recursos de infraestructura bajo demanda, proporcionando procesamiento, almacenamiento, redes y virtualización, mientras que el usuario tiene el control sobre los sistemas operativos y las aplicaciones desplegadas. En el MDEF se dan diversos casos de uso en los que los Ámbitos van a requerir este tipo de servicios para, a partir de él, poder desplegar sus propios sistemas liberándoles de una importante carga de gestión de la infraestructura.

- **Contenedor como Servicio (CaaS):** es un modelo que se encarga de entregar y gestionar todos los recursos *hardware* y *software* para desarrollar y desplegar aplicaciones mediante contenedores. Podría considerarse un subconjunto o una extensión de *IaaS*, pero usando contenedores como recurso principal en lugar de máquinas virtuales. Este modelo se considera especialmente útil para los desarrolladores ya que les permite diseñar aplicaciones flexibles y más seguras en los contenedores y, tal y como se ha expresado, se establece como obligatorio para los nuevos desarrollos de *software* que se lleven a cabo en el MDEF.
- **Plataforma como Servicio (PaaS):** es un modelo que se encarga de entregar una plataforma a la organización cliente. El cliente no va a administrar ni controlar la infraestructura, pero sí va a tener el control sobre las aplicaciones instaladas y su configuración, pudiendo incluso instalar nuevas aplicaciones. Como factor diferencial, este modelo va a proporcionar herramientas y utilidades para el desarrollo de aplicaciones en nube, tales como bases de datos o entornos de programación, en las que los Ámbitos van a poder desarrollar sus propias soluciones.
- **Software como Servicio (SaaS):** es un modelo de distribución de *software* en el que las aplicaciones están alojadas en un proveedor de servicios y se ponen a disposición de los usuarios a través de la red. De este modo, los usuarios individuales del MDEF van a disponer en la nube de las herramientas con las que poder llevar a cabo sus cometidos básicos: aplicaciones ofimáticas, correo electrónico, etc., de tal modo que el CESTIC quede liberado de la administración y control de la infraestructura de la que estas herramientas hagan uso.

En resumen, según la estructura de Operación de la Nube MDEF propuesta, la primera cuestión a determinar a la hora de operar un servicio en nube es si dicho servicio deberá estar alojado en nube privada o en nube pública. Para ello, básicamente se deberán tener en cuenta los siguientes parámetros:

<u>Parámetro</u>	<u>Descripción</u>
Sensibilidad de los datos	Confidencialidad, integridad y disponibilidad necesarias.
Tiempo de respuesta	Capacidad de respuesta rápida a las demandas operativas.
Riesgo de continuidad del servicio en la migración	Posibles interrupciones del servicio, pérdida de datos o problemas de rendimiento durante el proceso de migración.
Integración con aplicaciones estrechamente relacionadas	Capacidad de compartir datos y funcionalidades con otras aplicaciones.
Coste y complejidad de la migración	Evaluación del coste asociado y complejidad técnica y operativa.
Acreditación	Cumplimiento de estándares de seguridad y protección de datos.

Tabla 3-1 Criterios básicos para decidir operar un servicio en Nube MDEF desde nube privada o nube pública.

Una vez realizado el análisis anterior, si se determina que un servicio va a ser proporcionado desde nube pública se planteará una segunda cuestión, relativa a la modalidad de servicio a provisionar, así como el proveedor del mismo. Para ello se analizarán, como mínimo, los siguientes parámetros:

<u>Parámetro</u>	<u>Descripción</u>
Estandarización funcional	Cumplimiento con los estándares y requisitos funcionales establecidos.
Volatilidad de la demanda	Capacidad del servicio para adaptarse a las variaciones de las necesidades operativas.
Complejidad de la migración a la nube	Dificultad y esfuerzo requerido para migrar al entorno de la nube del proveedor en cuestión.
Operación autónoma	Garantía de disponibilidad y rendimiento del servicio sin necesidad intervención manual.

Tabla 3-2 Criterios básicos para decidir el modelo de provisión de un servicio en Nube MDEF desde nube pública.

No obstante, antes siquiera de plantear las dos cuestiones precedentes, el primer análisis a realizar debería ser si un determinado servicio es susceptible de ser migrado al entorno de Nube MDEF, o por el contrario es más conveniente que continúe residiendo en la infraestructura tradicional. Este análisis es clave ya que, tal y como se ha dejado entrever al mencionar el principio de Preferencia en Nube (*Cloud First*), no todos los servicios actualmente en producción serían migrados a la Nube MDEF¹⁶.

3.3.2 Atribución de roles y responsabilidades de Operación

Adicionalmente a este modelo de responsabilidad compartida entre el MDEF, por medio del CESTIC, y el proveedor o proveedores de nube pública, para la correcta explotación de los servicios de la Nube MDEF se establecerán los siguientes roles y responsabilidades estipulados según el documento de la referencia [1], los cuales quedarán atribuidos a las siguientes autoridades:

<u>Gestor de Servicios en la Nube (GSN) - CESTIC</u>
El rol de GSN del MDEF queda atribuido al CESTIC, según se define en [1], quien lo desempeñará sobre la base de sus unidades orgánicas. El GSN será responsable de: • Asegurar el aprovisionamiento, monitorización y funcionamiento de los servicios en la nube. • Garantizar que los servicios en la nube se integren eficazmente con los sistemas y aplicaciones del MDEF. • Monitorizar los acuerdos de nivel de servicio (SLA) de los proveedores de la nube. • Integrar los servicios en la nube en el proceso de gestión de servicios CIS/TIC. • Gestionar de forma activa la seguridad y los riesgos en la nube. • Implementar controles de seguridad administrativos y técnicos para garantizar el cumplimiento de las políticas de seguridad de la información del MDEF y garantizar que la información no se expone inadvertidamente a través de cualquier red pública. • Proporcionar informes de facturación y uso. • Administrar la identidad y el acceso. • Garantizar y acreditar el cumplimiento de las políticas de seguridad la información conforme a la establecido en el Esquema Nacional de Seguridad.

¹⁶ El mencionado análisis, precisamente, será el que se desarrolle en el Capítulo 4 del presente trabajo bajo la forma de ejercicio práctico que permita validar o probar el modelo de Nube MDEF propuesto.

Proveedor de servicios en la Nube (PSN) - CESTIC

El rol de PSN quedará atribuido al CESTIC cuando se trate de la nube privada, y a un proveedor o proveedores comerciales para la nube pública. El PSN será responsable de:

- Poner a disposición del Gestor de Servicios en la Nube (GSN CESTIC) los servicios en la nube, ya que este rol se centra en las actividades necesarias para proporcionar un servicio en la nube a usuarios (USN) y desarrolladores (DSN).
- Proporcionar los servicios de supervisión y administración.
- Proporcionar datos de auditoría del sistema gestionado.
- Desarrollar la implementación y el aprovisionamiento de servicios en la nube.
- Gestionar la seguridad y los riesgos en la nube e informar al gestor (GSN) y al auditor pertinente (ASN) en caso de que se sospeche o detecte un incidente de seguridad que afecte a la información del MDEF.
- Garantizar el cumplimiento de las políticas del MDEF para la protección de la información clasificada y no clasificada, y el Esquema Nacional de Seguridad. Las pruebas justificativas de este cumplimiento serán revisadas y aprobadas por el auditor pertinente (ASN).

Auditor de servicios en la Nube (ASN) - MCCE

El rol de ASN quedará atribuido al Mando Conjunto del Ciberespacio (MCCE), con objeto de asignar esta labor auditora a una entidad externa al CESTIC.

La función de ASN será responsable de evaluar el cumplimiento de diversos aspectos de la nube, tales como:

- Seguridad: definir los procesos de cumplimiento en la nube (procesos de acreditación, certificación y aprobación específicos de la nube).
- Verificación: establecer la evaluación y seguimiento de los acuerdos de nivel de servicio (SLA) relativos a la prestación de servicios en la nube, la operación del servicio, el rendimiento y la seguridad de la implementación en la nube.
- Medición: realizar auditorías para confirmar y medir, mediante indicadores, el cumplimiento de los niveles de servicio por parte del Proveedor de Servicios en la Nube (PSN) de conformidad con los términos y condiciones acordados.

Usuario de Servicios en la Nube (USN)

Usuario del MDEF que utiliza los servicios en la nube disponibles en el Catálogo de Servicios. Pertenecerán a los Ámbitos o al propio CESTIC.

Desarrollador de Servicios en la Nube (DSN)

Personal técnico responsable del desarrollo y la validación de las aplicaciones que se implementarán en el entorno de nube. Pertenecerán a los Ámbitos o al propio CESTIC.

Tabla 3-3 Resumen de roles y responsabilidades junto con su atribución para la Operación de la Nube MDEF (tomada de [1]).

3.3.3 Modelo de Operación

El modelo de Operación para la Nube MDEF que se muestra a continuación, proporciona una vista de alto nivel de las funcionalidades de la nube, los modelos de implementación, los modelos de servicios y los principales activos involucrados en la operación del servicio, así como los roles necesarios para la operación de dichos servicios:

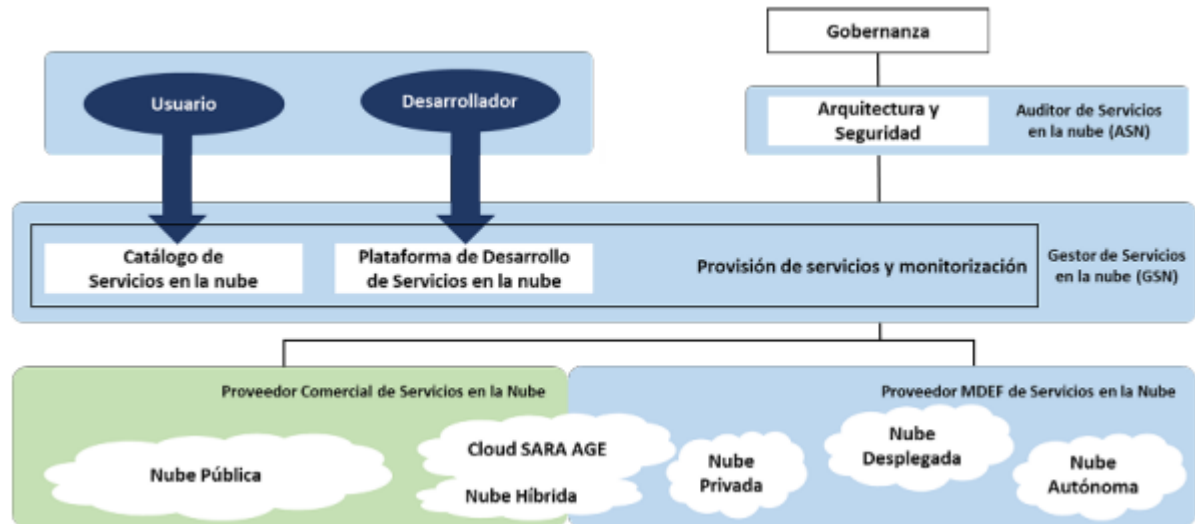


Figura 3-23 Modelo de Operación de servicios en la Nube MDEF (tomada de [1]).

Como componentes fundamentales de este Modelo de Operación deberán definirse y mantenerse completamente actualizados tres elementos básicos: los servicios residentes en la nube, los activos implicados y los clientes, o Ámbitos, destinatarios de estos servicios.

Con carácter general, definiremos:

- Catálogo de Servicios: relación de los servicios y las capacidades que se pueden prestar por los Equipos de Operaciones desde la Nube MDEF. Deberá contener, al menos:
 - Definición del servicio: nombre, categoría del servicio, descripción y nombre de la línea del servicio. Además deberá determinar de forma inequívoca si el servicio se opera desde nube privada, desde nube pública o desde Nubes de Terceros.
 - Características del servicio: responsable, valoración económica, disponibilidad, medios de acceso al servicio y modalidad de provisión.
 - Soporte a los clientes: identificación del responsable del soporte, horario de atención, formación para el uso correcto del servicio y procedimientos.

Este elemento constituirá un aspecto fundamental a la hora de determinar aquellos servicios sobre los cuales desarrollar una adecuada “Gestión del Servicio” (*Information Technology Service Management - ITSM*), bajo las siguientes perspectivas correspondientes con procesos de gestión de los servicios CIS/TIC del MDEF:

- Gestión de Incidencias y Peticiones.
- Gestión de Problemas.
- Gestión de Cambios.
- Gestión de los Niveles de Servicio.
- Gestión del Conocimiento de los Servicios.
- Gestión de la Continuidad del Servicio.

Se entiende que este Catálogo de Servicios quedará englobado dentro del Catálogo de Servicios General del MDEF en los que también se añadirían aquellos servicios residentes sobre la infraestructura tradicional y no migrados al entorno de nube.

- **Inventario de Activos:** se define como cualquier componente o recurso *hardware* o *software* que se requiera gestionar para poder entregar un servicio. Este elemento constituirá un aspecto fundamental a la hora de determinar aquellos activos sobre los cuales desarrollar una adecuada “Gestión de Activos” (*Information Technology Asset Management - ITAM*), bajo las siguientes perspectivas correspondientes con procesos de gestión de los activos CIS/TIC del MDEF:
 - Gestión de la Configuración (*Configuration Management Data Base - CMDB*).
 - Gestión de la Capacidad y la Disponibilidad.
 - Gestión de los Proveedores y Contratos.

En lo que se refiere a la monitorización de estos activos, se recomienda la centralización de la misma, buscando una solución única, consolidada e integrada para todos aquellos activos ubicados en los CPD del MDEF, relativos a la nube privada junto con la infraestructura tradicional. En cuanto a la nube pública, existen herramientas en la nube que permiten la monitorización a todos los niveles, y en muchas ocasiones sobre soluciones multi-proveedor, lo que facilita su operación al requerirse de un único servicio. Para cada caso particular y en función de los servicios desplegados deberá evaluarse esta posibilidad.

- **Ámbitos o clientes e Inquilinos o *Tenants*:** la aproximación a los clientes, o Ámbitos, desde el punto de vista de operación de la Nube MDEF, se realizará bajo el concepto de Inquilino o *Tenant*, según terminología del documento de la referencia [12] en su apartado de modelos de inquilinato [24], entendiéndose el mismo como una organización, unidad o grupo que utiliza los recursos proporcionados por el proveedor de servicios en la nube. En particular, consideraremos que cada Ámbito se corresponde con un Inquilino o *Tenant*. Hay diversas maneras de plantear cómo operar con los Inquilinos. La elección depende en gran medida de si se van a compartir recursos entre los mismos y cómo lo van a hacer. A la hora de operar, cuando se recibe una solicitud procedente de un Inquilino concreto, esta debe asignarse a la infraestructura que contenga los datos de ese Inquilino, tal y como se indica:

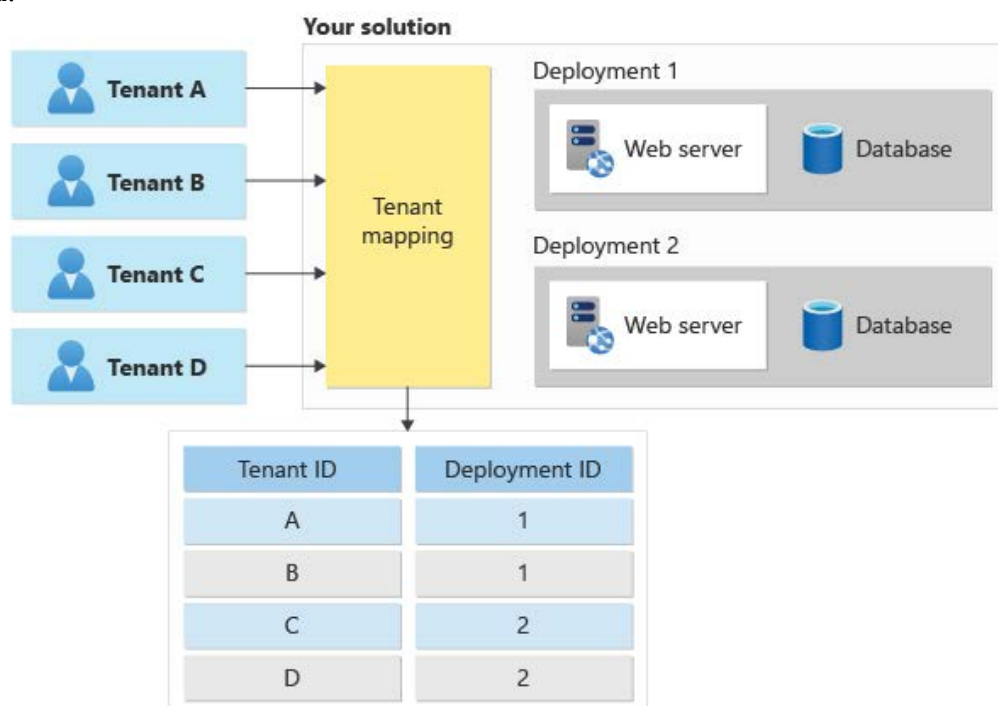


Figura 3-24 Representación de la asignación de recursos a un Inquilino (tomada de [24]).

La diferencia clave entre Inquilinos y modelos de operación radica precisamente en cómo se aplica el aislamiento entre recursos. Cuando varios Inquilinos comparten un único conjunto de infraestructura, se suele confiar en el código de la aplicación y en un identificador de Inquilino que está en una base de datos, para mantener separados los datos de cada Inquilino. Como se puede apreciar en la figura siguiente, el nivel de aislamiento que puede aplicarse entre Inquilinos es determinante, afectando a diversos factores tales como seguridad, rendimiento o coste, y será una característica a decidir para nuestro Modelo de Operación de Nube MDEF:

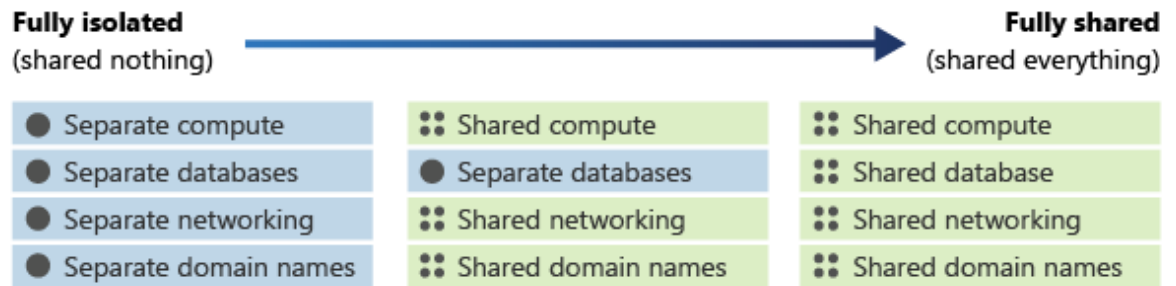


Figura 3-25 Representación del nivel de aislamiento de recursos entre Inquilinos (tomada de [24]).

Existirán, por tanto, diferentes modelos de Inquilino para la nube, cada uno con sus propias consideraciones:

- Inquilino Único: cada Inquilino o Ámbito tiene sus propios componentes, como *interfaz web*, *middleware* y base de datos, operando de manera independiente sin compartir recursos con otros.

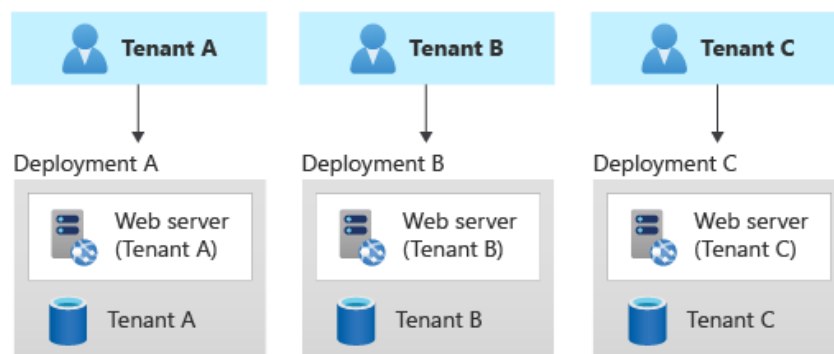


Figura 3-26 Representación del modelo de Inquilino Único (tomada de [24]).

Una ventaja clara de este modelo es que los datos de cada Inquilino están aislados, lo que reduce el riesgo de pérdida accidental. Además, es poco probable que unos Inquilinos influyan en el rendimiento del sistema de los otros, un problema que a veces se denomina problema de “vecino ruidoso” [25]. Por el contrario, si se usa este enfoque, la rentabilidad es baja ya que no se comparte ningún tipo de infraestructura entre los Inquilinos. Además, es probable que los mantenimientos de las aplicaciones, tales como actualizaciones de *software* o de configuración, se vuelvan más complicados.

- Multi Inquilino: en el extremo opuesto al modelo anterior se encontraría este otro modelo, en el cual varios Inquilinos o Ámbitos comparten la *interfaz web*, el *middleware* y la base de datos, de modo que se dispone de un único conjunto de infraestructura para mantener, el cual es utilizado por todos ellos.

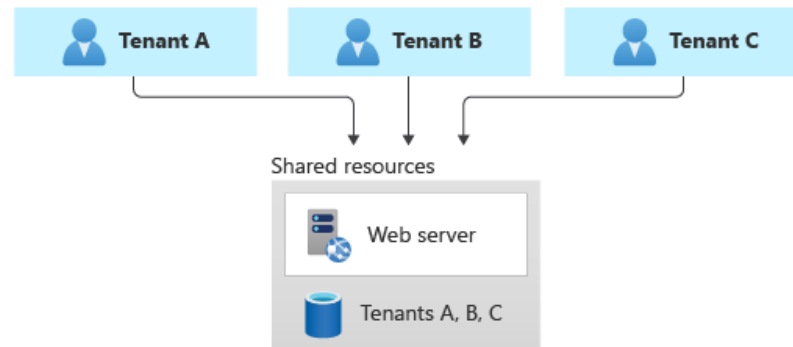


Figura 3-27 Representación del modelo de Multi Inquilino (tomada de [24]).

Este modelo presenta como ventaja principal el ahorro en su implementación, dado que el uso de una solución con componentes compartidos resulta menos costosa que usar recursos individuales para cada Inquilino. Además, si se requiere que un Inquilino tenga que mover sus datos hacia otro Inquilino, es posible que pueda hacerlo únicamente actualizando los identificadores y claves del Inquilino, sin necesidad de migrar datos entre dos implementaciones independientes. En el apartado de inconvenientes, debe tenerse en cuenta que este modelo no soluciona de forma nativa la separación de los datos de cada Inquilino y la posible pérdida de datos entre los Inquilinos. Para paliar este problema se deberá añadir una solución que permita administrar los datos de particionamiento. Además, se deberán tener en cuenta los efectos que puedan tener los Inquilinos individuales en el sistema general, como por ejemplo, el hecho de que un Inquilino de gran volumen intente realizar una consulta o una operación grande, lo cual podría afectar a otros Inquilinos. En el caso particular del MDEF está circunstancia podría darse por parte del Ejército de Tierra, el cual es un Ámbito comparativamente mucho mayor que el resto de Ámbitos presentes.

- Inquilino Mixto: este modelo representaría una aproximación intermedia a las dos anteriores, estableciéndose particiones verticales u horizontales entre Inquilinos o Ámbitos. Con este modelo todos ellos pueden compartir los componentes básicos, mientras que otros recursos específicos están separados en términos de datos y configuraciones.

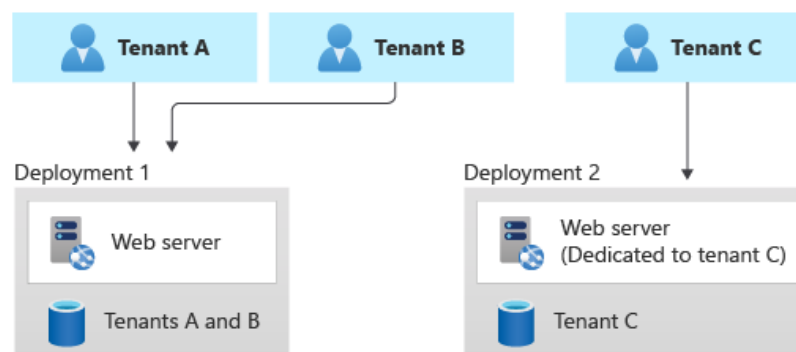


Figura 3-28 Representación del modelo de Inquilino Mixto con partición vertical (tomada de [24]).

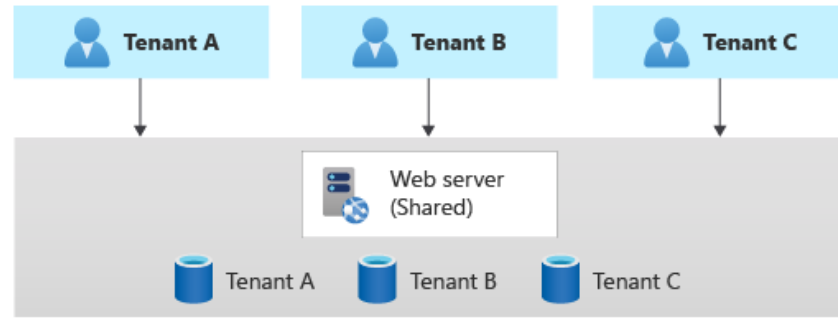


Figura 3-29 Representación del modelo de Inquilino Mixto con partición horizontal (tomada de [24]).

Estos modelos de tipo mixto representan un equilibrio adecuado entre las ventajas e inconvenientes expuestos en los dos modelos extremos (Inquilino Único y Multi Inquilino), permitiendo adaptarse de forma adecuada a las necesidades de operación de los Ámbitos del MDEF.

Debe tenerse en cuenta que, tal y como se ha adelantado, cada Ámbito del MDEF presenta características y casuísticas muy particulares tanto por volumen y dispersión de los usuarios como por características de los servicios a desplegar. Por este motivo es fundamental elegir el modelo de Inquilino adecuado según las necesidades específicas de los Ámbitos, y las opciones ofrecidas por cada proveedor de servicios en la nube, de modo que permita adaptarse a las distintas situaciones y requisitos. En nuestro caso, tanto para el Dominio de Seguridad DS0 como para el DS1, el modelo a implantar para operar sería un modelo de Inquilino Mixto con partición horizontal. De este modo cada uno de los Dominios de Seguridad quedaría agrupando a varios Inquilinos que comparten el mismo nivel de seguridad, con una *interfaz web* y *middleware* comunes, pero con bases de datos separadas para cada Ámbito.

El modelo de Inquilino Mixto con partición horizontal debería contribuir a reducir los mencionados problemas de “vecino ruidoso”, si se lleva a cabo una identificación anticipada acerca de qué Inquilino en particular representa la mayor parte de la carga de trabajo y se dota al sistema de los recursos necesarios que eviten sobrepasar el umbral de capacidad. A pesar de todo, debe tenerse en cuenta que este problema de “vecino ruidoso” se puede llegar a producir incluso cuando cada Inquilino individual consume cantidades relativamente pequeñas de la capacidad del sistema, pero el uso de recursos colectivos de muchos Inquilinos da como resultado un pico en el uso general. Esta situación puede suceder si hay varios Inquilinos que tienen patrones de trabajo similares o si no se ha proporcionado suficiente capacidad para la carga colectiva en el sistema:

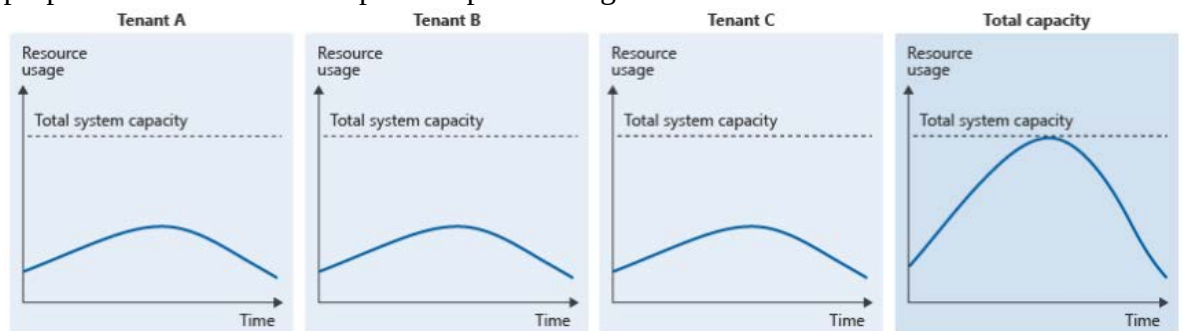


Figura 3-30 Representación del problema de “vecino ruidoso” en un modelo de Inquilino Mixto (tomada de [25]).

En conclusión, el modelo de operación elegido para los clientes o Ámbitos consistiría en adoptar una implementación de Inquilino Mixto con partición horizontal en la que se asignase un Inquilino o *Tenant* para cada uno de los Ámbitos. Este modelo permitiría proporcionar el equilibrio suficiente entre funcionalidad y eficiencia en la operación, efectuando únicamente una partición horizontal a la hora de separar las bases de datos para cada uno de los Ámbitos. Otras capacidades tales como el cómputo, las comunicaciones de red o el dominio de red, se mantendrían de forma común para todos los Ámbitos a semejanza de como se lleva a cabo en la infraestructura tradicional en la cual, por ejemplo, se cuenta con un único Directorio Activo llamado MDEF.ES.

3.3.4 Racionalización y control del gasto de Operación

A la hora de hacer uso de recursos de nube pública para poder operar, según la estructura y modelo de Operación de la Nube MDEF definidos, debe tenerse en cuenta que dichos recursos, proporcionados por un único proveedor o en formato multi-proveedor, conllevan un coste por servicio.

Aunque esto pueda resultar una obviedad, no es menos obvio que la diversidad de Ámbitos que pueden hacer uso de la Nube MDEF va a exigir un control del gasto de Operación, para lo cual deberán establecerse mecanismos de monitorización y control de dicho gasto.

Para hacer frente al coste de los recursos de nube pública existen diferentes mecanismos de facturación, existiendo la flexibilidad de poder cambiar entre ellos según las necesidades de cada momento.

De modo general podríamos establecer dos categorías principales de facturación:

- Instancias reservadas en nube pública (por un tiempo acordado, normalmente un plazo de varios años). Modalidad utilizada para proyectos de envergadura y con patrones de uso conocidos. Se trataría de una visión a largo plazo del empleo de los recursos de nube pública.
- Pago por uso de nube pública (bajo demanda). Modalidad utilizada para situaciones de desbordamiento y despliegues iniciales. Se trataría de una visión a corto plazo del empleo de los recursos de nube pública.

Como aproximación inicial se consideraría contar con una serie de instancias reservadas según las necesidades de los Ámbitos, las cuales se complementarían con capacidades adicionales bajo demanda destinadas a hacer uso de las mismas en caso de situaciones puntuales y sobrevenidas.

Para poder materializar la contratación de estas modalidades, se deben establecer suscripciones con el correspondiente proveedor o proveedores de servicios de nube pública. Las suscripciones son las unidades de gestión, facturación y escalabilidad, a través de las cuales se permite una organización de los servicios y una fácil facturación.

A su vez, estas suscripciones deben quedar vinculadas a una cuenta de gestión, de manera que una cuenta con múltiples suscripciones permite hacer uso de diferentes modelos de facturación para cada una de ellas, permitiéndose definir limitaciones en el uso. Dado el rol de “Gestor de Servicios en la Nube” (GSN), asignado de manera unívoca al CESTIC según el documento de la referencia [1], se considera que lo más adecuado para operar en la Nube MDEF es la creación de una cuenta principal sobre la que se pueda realizar la facturación conjunta de todos los Ámbitos.

Esta aproximación de desplegar todos los servicios sobre una misma cuenta principal puede traducirse en ahorro de costes por volumen de servicios contratados, dado que todo lo que se contrate formará parte de la misma cuenta principal. Si posteriormente se requiere una mayor granularidad en el detalle de los costes por Ámbito, existen herramientas implantadas por los propios proveedores de nube pública que pueden facilitar esa tarea.

En cuanto a la financiación de los gastos, a la hora de operar mediante un modelo basado en nube, los costes derivados de los gastos de capital asociado a inversión económica en tecnología a largo plazo generados por la adquisición y el mantenimiento de la infraestructura y las instalaciones (*Capital Expenditure - CapEx*) van a disminuir, mientras que, por el contrario, los gastos de tipo operativo derivados del alquiler de la infraestructura o servicios a medida que se necesitan, ya sea cómputo, almacenamiento, red o cualquier otro servicio o recurso (*Operational Expenditure - OpEx*) van a aumentar. En líneas generales:

- *CapEx* se refiere a los gastos realizados con la expectativa de un beneficio futuro. Se manifiesta, entre otros, como:
 - Adquisiciones de activos: asociados con la adquisición de máquinas o infraestructura nueva.
 - Revisiones mayores: actualizaciones profundas que extienden la vida útil de un activo o aumentan su valor.
 - Inversiones tecnológicas: integración de nuevas tecnologías.
- *OpEx* representa los gastos diarios derivados de ejecutar y mantener las operaciones dentro de una organización. Se manifiesta, entre otros, como:
 - Mantenimientos rutinarios: tareas de mantenimiento predictivo, preventivo y reactivo.
 - Costes de mano de obra: salarios, beneficios, capacitación y otros costes asociados al personal.
 - Servicios públicos y consumibles: relacionados con energía y otros consumibles.
 - Licencias de *software*: cuotas recurrentes por el consumo de recursos *software*.

Es fundamental tener claro este cambio de enfoque en los gastos para poder financiar de forma efectiva el paso o transición a un modelo de nube desde un modelo basado puramente en infraestructura tradicional ya que, en los primeros ejercicios económicos a desarrollar, se van a tener que reforzar una serie de partidas económicas en detrimento de otras que deberían disminuir. A modo de resumen:



Figura 3-31 Comparativa de la diferente naturaleza de los gastos *CapEx* y *OpEx* (tomada de [26]).

Como herramienta de base para obtener unos adecuados análisis, comparativas y ahorros de costes relativos a los recursos de nube pública, se dispone del conocido como servicio de Gestión de Costes (*Cost Management*)¹⁷, el cual se encuentra presente y a disposición de sus clientes en los principales proveedores (*Microsoft Cost Management* [12] y *AWS Billing & Cost Management* [27]) proporcionando la capacidad de comprobar rápidamente los costes de los recursos, crear alertas basadas en el gasto y presupuestos que se pueden usar para automatizar la administración de gastos. El análisis de costes es un subconjunto de *Cost Management*, el cual proporciona información visual de los costes del proveedor comercial pudiéndose identificar fácilmente el coste total de varias formas diferentes, tales como por ciclo de facturación, empleo de un determinado recurso, etc.



Figura 3-32 Representación del servicio de *Microsoft Cost Management* para los recursos de nube pública junto con sus funcionalidades asociadas (tomada de [12]).

Dentro de las funcionalidades de la herramienta de *Cost Management* uno de los elementos claves para la Operación de la Nube MDEF lo constituyen las alertas de costes. Los principales tipos de alertas que pueden definirse a la hora de operar son:

- Alertas presupuestarias: las alertas de presupuesto lanzan un aviso cuando el gasto, en función del parámetro de uso o de coste, alcanza o supera un importe definido en la condición de alerta del presupuesto. Un presupuesto es el elemento en el que se establece un límite de gasto. Se pueden establecer presupuestos en función de una suscripción, un grupo de recursos, un tipo de servicio u otros criterios. Al establecer un presupuesto, también se pueden definir alertas vinculadas al mismo, de modo que cuando se alcanza el nivel establecido, se activará una alerta presupuestaria que se mostrará en el área de alertas de costes.

Esta posibilidad, para el caso particular del CESTIC como GSN, adquiere especial importancia ya que las contrataciones en ningún caso pueden exceder el importe fijo definido que haya para las mismas. En este caso se requiere hacer un seguimiento exhaustivo y riguroso, no ya únicamente del consumo realizado, sino también de la previsión de mismo. En este caso, desde el punto de vista de Gestión del Coste, se considera procedente categorizar dos tipos de servicios¹⁸:

- Servicios que sea necesario mantener en todo momento.
- Servicios que no sea necesario seguir manteniendo en el caso de alcanzarse un umbral de alerta presupuestaria definida (por ejemplo, un consumo superior al 80%).

¹⁷ Gestión de Costes (*Cost Management*): mecanismo encargado de proporcionar un cuadro de mando asociado a los costes relativos al empleo de recursos de nube pública.

¹⁸ En el Capítulo 4 del presente trabajo se ahondará en los criterios de clasificación de los servicios, ya que este aspecto constituye un importante condicionante a la hora de determinar su capacidad para ser migrados a un entorno de nube.

En el caso de alcanzarse cierto límite preestablecido y configurado, el procedimiento habitual pasaría por informar al Ámbito responsable de dichos servicios y consensuar algún tipo de acción, tal como la parada de entornos o la solicitud de ampliación del presupuesto.

Además de lo comentado, los proveedores de nube pública proporcionan la posibilidad de un uso más avanzado de los presupuestos permitiendo que las condiciones presupuestarias desencadenen mecanismos automáticos que suspendan o modifiquen los recursos una vez se produzca la condición definida. Para los servicios que sea necesario mantener en todo momento no se recomienda el uso de esta funcionalidad, pudiendo sí ser aplicable para los servicios que no sea necesario seguir manteniendo en el caso de alcanzarse un umbral presupuestario o entornos de prueba y desarrollo, siempre y cuando quede consensuado con el Ámbito correspondiente.

- Alertas de cuotas de gasto por Ámbito: este tipo de alertas se activan cuando el gasto del Ámbito en cuestión alcanza un umbral fijo de la cuota que tiene asignada (por ejemplo, el 50 ó 75% de la cuota).

Como complemento para este control de consumo basado en alertas aparece un concepto fundamental que son las etiquetas. Las etiquetas de recursos son otra forma de organizar los recursos, además de la propia organización que ya pueda estar definida vía suscripción o grupo de recursos, siendo capaces de proporcionar información adicional, o metadatos, sobre los recursos. Estos metadatos son útiles para los aspectos siguientes:

- Gestión de recursos: permiten localizar y actuar sobre los recursos asociados a cargas de trabajo, entornos, unidades tipo Ámbito y propietarios específicos.
- Gestión y optimización de costes: permiten agrupar recursos para generar informes sobre los costes, asignar centros de costes internos, realizar un seguimiento de los presupuestos y pronosticar el coste estimado.
- Gestión de operaciones: permiten agrupar los recursos según la importancia de su disponibilidad para la organización. Esta agrupación ayuda a formular Acuerdos de Nivel de Servicio (SLA)¹⁹.

En cuanto al modelo de consumo comentado para el caso de nube pública, sería deseable adoptar un modelo similar y a medida del CESTIC, como GSN, para el caso de la nube privada, de modo que permitiese tener un control exhaustivo de la utilización de los recursos de la nube privada por parte de cada uno de los Ámbitos. Para este control y gestión de los recursos de la nube privada, el CESTIC puede plantearse diferentes mecanismos, algunos ya extensamente utilizados por diferentes organizaciones, o directamente desarrollar y definir uno a medida y personalizado para su uso particular.

Dado que en la actualidad no se dispone de ningún mecanismo para este propósito a nivel de infraestructura tradicional, se podría comenzar por la aplicación de un modelo de consumo basado en Unidades de Recurso (*Resource Units - RU*), con el que se podría conocer y asignar de manera eficiente el consumo de recursos a los diferentes Ámbitos durante la renovación y adquisición de infraestructura.

¹⁹ Acuerdo de Nivel de Servicio (*Service Level Agreement - SLA*): es un acuerdo escrito entre un proveedor de servicio y su cliente con el objetivo de fijar el nivel acordado para la calidad de dicho servicio. El *SLA* es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

El modelo de consumo basado en *RU* debería presentar, en una primera versión, un catálogo limitado a elementos clave, tales como CPU, memoria, almacenamiento y bases de datos, evitando detalles operativos de bajo nivel, aunque sí incorporándolos implícitamente (necesidades de *backup*, licenciamiento, etc.), con la posibilidad de poder evolucionarse a futuro según las necesidades que pudieran surgir, y con el propósito final de asociar estas *RU* a un valor económico que pudiera dar lugar a un sistema de facturación dirigido a los Ámbitos. De este modo, el CESTIC podría proporcionar una facturación detallada a cada Ámbito tanto a nivel de consumo de infraestructuras de nube privada de los CPD del MDEF como de utilización de recursos en nube pública, de uno o varios proveedores comerciales. Si bien el propósito último de esta facturación no estaría ligada a un propósito recaudatorio, sí podría constituir un excelente mecanismo para racionalizar el gasto y facilitar una mejor planificación del recurso financiero dedicado a la Nube MDEF.

Adicionalmente a lo comentado, no debe dejar de mencionarse en este apartado relativo al consumo la aproximación dirigida a la optimización del gasto basada en *FinOps* [28]. Este aspecto, nuevamente, no solo aplica para el caso de servicios desplegados en nube pública, sino también para el caso de nube privada, e incluso para la infraestructura tradicional del MDEF.

FinOps es un marco de buenas prácticas destinado a administrar los gastos operativos de los costes derivados de la nube. Normalmente va a estar ligado al empleo de herramientas de administración de costes en la nube, como la ya mencionada *Cost Management*. Su planteamiento se articula en la secuencia siguiente:

- Analizar y realizar un seguimiento del gasto en la nube.
- Identificar las oportunidades de ahorro de costes.
- Asignar costes a equipos, proyectos o productos específicos.

Implica la colaboración entre los equipos financieros, tecnológicos y empresariales para establecer y aplicar directivas y procesos que permitan a los equipos realizar un seguimiento, analizar y optimizar los costes de la nube. En definitiva, se pretende ajustar el gasto derivado de la nube a los objetivos de la organización, encontrando un equilibrio entre la optimización de costes y el rendimiento.

El siguiente cuadro presenta un resumen de este marco de buenas prácticas, emitido por la *FinOps Foundation*, organización sin ánimo de lucro dedicada a la administración y optimización de costes en la nube a través de procedimientos recomendados, educación y estándares:



Figura 3-33 Marco de buenas prácticas *FinOps* (tomada de [28]).

Microsoft se unió a la *FinOps Foundation* en febrero de 2023 [29], momento desde el cual participa activamente en múltiples grupos de trabajo, contribuye al contenido de la fundación e integra las enseñanzas extraídas de la comunidad *FinOps* en los productos y directrices de *Microsoft*. Por este motivo se considera que la referencia *Microsoft Azure Well-Architected Framework* [12], y en particular la herramienta *Microsoft Cost Management*, se encuentra totalmente alineada con el marco de buenas prácticas de *FinOps* para la optimización del gasto de nube.

3.4 Seguridad de la Nube MDEF

3.4.1 Enfoque de Seguridad Confianza Cero (Zero Trust)

Para abordar la Seguridad en la Nube MDEF debemos enfocarnos en dos cuestiones fundamentales, por un lado, el hecho de que el personal del MDEF pueda llevar a cabo su trabajo desde ubicaciones físicas externas a las propias sedes del MDEF, y por otro la realidad de que los servicios a los que debe acceder este personal del MDEF se trasladen, efectivamente, a la nube. Ambas cuestiones se encuentran íntimamente relacionadas, y rompen con el tradicional paradigma de la seguridad del MDEF, sustentada fundamentalmente en la protección basada en la securización del emplazamiento físico y con escasa o nula posibilidad de trabajar de manera remota.

En la situación actual de provisión de servicios desde infraestructura tradicional, con carácter general, los usuarios de tipo remoto hacen uso de Redes Privadas Virtuales (*Virtual Private Network - VPN*) ²⁰ para acceder a recursos del MDEF a través de Internet. Sin embargo, el servicio de acceso remoto mediante *VPN* presenta varios desafíos:

- Es difícil gestionar y ampliar su infraestructura local.
- Es costoso de desplegar en un amplio conjunto de ubicaciones.
- Resulta ineficaz redirigir el tráfico de red hacia aplicaciones privadas.

Para superar adecuadamente estos retos se requiere un enfoque diferente. La solución debe ser fácil de gestionar y escalar, proporcionar una cobertura rentable y omnipresente, y ofrecer el mejor rendimiento para las aplicaciones, independientemente de su ubicación. Para avanzar en esta dirección, se debe proteger la información, los servicios y el personal del MDEF, con un nuevo enfoque, sin importar dónde se encuentren, y posibilitando precisamente por este motivo transitar hacia un modelo de nube. De esta manera, se ganará en agilidad, permitiendo romper los silos internos, fortaleciendo la colaboración, y elevando la consciencia de que la seguridad es responsabilidad de todos.

En este contexto se sitúa el enfoque de Confianza Cero (*Zero Trust*). Este concepto se fundamenta en considerar de antemano que la seguridad ha sido potencialmente comprometida, estableciendo así una filosofía de funcionamiento basada en el concepto de nunca confiar y siempre verificar, aplicando la desconfianza por defecto. De forma general, se apoyará en los siguientes principios básicos:

- Verificar explícitamente: proporcionado autenticación y autorización en función de múltiples datos de seguridad, incluida la identidad del usuario, la fortaleza del método de autenticación, la ubicación, el estado del dispositivo y las anomalías.
- Conceder privilegios mínimos: limitando el acceso de los usuarios a los privilegios y tiempo necesarios, y combinando este acceso con políticas adaptativas basadas en el riesgo.
- Asumir la brecha: minimizando el impacto, segmentando el acceso, garantizando la protección de datos extremo a extremo y aprovechando la analítica para detectar amenazas.

²⁰ Red Privada Virtual (*Virtual Private Network - VPN*): tecnología de red de que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet. Permite que un ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Todo ello se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

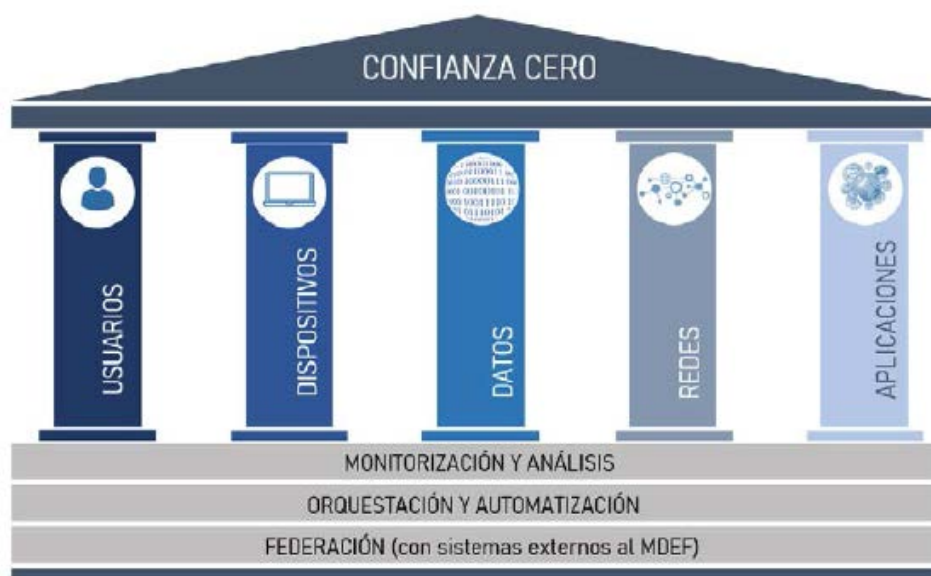


Figura 3-34 Modelo de referencia del concepto de seguridad Confianza Cero (Zero Trust) (tomada de [22]).

En definitiva, se deben contemplar nuevos marcos de seguridad que consideren las necesidades de protección, y que logren complementarse para incorporar la Estrategia de implantación del concepto de seguridad Confianza Cero (*Zero Trust*) [22] a la Nube MDEF. Ambas iniciativas, Confianza Cero (*Zero Trust*) y Nube MDEF, tal y como veremos a lo largo del desarrollo de este aspecto de seguridad en la nube, se encuentran íntimamente relacionadas, lo cual debe motivar que se habiliten herramientas de seguridad específicamente destinadas al modelo de nube, superando el concepto de seguridad actual.

3.4.2 Herramientas de Seguridad

Para logra implantar, de modo completo y efectivo, la seguridad de la Nube MDEF deberemos ser capaces de desplegar otros sistemas y tecnologías completamente integradas en el mencionado concepto Confianza Cero (*Zero Trust*). Concretamente nos referiremos a dos grupos de ellas, complementarios entre sí, como las principales herramientas de seguridad focalizadas en el modelo de nube, el Servicio Perimetral de Acceso Seguro (*Secure Access Service Edge - SASE*) y el Perímetro de Servicio de Seguridad (*Security Service Edge - SSE*):

- *SASE* quedará referido a un conjunto de soluciones y herramientas de seguridad basadas en la nube con capacidad de ofrecer soluciones integrales para las necesidades dinámicas de acceso seguro por parte de los usuarios autorizados, incluidas las redes definidas por *software*. Consiste en un modelo tecnológico de seguridad basada en identidad de usuarios y dispositivos, que maximiza el valor y la utilidad de las tecnologías de nube.
- *SSE* quedará definido como un subconjunto de *SASE* que se centra únicamente en los servicios de seguridad necesarios de una plataforma en la nube de tipo *SASE*. *SSE* está integrado por una serie de servicios de seguridad que sirven de fundamento al modelo de seguridad de *SASE*.

El conjunto de soluciones *SASE* incluye, entre otras, la solución de Acceso a Red con Confianza Cero (*Zero Trust Network Access - ZTNA*). Se trata de un modelo de acceso a red que aplica el principio de Confianza Cero a las redes, es decir, ningún usuario, dispositivo o aplicación se va a considerar confiable por defecto, sino que se verificará su identidad y autorización antes de acceder a los recursos. El objetivo es reducir la superficie de ataque y evitar que los intrusos puedan moverse libremente por el sistema, una vez hayan accedido a él. Es, por tanto, la principal herramienta para la implantación del concepto de Confianza Cero (*Zero Trust*) en la Nube MDEF.

Todo ello supone que, tal y como ya se adelantó al hablar de la Estructura de Operación de la Nube MDEF, la Gestión de Identidades y Accesos (*Identity and Access Management – IAM*) constituya la “piedra angular” para abordar el aspecto de Seguridad de la Nube MDEF. Este condicionante suponía, de hecho, suprimir este componente de los mencionados en el modelo de responsabilidad compartida para la provisión de servicios desde nube pública, según venía establecido en la referencia [1]. Este aspecto de la Gestión de Identidades, precisamente por su importancia, será desarrollado en el presente trabajo como un punto específico del apartado de seguridad.

Para alcanzar el óptimo despliegue de estos modelos de seguridad, se integrarán soluciones que ofrezcan acceso seguro a los recursos de una forma dinámica y adaptable al riesgo asociado. Entre otras herramientas de seguridad, y en línea con lo especificado en la referencia [22], se habilitarán el Agente de Seguridad de Acceso a la Nube (*Cloud Access Security Broker - CASB*), la capacidad de Inspección Basada en Riesgos (*Risk-Based Inspection - RBI*), la capacidad de Prevención de Filtración y Pérdida de Datos (*Data Loss Prevention - DLP*), y la Analítica de Comportamiento de Usuario y Entidad (*User and Entity Behaviour Analytics - UEBA*):

- *CASB (Cloud Access Security Broker)* es un intermediario entre los usuarios y los servicios en la nube que ofrece una serie de funciones de seguridad, tales como el control de acceso, la prevención de pérdida de datos, el cifrado, la detección de amenazas y el cumplimiento normativo. *CASB* se integra en *SASE* y *SSE* mediante la creación de una capa de protección unificada para todos los recursos en la nube, ya sean públicos o privados. De esta forma, *CASB* facilita la adopción de la nube sin comprometer la visibilidad, el control y la seguridad de los datos y las aplicaciones.
- *RBI (Risk-Based Inspection)* es un enfoque que utiliza el análisis de riesgo para determinar el nivel de acceso que se otorga a los usuarios o dispositivos que intenten acceder a los recursos del MDEF. El objetivo es minimizar el riesgo de que se produzcan brechas de seguridad o fugas de datos por parte de actores maliciosos o usuarios descuidados. El nivel de acceso se basa en factores como la identidad, el contexto, el comportamiento y la confianza del usuario o dispositivo.
- *DLP (Data Loss Prevention)* es un conjunto de herramientas y políticas que tienen como finalidad prevenir la pérdida, el robo o la exposición no autorizada de datos sensibles o críticos para el MDEF. El objetivo es proteger la información que así lo requiera, y cumplir con las normativas legales y regulatorias sobre privacidad y seguridad de datos. *DLP* se puede aplicar tanto a los datos en reposo (almacenados en dispositivos o servidores), como a los datos en tránsito (transferidos por redes o por Internet) o a los datos en uso (procesados por aplicaciones o usuarios).
- *UEBA (User and Entity Behaviour Analytics)* es una tecnología que analiza el comportamiento de los usuarios y las entidades para detectar anomalías, riesgos y amenazas. Se trata de un análisis de seguridad que utiliza el aprendizaje automático y el análisis estadístico para detectar comportamientos anómalos o sospechosos de los usuarios y las entidades dentro de una red. El objetivo de *UEBA* es identificar amenazas internas, ataques dirigidos, compromiso de cuentas, fraude y otras actividades maliciosas, que pueden poner en riesgo la seguridad del MDEF. Se basa en el establecimiento de un perfil de comportamiento normal para cada usuario y entidad, y luego comparar las actividades actuales con ese perfil para detectar desviaciones significativas. Permite la respuesta ante ataques realizados mediante técnicas novedosas, *malware* con firma desconocida, etc., ya que no se basa en reaccionar contra patrones o *malware* conocidos, sino en la proactividad a la hora de detectar ataques ante comportamientos inusuales.

De esta forma, el papel de *UEBA* en *SASE* y *SSE* es proporcionar una visión más profunda y precisa del comportamiento de los usuarios y las entidades, tanto en la nube como en la infraestructura tradicional, y alertar sobre posibles incidentes de seguridad o incumplimientos de políticas. También puede contribuir a optimizar el rendimiento de la infraestructura, al identificar actividades innecesarias o ineficientes.

En conclusión, el empleo combinado de las herramientas de seguridad presentes en *SASE* y *SSE* está llamado a dar cobertura a las necesidades de seguridad de la Nube MDEF, con la finalidad de proteger todos los activos del MDEF incluyendo datos, infraestructura, sistemas y servicios. Para ello, deberán ser capaces de proporcionar un acceso seguro y fiable a los servicios, las aplicaciones y los datos, aplicando principios de Acceso a Red con Confianza Cero (*Zero Trust Network Access - ZTNA*). Todo ello preservando el acceso a los activos por medio de un conjunto de funciones de Autenticación, Autorización y Responsabilidad (*Authentication, Authorization & Accounting - AAA*) en cada usuario y dispositivo.

Estas herramientas serán además capaces de llevar a cabo inspecciones en profundidad de toda la infraestructura, pudiendo ofrecer protección ante amenazas conocidas y desconocidas, aprovechando las tecnologías de prevención de amenazas basadas en Inteligencia Artificial (*Artificial Intelligence - AI*) y Aprendizaje de Máquina (*Machine Learning - ML*).

3.4.3 Gestión de Identidades

Según se ha expuesto con anterioridad, la pieza clave a la hora de implantar el concepto de Confianza Cero (*Zero Trust*) y, en consecuencia, organizar la Seguridad de la Nube MDEF, es la identidad.

Actualmente, el MDEF dispone de una plataforma que gestiona las necesidades de identidad en la infraestructura tradicional. Esta plataforma, cuenta con una serie de componentes, y está diseñada para dar cobertura a las necesidades del ciclo de vida de identidades dentro de la Infraestructura para Baja Clasificación de la I3D. En la Infraestructura para Alta Clasificación, existen otros componentes que cubren las mismas necesidades pero que, por motivos de seguridad, están desconectados de los de Baja Clasificación. Como se ha mencionado anteriormente, al tratar el aspecto de Gestión de Identidades y Accesos (*Identity and Access Management – IAM*), el objetivo último sería el de contar con una identidad de usuario única (híbrida) para el DS0, al estar integrado tanto para el entorno de nube pública como de nube privada. Este es, realmente, el problema de fondo a abordar ya que, para el DS1 por condicionantes de seguridad, siempre deberemos permanecer en un entorno de nube privada en el cual la Gestión de Identidades se llevará a cabo de manera unilateral por el CESTIC sin ningún tipo de responsabilidad compartida con el proveedor comercial. Por este motivo, en el presente punto nos centraremos en el Dominio de Seguridad No Clasificado o DS0, por ser el que aglutina capacidades de nube pública y nube privada, y además ser el único que permite su acceso desde ubicaciones físicas externas a las propias sedes del MDEF.

Por tanto, y como punto de partida para abordar la problemática de la Gestión de Identidades, enumeraremos los principales componentes de la plataforma de identidad de la Infraestructura para Baja Clasificación de la I3D:

- **DICODEF** (Directorio Corporativo de MDEF). El núcleo de la identidad en la Infraestructura para Baja Clasificación de la I3D es proporcionado por DICODEF. Básicamente, se encarga de proporcionar los servicios de directorio, de manera que todas las identidades residen en DICODEF. De este modo, todo el personal militar y civil que trabaja en el MDEF, junto con el personal que es colaborador externo, dispone de una identidad que reside en este directorio. DICODEF también se encarga de gestionar el ciclo de vida de las identidades (altas, bajas, modificaciones, roles de acceso, etc.), a partir de su integración con otros sistemas como el Sistema de Información de Personal del MDEF (SIPERDEF).

De manera resumida los flujos de las identidades de los usuarios son:

- El personal de la plantilla del MDEF se obtiene de SIPERDEF, con este interfaz se crean las identidades de manera automática para el personal militar y funcionarios. Esta conexión también permite recibir información de esas identidades, como son el empleo o destino, y gestionar eventos como son el alta, baja, cambio de destino, etc.
- El personal externo se gestiona de manera manual utilizando el portal de administración de DICODEF, desde este portal se gestiona el ciclo de vida de las identidades correspondientes al personal externo.
- Como parte de la gestión de este ciclo de vida de identidades, DICODEF se conecta con otros elementos de la plataforma de identidades como es el Directorio Activo (MDEF.ES), para las altas, bajas y modificaciones de usuarios.

Otra capacidad que proporciona DICODEF son los servicios de autenticación y autorización para usuarios. Para ello, dentro de DICODEF todos los usuarios tienen credenciales DICODEF, usuario y contraseña, permitiendo además mecanismos de validación de estas credenciales: *LDAP*²¹, *interfaz web* o integración mediante *API*. Estas credenciales DICODEF se usan como mecanismo de autenticación en múltiples aplicaciones y servicios, como el servicio de navegación. Relacionado con estas credenciales, DICODEF mantiene la política de complejidad, caducidad y bloqueo de credenciales. Además de estas credenciales de usuario y contraseña, algunos usuarios disponen de certificados digitales emitidos por el Servicio de Infraestructura de Clave Pública del MDEF (PKIDEF). En este caso, DICODEF permite también la autenticación mediante la Tarjeta Electrónica del MDEF (TEMD), la cual dispone de una clave privada y un certificado de autenticación emitido por PKIDEF.

- SIPERDEF (Sistema de Información de Personal del MDEF). Constituye la fuente maestra y confiable de información de la identidad para el conjunto de los usuarios del MDEF, salvo los colaboradores externos. Aunque la mayoría de los servicios y capacidades de SIPERDEF no son relevantes para el objeto del presente trabajo, sí que resulta conveniente resaltar que DICODEF utiliza como fuente confiable para la gestión del ciclo de vida de la identidad la información que obtiene desde SIPERDEF.
- Directorio Activo (*Active Directory* - MDEF.ES). La infraestructura de Directorio Activo en la Infraestructura para Baja Clasificación de la I3D es otro componente clave de la identidad dentro del MDEF. Integrado ya con DICODEF, el Directorio Activo sirve como dominio de seguridad para los equipos *Windows* y además permite la autenticación para las aplicaciones integradas en el dominio. A alto nivel proporciona los siguientes servicios:
 - Servicios de directorio.
 - Gestión de los puestos de trabajo.
 - Autenticación y autorización.
 - Servicios de libreta de direcciones para el correo electrónico.

²¹ Protocolo ligero de acceso a directorios (*Lightweight Directory Access Protocol* - *LDAP*): protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse, aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.).

- PKIDEF (Servicio de Infraestructura de Clave Pública del MDEF). Tiene una doble relación con los servicios de identidad de la Infraestructura para Baja Clasificación de la I3D: consumidor de servicios y proveedor de autenticación fuerte. PKIDEF se conecta con DICODEF para la gestión del ciclo de vida de los certificados digitales, de manera que la información que acaba formando parte de los diferentes certificados (autenticación, cifrado, firma con no repudio) se obtiene de DICODEF. PKIDEF proporciona tanto la emisión de certificados, como la emisión de *CRL*²² y servicios de validación, ya sea mediante *OCSP*²³ o *interfaz web*. Un componente relevante de PKIDEF es la TEMD (tarjeta electrónica del MDEF), la cual constituye el soporte criptográfico para los certificados que emite PKIDEF. La TEMD se puede usar como mecanismo de autenticación fuerte por tratarse de una tarjeta criptográfica (algo que se posee), que además requiere de un PIN (algo que se conoce), para las operaciones de autenticación y firma.

Desde un punto de vista de gobierno, la provisión, mantenimiento y eliminación de cuentas de usuario, grupos o dispositivos para la Nube MDEF debe ser un proceso automático gobernado desde DICODEF. Para ello debe contarse con un mecanismo que permita identificar que elementos deben tener identidad en la nube, de modo que sea similar al que permite identificar que un determinado usuario debe tener cuenta en MDEF.ES, buzón de correo electrónico, navegación por Internet, etc.

Más allá del detalle del mecanismo de implementación por el cual finamente se optase (podría ser un *Tenant* específico a tal efecto, proporcionado por el proveedor comercial), lo verdaderamente relevante es establecer a DICODEF como fuente de confianza para esta gestión de identidades, en línea con los parámetros de funcionamiento de la actual Infraestructura para Baja Clasificación de la I3D. Estos parámetros establecen, precisamente, que DICODEF sea la fuente de identidades de Directorio Activo (MDEF.ES) en la parte de nube privada, por lo que también debería serlo para la parte de nube pública.

De esta manera, y una vez se decidiese el mecanismo de implementación, sólo las cuentas de usuario, los grupos y los dispositivos designados de esta manera, se provisionarían y sincronizarían con la nube pública. Este mecanismo permitiría que, por ejemplo, cuando un usuario causase baja en DICODEF automáticamente la cuenta en nube pública fuese eliminada, que cuando algún elemento de la identidad cambie éste se actualice igualmente, y que cuando se cambie la pertenencia de un grupo desde el entorno de nube privada, esta pertenencia se actualice en el entorno nube pública.

En conclusión, se requiere una solución de Gestión de Identidades para la Nube MDEF basada en “identidad híbrida”, entendiendo la misma como aquellos servicios de identidad que abarcan funcionalidades tanto locales, en entorno de nube privada, como en la nube pública, y que crean una identidad de usuario común para la autenticación y autorización en todos los recursos, independientemente de su ubicación y entorno privado o público.

3.4.4 Identidad Híbrida

Según se ha explicado, la Nube MDEF se configura en su Dominio de Seguridad No Clasificado o DS0, como una combinación de servicios de carácter local y en la nube pública, lo que va a suponer tener que gestionar el acceso a esos servicios tanto en el entorno local como en la nube pública.

²² Lista de Revocación de Certificados (*Certificate Revocation List - CRL*): registro utilizado en la operación de algunos sistemas criptográficos, usualmente los de infraestructura de clave pública (*PKI*), para mantener un listado de aquellos certificados (más concretamente sus números de serie) que han sido revocados y que, por tanto, ya no son válidos y no se debería confiar.

²³ Protocolo de Verificación de Certificados en Línea (*Online Certificate Status Protocol- OCSP*): método para determinar el estado de vigencia de un certificado digital usando otros medios que no sean el uso de *CRL*. Este protocolo se describe en el *RFC 6960*, y está en el registro de estándares de Internet.

Sin embargo, la administración de usuarios tanto a nivel local como en la nube plantea escenarios complicados. Las soluciones de identidad con capacidad para abarcar funcionalidades locales y basadas en la nube, requieren crear una identidad de usuario común para la autenticación y autorización en todos los recursos, independientemente de la ubicación. A esto lo llamamos identidad híbrida.

Según se desprende de las soluciones que a este respecto ofrece la documentación de la referencia de *Microsoft* [30], y que en particular se alinea con el *Microsoft Azure Well-Architected Framework* [12], la identidad híbrida se logra mediante la sincronización y el aprovisionamiento.

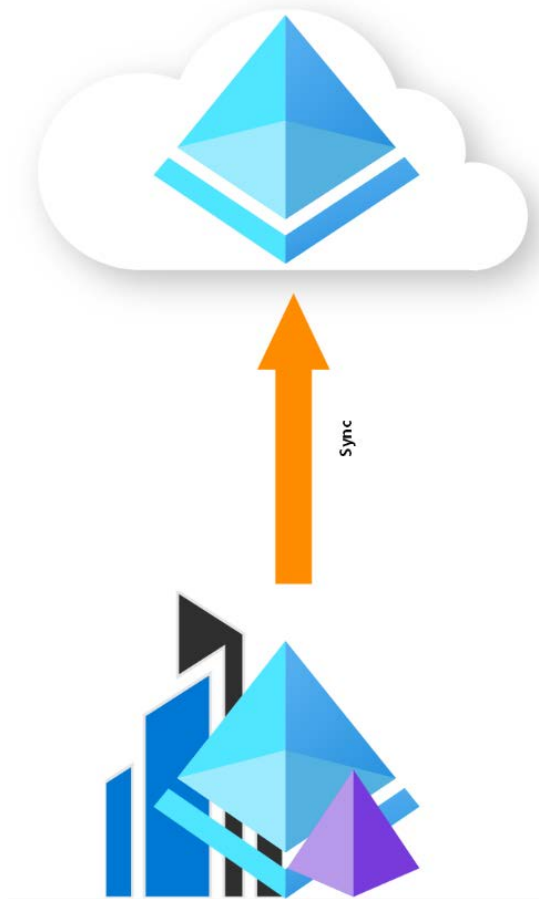


Figura 3-35 Ideograma de la solución de identidad híbrida (según *Microsoft*) (tomada de [30]).

Particularizando ambos elementos para el caso específico de la Nube MDEF tendríamos:

- Sincronización: garantiza que la información de identidad de los usuarios, grupos y dispositivos en el entorno local coincida con la de la nube. Al igual que sucede con la información de identidad en Directorio Activo (MDEF.ES) que se mantiene sincronizada con DICODEF, en el caso concreto de *Microsoft Azure*, el mecanismo de *Entra ID* [30] mantendría sincronizadas aquellas identidades autorizadas en DICODEF.
- Aprovisionamiento: es el proceso de crear un objeto de identidad, en función de varias condiciones, mantener el objeto actualizado y eliminar el objeto cuando dejan de cumplirse las condiciones. No todos los usuarios, grupos y dispositivos existentes en el entorno local existirían en el entorno nube, pero para aquellos que existan en el entorno nube, su creación, mantenimiento y eliminación se debería realizar automáticamente mediante el mecanismo que se determine en coordinación con el proveedor comercial. En el caso concreto de *Microsoft Azure* se trataría de *Entra Connect* [31]).

En el esquema siguiente se puede apreciar la solución completa de identidad híbrida, planteada por Microsoft, sustentada sobre los tres elementos descritos, y que encajaría del modo siguiente para la Nube MDEF:

- Directorio Activo (MDEF.ES): actualmente en producción sobre la Infraestructura para Baja Clasificación de la I3D, en las condiciones anteriormente expuestas.
- *Entra ID*: ejerciendo como mecanismo de sincronización de identidades, entre el entorno local y el de nube, a partir de la información proporcionada por DICODEF.
- *Entra Connect*: ejerciendo como mecanismo de aprovisionamiento para la creación, mantenimiento y eliminación automáticas de objetos de identidad.

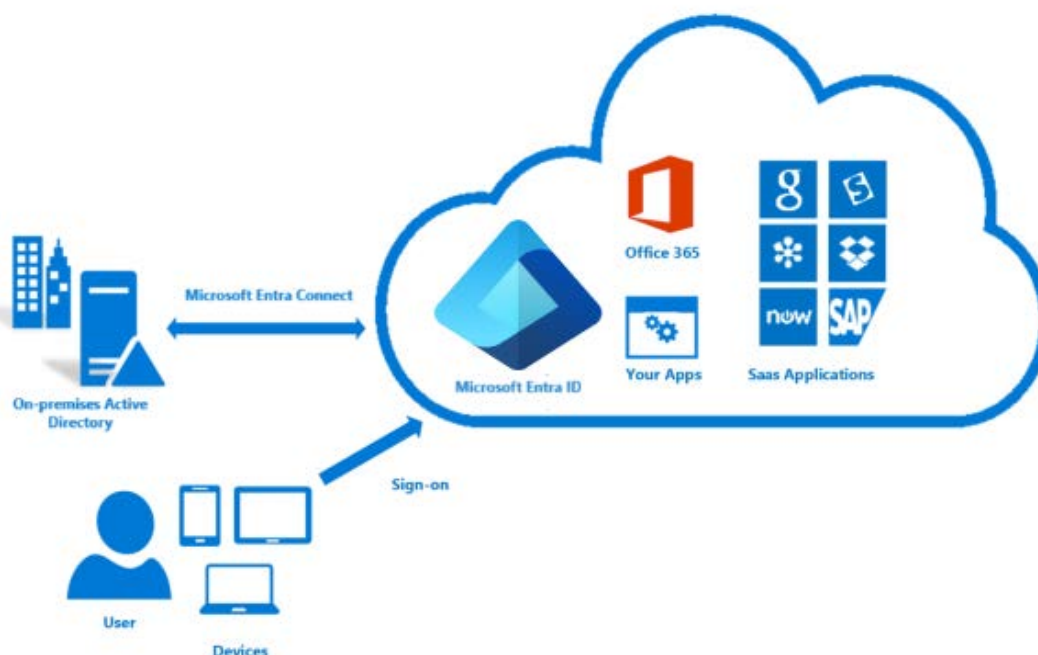


Figura 3-36 Esquema de funcionamiento para la implementación de la solución de identidad híbrida (según Microsoft) (tomada de [31]).

3.4.5 Autenticación y Acceso

Una vez establecida la solución de identidad híbrida como base para afrontar la gestión de identidades para la Nube MDEF, es necesario afrontar un problema derivado del uso de este tipo de identidad, el cual es precisamente, la gestión de la autenticación y acceso a los servicios que se encuentren en un entorno de tipo híbrido.

Bajo este planteamiento, la identidad híbrida permitiría el acceso a los servicios de nube pública en el Dominio de Seguridad No Clasificado o DS0, evaluando los siguientes elementos. La revisión, precisamente, de estos elementos, se alinea con la implantación del concepto de seguridad Confianza Cero (*Zero Trust*) [22] en la Nube MDEF:

- Identidad del usuario: la política de acceso que se determine podrá permitir el acceso, denegar el acceso o requerir condiciones de acceso en base al usuario concreto, los grupos a los que pertenezca o los roles que tenga asignados.
- Método utilizado para la autenticación: la política de acceso que se determine podrá definir diferente nivel de acceso o denegarlo en base a si la autenticación ha sido fuerte (incluyendo el uso de la TEMD) o no.

- Dispositivo utilizado para el acceso: otro de los parámetros que se podrá incluir en la política de acceso condicional es si el dispositivo es un dispositivo corporativo, gestionado por el MDEF o no.
- Ubicación del acceso: permitiendo, denegando o limitando el acceso en base a la confianza de la ubicación desde la que se realiza el acceso.
- Nivel de riesgo del inicio de sesión: otro factor que se puede tener en cuenta en la evaluación de la política de acceso es el nivel de riesgo asignado a un inicio de sesión. Ese nivel de riesgo se establece en base a un modelo de aprendizaje, sustentado sobre los inicios de sesión anteriores, los cuales determinan el nivel de riesgo por parámetros como ubicación, dispositivo usado, navegador, horario, distancia física y distancia horaria entre inicios de sesión, etc.
- Nivel de riesgo del usuario: de manera similar, el modelo asignará un riesgo a la cuenta de usuario en base a intentos fallidos de inicios de sesión, contraseñas exfiltradas, etc.
- Aplicación o servicio al que se quiere acceder: otro componente que puede, y debe tenerse en cuenta a la hora de establecer la política de acceso, es la aplicación o servicio al que se quiera acceder. En este punto es importante destacar que esa política no reemplaza la autorización en sí del acceso a una aplicación, sino que la complementa requiriendo condiciones para permitir el acceso²⁴.
- Privilegios o permisos a obtener: otro elemento que se debe incluir en las políticas de acceso son los requisitos para tener un rol privilegiado. De igual modo que en el caso anterior, la política no reemplaza la posibilidad del usuario para obtener el rol, pero establece las condiciones que se requieren.



Figura 3-37 Elementos a evaluar para el acceso a los servicios bajo la solución de identidad híbrida (según Microsoft) (tomada de [30]).

²⁴ A modo de ejemplo, si un usuario X no puede acceder a la aplicación A, la política establecida no le concederá el acceso. Pero si el usuario X puede acceder a la aplicación B y a la aplicación C, la política puede establecer diferentes condiciones requiriendo, por ejemplo, que para acceder a la aplicación B se tenga que hacer con autenticación fuerte y además desde un dispositivo gestionado por el MDEF y desde una ubicación confiable, mientras que para la aplicación C se pueda hacer únicamente con autenticación fuerte.

Desde el punto de vista de la implementación de métodos a aplicar, para acceder a los servicios alojados en nube pública, los usuarios pueden usar diferentes métodos de autenticación, dependiendo según hemos visto, de la política de acceso que se determine. Esta política de acceso debe establecerse en coordinación con el proveedor comercial de los servicios de nube y, a modo de ejemplo, las recomendaciones proporcionadas por *Microsoft* serían las siguientes, según establece en su documentación de referencia [32]:

Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456 qwerty password iloveyou Password1	 SMS  Voice	 Authenticator (Push Notifications)  Software Tokens OTP  Hardware Tokens OTP (Preview)	 Authenticator (Phone Sign-in)  Window Hello  FIDO2 security key  Certificates

Figura 3-38 Métodos de autenticación recomendados para el acceso a los servicios bajo la solución de identidad híbrida (según *Microsoft*) (tomada de [32]).

Tal y como puede verse, un mismo usuario podría llegar a tener múltiples métodos de autenticación y las políticas de acceso definidas pueden hacer que tenga diferente nivel de acceso dependiendo del método de autenticación utilizado.

Particularizando, nuevamente, esta cuestión a la casuística particular de la Nube MDEF, partiremos de la situación actual existente en la Infraestructura para Baja Clasificación de la I3D, en la que el método de autenticación disponible es el de autenticación con contraseña. En este método, las cuentas de usuario tienen una contraseña y esta contraseña se puede utilizar como único factor de autenticación, caso del MDEF, o podría llegar a combinarse con otros factores para dar lugar a una autenticación multifactor.

Por motivos de seguridad, la política habitual en cualquier proveedor de servicios de nube va a ser la de exigir autenticación multifactor y, de modo general, es recomendable que todas las cuentas tengan una autenticación fuerte. Esto nos plantea dos posibles escenarios principales de solución, con sus subescenarios particulares:

- Autenticación con contraseñas propias del entorno nube: cada usuario tendría su contraseña propia para el entorno de nube, sin ninguna relación con la contraseña del entorno local. En dicho entorno de nube existirán unas políticas de complejidad y de expiración de contraseñas y unos procedimientos para reestablecer la contraseña en caso de olvido, que serían determinadas por el proveedor de servicios. En este escenario el usuario tendría que manejar una contraseña diferente a la existente en el entorno de DICODEF y de Directorio Activo (MDEF.ES), si bien el usuario puede establece las mismas contraseñas de forma manual. Se considera procedente descartar este posible escenario, por la dificultad que añade sobre el usuario y por el hecho de tener que delegar en el proveedor de servicios de nube la política de acceso a este respecto.

- Métodos de autenticación sin contraseña (*passwordless*): además de los métodos listados anteriormente en los que el usuario requiere de una contraseña, existen otros métodos de autenticación sin contraseña. Se expondrá una posible solución sobre este tipo de métodos por ser los que mejor experiencia de usuario y características de seguridad proporcionan:
 - *Microsoft Authenticator*: el usuario debe disponer de esta aplicación en su teléfono *iOS* o *Android* y le permite utilizar una credencial segura sin contraseña en el procedimiento de autenticación. Permite a los usuarios iniciar sesión en cualquier plataforma o explorador sin necesidad de recordar contraseñas. Cuando la aplicación del teléfono del usuario es registrada como método de autenticación, el proceso de autenticación en *Entra ID* genera un número aleatorio y la aplicación solicita la autenticación del usuario en el teléfono (*PIN* del teléfono o biometría), y el número generado para realizar el proceso de autenticación sin contraseña. No se recomienda optar por esta solución, ya que corresponde a un método propietario de un proveedor específico, si bien podría implantarse sobre los terminales móviles corporativos *iOS* o *Android* que el MDEF proporciona a sus usuarios.
 - *Windows Hello for Business*: el usuario debe disponer de un equipo *Windows* en el que se haya configurado *Windows Hello for Business*. En este caso, las credenciales están custodiadas en el chip *TPM* (según referencia [33], particularmente para sistemas *Windows 11*) del equipo, y el usuario tiene que utilizar información biométrica o un *PIN* para desbloquear su uso. Una vez desbloqueadas, las credenciales, basadas en criptografía asimétrica, permiten la autenticación del usuario sin necesidad de utilizar contraseñas. No se recomienda optar por esta solución, ya que corresponde a un método propietario de un proveedor específico, si bien podría implantarse sobre los equipos *Windows* que el MDEF proporciona a sus usuarios.
 - Llaves *FIDO2*²⁵ [34]: el usuario dispone de una llave que sigue el protocolo *FIDO2*, la cual puede conectarse al equipo de trabajo mediante puertos *USB*, *NFC* o de manera similar. Esta llave se desbloquea con un *PIN* o mediante biometría y permite la autenticación sin contraseña de los usuarios. Esta solución sería aplicable a la Nube MDEF, contando con el aval y la recomendación del Centro Criptológico Nacional (CCN) [35], por tratarse de un método de autenticación resistente a la suplantación de identidad o *phishing*.
 - Autenticación basada en certificados (*CBA*): los usuarios se autentican mediante un certificado digital emitido por una autoridad de certificación reconocida, que para el caso de la Nube MDEF podrían ser los certificados emitidos para la PKIDEF. Los usuarios podrían iniciar sesión con su nombre de usuario (correo electrónico corporativo) y el certificado disponible en la TEMD que se insertaría en su equipo de trabajo. Este método permitiría aprovechar los certificados existentes en TEMD para acceder a los servicios de la nube, y ofrece un alto nivel de seguridad y comodidad para el usuario. Implica que los dispositivos de los usuarios dispongan de lectores de tarjetas, hecho habitual en los equipos de trabajo del MDEF, así como la configuración adecuada de los dispositivos y navegadores. Esta solución sería aplicable a la Nube MDEF y, junto con la anterior, sería la recomendable por sus características de protección frente al *phishing*.

²⁵ Alianza *FIDO* (*Fast IDentity Online*): es una asociación abierta de la industria lanzada en febrero de 2013 cuya misión declarada es desarrollar y promover estándares de autenticación que ayuden a reducir la dependencia excesiva del mundo de las contraseñas. *FIDO* aborda la falta de interoperabilidad entre los dispositivos que utilizan una autenticación sólida y reduce los problemas a los que se enfrentan los usuarios al crear y recordar varios nombres de usuario y contraseñas.

En conclusión, teniendo en cuenta las características de experiencia de usuario y seguridad, y contando con el hecho de que todo el personal del MDEF dispone ya de una TEMD, para ejercer como soporte criptográfico para los certificados que emite PKIDEF, el método *CBA*. Su implementación podría ser relativamente inmediata, a diferencia de cómo ocurriría con las llaves *FIDO2*, las cuales tendría que ser adquiridas por no disponerse actualmente de las mismas. La implementación y consideraciones sobre el empleo del *CBA* vienen recogidas en la siguiente documentación de referencia de *Microsoft* [36]:

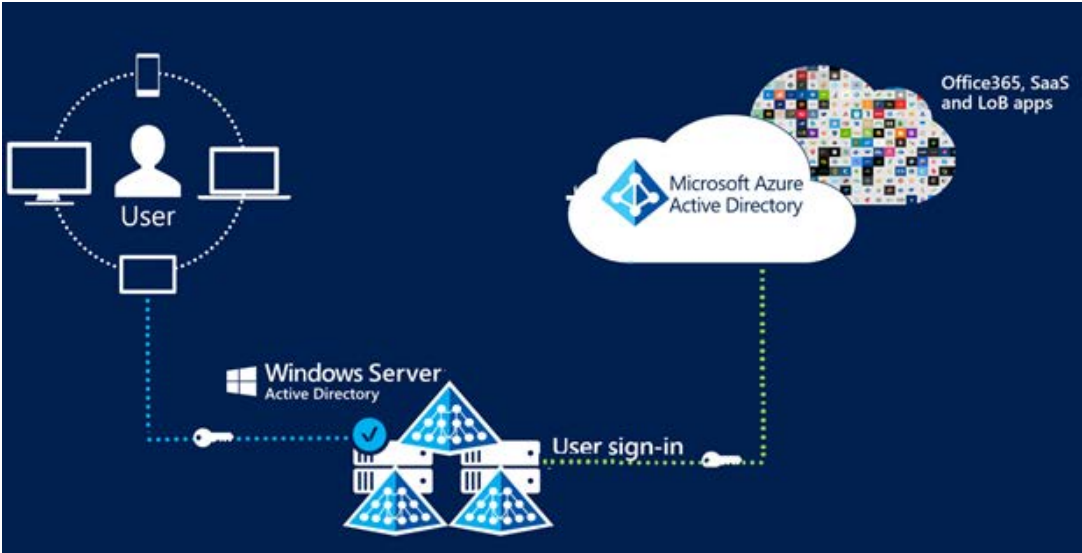


Figura 3-39 Implementación de CBA como método de autenticación (según Microsoft) (tomada de [36]).

Ventajas	Descripción
Mejor experiencia del usuario	- Los usuarios que necesitan la autenticación basada en certificados ahora pueden autenticarse directamente en Microsoft Entra ID y no tienen que invertir en la federación. - La interfaz de usuario del portal permite a los usuarios configurar fácilmente cómo asignar campos de certificado a un atributo de objeto de usuario para buscar al usuario en el inquilino (enlaces de nombre de usuario de certificado). - Interfaz de usuario del portal para configurar directivas de autenticación que ayuden a determinar qué certificados son de un solo factor frente a multifactor.
Fácil de implementar y administrar	- La CBA de Microsoft Entra es una característica gratuita y no necesita ninguna edición de pago de Microsoft Entra ID para utilizarla. - No se requieren complejas implementaciones locales ni la configuración de la red. - Autenticación directa en Microsoft Entra ID.
Seguridad	- No es necesario que las contraseñas locales se almacenen en la nube. - Protege las cuentas de usuario al trabajar sin problemas con directivas de acceso condicional de Microsoft Entra, incluida la autenticación multifactor resistente al phishing (MFA requiere una edición con licencia) y el bloqueo de la autenticación heredada. - Compatibilidad con la autenticación sólida, donde los usuarios pueden definir directivas de autenticación a través de los campos de certificado, como emisor u OID (identificadores de objeto) de directiva, para determinar qué certificados se califican como de factor único frente a multifactor. - La característica funciona perfectamente con las características de acceso condicional y la capacidad de seguridad de autenticación para aplicar MFA con el fin de ayudar a proteger a los usuarios.

Figura 3-40 Valoración de CBA como método de autenticación (según Microsoft) (tomada de [36]).

3.4.6 Protección de los Servicios

A la hora de considerar la protección de los servicios de la Nube MDEF que finalmente quedasen alojados en un entorno de nube pública proporcionado por un proveedor de servicios, debemos tener en cuenta una serie de factores, todos ellos alineados con el concepto de Confianza Cero (*Zero Trust*).

En primer lugar y como premisa básica, se ha indicado en apartados anteriores que la elección de los posibles proveedores de nube va a quedar supeditada a que estos cuenten con la certificación de conformidad con el Esquema Nacional de Seguridad [7] de categoría Alta, como exigencia mínima. Además, sin contravenir lo anterior, deberá procurarse mediante contrato que los CPD de los proveedores de servicios de nube se encuentren ubicados en territorio nacional²⁶, máxime cuando se traten de proveedores comerciales no nacionales, y evitando en la medida de lo posible una dependencia específica de un proveedor concreto.

Todas estas consideraciones van a conferir, de partida, una protección y garantías de seguridad intrínsecas para todos los servicios que se alojen en nube pública, los cuales, si bien pertenecerían al Dominio de Seguridad DS0, siguen requiriendo de unas condiciones de seguridad acorde a la naturaleza de la misiones y cometidos del MDEF.

En un siguiente paso, la protección de los servicios se llevará a cabo haciendo uso de las herramientas de seguridad ya descritas, agrupadas en las soluciones *SASE* y *SSE*. De entre todas ellas, el *CASB* emerge como una solución clave [37], sirviendo de enlace entre la infraestructura local y el entorno de nube, operando como controladores de medidas de seguridad que se sitúan entre los usuarios y los proveedores de los servicios de nube. Además de proporcionar control y visibilidad esenciales para proteger datos sensibles a través de todas las etapas del flujo de información, los *CASB* integran una variedad de estrategias de seguridad que abarcan desde la validación y otorgamiento de permisos hasta el cifrado y detección de software malicioso, independientemente de si los dispositivos están supervisados o no.

En cuanto a funcionamiento, el *CASB* en primer lugar, realiza una identificación, en la que detecta todos los servicios de nube en uso. Posteriormente, entra en la fase de evaluación, donde cada servicio es analizado, reconociendo sus datos y estimando un índice de riesgo. Finalmente, en la etapa de mitigación, se configura una directiva de seguridad para el servicio basada en sus requisitos de seguridad, permitiendo al *CASB* detectar y neutralizar cualquier peligro o violación emergente.

En cuanto a su implementación, los *CASB* se destacan por su simplicidad en la integración y manejo. Existen tres modos principales de despliegue para *CASB* y, aunque la mayoría se instalan en la nube, también hay alternativas para despliegues locales.

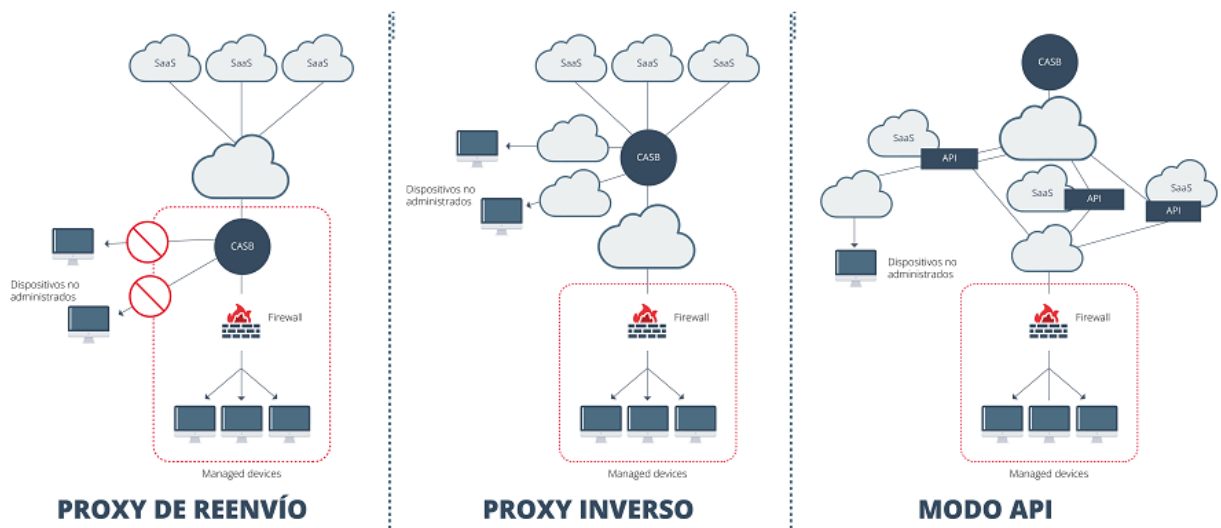


Figura 3-41 Modos básicos de funcionamiento de CASB (tomada de [37]).

²⁶ No únicamente por consideraciones operativas de defensa nacional, sino también por otras cuestiones derivadas de legislaciones relativas a la protección de datos de carácter personal. En caso de no poderse contar con CPD en territorio nacional, el proveedor de servicios debería, al menos, disponer de CPD ubicados en territorio de la Unión Europea. Se descartarían, por tanto, otras ubicaciones incluso de un país de la OTAN (Ejemplo: Turquía, Estados Unidos, Reino Unido, etc.).

La descripción realizada en cuanto a funcionamiento e implementación de los CASB, es perfectamente trasladable a proveedores de servicio de nube como *Microsoft*, quien en su documentación de referencia [38] recoge estas mismas consideraciones respecto a los CASB.

A continuación, se detalla el despliegue, la configuración del cliente, el control y el uso de estos métodos de implementación:

	Proxy de reenvío (Forward Proxy)	Proxy inverso (Reverse Proxy)	Modo API
Despliegue	El forward proxy se coloca entre el usuario final e Internet. Esto significa que todo el tráfico de los usuarios primero pasa por el CASB antes de llegar al servicio en la nube.	El reverse proxy se sitúa entre Internet y el servicio en la nube. A diferencia del Forward Proxy, no requiere ninguna configuración en el dispositivo del usuario.	El modo API no actúa como un proxy entre el usuario y el servicio en la nube. En su lugar, se integra directamente con la API del servicio en la nube, lo que le permite inspeccionar y controlar los datos en reposo dentro de la aplicación.
Configuración del cliente	Requiere una configuración en los dispositivos de los usuarios finales. Esto puede ser problemático para los dispositivos no administrados o BYOD, ya que las organizaciones no tienen control directo sobre estos dispositivos.	No requiere configuración en los dispositivos de los usuarios. Los usuarios son redirigidos a través del CASB mediante técnicas como la reescritura de URL.	No requiere ninguna configuración en el lado del cliente, ya que no interfiere con el tráfico en tiempo real entre el usuario y el servicio en la nube.
Control	Puede controlar el tráfico hacia aplicaciones autorizadas y no autorizadas, ya que todo el tráfico pasa a través del proxy.	Generalmente, está limitado a aplicaciones específicas o autorizadas, ya que depende de la integración entre el CASB y la aplicación específica en la nube.	Su control está principalmente centrado en los datos en reposo. Puede realizar funciones como la clasificación de datos, la detección de contenido sensible y la implementación de directivas de control de acceso basadas en datos específicos. Sin embargo, no inspecciona ni controla el tráfico en tiempo real.
Uso	Es especialmente útil en escenarios donde las organizaciones quieren controlar qué servicios en la nube pueden ser accesibles y cuáles no.	Es ideal para organizaciones que utilizan aplicaciones específicas en la nube (como Office 365 o Salesforce) y desean un control y una visibilidad detallados sobre esas aplicaciones.	El modo API es particularmente útil para escenarios donde las organizaciones desean inspeccionar el contenido almacenado en aplicaciones en la nube (como servicios de almacenamiento o colaboración) y aplicar directivas de control de acceso y seguridad sin afectar la experiencia del usuario en tiempo real.

Figura 3-42 Características de los distintos modos básicos de funcionamiento de CASB (tomada de [37]).

Como solución a aplicar a la Nube MDEF, se optaría por un tipo de CASB “multimodal”, el cual tiene la capacidad de aprovechar todos estos modos de funcionamiento para brindar una adaptabilidad óptima.

Finalmente indicar que todo el conjunto de soluciones descritas y agrupadas en SASE y SSE, se materializan por parte de los principales proveedores de servicios de nube en “suites” de herramientas de seguridad que conforman un abanico multidisciplinar enmarcado en el concepto de Confianza Cero (*Zero Trust*). Para el caso particular de *Microsoft*, este paquete de herramientas se denomina *Entra Suite* [39], y permite proporcionar la práctica totalidad de las funcionalidades de seguridad recogidas bajo el paraguas de Confianza Cero (*Zero Trust*), y operar como una plataforma unificada.

En cuanto al detalle de las medidas de seguridad a implantar, con objeto de alcanzar la necesaria protección de los servicios de la Nube MDEF alojados en nube pública, es de obligada aplicación las guías CCN-STIC [40], las cuales son normas, instrucciones, y recomendaciones desarrolladas por el CCN con el fin de mejorar el grado de seguridad. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.

En particular, se considera de interés la guía “CCN-STIC-499 Arquitecturas de Seguridad *Cloud*” por tratarse de la guía general para seguridad de los servicios en la nube, la cual constituiría la documentación de base elaborada por el CCN para la conferir protección a este tipo de servicios.

En cuanto a los proveedores de servicios de nube, son aplicables distintas guías de la serie “CCN-STIC-800”. Estas guías responden a cuestiones de seguridad de algunos de los principales proveedores de servicios como son *Microsoft Azure* y *AWS*, a la par que posicionan a ambos proveedores en una posición privilegiada en cuanto a su nivel de seguridad para alojar servicios en la nube.

Por último, es igualmente relevante la guía “CCN-STIC-442 Seguridad en *VMware vSphere*” por ser una solución ampliamente extendidas entre los principales proveedores de servicios de nube, y estar relacionada con los servicios de virtualización (en la nube) y de interconexión (entre nube privada y nube pública). Tal y como se expuso, el primero proporciona la infraestructura virtual en la nube pública para el despliegue de máquinas virtuales, y el segundo permite la interconexión de un entorno en nube pública y los entornos existentes en infraestructura de CPD del MDEF.

Documento: azure

Total: 4 documentos

Mostrar: 20

 Pág. 1 de 1

Documento	Categoría	Publicado desde	Actualizado desde
CCN-STIC-884A Guía de Configuración segura para Azure	800 Guías Esquema Nacional de Seguridad	Dic 2019	May 2024
CCN-STIC-884 Specific Compliance Profile for Azure Corporate Cloud Service	800 Guías Esquema Nacional de Seguridad	Jun 2020	Jun 2020
CCN-STIC-884B Secure configuration guide for Azure Kubernetes Services	800 Guías Esquema Nacional de Seguridad	Ene 2020	Ene 2020
CCN-STIC-884 Perfil de cumplimiento específico Azure	800 Guías Esquema Nacional de Seguridad	Dic 2019	Dic 2019

Figura 3-43 Relación de guías CCN-STIC-800 aplicables a Microsoft Azure (tomada de [40]).

Documento: aws

Total: 6 documentos

Mostrar: 20

 Pág. 1 de 1

Documento	Categoría	Publicado desde	Actualizado desde
CCN-STIC-887G Guía de Configuración segura para Monitorización y gestión AWS	800 Guías Esquema Nacional de Seguridad	Ene 2023	Mar 2024
CCN-STIC-887F Guía de respuesta a incidentes en AWS	800 Guías Esquema Nacional de Seguridad	Feb 2022	Mar 2024
CCN-STIC-887D Guía de configuración segura Multi Cuenta AWS	800 Guías Esquema Nacional de Seguridad	Abr 2021	Mar 2024
CCN-STIC-887C Guía de Configuración Segura de Conectividad Híbrida en AWS	800 Guías Esquema Nacional de Seguridad	Feb 2021	Nov 2023
CCN-STIC-887A Guía de configuración segura AWS	800 Guías Esquema Nacional de Seguridad	Dic 2020	Sep 2023
CCN-STIC-887 Perfil de cumplimiento específico para AWS Servicio de Cloud Corporativo	800 Guías Esquema Nacional de Seguridad	Dic 2020	Sep 2023

Figura 3-44 Relación de guías CCN-STIC-800 aplicables a AWS (tomada de [40]).

3.4.7 Características de la Golden Copy

Para establecer el marco de aplicación en el que se ubicaría el recurso de la *Golden Copy*, es preciso detallar una serie de documentos cuyo alcance va más allá de la propia implantación de la Nube MDEF. Sería recomendable, según indica el INCIBE [41], disponer de los siguientes planes en cuya elaboración debería participar necesariamente el CESTIC por su condición de GSN:

- Planes de Contingencia: formado conjunto de planes de actuación, planes de emergencia, planes financieros y planes de comunicación destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos operativos del MDEF.
- El Plan de Contingencia TIC: como parte del conjunto anterior, este plan definiría una estrategia planificada en fases. Quedaría constituido por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los CIS/TIC, que soportan la información y los procesos operativos considerados críticos para el MDEF.

- Plan de Recuperación ante Desastres: derivado del anterior, abarcaría los procesos de restauración de los datos, el *hardware* y el *software* crítico del MDEF ante un desastre. Es decir, se centraría en el restablecimiento de los CIS/TIC que soportan los procesos críticos, tras haber ocurrido un incidente grave.

En este escenario de Recuperación ante Desastres contaríamos con la *Golden Copy*, la cual consiste en una copia de datos íntegra e inmutable que se puede utilizar como fuente confiable para una recuperación de infraestructura y de datos ante un desastre, garantizando el nivel mínimo de funcionamiento y la rápida reanudación de aquellos servicios que se consideren críticos. La copia serviría de respaldo tanto para el Dominio de Seguridad DS0 como para el DS1.

Cabe reseñar que la *Golden Copy* se enmarcaría en la necesidad de contar con una aproximación “3-2-1-1” [42], a efectos de disponer de una estrategia de *backup* eficaz frente a las posibles contingencias que podrían requerir su empleo. La regla establece la necesidad de:

- Se deben tener al menos 3 copias de los datos, incluida la copia o copias de producción.
- Se deben utilizar al menos 2 medios de almacenamiento diferentes (por ejemplo, en disco y en nube).
- Al menos 1 de las copias debe mantenerse geolocalizada lejos de los emplazamientos de producción (*off-site*).
- Al menos 1 copia debe mantenerse desconectada (*off-line*) o, en caso de no ser posible, ser inmutable.

En línea con esta aproximación, la *Golden Copy* (como 3ª copia) se alojaría en nubes de otras organizaciones pertenecientes a la AGE y sin fines comerciales (Nubes de Terceros). Las copias de seguridad se realizarían sobre una infraestructura ubicada a no menos de 300 km de la región en la que se ubican ambos CPD del MDEF.

Esta copia íntegra e inmutable complementaría a las copias de seguridad y procedimientos ya existentes, que se puedan ejecutar con carácter local, de modo que conformaría una capacidad adicional, escalable y que sería utilizada si el escenario de desastre lo requiere, no reemplazando la infraestructura de CPD Activo-Activo que se ha descrito con anterioridad.

De este modo, los procedimientos de protección y retención de copias de *backup* definirían, entre otras cuestiones, los tipos de copias que deben realizarse, periodicidad de las mismas, lugar de almacenamiento y formato de manera local para cada uno de ambos CPD. Sobre estos procedimientos ya existentes se realizaría una copia adicional que se almacenaría en Nubes de Terceros. Esto implicaría que, con la configuración de CPD funcionando en Activo-Activo, se proporcionaría una alta disponibilidad a las aplicaciones y a los datos de manera que un desastre que sólo afectase a uno de los CPD no necesitaría hacer uso de esa *Golden Copy*.

Para realizar la copia de la información se propone utilizar una conexión privada y dedicada con la que se pudieran conectar los CPD propios del MDEF con los servicios en la Nube de Terceros sin pasar por la red pública de Internet. El uso de esta conexión dedicada permitiría ofrecer el ancho de banda, la disponibilidad y la latencia necesarias para implementar esta copia de seguridad. Además, durante el tránsito esta información debería viajar cifrada, puesto que la protección de dichos datos en tránsito es una parte esencial de cualquier estrategia de protección de la información. En este caso, sería fundamental proteger la confidencialidad y la integridad de los datos.

Las dos contingencias más comunes en las que podría ser necesario hacer uso de esta *Golden Copy* serían, por un lado, desastres naturales o eventos adversos (afectando a la disponibilidad de los datos), y por otro, ataques de tipo *ransomware* que pudiesen conducir a un escenario de recuperación de datos comprometidos (afectando a la confidencialidad e integridad de los datos).

Para el primer tipo de contingencia, la aproximación ya expuesta anteriormente en base a la referencia [42], indica que lo conveniente sería la de alojar esta *Golden Copy* en una región secundaria. Este enfoque proporciona un mecanismo de mitigación ante un incidente o desastre que afectase a toda la región principal. A su vez, proveedores como *Microsoft Azure* contemplan dos posibles opciones principales para llevar a cabo la copia de los datos en una región secundaria, según se desprende de su documentación de referencia [43]. Si bien esta *Golden Copy* estaría llamada a alojarse en Nubes de Terceros, se siguen considerando igualmente válidas estas estrategias de almacenamiento redundante llevadas a cabo por proveedores comerciales de nube pública, ya que podrían replicarse sobre esas Nubes de Terceros.

En primer lugar, los datos de una cuenta de almacenamiento siempre se deberían replicar tres veces en la propia región primaria. En esta situación se ofrecen dos métodos para replicar los datos en la región primaria:

- Almacenamiento con redundancia local (*LRS*): los datos se copian de forma síncrona tres veces dentro de una única ubicación física en la región primaria.
- Almacenamiento con redundancia de zona (*ZRS*): los datos se copian de forma síncrona en tres zonas de disponibilidad en la región primaria.

Microsoft recomienda llevar a cabo una réplica en una región secundaria. Esta es precisamente la situación que se ha presentado desde el primer momento para el caso de la Nube MDEF, y sobre ella se verán las dos opciones principales.

- Almacenamiento con redundancia geográfica (*GRS*): los datos se copian de forma síncrona tres veces dentro de una única ubicación física en la región primaria mediante *LRS*. Posteriormente los datos se copian de forma asíncrona en una única ubicación física en la región secundaria. Dentro de la región secundaria, los datos siempre se replican de forma síncrona tres veces mediante *LRS*.
- Almacenamiento con redundancia de zona geográfica (*GZRS*): los datos se copian de forma síncrona en tres zonas de disponibilidad en la región primaria mediante *ZRS*. Posteriormente los datos se copian de forma asíncrona en una única ubicación física en la región secundaria. Dentro de la región secundaria, los datos siempre se replican de forma síncrona tres veces mediante *LRS*.

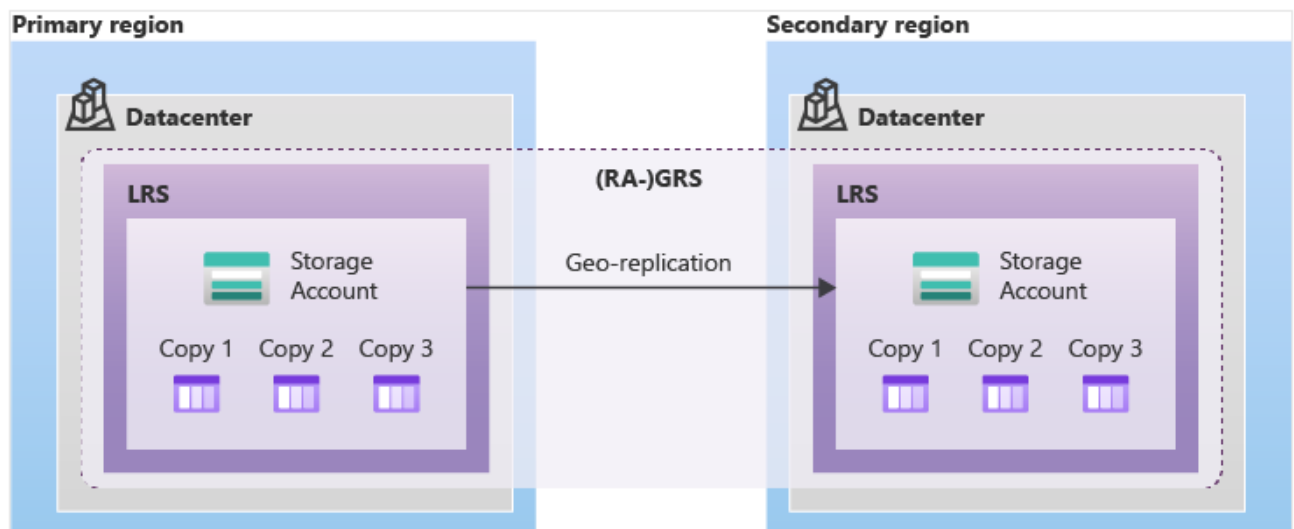


Figura 3-45 Réplica de datos para la *Golden Copy* mediante *GRS* (según *Microsoft*) (tomada de [43]).

Para el caso específico de la Nube MDEF, se ha indicado con anterioridad que se contaría con una única región en la que existirían dos zonas de disponibilidad, cada una de las cuales tendría un único CPD. Este hecho imposibilita el planteamiento de poder implementar GZRS, por no disponerse de tres zonas de disponibilidad en la región primaria. Sin embargo, y siguiendo la recomendación de llevar a cabo una réplica en una región secundaria, si podría implementarse GRS, en las condiciones expuestas.

El segundo tipo de contingencia desembocaría en un escenario de recuperación de datos comprometidos. En este caso, los datos podrían haber sido cifrados o modificados por un atacante malicioso, incluyendo las copias de seguridad que se utilizan para los procedimientos estándar de recuperación. En el caso de una modificación maliciosa, esta se puede haber producido con anterioridad a su detección y en algunos casos puede resultar complejo determinar el momento del compromiso de la información. Un ejemplo de este escenario es cuando un atacante ha sido capaz de comprometer unas credenciales privilegiadas del entorno de Directorio Activo, MDEF.ES, para el caso particular del MDEF. Se podría llegar a detectar el uso de estas credenciales por parte del atacante, pero resultaría complejo determinar desde cuando dispone de esas credenciales y si ha podido obtener credenciales adicionales, ya sea inyectándolas o capturándolas, lo cual provocaría que las distintas copias de seguridad de los datos pudieran estar comprometidas.

Llegada esta situación, la pieza clave para la recuperación es la copia íntegra e inmutable almacenada en el entorno de nube.

El procedimiento de recuperación [44] requeriría de un administrador que seleccionase la versión adecuada a recuperar. Esta cuestión es importante, ya que se debe recuperar una versión anterior a la modificación de la integridad de los datos y que se considere confiable para el restablecimiento de los servicios. Para determinar la versión adecuada para la recuperación, el administrador se conectaría al entorno de almacenamiento de copias de seguridad íntegras e inmutables, examinaría las copias existentes y determinaría que copia es confiable para la recuperación. Determinar la copia a restaurar puede requerir realizar una recuperación en un entorno desconectado, con la finalidad de permitir identificar al administrador si la copia es confiable o no.

Precisamente los parámetros de RTO (*Recovery Time Objective*), o Tiempo Objetivo de Recuperación, y RPO (*Recovery Point Objective*), o Punto Objetivo de Recuperación, serán claves para, por un lado, concretar la pérdida asumible ante este tipo de contingencia y, por otro, definir las capacidades de almacenamiento a demandar a las Nubes de Terceros para poder alojar la *Golden Copy* de la Nube MDEF. En cualquier caso, y sin ánimo de establecer en este trabajo los RTO y RPO precisos, es necesario indicar que un ataque de tipo *ransomware* puede constar de semanas, o incluso meses en su desarrollo. Por este motivo, una estrategia de recuperación de un *ransomware* requiere poder almacenar un *backup* de meses para tener un RPO aceptable. En cuanto al RTO, se estima que puede ser necesario alrededor de un mes de tiempo para una recuperación completa.

4 RESULTADOS / VALIDACIÓN / PRUEBA

4.1 Planteamiento de un supuesto práctico

4.1.1 Punto de partida

Cuando se ha expuesto la forma en la que se organizaría la “Operación de la Nube MDEF” se han puesto de manifiesto una serie de cuestiones que, finalmente, ahondan en la pregunta inicial que el responsable de un proyecto de estas características debería hacerse antes de emprender cualquier acción de carácter práctico:

“¿El modelo de Nube MDEF planteado cumple satisfactoriamente con las necesidades y requerimientos de los servicios CIS/TIC del MDEF?”

Una pregunta así, enmarcada en un proyecto como este, nunca podría tener una respuesta de tipo sí o no. Con esta afirmación, lo que se quiere expresar es que la variada casuística de servicios a los que aludiría esta pregunta dará, sin dudas, una serie de resultados muy diversos. Es precisamente el análisis de esa diversidad de resultados lo que hará ver si el modelo de Nube MDEF planteado podría llegar a ser operativamente válido o no. Y es que parece claro anticipar que los servicios a migrar a la Nube MDEF deberían cumplir una serie de características y requisitos definidos y determinados por el CESTIC, como Gestor de Servicios en la Nube o GSN, considerándose aspectos técnicos, funcionales y operativos, además de otros como compatibilidad, seguridad, escalabilidad, rendimiento y coste.

En el presente capítulo se va a abordar este análisis, sobre la base de un supuesto práctico de proceso de migración de servicios existentes a la Nube MDEF planteada. Con el mismo, deberíamos poder determinar si un servicio concreto es susceptible de ser migrado al entorno de Nube MDEF, o por el contrario es más conveniente que continúe residiendo en la infraestructura tradicional. Este análisis es clave ya que, según se ha dejado entrever al mencionar el principio de Preferencia en Nube (*Cloud First*), no todos los servicios actualmente en producción serían migrados a la Nube MDEF.

4.1.2 Plan de migración

El primer paso a adoptar, a la hora de afrontar un proceso de migración de estas características, sería establecer un plan de migración completo que nos permita definir, la secuencia, fases y situación final deseada, de tal modo que se consiga llegar a un estado de implantación del modelo de Nube MDEF mientras se mantiene el estado actual de servicios en producción.

Se trata de identificar la infraestructura local actualmente en producción, los servicios alojados sobre dicha infraestructura y las dependencias entre los mismos, todo ello con el objetivo de evaluar las cargas de trabajo y obtener orientación y herramientas que ayudan a facilitar el proceso de migración.

Los grandes proveedores comerciales de servicios de nube como *Microsoft Azure* y *AWS* cuentan con sus respectivas soluciones de migración a la nube. Como puede suponerse, cada uno de los proveedores ha desarrollado sus propias soluciones a este respecto, así *Microsoft Azure* cuenta para su plan de migración [45] con la herramienta *Azure Migrate* [46] y *AWS* cuenta para su plan de migración [47] con la herramienta *MAP* [48]. En ambos casos, el denominador común de estas herramientas consiste en contar con un plan detallado para encontrar la mejor ruta de migración a la nube.

4.1.3 Estrategias de migración

El documento de la referencia [1] define que:

“Los servicios se migrarán a entornos en la nube siguiendo un proceso que desarrolle los siguientes cinco enfoques para determinar las mejores estrategias de migración: racionalizar servicios, renovar aplicaciones, reubicar aplicaciones, reemplazar aplicaciones y retirar aplicaciones.”

Ahondando en este aspecto de posibles estrategias de migración, se interpretará el párrafo anterior para cada uno de los mencionados cinco enfoques, más uno adicional correspondiente a la “no migración” de servicios, en línea con lo que estipulan los grandes proveedores comerciales de servicios de nube tales como *Microsoft Azure* [49] y *AWS* [50]:

- Estrategia tipo Racionalizar: esta estrategia recogería el proceso de rediseñar (*refactor/rearchitect*) y trasladar una aplicación a la nube con la intención de modernizar su arquitectura para aprovechar funciones nativas en la nube. Gracias a este rediseño de la aplicación se puede introducir, por ejemplo, una arquitectura de microservicios destinada a facilitar el desarrollo, pruebas y el lanzamiento de nuevas funciones, en línea con la aproximación recogida en la Estrategia de Desarrollo de *Software* en el MDEF [23], y su vinculación al empleo de contenedores.
- Estrategia tipo Renovar: esta estrategia consiste en reemplazar (*replatform*) aquellas aplicaciones que no se pueden migrar al entorno de nube por su naturaleza o complejidad. Se aplica cuando las aplicaciones dependen de *hardware* específico, tienen requisitos muy estrictos de seguridad o rendimiento, o no son compatibles. Implica un alto esfuerzo y coste, pero también puede suponer una oportunidad de mejora e innovación.
- Estrategia tipo Reubicar: esta estrategia consiste en trasladar las aplicaciones, realojándolas (*rehost*) tal cual a la nube sin realizar cambios significativos. Se aplica cuando las aplicaciones son compatibles con la nube, tienen una baja complejidad o dependencia, o no requieren una optimización o mejora. Implica un bajo esfuerzo y coste, pero también puede limitar el aprovechamiento de las ventajas y funcionalidades en la nube.
- Estrategia tipo Reemplazar: esta estrategia sustituye una aplicación por otra tipo *SaaS*, basada en la nube y creada por el proveedor de la nube, implicando la readquisición (*repurchase*) de la aplicación. Es un proceso que lleva tiempo y planificación y puede suponer un cambio organizativo para los Equipos de Operaciones.
- Estrategia tipo Retirar: esta estrategia tiene lugar cuando, al estudiar detenidamente una aplicación o servicio, se llega a la conclusión de que su funcionalidad apenas se utiliza o ya no se necesita por lo que se procede a la retirada (*retire*) de la misma. La retirada de una aplicación requiere tiempo y planificación, ya que pueden existir dependencias con respecto a otras aplicaciones que se deberán solucionar antes de la retirada, no obstante, esta estrategia sugiere un gran ahorro de costes.
- Estrategia tipo “No Migrar”: esta estrategia supone, tras realizar la correspondiente valoración de factores, retener (*retain*) la aplicación o servicio en la infraestructura local por descartarse su migración al entorno de nube.

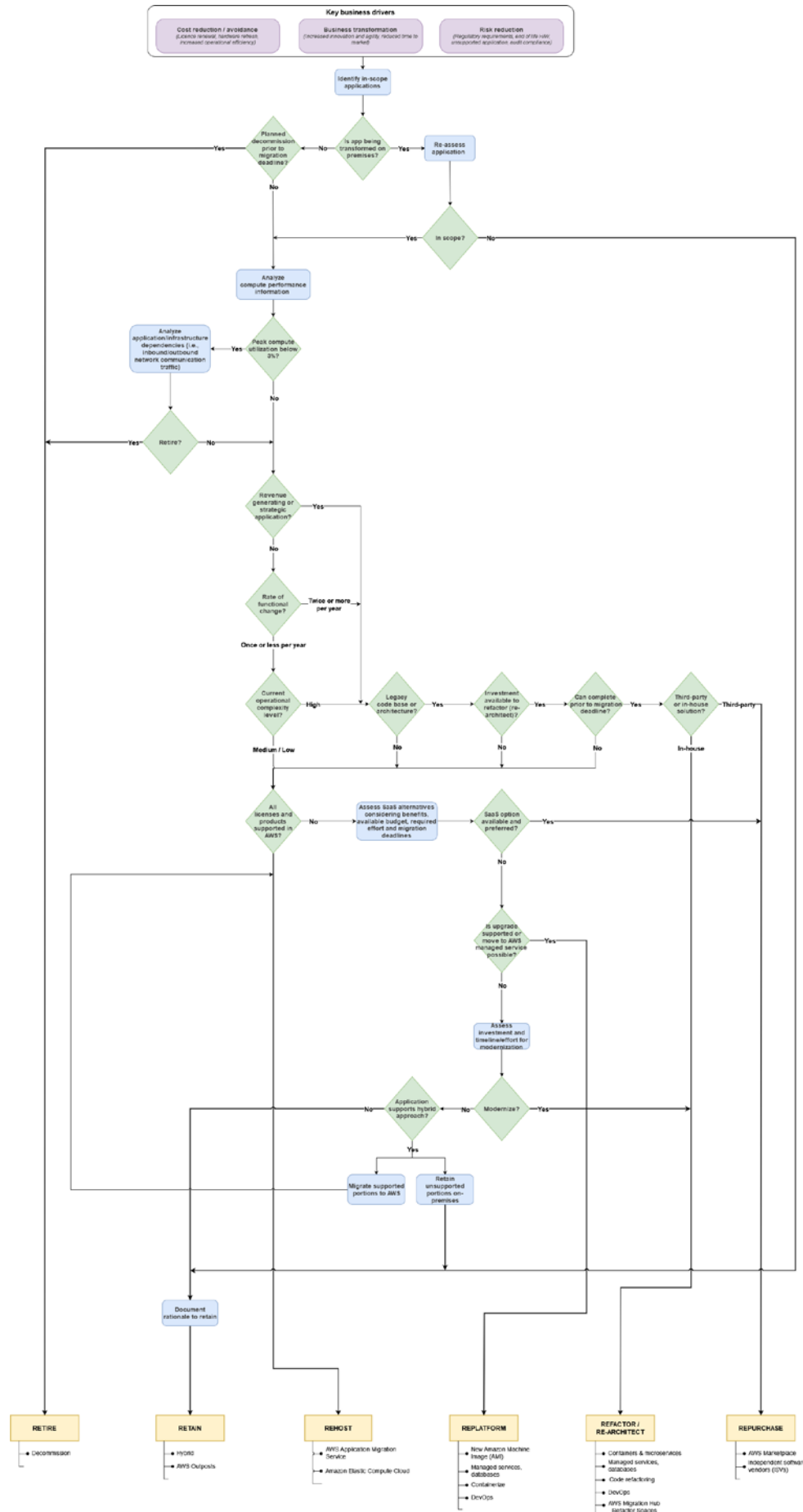


Figura 4-1 Diagrama de decisión de las 6Rs para migración de servicios a nube (según AWS) (tomada de [50]).

4.2 Desarrollo del supuesto práctico

4.2.1 Casos a considerar

Una vez definidas las diferentes estrategias de migración detalladas en el punto anterior, pasaremos a establecer una serie de situaciones o casos que nos llegaremos a encontrar en el desarrollo del supuesto práctico. Fundamentalmente, y con objeto de hacer más sencillo el análisis, estableceremos cuatro posibles casos resultantes, sobre los cuales iremos clasificando los distintos servicios que someteremos al análisis. De este modo podremos tener:

- **Migrar a nube:** este caso correspondería a todos aquellos servicios que cuentan con bajo grado de complejidad-riesgo pero con un valor alto para el MDEF. Estos servicios se caracterizan por ser estables, no requerir mucho soporte, estar bien diseñados y disponer de una documentación detallada. Todos estos elementos se encontrarían alineados para facilitar el proceso de migración, y además aportan valor al MDEF sobre la base de factores como ayudar a optimizar la eficiencia operacional, aumentar el rendimiento, mejorar la calidad de los datos y mejorar los procesos de trabajo. En definitiva, son servicios que contarían con un valor atribuible y reconocible, por lo que estarían abiertos a nuevos aportes de inversión con objeto de obtener aún mejores rendimientos de los mismos. Este tipo de servicios se migrarían en un primer lugar, logrando la optimización de su infraestructura y obteniendo “*quick wins*”.
- **Mitigar riesgos y migrar:** en este caso se encuadrarían servicios que representan un valor nuevamente importante para el MDEF pero, por contra, cuentan con una serie de problemas mayores para recibir el mantenimiento necesario, desde un punto de vista tecnológico. Serían servicios con casuísticas tales como un alto coste de soporte, falta de conocimiento detallado sobre el servicio, o una variedad de diferentes factores que hacen del mismo un elemento caro de mantener. En este caso, y con objeto de optimizar costes, se debería buscar migrar el servicio pero realizando los ajustes previos necesarios sobre el mismo, para adaptarlo al entorno de nube a la par que se solucionan las carencias detectadas. En muchas ocasiones este caso puede llegar a confundirse con el anterior, sin embargo se refiere a aquellos servicios que pueden llegar a migrarse teniendo muy presente las dependencias y complejidad del mismo. Este tipo de servicios se podrían migrar en un segundo bloque, previo ajuste de los mismos.
- **Revisar si migrar:** este caso pertenece a aquellos servicios que cuentan con un bajo componente de complejidad-riesgo y, a su vez, con un bajo valor para el MDEF. Estaríamos refiriéndonos a servicios que, en ocasiones, no ofrecen la funcionalidad requerida, presentan largos periodos de fallos, requieren de mucho tiempo para su restablecimiento, o disponen de un grupo muy limitado de técnicos con capacidad de proporcionar su mantenimiento. En este caso, puede darse la situación de derivar en una decisión que suponga la eliminación del servicio, lo cual supone una parte esencial del ciclo de vida de los servicios, aunque a menudo se ignora. En caso de que se considerase mantener el servicio y, finalmente, se optase por su migración, este grupo de servicios se migrarían en un tercer bloque.
- **No migrar:** este caso corresponde a aquellos servicios que cuentan con alto grado de complejidad-riesgo y bajo valor para el MDEF. Este tipo de servicios únicamente pueden tolerarse si su valor generado, aunque bajo, no llega a ser despreciable y mantenerlo en funcionamiento no comporta un gasto excesivo. Sin embargo, sería recomendable no aumentar la inversión sobre estos servicios por lo que no parece adecuado plantear su migración y, en todo caso, se valoraría su eliminación del Catálogo de Servicios.

4.2.2 Servicios a considerar

Para que el análisis resulte concluyente deberán analizarse un número lo suficientemente significativo de servicios de la I3D, a la vez que deberán definirse posibles casos de migración para los mismos. En este sentido, y con objeto de no desvirtuar este análisis, se excluirán del mismo aquellos servicios que en el MDEF correspondan a:

- Servicios pertenecientes al Dominio de Seguridad Reservado Nacional o DS1.
- Servicios esenciales, entendidos como aquellos servicios desplegados en la I3D que sirven de apoyo a un gran número de servicios, por lo que desde el punto de vista técnico del CESTIC son de vital importancia.

Esta decisión se fundamenta en el hecho de que muchos de estos servicios, podrían devenir en mantenerlos tal y como están actualmente por razones funcionales y de seguridad. Baste como ejemplo pensar en servicios destinados al Mando y Control, pertenecientes por consiguiente al DS1, muchos de los cuales han sido desarrollados como aplicativos específicos “*ad-hoc*” para el MDEF, y no cuentan con una visión de tipo comercial sobre la que aplicar posibles estrategias de migración tal y como se definen en el documento de la referencia [1].

4.2.3 Análisis y resultados

Consideraremos dos ejes de medida, aplicables a los servicios objeto del análisis:

- Eje Beneficio-Valor: por el que la evaluación de los beneficios, permite identificar los servicios que aportan mayor valor al MDEF.
- Eje Complejidad-Riesgo: por el que al clasificar la complejidad de los servicios, se puede determinar el grado de riesgo asumible en el proceso de migración.

Ambos ejes de medida darán lugar a los cuatro posibles casos a considerar, descritos en el punto anterior:

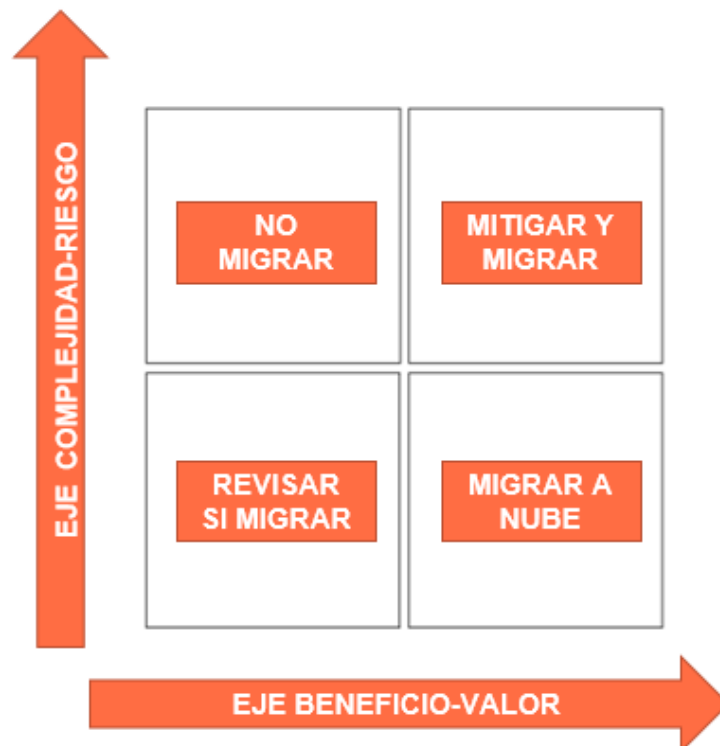


Tabla 4-1 Representación de ejes de medida y posibles casos a considerar para un supuesto práctico de migración de servicios a la Nube MDEF.

Para poder varemar adecuadamente cada uno de los ejes, se han definido una serie de campos de valor en cada uno de ellos. De este modo:

Para el eje Beneficio-Valor:

- Fecha del último paso a producción del servicio: aquellos servicios cuya fecha de último paso a producción sean más cercanas a la actualidad, se consideran con mayor beneficio.
- Proyectos planificados para la evolución del servicio: identifica el potencial de crecimiento y la mejora del servicio, de cara al futuro.
- Número de subidas a producción (correctivos o evolutivos) del servicio a lo largo del último año: proporciona información sobre el estado del servicio y su mantenimiento.
- Tipo de servicio en función del valor aportado al MDEF: el valor aportado al MDEF por las aplicaciones de negocio es mayor que el valor aportado por las aplicaciones de infraestructura.
- Vigencia de los datos del servicio:

Para el eje Complejidad-Riesgo:

- Alto grado de dependencia de comunicación entre procesos: medido a través del número de integraciones del servicio, de modo que cuanto mayor sea el número de integraciones, mayor es la cantidad de sistemas externos y componentes internos que necesitarán ser considerados y adaptados durante el proceso de migración. Todo ello implica un mayor esfuerzo para garantizar la continuidad de las funcionalidades y la interoperabilidad de los sistemas conectados.
- Alto requisito de rendimiento: proporciona información sobre la carga de trabajo y la capacidad del servicio para dar soporte a múltiples usuarios a la vez. Cuanto mayor es el requisito de rendimiento, mayor es la concurrencia de usuarios a la que puede hacer frente.
- Alto requisito de seguridad: especifica si el servicio considerado requiere requisitos adicionales de seguridad, tales como el cifrado de datos sensibles.
- Criticidad del servicio: con objeto de medir el impacto de la indisponibilidad de un servicio concreto, considerándose un un riesgo por el impacto que puede tener durante el proceso de migración.
- Virtualización del servicio: considera si el servicio se aloja sobre servidores físicos o virtuales, en el entendimiento de que si todos los servidores necesarios para proporcionar el servicio están virtualizados, su migración tiene menor complejidad.
- Grado de disponibilidad del servicio: considerando si el servicio está configurado en format mono-nodo o multi-nodo. En el caso de servicios multi-nodo se les supondrá una alta disponibilidad, por lo que la migración respresenta un menor riesgo.
- Grado de estandarización del servicio: aquellos servicios con menor grado de estandarización, o que hayan sido desarrollados de forma específica “*ad-hoc*” para el MDEF, contarán con una mayor complejidad para su migración.

Una vez definidos los casos y servicios a considerar, así como los varemos para valorar cada uno de los campos de los respectivos ejes Beneficio-Valor y Complejidad-Riesgo, se aplican dichos varemos para los distintos servicios de la I3D a considerar (una muestra de 66 servicios), obteniéndose los resultados siguientes para cada caso:

- Migrar a la nube: 14 servicios de 66, lo que equivale a un 21,21 %
- Mitigar riesgos y migrar: 42 servicios de 66, lo que equivale a un 63,63 %
- Revisar si migrar: 6 servicios de 66, lo que equivale a un 9,09 %
- No migrar: 4 servicios de 66, lo que equivale a un 6,06 %

Nombre Servicio	Acciones resultantes
AIDA GESTIÓN DE TURNOS	MIGRAR A NUBE
DICODEF PROVISION	MIGRAR A NUBE
EXPEDIENTES DIGENPER	MIGRAR A NUBE
FCTTD	MIGRAR A NUBE
GESENCU	MIGRAR A NUBE
GESOPRE	MIGRAR A NUBE
GIS	MIGRAR A NUBE
IMPOEXPO	MIGRAR A NUBE
MILES	MIGRAR A NUBE
OFICIALES GENERALES	MIGRAR A NUBE
PASARELA-GEISER	MIGRAR A NUBE
REGISTRO CIVIL	MIGRAR A NUBE
SIGESEVA	MIGRAR A NUBE
TARJETA SANITARIA	MIGRAR A NUBE
3M CODIFICACION	MITIGAR RIESGOS Y MIGRAR
ACCEDA - DEFENSA WEB - SERVICES	MITIGAR RIESGOS Y MIGRAR
ACCEDA DEFENSA Tramitador	MITIGAR RIESGOS Y MIGRAR
ACCEDA Firma Cran	MITIGAR RIESGOS Y MIGRAR
ACCEDA Jabr	MITIGAR RIESGOS Y MIGRAR
ACCEDA SEDE ELECTRONICA	MITIGAR RIESGOS Y MIGRAR
AGT	MITIGAR RIESGOS Y MIGRAR
ASESORIA JURIDICO REGISTRO	MITIGAR RIESGOS Y MIGRAR
ASODEF	MITIGAR RIESGOS Y MIGRAR
ATHOS	MITIGAR RIESGOS Y MIGRAR
BIBLIOTECA VIRTUAL	MITIGAR RIESGOS Y MIGRAR
CAMPAÑA ANTARTICA	MITIGAR RIESGOS Y MIGRAR
CARGA PORTAL CC	MITIGAR RIESGOS Y MIGRAR
CL@VEDEF	MITIGAR RIESGOS Y MIGRAR
COMER	MITIGAR RIESGOS Y MIGRAR
CSV BROKER	MITIGAR RIESGOS Y MIGRAR
CVCDEF	MITIGAR RIESGOS Y MIGRAR
DCORE	MITIGAR RIESGOS Y MIGRAR
DICODEF DICOUSOFT	MITIGAR RIESGOS Y MIGRAR
DIETOOLS	MITIGAR RIESGOS Y MIGRAR
E-DELPHYN	MITIGAR RIESGOS Y MIGRAR
HCIS	MITIGAR RIESGOS Y MIGRAR
NOTIFIC@DEF	MITIGAR RIESGOS Y MIGRAR
PLATAFORMA_BI COGNOS11	MITIGAR RIESGOS Y MIGRAR
PLATAFORMA_BI ETL (TALEND)	MITIGAR RIESGOS Y MIGRAR
PORTAL PERSONAL	MITIGAR RIESGOS Y MIGRAR
RECONFAS	MITIGAR RIESGOS Y MIGRAR
RUBRICA	MITIGAR RIESGOS Y MIGRAR
SALVANY	MITIGAR RIESGOS Y MIGRAR
SAPROMIL	MITIGAR RIESGOS Y MIGRAR
SAS	MITIGAR RIESGOS Y MIGRAR
SCSP V3	MITIGAR RIESGOS Y MIGRAR
SEMILCAR	MITIGAR RIESGOS Y MIGRAR
SETI	MITIGAR RIESGOS Y MIGRAR
SIACUDEF	MITIGAR RIESGOS Y MIGRAR
SIDAE	MITIGAR RIESGOS Y MIGRAR
SIGEI	MITIGAR RIESGOS Y MIGRAR
SINFRADEF	MITIGAR RIESGOS Y MIGRAR
SIPEC	MITIGAR RIESGOS Y MIGRAR
SIPEROPS	MITIGAR RIESGOS Y MIGRAR
SIRSEA	MITIGAR RIESGOS Y MIGRAR
SISANDEF-CENDALA	MITIGAR RIESGOS Y MIGRAR
DIR3DEF	NO MIGRAR
PLATAFORMA_BI COGNOS10	NO MIGRAR
REGISTRO ELECTRONICO	NO MIGRAR
SIPRAM	NO MIGRAR
DIGITADEF	REVISAR SI MIGRAR
DOCAM	REVISAR SI MIGRAR
GESHAB OTAN	REVISAR SI MIGRAR
INGRESOS CRIA CABALLAR	REVISAR SI MIGRAR
SIADIDEF	REVISAR SI MIGRAR
SSRL	REVISAR SI MIGRAR

Tabla 4-2 Acciones resultantes obtenidas sobre una muestra de 66 servicios de la I3D para un supuesto práctico de migración de servicios a la Nube MDEF.

Para poder representar los resultados obtenidos, se ha hecho uso de un gráfico normalizado con valores 01-10 en el que se han representado ambos ejes Beneficio-Valor y Complejidad-Riesgo, dando lugar a cuatro cuadrantes que corresponden con los cuatro posibles casos a considerar.

En el gráfico se ha incluido el parámetro de tamaño de burbuja por servicio, en el entendimiento de representar el número de componentes que forman parte de cada uno de los servicios y emparejar el “volumen de la burbuja” con el “volumen del servicio”.

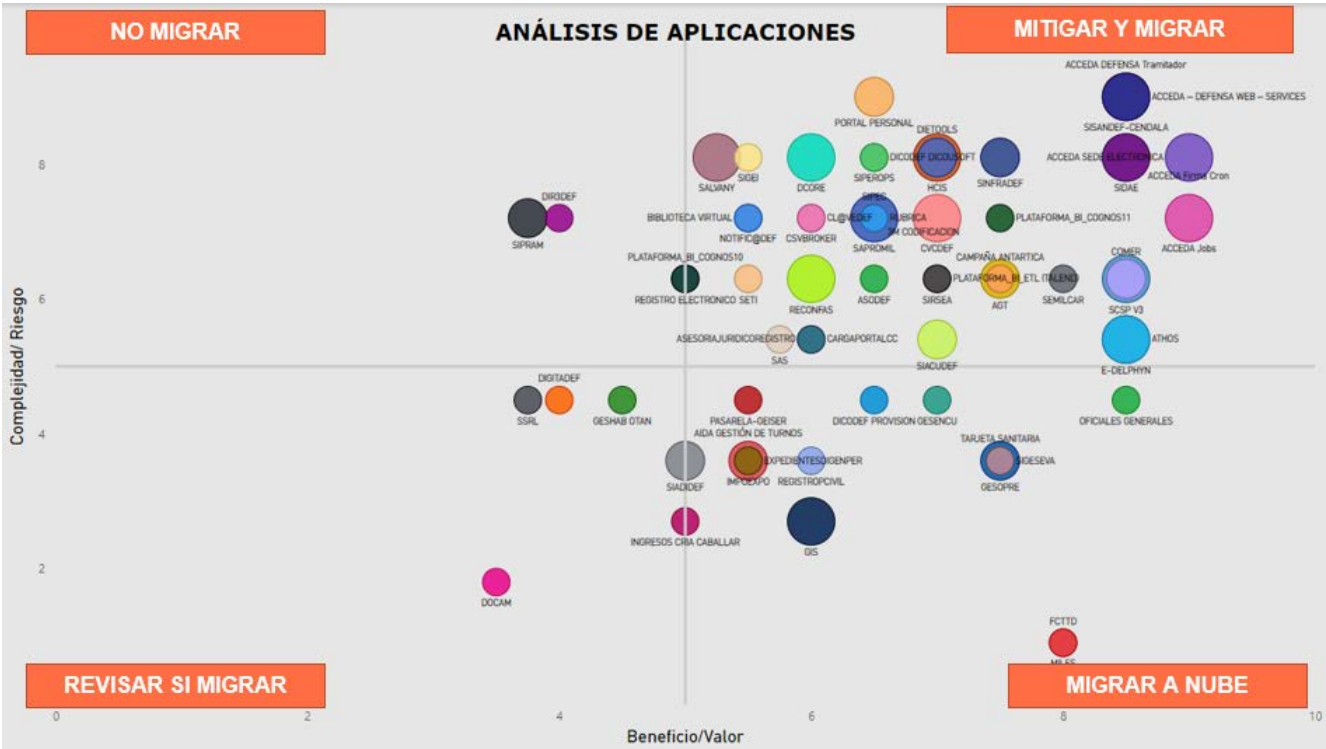


Tabla 4-3 Representación gráfica de las acciones resultantes obtenidas sobre una muestra de 66 servicios de la I3D para un supuesto práctico de migración de servicios a la Nube MDEF.

La conclusión base que se puede extraer, a la vista de la distribución de los servicios a considerar en cada uno de los cuadrantes que representan los casos a considerar, es que la gran mayoría de los servicios (más de un 80 %) están en disposición de ser migrados directamente a nube, o hacerlo tras una revisión inicial dirigida a mitigar carencias y adaptar las características del servicio al entorno de nube. Ambos bloques conformarían, respectivamente, las dos oleadas iniciales de migración de servicios a la Nube MDEF.

Esta conclusión nos conduce a establecer que la implantación del modelo de Nube MDEF planteado tiene sentido a la hora de plantearlo como una evolución de la I3D actual y, sobre la muestra de 66 servicios escogidos, se considera que cumple satisfactoriamente con las necesidades y requerimientos de los servicios CIS/TIC del MDEF.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

5.1.1 Sobre aspectos generales

La tecnología de nube proporciona capacidades constituidas por un conjunto de recursos, servicios y paradigmas tecnológicos, que pueden ser accedidos remotamente, aislando al consumidor de la infraestructura subyacente empleada por el proveedor. La adopción de un modelo de nube en el MDEF no puede tratarse como un mero proceso de implantación tecnológica, sino que implica una evolución que afecta al MDEF como organización, impactando al CESTIC como proveedor de los servicios CIS/TIC, y a sus relaciones con los Ámbitos como destinatarios de estos servicios.

Para maximizar los beneficios y reducir los riesgos de una posible implantación de un modelo de nube en el MDEF, se requiere adoptar una perspectiva transformacional:

- Desplegando la capacidad de forma progresiva, y en armonía con la base tecnológica existente, o base legada, que tendrá que converger progresivamente hacia la nube.
- Evolucionando la arquitectura de las aplicaciones, para facilitar la producción y consumo de los servicios en nube.
- Actualizando los procesos de desarrollo y despliegue, para aprovechar las ventajas que ofrecen los paradigmas de explotación inherentes a la nube.
- Permitiendo la explotación autónoma, pero supervisada, de las capacidades de nube por parte de los Ámbitos del MDEF.
- Armonizando, con sus particularidades, los procesos que intervienen en el ciclo de vida de los servicios en nube.
- Avanzando hacia una gestión centralizada y global de la capacidad CIS/TIC de la I3D que brinda el modelo de nube.
- Promoviendo una adecuada gestión del cambio entre la comunidad CIS/TIC del MDEF, con especial foco en la formación del personal técnico.

De este modo, los beneficios que puede proporcionar al MDEF la adopción de la Nube MDEF, y las expectativas que puede generar, deben fundamentarse exclusivamente en el análisis riguroso de las características y necesidades del propio MDEF, alejándose de argumentos preconcebidos e interesados de los proveedores comerciales de servicios de nube.

En cuanto a posibles riesgos, y derivado del carácter transversal de este modelo, su adopción afecta a múltiples aspectos de la I3D, tales como comunicaciones, infraestructuras, arquitecturas, aplicaciones, seguridad, gestión, operación, normativa, gobierno, inversiones, personal, etc.

Posiblemente, el mayor riesgo a gestionar sea el concerniente al desarrollo, despliegue y puesta a disposición de servicios y aplicaciones, que constituye la utilidad más relevante de la nube. En consecuencia, es preciso conseguir un alineamiento entre los actores, estrategias y estructuras de gobierno CIS/TIC afectadas, llevando a cabo la implantación de la Nube MDEF sin menoscabo de la calidad del servicio y la experiencia de usuario.

Para todo ello, se contemplarán dos líneas de implantación diferenciadas, pero intrínsecamente relacionadas:

- Por un lado, el proceso de implantación de una nube privada del MDEF, para los Dominios de Seguridad DS0 y DS1.
- Por otro lado, las iniciativas de despliegue de servicios, aplicaciones corporativas y capacidades concretas en nubes públicas, tanto comerciales como pertenecientes a Nubes de Terceros.

Para desarrollar ambas líneas de implantación, el MDEF debe mantenerse especialmente atento a aquellos organismos e instituciones que, por su grado de madurez en la adopción de un modelo de nube, ya disponen de lecciones aprendidas sobre sus ventajas e inconvenientes.

Finalmente es preciso mencionar que, sobre ambas líneas de implantación, se deberá considerar prioritaria para el MDEF la correspondiente a la nube privada. Algunos de los motivos que fundamentan el empleo prioritario de una nube privada, además de las condicionantes obvios de seguridad, son:

- La naturaleza de las misiones del MDEF siempre va a requerir inversiones en sus instalaciones, comunicaciones específicas, equipamiento propio, *software* propietario y personal interno para mantener una capacidad de nube privada en la I3D. Es decir, se debe disponer necesariamente de un factor humano y unos recursos que, si están disponibles, siempre van a resultar más ventajosos, en cuanto a lo que supone el coste de mantenimiento interno de un recurso propio, que su equivalente comercial.
- La práctica habitual del MDEF de maximizar el ciclo de vida del equipamiento, propicia la preferencia de la nube privada sobre la pública. También la disposición de una infraestructura adquirida, cuyo mantenimiento puede modularse en función de las disponibilidades presupuestarias, otorga mayor flexibilidad que una contratación forzada externa para poder mantener el servicio.
- El MDEF no presenta casos de uso que sí están presentes en otras organizaciones, normalmente de índole comercial, las cuales aprovechan las capacidades de “pago por uso” de la nube pública, para hacer frente a aumentos estacionales de demanda que puedan exceder significativamente su capacidad CIS/TIC habitual.

5.1.2 Sobre la Nube Privada

La nube privada del MDEF debe constituir la opción prioritaria, sobre las soluciones de nube pública, para alojar servicios y capacidades, puesto que garantiza el cumplimiento de los principios de seguridad hasta los niveles exigidos para el desarrollo de las capacidades operativas de la Fuerza y del resto del MDEF, los cuales precisan de entornos en los que la nube pública no alcanza, actualmente, el grado de seguridad requerido.

El MDEF debe, por ello, llevar a cabo el despliegue de las capacidades de nube privada tanto en el Dominio de Seguridad de Baja Clasificación, DS0 orientado a un carácter corporativo, como en Dominio de Seguridad de Alta Clasificación, DS1 orientado a las operaciones militares y al tratamiento de la información clasificada nacional. Es preciso, por tanto, alcanzar el grado de madurez necesaria para poder proporcionar servicios tecnológicos a la Fuerza y al resto del MDEF, desde la nube privada, asegurando así una autonomía estratégica imprescindible.

Para ello, deben resolverse prioritariamente los aspectos clave que conlleva la adopción de la nube privada, referentes al menos, a su diseño, arquitectura, operación, y seguridad, antes de trasladar dichas cuestiones a la nube pública, el cual es un espacio de mayor complejidad técnica.

Los Ámbitos y el CESTIC, usuarios y proveedor de servicios respectivamente, han de obtener y consolidar las competencias técnicas y realizar los ajustes organizacionales que va a requerir la utilización coherente y gobernada de los Dominios de Seguridad mencionados, con la finalidad de alcanzar los objetivos esenciales del modelo de nube, como son el autoaprovisionamiento y la autogestión de servicios.

Una nube privada efectiva concentraría de forma natural las capacidades CIS/TIC de la I3D, con el CESTIC como “Proveedor de Servicios en la Nube” (PSN) para la nube privada, en el seno del MDEF. El desarrollo de estas capacidades habilitaría la compartición efectiva de los recursos físicos de los Dominios de Seguridad DS0 y DS1 con el resto de Ámbitos del MDEF. De hecho, se podrá hablar propiamente de una nube privada del MDEF cuando el CESTIC pueda ofrecer a los Ámbitos esas capacidades, materializadas en forma de portal de autogestión, equivalente al que ofrecen los proveedores comerciales de nube.

Para obtener su máximo potencial es preciso entender que no se puede concebir la nube privada bajo la perspectiva de los CPD del MDEF actuales. El aprovechamiento de las ventajas de la nube privada dependerá, principalmente, de la habilidad del CESTIC (PSN) para migrar adecuadamente los servicios y aplicaciones a una nueva infraestructura, y adoptar para su explotación las modalidades de provisión *IaaS*, *SaaS* y *PaaS*, de manera sucesiva.

Por ello, y con la finalidad de reducir el coste y complejidad asociado al mantenimiento de los servicios así como dotar de capacidad de autoaprovisionamiento y autogestión de los mismos, es preciso evolucionar el paradigma tradicional de despliegue de servicios hacia:

- La provisión de acceso al almacenamiento, las redes, los servidores y otros recursos informáticos (*IaaS*).
- La disposición de un entorno basado en nube, proporcionando la infraestructura necesaria subyacente, en el cual los usuarios pueden crear, distribuir y gestionar aplicaciones (*PaaS*).
- El suministro de *software* y aplicaciones a través de una *interfaz web* (*SaaS*).

5.1.3 Sobre la Nube Pública

En lo que respecta a las soluciones de nube pública, se estudiarán los casos en los que ésta proporcione un valor diferencial respecto a la nube privada, por el hecho de permitir minimizar el empleo de recursos humanos y tecnológicos propios, siempre escasos, en entornos cuya utilidad sea secundaria y que requirieran el alojamiento de servicios donde prime la inmediatez.

Se debe asumir como principio de diseño una solución “multi-nube” que permita abstraerse de implementaciones comerciales concretas, y proporcione una completa independencia, así como la necesaria autonomía estratégica requerida por el MDEF. No obstante, se tendrá en consideración la dificultad de aplicar este principio estudiando la viabilidad técnica, y los procesos de gestión derivados del traspaso del alojamiento de servicios entre la nube privada y la pública, y entre los diferentes proveedores de nube pública, al evolucionar sus relaciones contractuales con el MDEF. A este respecto, los potenciales escenarios básicos de hibridación/deshibridación que podrían llegar a darse deben considerarse como una referencia, y garantizarse siempre su posible aplicación, para evitar convertir al MDEF en un “cliente cautivo” de un proveedor comercial concreto.

A todos los efectos, las capacidades de nube pública bajo responsabilidad del MDEF deben considerarse una extensión de la I3D y, considerando las misiones y cometidos del MDEF, el grado de adopción de las capacidades de nube pública deberá atender de forma prioritaria a criterios que aseguren su soberanía sobre la información y los canales de acceso a ella, basados en el cumplimiento de las normativas CCN-STIC y las reglamentaciones de protección de datos aplicables al MDEF.

Como cualquier proceso de transformación, y la adopción de capacidades de nube pública en el MDEF lo es, se requiere de un proceso de gestión del cambio que, para la nube pública, implica tener en cuenta las consideraciones siguientes:

- No puede garantizar al MDEF el cumplimiento de todas sus exigencias inherentes al principio de seguridad.
- Precisa de una integración coordinada y segura con una plataforma independiente del proveedor, que cuenta con sus propios medios de monitorización, *backup*, seguridad etc.
- Requiere de competencias específicas que no comparten, necesariamente, estandarizaciones y sinergias con las arquitecturas y productos internos del MDEF.
- Incrementa la superficie de exposición de la I3D, por lo que se deben asignar recursos propios para monitorizaciones y auditorías de seguridad.
- Contrapone un mayor grado de dependencia externa, a pesar del alivio que supone el empleo de recursos ajenos al MDEF.

A pesar de las limitaciones mencionadas, se pueden identificar de inicio algunos casos de uso de nube pública, que podrían resultar de interés para el MDEF:

- *SaaS* en el que un proveedor asume la totalidad del ciclo de vida de un servicio específico del MDEF.
- *SaaS* de aplicaciones genéricas, tales como herramientas de gestión, ofimática o seguridad.
- Aplicaciones que por sus características deban residir fuera de la I3D, o que requieran de acceso a Internet.
- Servicios cuyo ciclo de vida completo se encomiende a un proveedor externo, pero sobre una infraestructura diseñada y securizada por el MDEF, en un *Tenant* específico de su propiedad.
- Servicios requeridos para aplicaciones del MDEF que solo estén disponibles en la nube pública, o requieran de una inversión no justificable para su despliegue en local, como pueden ser los motores de Inteligencia Artificial.

En cualquier caso, el uso futuro de la nube pública estará condicionado por las circunstancias concretas que concurran en cada servicio, y por las capacidades disponibles por parte de los proveedores comerciales de nube.

5.1.4 Sobre la Nube Híbrida

El interés principal del MDEF reside en alcanzar un modelo que permita extender las capacidades de su nube privada, por medio de la integración de los servicios en nube pública ofrecidos por un conjunto de proveedores comerciales. A partir de esta combinación de capacidades, pueden desarrollarse servicios de mayor valor añadido para el MDEF, dando lugar a la versión más completa prevista para la Nube MDEF.

Aunque el caso más habitual sea la hibridación con un proveedor comercial de nube, deberán definirse estándares de diseño para la hibridación que permitan desplegar con agilidad modelos híbridos con otros actores, como la AGE, sumando al modelo las capacidades diferenciales que este entorno, denominado como Nubes de Terceros, puede aportar en aspectos tales como la seguridad por medio del hospedaje de una *Golden Copy*.

En conclusión, el modelo híbrido se presenta como la solución más completa para la Nube MDEF, contando con la posibilidad de combinar las capacidades de las nubes privada y pública expuestas, y permitiendo la integración de ambas y el despliegue de los servicios de manera indistinta. Es preciso destacar, como condicionante de seguridad, que la hibridación implica el desarrollo de un modelo de identidad híbrida cuya fuente autoritativa siempre deberá residir en la nube privada del MDEF.

5.1.5 Sobre la Nube de Combate

La Nube de Combate constituye una iniciativa tecnológica que responde a las necesidades identificadas para el Mando y Control de la Fuerza en las Operaciones Multidominio, que ayudará a mejorar la interoperabilidad, adaptabilidad y eficacia operativa de la propia Fuerza, permitiendo una integración de capacidades más eficiente y una toma de decisiones más ágil y precisa en entornos Multidominio.

Los escenarios que la Nube de Combate deberá afrontar se referirán principalmente a situaciones altamente demandantes, como aquellas relativas a tropas en contacto (*combat engagement*) o que requieran de la aplicación de autodefensa (*selfdefense*). En estos escenarios, abocados a la inmediatez del enfrentamiento, se realizarán acciones en las que no será posible llevar a cabo los procesos habituales de Mando y Control y que conllevará orquestar capacidades de todos los dominios. Estas acciones exigirán gran agilidad y nuevas topologías de Mando y Control distribuidas que permitan a las plataformas interconectarse, constituyendo nubes tácticas, y utilizar armas y sensores con un alto grado de automatización para conseguir los efectos deseados, pero siempre evitando el fratricidio.

Concebida como un “sistema de sistemas” interconectados, la Nube de Combate deberá contar con las siguientes características de diseño:

- Capacidad de almacenar, procesar y compartir información entre todos los dominios, niveles o funciones, tales como inteligencia, logística, vigilancia, objetivos, amenazas, etc.
- Infraestructura global sustentada principalmente sobre las capacidades de comunicaciones y los sistemas de Mando y Control de la Fuerza, incluyendo sensores, sistemas de armas, e interfaces.
- Seguridad, robustez y resiliencia para que cada uno de sus componentes pueda funcionar de forma aislada, en condiciones degradadas o en entornos con conectividad limitada, que puedan tener lugar en el ciberespacio y el espectro electromagnético.
- Modelo evolutivo y ampliable a mayor número de participantes, capacidades y tecnologías.

En cuanto al procesamiento disponible en la Nube de Combate, hay que considerar factores como capacidad de computación, latencia, seguridad y accesibilidad. En este sentido, las soluciones de la futura Nube de Combate ofrecerán alternativas prometedoras para distribuir apropiadamente la carga de trabajo y brindar capacidad de procesamiento cercana a la fuente de los datos, lo que permitirá un análisis más rápido y un mayor rendimiento del sistema, gracias a la optimización del canal de comunicaciones y la hiperconectividad.

La contribución de la Nube de Combate al esquema general de la Nube MDEF, se circunscribirá a su vertiente desplegable permitiendo extender los servicios disponibles en nube a una mayor distancia a vanguardia, y dotando a la Fuerza de las capacidades de Mando y Control necesarias tanto para su preparación como para la ejecución de operaciones militares, incluyendo las Multidominio.

5.2 Líneas futuras

El documento de la referencia [1] establece los principios que regirán la Estrategia de Explotación de la Nube en el MDEF, siendo el primero de ellos el hecho de primar la provisión de servicios CIS/TIC mediante tecnologías de nube respecto al modelo tradicional de servicios, aprovechando los beneficios que ésta aporta.

Este principio denominado Preferencia en Nube (*Cloud First*) se desarrollará por el MDEF en un concepto de empleo de la Nube MDEF, basado en la explotación de una nube híbrida compuesta por una nube privada del propio MDEF y una nube pública, “multi-nube”, externa construida a partir de nubes públicas provenientes tanto de proveedores comerciales como de la AGE (Nubes de Terceros). Tanto este concepto de empleo, como los documentos y normas técnicas derivadas que lo completarán y detallarán, se podrán fundamentar en el contenido recogido en el presente trabajo.

Además, para desarrollar las capacidades necesarias con las que deberá contar la nube privada del MDEF, y teniendo en cuenta el carácter prioritario de ésta sobre la nube pública, será preciso dar respuesta a unos prerequisites previos como primer paso para la implantación de la Nube MDEF:

- El Catálogo de Servicios que ha de ofrecer la nube privada, estipulando la relación de los servicios y capacidades que se pueden prestar desde la Nube MDEF.
- El Modelo de Gobierno, detallando qué se puede hacer en cada Dominio de Seguridad y quién puede hacerlo.
- El Proceso de Transición de servicios, evolucionando desde el modelo tradicional CIS/TIC vigente hacia el de nube.
- El Plan de Gestión del Cambio, prestando especial atención a la evolución de las capacidades de personal requeridas para adoptar y operar el modelo de nube.

La adopción de la nube pública requiere desarrollar los mismos prerequisites expuestos para la nube privada, particularizándolos a la nube pública, aunque se limite su aplicación a un conjunto inicial de casos de uso. El motivo de esta limitación radica en que estos prerequisites serán de utilidad siempre que se especifiquen sobre las capacidades de una solución comercial concreta, lo que requiere establecer un proceso previo de contratación. No se podrán concluir trabajos de diseño sin profundizar en las características de un producto determinado, y éste depende de su obtención de acuerdo con la normativa contractual vigente en el MDEF.

6 BIBLIOGRAFÍA

- [1] Ministerio de Defensa, Resolución 307/08136/21, de 17 de mayo de 2021, del Secretario de Estado de Defensa, por la que se establece la Estrategia de Explotación de la Nube en el Ministerio de Defensa, Madrid: MDEF, 2021.
- [2] Ministerio de Defensa, Orden DEF/2639/2015, de 3 de diciembre de 2015, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, Madrid: MDEF, 2015.
- [3] Ministerio de Defensa, Real Decreto 205/2024, de 27 de febrero de 2024, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, Madrid: MDEF, 2024.
- [4] Ministerio de Asuntos Económicos y Transformación Digital, Estrategia de servicios en la nube híbrida para las Administraciones Públicas, de diciembre de 2022, Madrid: MAETD, 2022.
- [5] OTAN, NATO Enterprise Cloud Adoption Action Plan, de diciembre de 2022, Bruselas: OTAN, 2022.
- [6] US Army, The US Army Cloud Plan, Washington DC: US Army, 2022.
- [7] Ministerio de Asuntos Económicos y Transformación Digital, Real Decreto 311/2022, de 27 de febrero de 2022, por el que se regula el Esquema Nacional de Seguridad, Madrid: MAETD, 2022.
- [8] Ministerio de Defensa, Orden Ministerial 807/2024, de 22 de julio de 2024, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Defensa, Madrid: MDEF, 2024.
- [9] Ministerio de Defensa, Instrucción 58/2016, de 28 de octubre de 2016, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa, Madrid: MDEF, 2016.
- [10] OTAN, «The future of NATO Decision-Making,» de *Seminar Review 2023*, La Haya (Holanda), 2023.
- [11] V. Krishnamurthy, «How to Actualize a Prescriptive Well-Architected Framework,» SPICEWORKS, 27 01 2022. [En línea]. Available: <https://www.spiceworks.com/tech/devops/guest-article/how-to-actualize-a-prescriptive-well->

- p>architected-framework/. [Último acceso: 30 10 2024].
- [12] Microsoft, «What is the Azure Well-Architected Framework?», MICROSOFT, 15 11 2023. [En línea]. Available: <https://learn.microsoft.com/en-us/azure/well-architected/what-is-well-architected-framework>. [Último acceso: 16 10 2024].
 - [13] Microsoft, «Recomendaciones para el uso de zonas de disponibilidad y regiones», MICROSOFT, 14 11 2023. [En línea]. Available: <https://learn.microsoft.com/es-es/azure/well-architected/reliability/regions-availability-zones>. [Último acceso: 16 10 2024].
 - [14] Microsoft, «¿Qué es una zona de aterrizaje de Azure?», MICROSOFT, 07 10 2024. [En línea]. Available: <https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/ready/landing-zone/>. [Último acceso: 16 10 2024].
 - [15] VMware, «Migrar máquinas virtuales», VMware, 15 08 2021. [En línea]. Available: <https://docs.vmware.com/es/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-FE2B516E-7366-4978-B75C-64BF0AC676EB.html>. [Último acceso: 16 10 2024].
 - [16] Ministerio de Defensa, Manuel Buesa Bueno, Transformación digital de las FAS para el Combate Multidominio, Madrid: MDEF, 2024.
 - [17] Ministerio de Defensa, Mando y Control de las Operaciones Multidominio, Madrid: MDEF, 2024.
 - [18] Ministerio de Defensa, Visión del JEMAD de la Nube de Combate, Madrid: MDEF, 2024.
 - [19] Amazon Web Services, «How Amazon is assisting in Ukraine», AWS, 21 06 2023. [En línea]. Available: <https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine>. [Último acceso: 02 11 2024].
 - [20] Amazon Web Services, «AWS employees help secure vital data so the Ukrainian government, education, and banking institutions can continue to serve Ukrainian people.», AWS, 14 04 2023. [En línea]. Available: <https://www.aboutamazon.eu/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future>. [Último acceso: 02 11 2024].
 - [21] Amazon Web Services, «Actualización de Seguridad Nacional y Defensa AWS», de *Conferencia de Seguridad Nacional y Defensa para ISDEFE*, Madrid, 2024.
 - [22] Ministerio de Defensa, Resolución 300/10776/24, de 28 de junio de 2024, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de Implantación del concepto de seguridad Confianza Cero en el Ministerio de Defensa, Madrid: MDEF, 2024.
 - [23] Ministerio de Defensa, Resolución 400/06254/23, de 9 de marzo de 2023, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de Desarrollo de Software en el Ministerio de Defensa, Madrid: MDEF, 2023.
 - [24] Microsoft, «Diseño de soluciones multiinquilino en Azure», MICROSOFT, 22 07 2024. [En línea]. Available: <https://learn.microsoft.com/es-es/azure/architecture/guide/multitenant/overview>. [Último acceso: 18 11 2024].
 - [25] Microsoft, «Antipatrón Vecino ruidoso», MICROSOFT, 13 04 2024. [En línea]. Available: <https://learn.microsoft.com/es-es/azure/architecture/antipatterns/noisy-neighbor/noisy-neighbor>. [Último acceso: 18 11 2024].

- [26] J. Rosales, «Capex y Opex en la gestión del mantenimiento,» FRACTTAL, 25 08 2023. [En línea]. Available: <https://www.fracttal.com/es/mantenipedia/capex-vs-opex-y-sus-diferencias>. [Último acceso: 18 11 2024].
- [27] Amazon Web Services, «What is AWS Billing and Cost Management?,» AWS, 25 01 2024. [En línea]. Available: <https://docs.aws.amazon.com/cost-management/latest/userguide/what-is-costmanagement.html>. [Último acceso: 18 11 2024].
- [28] FinOps Foundation, «Key 2024 Changes to the FinOps Framework,» FINOPS FOUNDATION, 21 03 2024. [En línea]. Available: <https://www.finops.org/insights/2024-finops-framework/>. [Último acceso: 18 11 2024].
- [29] Microsoft, «Microsoft joins the FinOps Foundation,» MICROSOFT, 14 02 2023. [En línea]. Available: <https://azure.microsoft.com/es-es/blog/microsoft-joins-the-finops-foundation/>. [Último acceso: 18 11 2024].
- [30] Microsoft, «¿Qué es la identidad híbrida con Microsoft Entra ID?,» MICROSOFT, 06 11 2023. [En línea]. Available: <https://learn.microsoft.com/es-es/entra/identity/hybrid/whatis-hybrid-identity>. [Último acceso: 22 11 2024].
- [31] Microsoft, «¿Qué es Microsoft Entra Connect?,» MICROSOFT, 06 11 2023. [En línea]. Available: <https://learn.microsoft.com/es-es/entra/identity/hybrid/connect/whatis-azure-ad-connect>. [Último acceso: 22 11 2024].
- [32] Microsoft, «¿Qué métodos de autenticación y comprobación están disponibles en Microsoft Entra ID?,» MICROSOFT, 18 11 2024. [En línea]. Available: <https://learn.microsoft.com/es-es/entra/identity/authentication/concept-authentication-methods>. [Último acceso: 02 12 2024].
- [33] Microsoft, «¿Qué es TPM?,» MICROSOFT, 01 08 2021. [En línea]. Available: <https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-tpm-705f241d-025d-4470-80c5-4feeb24fa1ee>. [Último acceso: 02 12 2024].
- [34] FIDO Alliance, «FIDO Authentication, a passwordless vision,» FIDO, 2024. [En línea]. Available: <https://fidoalliance.org/fido2/>. [Último acceso: 02 12 2024].
- [35] Centro Criptológico Nacional, «10 Claves para la prevención proactiva,» CCN, 07 06 2022. [En línea]. Available: <https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert/11832-nueva-infografia-sobre-el-decalogo-para-la-prevencion-proactiva.html>. [Último acceso: 02 12 2024].
- [36] Microsoft, «Introducción a la autenticación basada en certificados de Microsoft Entra,» MICROSOFT, 06 06 2024. [En línea]. Available: <https://learn.microsoft.com/es-es/entra/identity/authentication/concept-certificate-based-authentication>. [Último acceso: 02 12 2024].
- [37] INCIBE, «Maximizando la seguridad en la nube: el rol esencial de los CASB,» INCIBE, 2024. [En línea]. Available: <https://www.incibe.es/incibe-cert/blog/maximizando-la-seguridad-en-la-nube-el-rol-esencial-de-los-casb>. [Último acceso: 04 12 2024].
- [38] Microsoft, «¿Qué es un agente de seguridad de acceso a la nube (CASB)?,» MICROSOFT, 11 07 2024. [En línea]. Available: <https://www.microsoft.com/es-es/security/business/security-101/what-is-a-cloud-access-security-broker-casb>. [Último acceso: 4 12 2024].

- [39] Microsoft, «Simplified Zero Trust security with the Microsoft Entra Suite,» MICROSOFT, 11 07 2024. [En línea]. Available: <https://www.microsoft.com/en-us/security/blog/2024/07/11/simplified-zero-trust-security-with-the-microsoft-entra-suite-and-unified-security-operations-platform-now-generally-available/>. [Último acceso: 04 12 2024].
- [40] Centro Criptológico Nacional, «Guías CCN-STIC,» CCN, 2024. [En línea]. Available: <https://www.ccn-cert.cni.es/es/guias.html>. [Último acceso: 04 12 2024].
- [41] INCIBE, «¿Ya tienes tu Plan de Recuperación ante Desastres?,» INCIBE, 2019. [En línea]. Available: <https://www.incibe.es/empresas/blog/tienes-tu-plan-recuperacion-desastres>. [Último acceso: 04 12 2024].
- [42] VERITAS, «La regla de copia de seguridad 3-2-1: asegurar la protección y recuperación de datos,» VERITAS, 2023. [En línea]. Available: <https://www.veritas.com/es/es/information-center/3-2-1-backup-rule>. [Último acceso: 04 12 2024].
- [43] Microsoft, «Azure Storage redundancy,» MICROSOFT, 19 01 2024. [En línea]. Available: <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy>. [Último acceso: 04 12 2024].
- [44] INCIBE, «Cómo actuar en caso de un ataque de ransomware,» INCIBE, 2024. [En línea]. Available: <https://www.incibe.es/ciudadania/ayuda/ransomware>. [Último acceso: 04 12 2024].
- [45] Microsoft, «Creación de plan de migración con Azure Migrate,» MICROSOFT, 26 09 2024. [En línea]. Available: <https://learn.microsoft.com/es-es/azure/migrate/concepts-migration-planning>. [Último acceso: 11 12 2024].
- [46] Microsoft, «Introducción a Azure Migrate,» MICROSOFT, 29 09 2024. [En línea]. Available: <https://learn.microsoft.com/es-es/azure/migrate/migrate-services-overview>. [Último acceso: 11 12 2024].
- [47] Amazon Web Services, «Migración y modernización con AWS,» AWS, 15 08 2024. [En línea]. Available: <https://aws.amazon.com/es/migrate-modernize-build/cloud-migration/>. [Último acceso: 11 12 2024].
- [48] Amazon Web Services, «Programa de aceleración de la migración a AWS,» AWS, 15 08 2024. [En línea]. Available: <https://aws.amazon.com/es/migration-acceleration-program/>. [Último acceso: 11 12 2024].
- [49] Microsoft, «Cloud rationalization,» MICROSOFT, 06 07 2023. [En línea]. Available: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/digital-estate/5-rs-of-rationalization>. [Último acceso: 11 12 2024].
- [50] Amazon Web Services, «Prioritization and migration strategy,» AWS, 04 07 2024. [En línea]. Available: <https://docs.aws.amazon.com/prescriptive-guidance/latest/application-portfolio-assessment-guide/prioritization-and-migration-strategy.html#migration-r-type>. [Último acceso: 11 12 2024].

ANEXO I: ABREVIATURAS Y ACRÓNIMOS

Las definiciones, abreviaturas y acrónimos que se incorporan en esta tabla son acepciones aplicadas por el MDEF a conceptos comunes, o términos propios que designan otros particulares, y se recogen para facilitar la comprensión del trabajo:

AGE	Administración General del Estado
C2	Mando y Control
CCN	Centro Criptológico Nacional
CESTIC	Centro de Sistemas y Tecnologías de la Información y las Comunicaciones
CIS	Sistemas de Información y Comunicaciones
CPD	Centro de Procesamiento de Datos
DGAM	Dirección General de Armamento y Material
DICODEF	Directorio Corporativo del Ministerio de Defensa
DS0	Dominio de Seguridad No Clasificado
DS1	Dominio de Seguridad Reservado Nacional
DS2	Dominio de Seguridad <i>NATO Secret</i> (correspondiente a OTAN)
DS3	Dominio de Seguridad <i>EU Secret</i> (correspondiente a UE)
EMAD	Estado Mayor de la Defensa
ENS	Esquema Nacional de Seguridad
GTP	Grupo de Trabajo Permanente
I3D	Infraestructura Integral de Información para la Defensa
MCCE	Mando Conjunto del Ciberespacio (perteneciente al EMAD)
MDEF	Ministerio de Defensa
MDO	Operaciones Multidominio
OTAN	Organización del Tratado del Atlántico Norte
PKIDEF	Servicio de Infraestructura de Clave Pública del Ministerio de Defensa
SEDEF	Secretario de Estado del Ministerio de Defensa
SEGENPOL	Secretario General de Política de Defensa
SIPERDEF	Sistema de Información de Personal del Ministerio de Defensa
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
SUBDEF	Subsecretario de Estado del Ministerio de Defensa
TEMD	Tarjeta Electrónica del Ministerio de Defensa
TFM	Trabajo de Fin de Máster
TIC	Tecnologías de la Información y las Comunicaciones
TN	Territorio Nacional

UE	Unión Europea
UME	Unidad Militar de Emergencias
USOP	Uso Público (referido a información)
USOF	Uso Oficial (referido a información)
WAN PG	Red WAN de Propósito General
ZO	Zona de Operaciones

ANEXO II: CÁLCULO Y ANÁLISIS DE RESULTADOS SOBRE UN SUPUESTO PRÁCTICO DE MIGRACIÓN DE SERVICIOS A LA NUBE MDEF

Se adjunta, como anexo, la hoja de cálculo utilizada para el desarrollo del Capítulo 4 del presente trabajo.

En dicha hoja de cálculo se incluyen y detallan los criterios de valoración escogidos junto con las varemaciones asignadas en los diferentes campos, para la muestra de 66 servicios de la I3D considerada en el supuesto práctico.

Análisis de criterios de migración

Nombre Servicio	Beneficio	Riesgo	Tamaño Burbuja
3M CODIFICACION	6,5	7,2	0,10
ACCEDA – DEFENSA WEB – SERVICES	8,5	9	0,30
ACCEDA DEFENSA Tramitador	8,5	9	0,30
ACCEDA Firma Cron	8,5	8,1	0,30
ACCEDA Jobs	9	7,2	0,30
ACCEDA SEDE ELECTRONICA	9	8,1	0,30
AGT	7,5	6,3	0,20
AIDA GESTIÓN DE TURNOS	5,5	3,6	0,20
ASESORIA JURIDICO REGISTRO	6	5,4	0,10
ASODEF	6,5	6,3	0,10
ATHOS	8,5	5,4	0,30
BIBLIOTECA VIRTUAL	5,5	7,2	0,10
CAMPAÑA ANTARTICA	7,5	6,3	0,10
CARGA PORTALCC	6	5,4	0,10
CL@VEDEF	6	7,2	0,10
COMER	8,5	6,3	0,20
CSV BROKER	6	7,2	0,10
CVCDEF	7	7,2	0,30
DCORE	6	8,1	0,30
DICODEF DICOUSOFT	6,5	8,1	0,10
DICODEF PROVISION	6,5	4,5	0,10
DIETOOLS	7	8,1	0,20
DIGITADEF	4	4,5	0,10
DIR3DEF	4	7,2	0,10
DOCAM	3,5	1,8	0,10
E-DELPHYN	8,5	5,4	0,30
EXPEDIENTES DIGENPER	5,5	3,6	0,10
FCTTD	8	0,9	0,10
GESENCU	7	4,5	0,10
GESHAB OTAN	4,5	4,5	0,10
GESOPRE	7,5	3,6	0,20
GIS	6	2,7	0,30
HCIS	7	8,1	0,30
IMPOEXPO	5,5	3,6	0,10
INGRESOS CRIA CABALLAR	5	2,7	0,10
MILES	8	0,9	0,10
NOTIFIC@DEF	5,5	7,2	0,10
OFICIALES GENERALES	8,5	4,5	0,10
PASARELA-GEISER	5,5	4,5	0,10
PLATAFORMA_BI_COGNOS10	5	6,3	0,10
PLATAFORMA_BI_COGNOS11	7,5	7,2	0,10
PLATAFORMA_BI_ETL (TALEND)	7	6,3	0,10
PORTAL PERSONAL	6,5	9	0,20
RECONFAS	6	6,3	0,30
REGISTRO ELECTRONICO	5	6,3	0,10
REGISTRO PCIVIL	6	3,6	0,10
RUBRICA	6,5	7,2	0,10
SALVANY	5,25	8,1	0,30
SAPROMIL	6,5	7,2	0,30
SIADIDEF	5	3,6	0,20
SIDAE	8,5	8,1	0,30
SIGEI	5,5	8,1	0,10
SIGESEVA	7,5	3,6	0,10
SINFRADEF	7,5	8,1	0,20
SIPEC	6,5	7,2	0,10
SIPEROPS	6,5	8,1	0,10
SIPRAM	3,75	7,2	0,20
SIRSEA	7	6,3	0,10
SISANDEF-CENDALA	8,5	9	0,30
SSRL	3,75	4,5	0,10
TARJETA SANITARIA	7,5	3,6	0,10

Resultados análisis de migración

Nombre Servicio	Beneficio	Riesgo	Tamaño Burbuja
3M CODIFICACION	13	8	0,10
ACCEDA – DEFENSA WEB – SERVICES	17	10	0,30
ACCEDA DEFENSA Tramitador	17	10	0,30
ACCEDA Firma Cron	17	9	0,30
ACCEDA Jobs	18	8	0,30
ACCEDA SEDE ELECTRONICA	18	9	0,30
AGT	15	7	0,20
AIDA GESTIÓN DE TURNOS	11	4	0,20
ASESORIAJURIDICOREGISTRO	12	6	0,10
ASODEF	13	7	0,10
ATHOS	17	6	0,30
BIBLIOTECA VIRTUAL	11	8	0,10
CAMPAÑA ANTARTICA	15	7	0,10
CARGAPORTALCC	12	6	0,10
CL@VEDEF	12	8	0,10
COMER	17	7	0,20
CSVBROKER	12	8	0,10
CVCDEF	14	8	0,30
DCORE	12	9	0,30
DICODEF DICOUSOFT	13	9	0,10
DICODEF PROVISION	13	5	0,10
DIETOOLS	14	9	0,20
DIGITADEF	8	5	0,10
DIR3DEF	8	8	0,10
DOCAM	7	2	0,10
E-DELPHYN	17	6	0,30
EXPEDIENTESDIGENPER	11	4	0,10
FCTTD	16	1	0,10
GESENCU	14	5	0,10
GESHAB OTAN	9	5	0,10
GESOPRE	15	4	0,20
GIS	12	3	0,30
HCIS	14	9	0,30
IMPOEXPO	11	4	0,10
INGRESOS CRIA CABALLAR	10	3	0,10
MILES	16	1	0,10
NOTIFIC@DEF	11	8	0,10
OFICIALES GENERALES	17	5	0,10
PASARELA-GEISER	11	5	0,10
PLATAFORMA_BI_COGNOS10	10	7	0,10
PLATAFORMA_BI_COGNOS11	15	8	0,10
PLATAFORMA_BI_ETL (TALEND)	14	7	0,10
PORTAL PERSONAL	13	10	0,20
RECONFAS	12	7	0,30
REGISTRO ELECTRONICO	10	7	0,10
REGISTROPCIVIL	12	4	0,10
RUBRICA	13	8	0,10
SALVANY	10,5	9	0,30
SAPROMIL	13	8	0,30
SAS	11,5	6	0,10
SCSP V3	17	7	0,30
SEMILCAR	16	7	0,10
SETI	11	7	0,10
SIACUDEF	14	6	0,20
SIADIDEF	10	4	0,20
SIDAE	17	9	0,30
SIGEI	11	9	0,10
SIGESEVA	15	4	0,10
SINFRADEF	15	9	0,20
SIPEC	13	8	0,10
SIPEROPS	13	9	0,10
SIPRAM	7,5	8	0,20
SIRSEA	14	7	0,10
SISANDEF-CENDALA	17	10	0,30
SSRL	7,5	5	0,10
TARJETA SANITARIA	15	4	0,10

Nombre Servicio	Acciones resultantes
3M CODIFICACION	MITIGAR RIESGOS Y MIGRAR
ACCEDA – DEFENSA WEB – SERVICES	MITIGAR RIESGOS Y MIGRAR
ACCEDA DEFENSA Tramitador	MITIGAR RIESGOS Y MIGRAR
ACCEDA Firma Cron	MITIGAR RIESGOS Y MIGRAR
ACCEDA Jobs	MITIGAR RIESGOS Y MIGRAR
ACCEDA SEDE ELECTRONICA	MITIGAR RIESGOS Y MIGRAR
AGT	MITIGAR RIESGOS Y MIGRAR
AIDA GESTIÓN DE TURNOS	MIGRAR A NUBE
ASESORIAJURIDICOREGISTRO	MITIGAR RIESGOS Y MIGRAR
ASODEF	MITIGAR RIESGOS Y MIGRAR
ATHOS	MITIGAR RIESGOS Y MIGRAR
BIBLIOTECA VIRTUAL	MITIGAR RIESGOS Y MIGRAR
CAMPAÑA ANTARTICA	MITIGAR RIESGOS Y MIGRAR
CARGAPORTALCC	MITIGAR RIESGOS Y MIGRAR
CL@VEDEF	MITIGAR RIESGOS Y MIGRAR
COMER	MITIGAR RIESGOS Y MIGRAR
CSVBRKER	MITIGAR RIESGOS Y MIGRAR
CVCDEF	MITIGAR RIESGOS Y MIGRAR
DCORE	MITIGAR RIESGOS Y MIGRAR
DICODEF DICOUSOFT	MITIGAR RIESGOS Y MIGRAR
DICODEF PROVISION	MIGRAR A NUBE
DIETOOLS	MITIGAR RIESGOS Y MIGRAR
DIGITADEF	REVISAR SI MIGRAR
DIR3DEF	NO MIGRAR
DOCAM	REVISAR SI MIGRAR
E-DELPHYN	MITIGAR RIESGOS Y MIGRAR
EXPEDIENTESDIGNPER	MIGRAR A NUBE
FCTTD	MIGRAR A NUBE
GESENCU	MIGRAR A NUBE
GESHAB OTAN	REVISAR SI MIGRAR
GESOPRE	MIGRAR A NUBE
GIS	MIGRAR A NUBE
HCIS	MITIGAR RIESGOS Y MIGRAR
IMPOEXPO	MIGRAR A NUBE
INGRESOS CRIA CABALLAR	REVISAR SI MIGRAR
MILES	MIGRAR A NUBE
NOTIFIC@DEF	MITIGAR RIESGOS Y MIGRAR
OFICIALES GENERALES	MIGRAR A NUBE
PASARELA-GEISER	MIGRAR A NUBE
PLATAFORMA_BI_COGNOS10	NO MIGRAR
PLATAFORMA_BI_COGNOS11	MITIGAR RIESGOS Y MIGRAR
PLATAFORMA_BI_ETL (TALEND)	MITIGAR RIESGOS Y MIGRAR
PORTAL PERSONAL	MITIGAR RIESGOS Y MIGRAR
RECONFAS	MITIGAR RIESGOS Y MIGRAR
REGISTRO ELECTRONICO	NO MIGRAR
REGISTROPCIVIL	MIGRAR A NUBE
RUBRICA	MITIGAR RIESGOS Y MIGRAR
SALVANY	MITIGAR RIESGOS Y MIGRAR
SAPROMIL	MITIGAR RIESGOS Y MIGRAR
SAS	MITIGAR RIESGOS Y MIGRAR
SCSP V3	MITIGAR RIESGOS Y MIGRAR
SEMILCAR	MITIGAR RIESGOS Y MIGRAR
SETI	MITIGAR RIESGOS Y MIGRAR
SIACUDEF	MITIGAR RIESGOS Y MIGRAR
SIADIDEF	REVISAR SI MIGRAR
SIDAE	MITIGAR RIESGOS Y MIGRAR
SIGEI	MITIGAR RIESGOS Y MIGRAR
SIGSEVA	MIGRAR A NUBE
SINFRADEF	MITIGAR RIESGOS Y MIGRAR
SIPEC	MITIGAR RIESGOS Y MIGRAR
SIPEROPS	MITIGAR RIESGOS Y MIGRAR
SIPRAM	NO MIGRAR
SIRSEA	MITIGAR RIESGOS Y MIGRAR
SISANDEF-CENDALA	MITIGAR RIESGOS Y MIGRAR
SSRL	REVISAR SI MIGRAR
TARJETA SANITARIA	MIGRAR A NUBE

Tipo	Clasificación	Nombre del criterio	Descripción	Justificación	Peso
Beneficio	Vida útil restante	Obsolescencia funcional	Percepción de si el servicio no cubre todas las necesidades para las que fue diseñado.	Identifica posibles limitaciones funcionales y ayuda a determinar si son necesarias acciones de mejora o actualizaciones. Cuanto más baja mayor beneficio.	Alta: 1 Media: 2 Baja: 3
Beneficio	Vida útil restante	Fecha de discontinuación prevista	Fecha de baja en caso de que esté prevista.	Se considera con menor beneficio aquellos servicios cuya fecha de discontinuación está prevista en un futuro cercano.	2025: 1 2030: 1 2099: 2 No informada: 0
Beneficio	Vida útil restante	Fecha de último paso a producción	Fecha último paso a producción del servicio.	Aquellos servicios cuya fecha de último paso a producción sean más cercanas a la actualidad, se consideran con mayor beneficio.	2024: 5 2023: 4 2022: 4 2021: 3 2020: 3 2019: 2 2018: 1 < 2018: 0 NO INFORMADA: 0
Beneficio	General	Proyectos planificados para la evolución	Descripción de los proyectos planificados para la evolución del servicio.	Identifica el potencial de crecimiento y mejora del servicio en el futuro.	Si: 2 No: 1 0: 0 No Aplica: 0
Beneficio	General	Nº Subidas de correctivos	Nº subidas a producción año anterior.	Proporciona información sobre el estado del servicio y su mantenimiento.	0: 0 < 6 / año: 1 6-12 / año: 2 > 12 / año: 3 No Aplica: 0,5
Beneficio	Soporte al negocio	Tipo de servicio	Infraestructura/Negocio.	El valor al negocio aportado por los servicios de negocio es mayor al valor aportado por los servicios de infraestructura.	Infraestructura: 1 Negocio: 2
Beneficio	General	Vigencia de datos (años)	Años durante los que se mantienen los datos del servicio.	Aquellos servicios cuyos datos tienen mayor vigencia en el tiempo, se consideran con mayor aporte al negocio.	De 5-10 años: 1 De 10-20 años: 2 >20 años: 3 0: 0
Beneficio	General	Beneficio			
Riesgo	Alto grado de dependencia de red	Canales de acceso	Indica los canales desde los que es accesible el servicio.	Es posible evaluar las modificaciones necesarias para que el programa sea utilizable en diversos entornos. Lo más complejo es la Interfaz de aplicación, Intranet e Internet y luego Web e Intranet, Web, e Intranet.	Intranet: 1 Web: 2 Web e Intranet: 2 Intranet e Internet: 3 Interfaz aplicación: 4 No aplica: 0
Riesgo	Alto grado de dependencia de red	Nº Usuarios	Número total de usuarios que tienen acceso al servicio (se contará un usuario por acceso aunque el número de accesos sea mayor).	El número de usuarios ayuda a medir la amplitud del uso de la aplicación y la importancia en términos de alcance de usuarios, de forma que hay mayor dependencia de red cuanto mayor es el número de usuarios.	<100: 1 100-500: 2 500-1000: 3 >1000: 4 >10000: 5 Todos: 6
Riesgo	Bases de datos compartidas	Esquema a migrar de la BBDD	Si varias aplicaciones utilizan la misma base de datos para almacenar y acceder a sus datos, medido con el esquema a migrar de la base de datos	En la pestaña BBDD, se ha aplicado un filtro para ver si distintas aplicaciones comparten el mismo esquema a migrar. Si comparten es SI, sino comparten es NO.	Si: 2 No: 1
Riesgo	Elementos de infraestructura compartidos	Servidores	Situación en la que varias aplicaciones comparten recursos o componentes de infraestructura, en este caso, medido con los servidores. Si un servidor forma parte de distintas aplicaciones.	Para esta categoría se han observado los servidores de las aplicaciones para ver si había un mismo servidor para varias aplicaciones, lo que se clasificaría como SI y si no comparte servidor, sería un No. De esta forma, según la pestaña de Servidores, se ha filtrado por Hostname para ver si ese nombre del servidor era usado en aplicaciones distintas.	Si: 2 No: 1
Riesgo	Alto grado de dependencia de comunicación de procesos	Nº de integraciones	Define el número de integraciones que hay entre las distintas aplicaciones.	Se ha empleado el criterio del número de integraciones de cada aplicación que indica que cuantas más integraciones, mayor es la cantidad de sistemas externos y componentes internos que necesitarán ser considerados y adaptados durante el proceso de migración, lo que implica un mayor esfuerzo para garantizar la continuidad de las funcionalidades y la interoperabilidad de los sistemas conectados.	Si: 2 No: 1
Riesgo	Alto requisito de rendimiento	Concurrencia de usuarios	Número de usuarios que acceden a la vez.	Proporciona información sobre la carga de trabajo y la capacidad del servicio para dar soporte a múltiples usuarios a la vez. Cuanto mayor es el requisito de rendimiento, mayor es la concurrencia.	<10: 1 Entre 10-50: 2 >50: 3 0: 0
Riesgo	Alto requisito de seguridad	Existencia de datos sensibles	Manejo de datos sensibles.	Implica requisitos adicionales de seguridad y privacidad y sacar a la luz la necesidad de cifrado de datos sensibles o implantar controles de acceso adecuados para proteger la confidencialidad.	Si: 2 No: 1
Riesgo	Alto requisito de seguridad	Categoría ENS	Cumplimiento de requisitos del ENS.	El cumplimiento de la normativa del ENS (Esquema Nacional de Seguridad) incluye la utilización de un marco de referencia y reglamentario para salvaguardar la seguridad de los sistemas de información, lo que ayuda a decidir qué medidas de seguridad deben utilizarse durante la migración.	Alto: 3 Medio: 2 Bajo: 1 0: 0
Riesgo	Alto requisito de seguridad	Ámbito de seguridad	Ámbito que hace uso del servicio.	El grado de protección y clasificación necesario para el servicio dependiendo del Ámbito que hace uso del mismo, y teniendo en cuenta las precauciones y requisitos de seguridad necesarios dentro del Ámbito.	SUBDEF: 1 SEDEF: 1 SEGENPOL: 1 AIRE: 1 TIERRA: 1 EMAD: 1 ARMADA: 1 SIN DEFINIR: 0 CESTIC: 1
Riesgo	Alto requisito de seguridad	Grado de seguridad	Grado de seguridad de la información que se maneja.	La finalidad y el uso del servicio, en términos de seguridad, hacen evidente que las normas y controles de seguridad deben adaptarse a los requisitos y limitaciones de la información que maneja.	SINCLAS - PROPÓSITO GENERAL: 1 SINCLAS - USO OFICIAL: 2 SINCLAS - USO PÚBLICO: 1 OTROS: 0
Riesgo	General	Criticidad	Mide si el servicio es necesario para garantizar la continuidad de las misiones y cometidos.	Es necesario caracterizar el impacto de la indisponibilidad de un servicio concreto. La criticidad se considera un riesgo por el impacto que puede tener durante la migración.	Si: 2 No: 1
Riesgo	Grado de estandarización/modernización	Arquitectura de la aplicación	Modelo de Arquitectura de la Aplicación.	Una migración compleja modifica la arquitectura existente, lo que exige un examen en profundidad de las interdependencias entre componentes y una planificación de su transferencia o reconfiguración. De forma que lo más complejo es una arquitectura de aplicación de Servicios Middleware, seguida por Cliente-Servidor, Escritorio y Web.	Aplicación Cliente-Servidor: 3 Aplicación Escritorio: 2 Aplicación Web: 1 Otros: 0,5 Servicios Middleware: 4 Aplicación HOST: 5
Riesgo	Grado de estandarización/modernización	Tecnologías de desarrollo de la aplicación	Tecnologías de desarrollo de la Aplicación (Java, .Net, PHP, Otros).	Debido a su accesibilidad, madurez y compatibilidad con el entorno de destino, las tecnologías empleadas en el desarrollo de la aplicación pueden influir en la complejidad de la migración. Donde las mas complejas son Java/.Net, seguida de PHP/Java, Java, .net y PHP.	.Net: 3 Java: 4 PHP: 2 PHP / Java: 5 Otros: 0,5 Producto propietario: 1 Java / .Net: 6
Riesgo	Grado de estandarización/modernización	Nivel de deuda técnica	La deuda técnica se origina debido a deficiencias en el código que, por falta de tiempo o presupuesto, obligan a adoptar una solución más rápida del problema, aunque deficiente.	Aquellas aplicaciones con elevada deuda técnica, requerirán mayor complejidad debido a la posible ausencia de estandarización y calidad.	Alto: 3 Medio: 2 Bajo: 1 0: 0
Riesgo	General	Configuración de disponibilidad	Configuración de disponibilidad del servicio (mono-nodo, multi-nodo).	Aquellos servicios cuya disponibilidad esté configurada en multi-nodo implicarán menor complejidad durante la migración.	Otros: 2 Alta disponibilidad mono-nodo: 2 Mono-instantánea: 2 Alta disponibilidad multi-nodo: 1 0: 0
Riesgo	General	Virtualización	Mide si el servicio presenta servidores físicos, ya que supondrán un mayor riesgo, o no los presenta.	Si todos los servidores del servicio están virtualizados, presenta menor complejidad de migración, mientras que si cuenta con servidores físicos tendrá mayor complejidad en la migración.	Si: 1 No: 0
Tamaño de Burbuja	Tamaño	Volumen de componentes	Número de componentes que tiene el servicio.	Aquellos servicios cuyo volumen de componentes sea mayor, tendrán un tamaño de burbuja mayor.	Alto: 0,3 Medio: 0,2 Bajo: 0,1

EJE COMPLEJIDAD-RIESGO												
Nombre Aplicación	Alto grado de dependencia de red	Bases de datos compartidas	Elementos de infraestructura compartidos	Alto grado de dependencia de comunicación de procesos	Alto requisito de rendimiento	Alto requisito de seguridad	Criticidad	Virtualización	Grado de disponibilidad	Alto grado de modernización/estandarización	Complejidad	Puntuación
3M CODIFICACION	SI	NO	SI	NO	NO	SI	SI	SI	SI	SI		8
ACCEDA – DEFENSA WEB – SERVICES	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI		10
ACCEDA DEFENSA Tramitador	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI		10
ACCEDA Firma Cron	SI	SI	SI	NO	SI	SI	SI	NO	SI	SI		9
ACCEDA Jobs	SI	SI	NO	NO	SI	SI	SI	NO	SI	SI		8
ACCEDA SEDE ELECTRONICA	SI	SI	SI	SI	SI	SI	SI	NO	SI	NO		9
AGT	NO	NO	SI	NO	SI	SI	SI	NO	SI	SI		7
AIDA GESTIÓN DE TURNOS	SI	NO	NO	NO	NO	SI	NO	NO	SI	SI		4
ASESORIA JURIDICO REGISTRO	NO	SI	SI	NO	NO	SI	NO	SI	SI	NO		6
ASODEF	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI		7
ATHOS	SI	NO	NO	NO	SI	SI	SI	NO	SI	NO		6
BIBLIOTECA VIRTUAL	SI	NO	SI	NO	SI	NO	SI	SI	SI	SI		8
CAMPAÑA ANTARTICA	SI	NO	SI	NO	SI	NO	SI	SI	SI	NO		7
CARGAPORTALCC	NO	SI	SI	NO	NO	NO	SI	NO	SI	SI		6
CL@VEDEF	NO	NO	SI	NO	SI	SI	SI	SI	SI	SI		8
COMER	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI		7
CSV BROKER	NO	SI	SI	NO	SI	SI	SI	NO	SI	SI		8
CVCDEF	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO		8
DCORE	SI	SI	SI	SI	SI	NO	SI	SI	SI	NO		9
DICODEF DICOUSOFT	SI	NO	SI	NO	SI	SI	SI	SI	SI	SI		9
DICODEF PROVISION	SI	NO	SI	NO	NO	NO	NO	SI	SI	SI		5
DITTOOLS	SI	NO	SI	NO	SI	SI	SI	SI	SI	SI		9
DIGITADEF	NO	NO	NO	NO	SI	NO	SI	NO	SI	SI		5
DIR3DEF	NO	SI	SI	NO	SI	NO	SI	SI	SI	SI		8
DOCAM	NO	NO	SI	NO	NO	NO	NO	NO	SI	NO		2
E-DELPHYN	SI	NO	SI	NO	NO	SI	SI	NO	SI	NO		6
EXPEDIENTES DIGENPER	SI	NO	SI	NO	NO	NO	NO	NO	SI	SI		4
FCTTD	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO		1
GESENCU	NO	NO	SI	NO	NO	NO	SI	SI	SI	NO		5
GESHAB OTAN	SI	NO	SI	NO	NO	NO	NO	SI	SI	SI		5
GESOPRE	NO	NO	NO	NO	SI	NO	SI	NO	SI	NO		4
GIS	NO	SI	NO	NO	SI	NO	NO	NO	SI	NO		3
HCIS	SI	NO	SI	SI	SI	SI	SI	SI	NO	SI		9
IMPOEXPO	SI	SI	SI	NO	NO	NO	NO	NO	NO	SI		4
INGRESOS CRIA CABALLAR	SI	NO	NO	NO	NO	NO	NO	NO	SI	SI		3
MILES	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO		1
NOTIFIC@DEF	NO	NO	SI	NO	SI	SI	SI	SI	SI	SI		8
OFICIALES GENERALES	SI	SI	SI	NO	NO	NO	NO	SI	SI	NO		5
PASARELA-GEISER	SI	NO	NO	NO	NO	NO	SI	NO	SI	SI		5
PLATAFORMA_BI_COGNOS10	NO	NO	SI	SI	SI	SI	SI	NO	SI	NO		7
PLATAFORMA_BI_COGNOS11	NO	SI	SI	SI	SI	SI	SI	NO	SI	NO		8
PLATAFORMA_BI_ETL (TALEND)	SI	SI	SI	NO	NO	NO	SI	SI	SI	NO		7
PORTAL PERSONAL	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI		10
RECONFAS	NO	NO	SI	SI	SI	SI	NO	SI	SI	SI		7
REGISTRO ELECTRONICO	NO	NO	SI	NO	SI	SI	SI	NO	SI	SI		7
REGISTRO CIVIL	NO	NO	SI	NO	NO	SI	NO	SI	SI	NO		4
RUBRICA	SI	SI	SI	NO	SI	SI	SI	NO	SI	NO		8
SALVANY	SI	NO	SI	NO	SI	SI	SI	SI	SI	SI		9
SAPROMIL	SI	NO	SI	SI	SI	SI	SI	NO	NO	SI		8
SAS	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO		6
SCSP V3	NO	SI	SI	SI	NO	SI	SI	NO	SI	NO		7
SEMILCAR	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI		7
SETI	NO	NO	SI	NO	SI	NO	SI	SI	SI	SI		7
SIACUDEF	NO	NO	SI	NO	NO	SI	SI	NO	SI	SI		6
SIADIDEF	NO	NO	SI	NO	NO	SI	NO	NO	SI	SI		4
SIDAE	SI	SI	SI	SI	SI	NO	SI	SI	SI	NO		9
SIGEI	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI		9
SIGESEVA	SI	NO	NO	NO	NO	NO	SI	NO	SI	NO		4
SINFRADEF	SI	SI	SI	NO	SI	SI	SI	SI	SI	NO		9
SIPEC	NO	NO	SI	SI	SI	SI	SI	SI	SI	NO		8
SIPEROPS	NO	SI	SI	NO	SI	SI	SI	SI	SI	SI		9
SIPRAM	SI	NO	SI	NO	SI	NO	SI	SI	SI	SI		8
SIRSEA	NO	NO	SI	NO	SI	NO	SI	SI	SI	SI		7
SISANDEF-CENDALA	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI		10
SSRL	SI	NO	NO	NO	NO	NO	SI	NO	SI	SI		5
TARJETA SANITARIA	NO	SI	SI	NO	NO	NO	NO	SI	SI	NO		4

EJE BENEFICIO/VALOR									
Nombre Aplicación	Vida útil restante			Proyectos planificados	Nº Subidas	Soporte al Negocio	Vigencia de datos	Beneficio/Valor	Puntuación
	Obsolescencia funcional	Fecha de discontinuación prevista	Fecha de último paso a producción						
3M CODIFICACION	3	2	0	2	1	2	3	0	13
ACCEDA – DEFENSA WEB – SERVICES	3	0	4	2	3	2	3	0	17
ACCEDA DEFENSA Tramitador	3	0	4	2	3	2	3	0	17
ACCEDA Firma Cron	3	0	4	2	3	2	3	0	17
ACCEDA Jobs	3	0	5	2	3	2	3	0	18
ACCEDA SEDE ELECTRONICA	3	0	5	2	3	2	3	0	18
AGT	2	2	4	2	1	2	2	0	15
AIDA GESTIÓN DE TURNOS	2	2	1	1	1	2	2	0	11
ASESORIA JURIDICO REGISTRO	3	2	0	1	1	2	3	0	12
ASODEF	1	0	4	2	2	2	2	0	13
ATHOS	3	2	4	2	2	2	3	0	17
BIBLIOTECA VIRTUAL	2	0	4	1	1	2	1	0	11
CAMPAÑA ANTARTICA	3	2	4	2	1	2	1	0	15
CARGAPORTALCC	3	2	0	1	2	2	2	0	12
CL@VEDEF	3	0	4	1	1	2	1	0	12
COMER	3	2	4	2	1	2	3	0	17
CSV BROKER	3	0	4	1	1	2	1	0	12
CVCDEF	2	0	4	2	1	2	3	0	14
DCORE	2	0	4	1	3	1	1	0	12
DICODEF DICOUSOFT	2	0	4	2	1	2	2	0	13
DICODEF PROVISION	3	0	4	1	1	2	2	0	13
DIETOOLS	2	2	4	1	1	2	2	0	14
DIGITADEF	2	0	1	1	1	2	1	0	8
DIR3DEF	3	0	0	1	1	2	1	0	8
DOCAM	1	0	0	1	1	2	2	0	7
E-DELPHYN	3	2	4	2	1	2	3	0	17
EXPEDIENTES DIGENPER	3	2	0	1	1	2	2	0	11
FCTTD	3	2	4	1	1	2	3	0	16
GESENCU	3	2	3	1	1	2	2	0	14
GESHAB OTAN	1	2	0	1	1	2	2	0	9
GESOPRE	3	2	4	1	1	2	2	0	15
GIS	3	2	0	2	1	1	3	0	12
HCIS	1	2	1	2	3	2	3	0	14
IMPOEXPO	1	2	0	2	1	2	3	0	11
INGRESOS CRIA CABALLAR	1	2	0	1	1	2	3	0	10
MILES	3	2	4	1	1	2	3	0	16
NOTIFIC@DEF	2	0	4	1	1	2	1	0	11
OFICIALES GENERALES	3	2	4	1	2	2	3	0	17
PASARELA-GEISER	3	0	4	1	0	2	1	0	11
PLATAFORMA_BI_COGNOS10	3	0	0	1	3	1	2	0	10
PLATAFORMA_BI_COGNOS11	3	0	5	1	3	1	2	0	15
PLATAFORMA_BI_ETL (TALEND)	3	0	4	1	3	1	2	0	14
PORTAL PERSONAL	3	0	4	1	1	2	2	0	13
RECONFAS	2	0	4	2	1	2	1	0	12
REGISTRO ELECTRONICO	1	0	4	1	1	2	1	0	10
REGISTROPCIVIL	3	2	0	1	1	2	3	0	12
RUBRICA	3	1	4	2	0	2	1	0	13
SALVANY	1	1	1	2	0,5	2	3	0	10,5
SAPROMIL	3	0	4	2	2	2	0	0	13
SAS	3	0	4	1	0,5	1	2	0	11,5
SCSP V3	3	2	4	2	1	2	3	0	17
SEMILCAR	3	0	4	2	3	2	2	0	16
SETI	1	0	4	1	1	2	2	0	11
SIACUDEF	3	0	4	2	3	2	0	0	14
SIADIDEF	1	0	3	2	1	2	1	0	10
SIDAE	3	2	4	2	3	2	1	0	17
SIGEI	1	0	4	1	1	2	2	0	11
SIGSEVA	3	2	4	1	2	2	1	0	15
SINFRADEF	3	0	4	2	3	1	2	0	15
SIPEC	3	0	4	1	1	2	2	0	13
SIPEROPS	3	0	4	1	1	2	2	0	13
SIPRAM	1	1	0	2	0,5	2	1	0	7,5
SIRSEA	3	0	4	2	1	2	2	0	14
SISANDEF-CENDALA	2	2	4	2	2	2	3	0	17
SSRL	2	0	2	1	0,5	2	0	0	7,5
TARJETA SANITARIA	3	2	4	1	1	2	2	0	15