
# Modernizando Infraestructuras de Fabricación de Aplicaciones

# ÍNDICE

**1.- Motivación. 3**
*1.1.- Zero-Trust: Un Nuevo Modelo para la Ciberseguridad. 3*
*1.2.- Objetivos de Futuro: Soberanía Digital y Ciberseguridad en las Naciones Europeas. 4*
1.2.1.- Soberanía Digital: La Producción Industrial. 4
1.2.2.- Zero-Trust: Certificación de la Maquinaria Suministrada. 4
*1.3.- La Implementación. 5*
1.3.1.- El Diseño 5
1.3.1.1 Requisitos de Ciberseguridad: Aplicaciones y Entornos de Ejecución Seguros 5
1.3.1.2 Requisitos para el Diseño del Entorno de Ejecución de Aplicaciones. 5
1.3.2.- Un Proyecto Europeo 5

**2.- Los Medios de Producción. 6**
*2.1.- Boceto de un Prototipo. 6*
2.1.1.- Arquitectura Normalizada que Permita Distintas Estrategias de Diseño. 6
2.1.2.- Estrategia de Diseño para el Caso del Tráfico Aéreo. 6
2.1.2.1 Estrategia: las Prioridades de Diseño. 6
2.1.2.2 Tecnologías de Implementación: Un primer Boceto del Prototipo 7
*2.2.- Expectativas de Futuro: Las Opciones Tecnológicas. 8*
2.2.1.- Capas de Operación: Despliegue Aplicaciones. 8
2.2.2.- Capas de Articulación: Monitorización y Control de Recursos Lógicos. 10

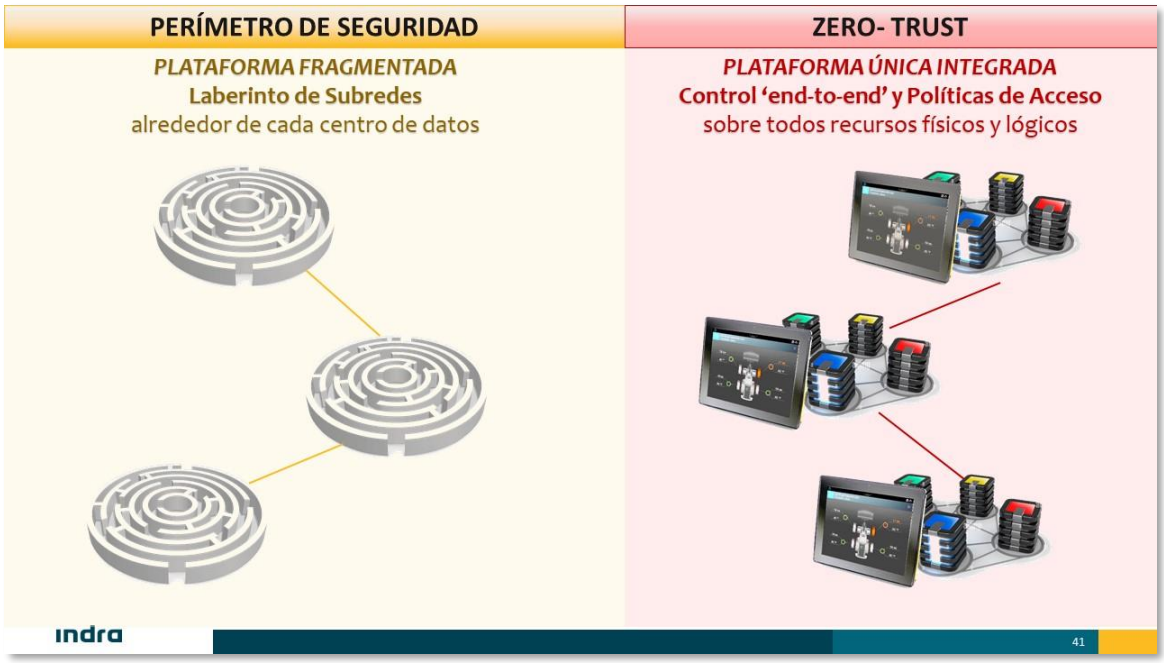
# 1.- MOTIVACIÓN.

## 1.1.- ZERO-TRUST: UN NUEVO MODELO PARA LA CIBERSEGURIDAD.

La imagen resume el cambio de modelo de seguridad en los entornos de ejecución de aplicaciones

- **De un perímetro de seguridad** que despliega diversos laberintos para dificultar los accesos a los centros de datos
- **A un control central de todos los recursos físicos y lógicos** de los centros de datos, con un sistema de identidad y políticas de acceso a cada uno de ellos (AAA, un "parquímetro" de uso).

Para visualizar esta evolución, nos sirve de muestra cómo los automóviles modernos, cada vez más, permiten un control de todas y cada una de las partes del vehículo desde un único cuadro de mandos.




Las capacidades de cómputo de antaño hacían inviable una discriminación exhaustiva de todos los recursos, sólo se podía optar por impedir el acceso al conjunto de ellos (al centro de datos). Las nuevas capacidades de cómputo y los estándares de kubernetes que sistematizan la gestión del ecosistema de servicios vienen decantando, tanto nuevos mecanismos de control de la maquinaria, como ubicuidad en los accesos a las aplicaciones, dejando obsoleto el perímetro de seguridad.

*En entornos desconectados, esa falta de control de los recursos lógicos deriva en problemas de fragmentación de los datos[1], una falla de seguridad inherente al diseño de las aplicaciones, imposible de corregir sin unos nuevos medios de producción.*

[1] ***VM Ware, Rawlinson Ribera,*** *Fragmentación Datos:* https://youtu.be/dFySwm2bKTg?t=220

# 1.2.- OBJETIVOS DE FUTURO: SOBERANÍA DIGITAL Y CIBERSEGURIDAD EN LAS NACIONES EUROPEAS.

## 1.2.1.- SOBERANÍA DIGITAL: LA PRODUCCIÓN INDUSTRIAL.

El cambio del modelo de seguridad implica:

- **Incorporar un controlador de recursos físicos y lógicos asociado a un AAA** en cada centro de datos que permita controlar qué usuarios y desde qué dispositivos están accediendo a qué recursos de computación en cada momento.
- **Desmantelar el antiguo perímetro de seguridad**.

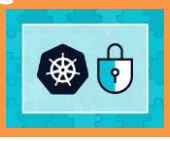
Eventualmente esta actualización sea más simple y económica a través de un reemplazo de los antiguos centros de datos por nueva maquinaria ensamblada en fábrica[2], ya que el uso de nube pública es absolutamente inviable en sectores estratégicos de la economía, como la aeronáutica.

Esta necesidad de maquinaria propia del sector de la aeronáutica es compartida por muchos otros sectores (como la Banca o las Administraciones del Estado de todas las naciones europeas) lo que recibe el nombre del problema de la *"Soberanía Digital Europea"*. Dicho de otro modo, *el suministro de esta maquinaria ensamblada de fábrica, abaratando costes y simplificando su mantenimiento, contribuye a disminuir la fuerte dependencia que vienen desarrollando las administraciones europeas con proveedores de servicios de nube pública*, como Azure, Amazon o Google.

## 1.2.2.- ZERO-TRUST: CERTIFICACIÓN DE LA MAQUINARIA SUMINISTRADA.

A imagen y semejanza de cómo se certifican los núcleos de red 5G[3], los centros de datos pueden recibir un proceso de pruebas que garantice un conjunto de capacidades mínimas para ser considerado entorno seguro para despliegue de aplicaciones.

Una certificación de maquinaria solo garantiza que el entorno puede ser seguro, pero sólo lo será si la aplicación hace uso de esas capacidades de ciberseguridad de manera implícita durante su desarrollo. Por listar alguna de ellas:

| ZERO-TRUST: Capacidades Mínimas | |
|---|---|
| **Microsegmentación**   | - Políticas de Lista blancas entre servicios.<br>- Cifrado automático de conexiones entre servicios.<br>- Refresco automático Front-Ends.<br>- Políticas acceso a los datos por llamada de API.<br>- SSH => No accesible desde el mundo exterior, solo desde el plano de control de plataforma. |
| **RBAC**  | - AAA (Authentication-Authorization-Accounting).<br>- Control de dispositivos de acceso.<br>- Monitorización Sesiones. |

[2] ***Nokia Datacenter Delivery Center:*** *https://youtu.be/nCKNIYdp7_Y?si=l7AUStkiY99sGb5C*
[3] ***OPNFV, Certificación núcleos 5G:*** *https://www.opnfv.org/community/projects/pharos*

# 1.3.- LA IMPLEMENTACIÓN.

## 1.3.1.- EL DISEÑO

### *1.3.1.1 REQUISITOS DE CIBERSEGURIDAD: APLICACIONES Y ENTORNOS DE EJECUCIÓN SEGUROS*

La ciberseguridad depende de dos factores: aplicaciones seguras de fábrica y entorno de ejecución seguro:

- **Factorías - Diseño aplicaciones seguras**, para ello han de gestionar:
  - El diseño del plano de lógica: APIs y dependencias.
  - El diseño del plano de datos: políticas de acceso.
  - El diseño de las comunicaciones internas de aplicación: políticas de lista blanca entre servicios.
  - Encapsulado de artefactos, las condiciones de instanciación.
- **Operadora de Centro de Datos – El Entorno de Ejecución**, las operadoras deben contar con la capacidad de gestionar centralmente todos los recursos de cada centro de datos (tanto físicos como lógicos), con su sistema de políticas de acceso.

### *1.3.1.2 REQUISITOS PARA EL DISEÑO DEL ENTORNO DE EJECUCIÓN DE APLICACIONES.*

Este documento se centra en el diseño de los entornos de ejecución de aplicaciones, necesarios tanto en fábrica como en operadora de centros de datos. Para establecer un plan de evolución a largo plazo en la producción centros de datos Zero-Trust… dos son los requisitos:

- **Laboratorio de Seguridad (sector aeronáutico)**: donde poder madurar los estándares Zero-Trust. Solo el sector de la aeronáutica mantiene un control de toda la cadena de suministro de aplicaciones (fábrica y operadora), lo que lo convierte en excepcional para integrar una solución completa y final para la ciberseguridad.
- **Control end-to-end (sector telecomunicaciones)**: el modelo Zero-Trust depende de la capacidad de controlar todos los recursos físicos y lógicos, extremo a extremo. La tradición de sistemas distribuidos asociada a las telecomunicaciones se torna decisiva para una adecuada maduración de las estructuras de control Zero-Trust. No es difícil intuir las implicaciones de un sistema de control capaz de gestionar todas las líneas telefónicas entre Nueva York y Los Ángeles.

## 1.3.2.- UN PROYECTO EUROPEO

Europa adolece del llamado problema de la *"Soberanía Digital"*. Para facilitar su cooperación, **tanto la arquitectura de la solución como el entorno de pruebas debieran estar liderados por agentes europeos**, aunque las tecnologías provengan de cualquier fabricante del mundo. Un primer potencial cliente podría ser el Departamento de Defensa de USA, dada la urgencia crítica de reemplazar su perímetro de seguridad por Zero-Trust[4].

[4] ***Evolución en la estrategia Zero Trust del Departamento Defensa USA:*** ***https://www.defense.gov/News/News-Stories/Article/Article/3400194/pentagon-cyber-official-provides-progress-update-on-zero-trust-strategy-roadmap/***

# 2.- LOS MEDIOS DE PRODUCCIÓN.

## 2.1.- BOCETO DE UN PROTOTIPO.

### 2.1.1.- ARQUITECTURA NORMALIZADA QUE PERMITA DISTINTAS ESTRATEGIAS DE DISEÑO.

El controlador de recursos físicos y lógicos de cada centro de datos debiera seguir una arquitectura normalizada que admita cualquier combinación de tecnologías, según estrategia de diseño. Un primer boceto de funcionalidades:

| ARQUITECTURA NORMALIZADA | |
|---|---|
| **Día 0** | -**Control Recursos Físicos**: base datos recurso/estado.<br>-**Instalaciones Desatendidas** de sistemas operativos.<br>-**Sectorización** en Clústeres k8s. |
| **Día 1** | -**Despliegue Plataforma DevSecOps** para los entornos de cada fase de la cadena de producción (build, test, etc.).<br>-**Inicialización de cada entorno de trabajo** para el tipo de sistema que se va a desarrollar (banca, tráfico aéreo, etc.). |
| **Día 2** | -**Control de Recursos Lógicos**: base datos recurso/estado para la infraestructura de servicios[5]. |

### 2.1.2.- ESTRATEGIA DE DISEÑO PARA EL CASO DEL TRÁFICO AÉREO.

#### *2.1.2.1 ESTRATEGIA: LAS PRIORIDADES DE DISEÑO.*

Para el caso particular del tráfico aéreo, tres son las prioridades que definen su estrategia de implementación:

- **Control Institucional**: que garantice ajustarse a los criterios de seguridad nacional de los distintos países.
- **Fiabilidad al Mínimo Coste**: diseño de un hardware específico para este tipo de aplicaciones, minimizando los puntos de error. Esto se traduce en diseños rústicos que reducen las funcionalidades a lo más fundamental para garantizar fiabilidad. De manera muy similar a como se diseñaban las cabeceras de telefonía (IMS o Red Inteligente), donde a partir de un entorno de pruebas diseñado muy a medida[6], se producen unas normas internacionales para este tipo de componentes de red.
- **Independencia Operativa**: es crítico no tener ninguna dependencia tecnológica con ningún fabricante (vendor lock-in), así como capacidades propias para operar las opciones tecnológicas por las que se opte. Esto implica, uso de Código Abierto adaptado por ingenieros propios, además de procesos de certificación de los casos de uso ATM para poder sustituir una tecnología por otra o emplear varias opciones simultáneamente en distintos emplazamientos, según el caso.

[5] ***Punto de Referencia:*** *la antigua S-RAMP, OASIS SOA Repository Artifact:* https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=s-ramp

[6] ***Nokia Bell Labs,*** *diseño de laboratorios IMS:* **https://ieeexplore.ieee.org/document/6768565**

### 2.1.2.2 TECNOLOGÍAS DE IMPLEMENTACIÓN: UN PRIMER BOCETO DEL PROTOTIPO

*Imagine if you were running all this as Virtual Machines*
*and you have to update them and patch them,*
*and you have a DevTest staging environment,*
*and you have different classification levels,*
*very quickly you will be overwhelmed…*
*and is not going to scale.*

*So that's why we pick containers,*
*and that's why we centrally accredit and harden them"*
**Mr. Nicolas M. Chaillan – US Department of Defense**
https://youtu.be/qGWmibFSAvk?si= DmeRRiZcZEYzrS&t=766

Tal como expresa Mr. Nicolas M. Chaillan, para evitar los sobrecostes que implican el uso de máquinas virtuales, en este tipo de entornos se opta por sectorizar las máquinas físicas de los centros de datos en clústeres OpenShift, quedando una combinación de tecnologías de este aspecto:

| ATM – BOCETO DE PROTOTIPO | |
|---|---|
| **Día 0** | -**Tinkerbell[7] / Equinix Metal**: MaaS (Metal as a Service, gestor recursos físicos para centros de datos medianos y pequeños)<br>-**Sparta[8]/UPI[9]**, sectorización OpenShift |
| **Día 1** | -**Big-Bang[10]**: despliegue plataforma DevSecOps sobre cada clúster.<br>-**API driven Ansible Framework**: inyectar configuraciones ATM sobre la Plataforma DevSecOps de cada entorno de trabajo (build, test, etc.), mediante GitOps con API k8s. |
| **Día 2** | -**OpenCluster Manager[11]:** gestor de recursos de clúster.<br>-**Kiali[12]**: gestor recursos lógicos (malla de servicios). |

La imagen de la izquierda muestra como las distintas operadoras de telefonía móvil ensamblan sus núcleos de red 5G, una referencia sobre cómo armar estos centros de datos Zero-Trust de manera institucionalizada.

La mayoría de las tecnologías de monitorización continua son soluciones comerciales de una elevada complejidad, haciéndolas inviables en este tipo de entornos, hay todo un proceso I+D de evaluación e integración de tecnologías Open Source hasta lograr una solución acorde a las necesidades de estos sectores estratégicos de la economía, como la aeronáutica.

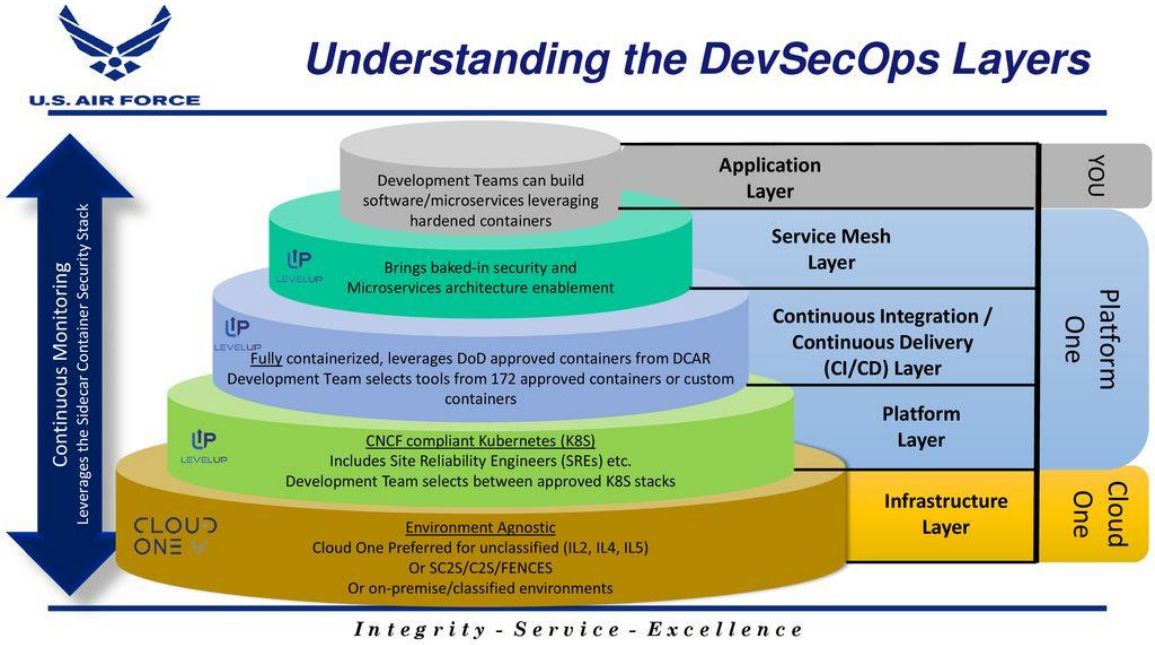

[7] ***Tinkerbell:*** *https://tinkerbell.org/*
[8] ***Sparta:*** *https://codectl.io/*
[9] ***RedHat OpenShift Bare Metal UPI:*** *https://demo.openshift.com/en/latest/bm-upi/*
[10] ***Big-Bang:*** *https://p1.dso.mil/services/big-bang*
[11] ***OpenCluster Manager:*** *https://open-cluster-management.io/*
[12] ***Kiali for Istio:*** *https://kiali.io/*

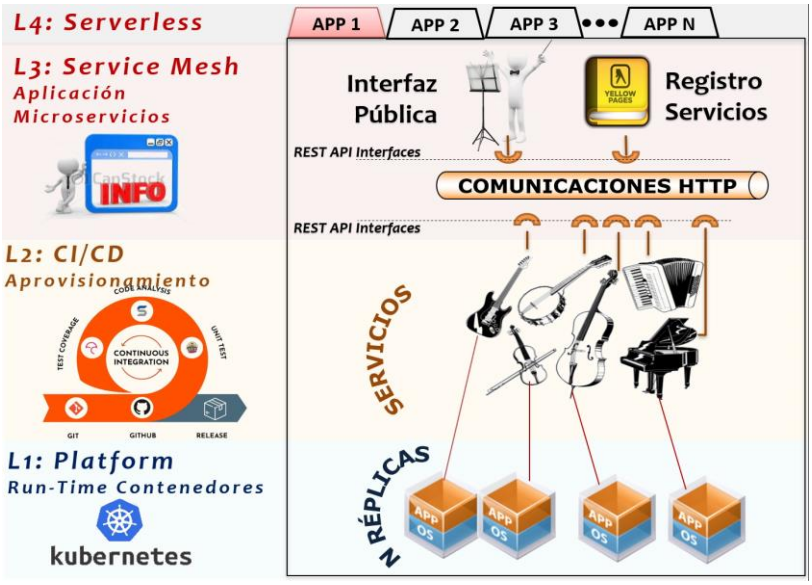
## 2.2.- EXPECTATIVAS DE FUTURO: LAS OPCIONES TECNOLÓGICAS.

El problema de la soberanía digital sólo puede resolverse democratizando el acceso a una maquinaria fácil de usar. Esto implica integrar plataforma DevSecOps para producirla industrialmente. Un buen volumen de ventas garantiza continuidad en el desarrollo, al animarse más fabricantes de tecnologías diversas a integrarse en el proyecto. El bajo coste de una producción industrial simplifica el reemplazo periódico de viejos centros de datos por nuevos durante esta "era de la nube", con esa explosión de procesos de mejora continua en busca de consolidar y miniaturizar esta maquinaria.

Una única arquitectura normalizada permite emplear distintas opciones tecnológicas, así cada actividad económica ajusta su estrategia de diseño acorde a sus necesidades específicas (tiempo real, persistencia datos, etc.).

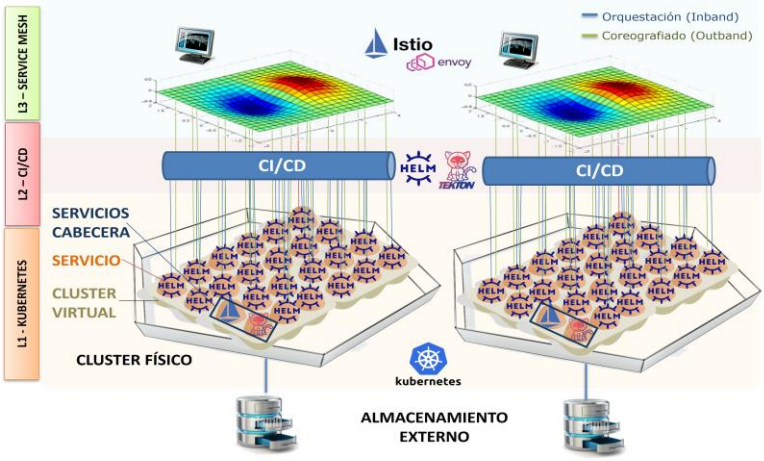
### 2.2.1.- CAPAS DE OPERACIÓN: DESPLIEGUE APLICACIONES.




PLATAFORMA ENTREGA CONTINUA

https://p1.dso.mil





SOFTWARE DEFINED DATA-CENTER (UNF)

CLOUD ONE FAST SECURE STREAMLINED

https://www.cloud.mil/

| CAPAS | OBJETIVO | TECNOLOGÍAS |
|---|---|---|
| **L0 Infraestructura (IaaS)** | • **Máquinas Físicas**: despliegue y control de una federación de racimos de ordenadores (o clústeres en inglés) desde una cabecera principal sobre una malla de máquinas físicas o virtuales. El conjunto de prácticas L0 suelen llamarse *"Infraestructura como Código"*, aplicadas a través de una metodología NetOps. | • MaaS: Metal as a Service (Equinix/Canonical)<br>• OpenFabrics Alliance<br>• Cisco Application Centric Infrastructure (ACI)<br>• Juniper Apstra<br>• Arista CloudVision<br>• Nokia Data-Center Fabric<br>• OpenStack, CloudStack |
| **L1 Plataforma (PaaS)** | • **Terminaciones de Lógica**: instanciar las pods (con sus contenedores) que componen un servicio sobre la federación de clústeres de la infraestructura L0. | • RedHat OpenShift<br>• Novell Rancher<br>• Canonical Charmed Kubernetes<br>• VM Ware Tanzu |
| **L2 CI/CD** | • **Servicios**: aprovisionamiento y actualización continua de servicios desplegados en varias terminaciones de lógica (entre frontales y back-end) gestionadas por la plataforma L1. | • Helm Chart<br>• RedHat OpenShift Pipelines<br>• Tekton<br>• Jenkins, Jenkins X<br>• ArgoCD, GitLab |
| **L3 Service Mesh** | • **Aplicación**: automatización del despliegue de todos los servicios de una aplicación (en sus seis estrategias principales: recreate, ramped, blue/green, shadow, canary, a/b testing) y gestión de logs, en otras palabras, ensamblar los servicios aprovisionados por la capa L2. | • RedHat OpenShift Service Mesh<br>• Istio<br>• Traffik |
| **L4 Serverless (FaaS)** | • **Ecosistema Aplicaciones**: sistema de contextos para crear modelos de cohesión en el diseño de aplicaciones, es decir, facilitar la creación de ecosistemas, tal como hace un servidor de aplicaciones. | • RedHat OpenShift Serverless<br>• Knative |

### 2.2.2.- CAPAS DE ARTICULACIÓN: MONITORIZACIÓN Y CONTROL DE RECURSOS LÓGICOS.

Las capas de articulación monitorizan y controlan de manera centralizada todo el ecosistema de aplicaciones orientadas a servicios. En la imagen de la página anterior se representan con una doble flecha azul, etiquetada con *"Continuous Monitoring"*, indicando que son transversales a todas las capas de operación, que coordinan las operaciones a lo largo de toda la estructura de capas y así se articula los servicios de una manera sencilla. La gestión de recursos físicos la realiza un MaaS (Metal as a Service) o "*OpenFabrics Management Framework"* de cada centro de datos, mientras que los lógicos los gestiona un controlador de aplicaciones por centro de datos con estas responsabilidades:

| CAPAS | OBJETIVO | TECNOLOGÍAS |
|---|---|---|
| **A0 Coreografiado** Ecosistema Servicios (Outband) | • **CMP – Plataforma de Monitorización Continua**: gestión centralizada de una federación de mallas de servicio a lo largo del centro de datos. La monitorización de servicios se basa en el contenedor side-car, que integra logs y herramientas de monitorización de comunicaciones HTTP (ej: Jaeger). | • Sidecar Container Security Stack<br>• Kiali<br>• D2IQ<br>• Dynatrace<br>• Datalog<br>• SolarWinds<br>• IBM Instana |
| **A1 Orquestación** Ciclo de Vida del Servicio (Inband) | • **SDP – Plataforma de Despliegue de Servicios**: secuenciación de arranque de la plataforma de entrega continua y control centralizado de los despliegues: 1) creación e 2) inicialización de la red de clústeres, 3) asignación de pipelines de despliegue de artefactos a los distintos clústeres de la red; 4) arranque plataforma de monitorización continua. | • RedHat Advanced Cluster Manager<br>• Open Cluster Management<br>• D2IQ |