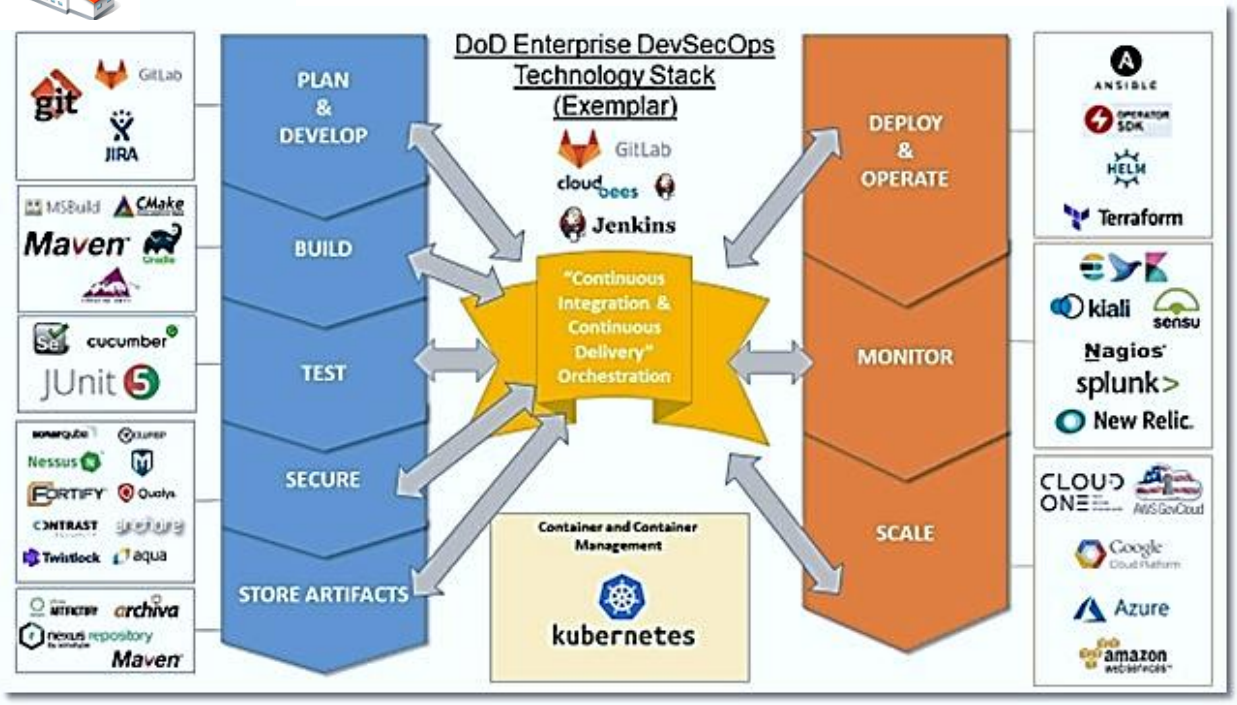
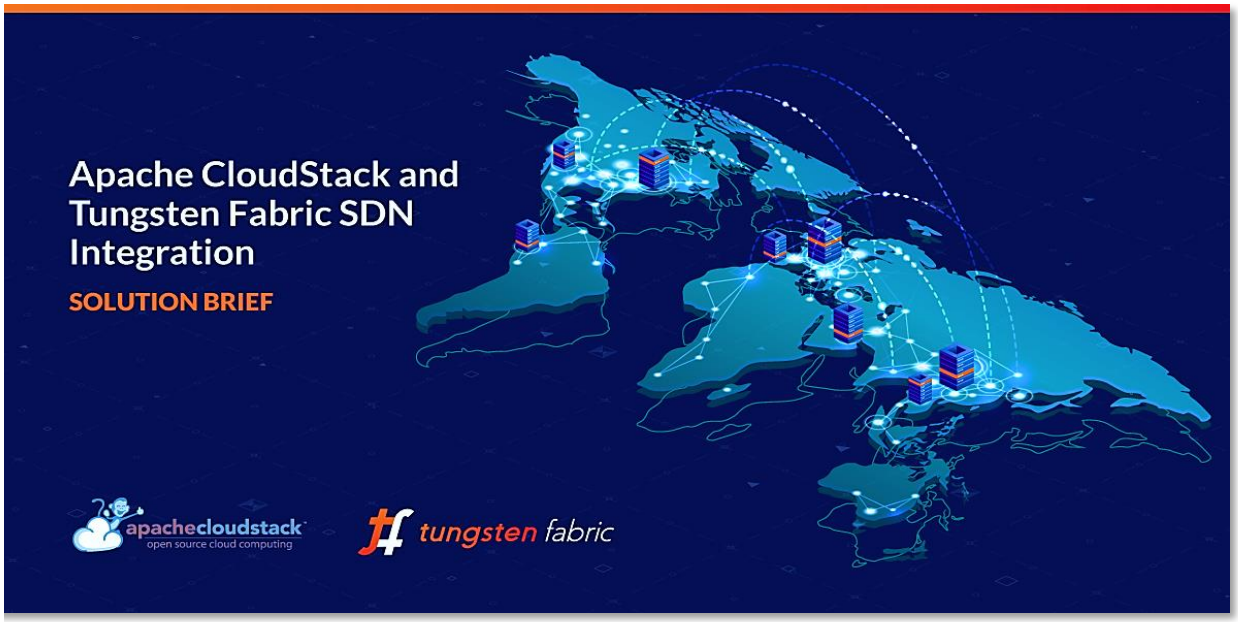
FACTORÍA – DISEÑO DE APLICACIÓN



OPERADORA CENTROS DE DATOS – ENTORNO EJECUCIÓN



Algunas Herramientas en Factorías de Aplicaciones (DevSecOps)

ÍNDICE

1.- TRANSICIÓN A DEVSECOPS.

1.1.- INCENTIVOS PARA LA TRANSICIÓN DEVSECOPS.

Cuatro pilares vertebran las motivaciones que llevaron a las Fuerzas Aéreas de Defensa de Estados Unidos a realizar una modernización radical de todo su sistema de producción de aplicaciones, que se intentan dilucidar aquí:

 **Ciberseguridad**	Blindar el sistema de armas más grande del mundo dentro del contexto del inminente internet de las cosas adoptando los siguientes principios: a. **USUARIO** - Eliminar la suplantación de identidad, al emplear un sistema de credenciales basado en tarjetas SIM en lugar de contraseñas (en línea de lo que viene proyectándose para el internet de las cosas)… similar a una asignación nominal de una línea telefónica y que podrá llegar a ser equiparable a un DNI electrónico… con una normativa en constante evolución. b. **USUARIO** - Sin simplicidad de uso, la seguridad no es posible: el empleo de tarjetas SIM hace innecesarias muchas incómodas medidas empleadas para impedir la suplantación de identidad (memorización de muchas y complejas contraseñas, renovación frecuente de esas contraseñas, un dispositivo asociado para autorizar transacciones, etc.). c. **PLATAFORMA** - Entorno de ejecución de aplicaciones cerrado: las plataformas DevSecOps son sistemas mucho más controlables al ser gestionadas en su totalidad vía software. d. **PLATAFORMA** - Microsegmentación reduce mucho la superficie y el tiempo de exposición del plano de datos. Políticas de lista blanca por servicio controla visibilidad entre servicios, minimizando la superficie de datos expuesta. Además, cada frontal da acceso a un fragmento de esa superficie de datos, y cada refresco de esos frontales renueva propiedades de autenticación reduciendo su tiempo de exposición. e. **FACTORÍA** - Análisis continuo del comportamiento de las aplicaciones: gracias a especialistas en seguridad que continuamente estudian y corrigen el comportamiento de las aplicaciones de las factorías.
 **Reducción Costes**	Software Defined Datacenter (Software Defined {Network & Storage & Compute}): centros de datos gestionados por software reducen hasta un 60% los costes de mantenimiento de la maquinaria. También llamados *"Sistemas Operativos para Centro de Datos"*, como serían OpenStack, CloudStack que gestionan mallas de máquinas virtuales, o Fabrics que gestionan mallas de máquinas físicas (OpenFabrics Alliance, Juniper Apstra, Cisco ACI, Arista CloudVision, Nokia NOS). Estas mallas de computadores se sectorizan en racimos (ejm.: kubernetes).
 **Entrega Continua**	Velocidad de Entrega: La integración y automatización de todos los procesos de una factoría garantizan poder afrontar los retos que impone esta nueva sociedad de la información.
 **Solución de futuro**	a. Garantiza una evolución futura en cada una de las piezas que componen la solución final, para adaptarse a la vertiginosa evolución de estas tecnologías de nube. b. Descartar sistemas obsoletos, reduciendo costes de mantenimiento de todo el legacy que va amontonándose en los centros de datos (ejm.: abandonar las máquinas virtuales cuya complejidad de gestión implica elevados costes de mantenimiento al punto de impedir la escalabilidad de las aplicaciones; sustituir por contenedores).

1.2.- REQUERIMIENTOS: UNA RENOVACIÓN DE LA RED DE CENTROS DE DATOS.

La transición a una metodología DevSecOps impone una renovación de los antiguos centros de datos por nuevos, por tres motivos principales:

1. **Control centralizado de la red de Centros de Datos**[1]: aumentar criterios de seguridad y adaptarse al inminente internet de las cosas… conducen a sistemas de difusión de aplicaciones y autenticación de usuarios centralizados en todo el sistema de nube, tal como hacen las operadoras de telefonía móvil con sus recursos de red a nivel nacional.
2. **Diseño específico de cada Centro de Datos para un *'Software Defined Datacenter'*[2] que garantice evolución futura**: la transición a una computación controlada por software no puede hacerse sin un diseño específico de los centros de datos (según su papel dentro de la red, se gestionarán máquinas virtuales sobre la maquinaria existente, o no quedará otra que reemplazarla por maquinaria nueva que admita certificación interoperabilidad[3])… eventualmente pueda integrarse los sistemas de autenticación de la telefonía móvil que formarán parte de la interfaz de infraestructura (en la líneas de cómo hace la industria del automóvil[4]). Los operadores de telefonía móvil exponen su base de usuarios a los proveedores de servicios de red a través de una interfaz (OSA=Open Services Access), tal vez pueda emplearse este mismo mecanismo en la capa L0 de los centros de datos, y mantener así un único sistema centralizado de credenciales basado en tarjetas SIM para todo el ecosistema de computación.
3. **Certificación de cada Centro de Datos**[5] **antes de su puesta en funcionamiento**: al tratarse de una estructura compacta (una plataforma con todas las piezas integradas) son imprescindibles las sinergias necesarias para lograr un eficaz andamiaje de pruebas de integración capaz de evaluar y versionar la evolución de la plataforma.

Obtener retorno a una inversión de estas características implica diversificar los resultados. En otras palabras, *certificar plataformas para todos los posibles escenarios* (tiempo real en Telco Clouds, persistencia para la Banca, etc.). Para ello resulta vital una estandarización de las interfaces de cada capa de la plataforma para que admita cualquier implementación interna… *y así poder levantar una misma arquitectura con distintas combinaciones tecnológicas, según estrategia a seguir en cada escenario*.

[1] ***Lt. Gen. Jack Shanahan*** *(director del centro de inteligencia artificial del Departamento de Defensa de Estados Unidos), "la falta de nube empresarial"* https://fcw.com/it-modernization/2020/05/pentagons-ai-chief-lack-of-enterprise-cloud-has-slowed-us-down/196057/

[2] ***ETSI, OSM Hackfest 9,*** *"OSM Architecture and Installation, the Software Defined Datacenter"***:** https://osm.etsi.org/wikipub/index.php/OSM9_Hackfest

[3] ***OpenFabrics Alliance,*** *"Interoperabilidad"*: https://www.iol.unh.edu/testing/hpc/ofa

[4] ***Ciberseguridad,*** *"iSIM, eSIM, XDR"*: https://www.nokia.com/networks/cyber-security/cybersecurity-tech-talk/

[5] ***OPNFV,*** *"Andamiaje Pruebas de Certificación Telco Clouds"*: https://www.opnfv.org/

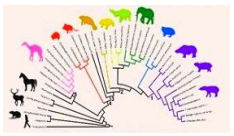
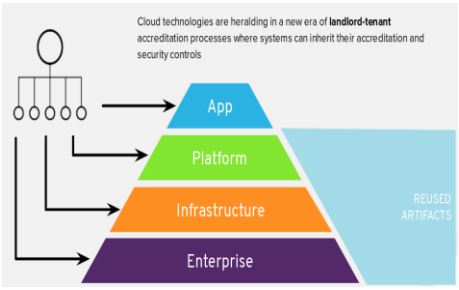
2.- CIBERSEGURIDAD: CONTROL DE LA CADENA DE SUMINISTRO DE APLICACIONES.

2.1.- RESPONSABILIDADES EN LA CADENA.

La seguridad informática no es posible abordarla sin un enfoque holístico que involucre a todos los eslabones de la cadena de suministro de aplicaciones. Este capítulo aspira a definir las responsabilidades que tiene cada eslabón de la cadena. En el siguiente capítulo, algunas propuestas de herramientas para cumplir con estas responsabilidades:

- **Acceso, despliegue de aplicaciones**: red de centro de datos donde desplegar servicios y sistema de identidad para acceder al ecosistema de aplicaciones, con la necesaria automatización extremo a extremo.
- **Distribución, homologación de servicios**: garantizar las condiciones de despliegue de los servicios que, cual piezas de lego, se emplean para componer aplicaciones finales… siendo suministrados y actualizados, de manera continua, a través de un sistema de repositorios.
- **Producción, factorías de aplicaciones**: diseñar aplicaciones bajo metodología DevSecOps que garantiza parámetros de estabilidad y seguridad. Esto implica:
  - *Datos – Diseño de la Exposición de la Superficie de Datos*: políticas de acceso de cada llamada de la API al plano de datos.
  - *Lógica – Diseño Interfaces:* Visualizar el sistema de dependencias entre servicios, para mantener estables los contratos de funcionalidades que ofrece cada servicio.
  - *Comunicaciones – Microsegmentación:* políticas de lista blanca entre los servicios que componen cada aplicación.
  - *Contenedor – Diseño del encapsulado:* metodología de encapsulado y securización en contenedores para su posterior distribución.
  - *Certificación de Artefactos* – sistema de puntos de autorización en la cadena de suministro software para acelerar las autorizaciones necesarias de cada entrega a producción.

2.2.- HERRAMIENTAS PARA CADA RESPONSABILIDAD.

DISEÑO – Factoría de Aplicaciones			
 EXPOSICIÓN DATOS	 DISEÑO APIS (DEPENDENCIAS)	 CONSTRUCCIÓN CONTENEDOR	 CERTIFICACIONES ANTES DE PRODUCCIÓN
 POLÍTICAS DE ACCESO A LOS DATOS (VISIBILIDAD FE -> BE)	 FILOGENÉTICA DE SERVICIOS	 METODOLOGÍA NSA & CISA	 CONTINUOUS AUTHORIZATION TO OPERATE

ENTORNO DE EJECUCIÓN – Operadoras de Centros de Datos				
 TARJETA SIM	 CONDICIONES CONEXIÓN		 µSEGMENTACIÓN	
 IP MULTIMEDIA SUBSYSTEM (AAA para Tarjetas SIM)	 EXTENDED DETECTION AND RESPONSE (XDR) (Escaneo Continuo de Accesos)	 SECURE ACCESS SERVICE EDGE (SASE) (Automatización extremo a extremo, Control central de accesos a cada recurso de la nube empresarial)	 MANIFIESTO MALLA SERVICIOS (Sidecar Container, Monitorización Plataforma)	 LENGUAJE DE POLÍTICAS LISTA BLANCA POR SERVICIO (Gestión de la Superficie de Datos Expuesta)

Metodología NSA &CISA, *"Guía de securización Kubernetes"* https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2716980/nsa-cisa-release-kubernetes-hardening-guidance/

Departamento de Defensa de Estados Unidos cATO, *"Continuous Authorization to Operate",* https://media.defense.gov/2022/Feb/03/2002932852/-1/-1/0/CONTINUOUS-AUTHORIZATION-TO-OPERATE.PDF

3.- OPERADORA: LA NUBE EMPRESARIAL.

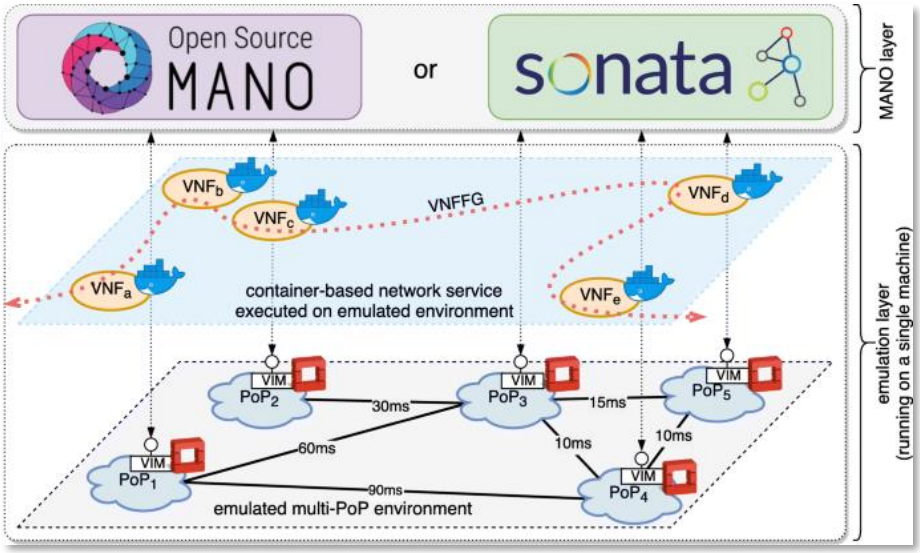
3.1.- UN ENTORNO DE EJECUCIÓN SEGURO.

Tal como se ilustra en la página anterior, 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 una nube empresarial, es decir, la capacidad de gestionar centralmente todos los recursos de una red de centros de datos (tanto físicos como lógicos), con su sistema de políticas de acceso.

3.2.- ARQUITECTURA DE LA NUBE EMPRESARIAL.

En la imagen cómo las operadoras de telecomunicaciones simulan[6] una red de cincos centros de datos controlados centralmente donde hacer pruebas de servicios de red en un solo ordenador. Se trata del esquema organizativo (o arquitectura) de una nube empresarial que permite desplegar un entorno de ejecución de aplicaciones seguro y con posibilidad de mejora constante de la ciberseguridad, agregando sistemas de autenticación por tarjeta SIM o detección y respuesta automática ante amenazas además federar aplicaciones para crear aplicaciones distribuidas que reducen la fragmentación de datos, un enrutamiento a largo del contenido requiere diseño de los meta-datos para visibilidad y crecimiento controlado del contenido.



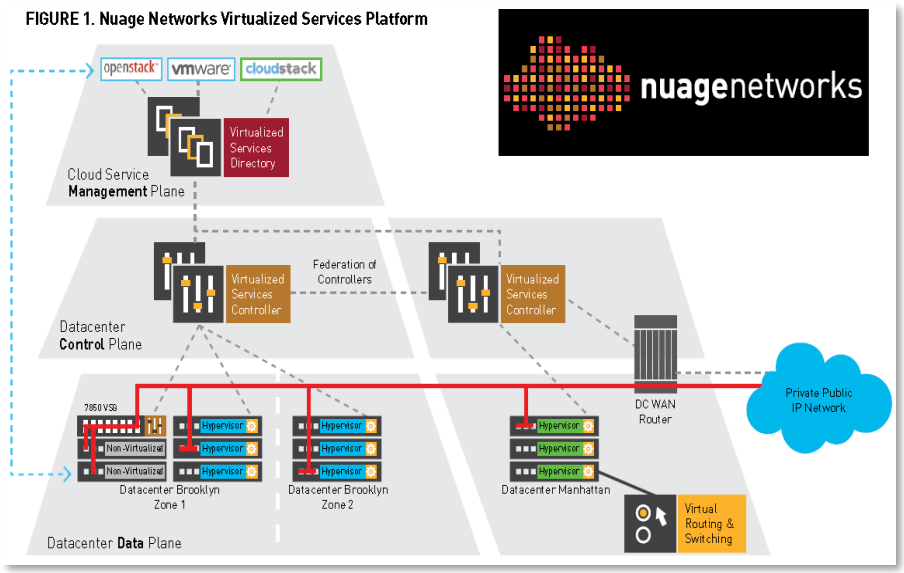
En la arquitectura de la imagen cabe destacar la siguiente estructura:

[6] ***Simulación de una nube empresarial:*** https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1493-2

- **Capa Emulación:** Infraestructura operativa de la red de centros de datos. Aparecen dos capas claramente desacopladas:
  - *Capa L0: NetOps - Software Defined Data Center*... en Telco Cloud esta capa recibe el nombre de VIM (Virtual Infrastructure Manager, Gestor de la Infraestructura de Virtualización), se simula cada uno de los centros de datos de la red con OpenStack metido en una máquina virtual. En un entorno de computación cada centro de datos consistiría en una red de clústeres kubernetes sobre una malla de máquina físicas[7] (OpenFabrics Alliance, Arista CloudVision, Juniper Apstra, Cisco ACI, Nokia NOS) o virtuales (OpenStack, CloudStack).
  - *Capa L1-L2-L3-L4: GitOps - Plataforma de Entrega Continua*... la simulación prescinde de toda esta estructura, despliegan las funciones virtualizadas de red directamente sobre Docker. En un entorno de computación, consistiría en las configuraciones de los clústeres, un sistema de entrega continua (como Jenkins) y un sistema de malla de servicios (como Istio).
- **Capa MANO**: Articulación de la red de centros de datos. Aparecen dos elementos principales:
  - *Capa MANO*: controlador que distribuye las funciones virtualizadas de red por toda la red de centros de datos. En computación, no existe un equivalente, cada factoría de aplicaciones debe diseñar un gestor que permita distribuir sus aplicaciones por todos los nodos de su nube empresarial desde un único centro de control.
  - *Interfaz VIM*: API a través de la cual el controlador MANO actúa sobre cada centro de datos (representada por un punto blanco en cada VIM). En un entorno de computación, se trata de un controlador de área de servicio capaz de gestionar la red de clústeres de cada centro de datos. Estas áreas de servicio se federan y se controlan desde una cabecera principal, lo que recibe el nombre Universal Networking Fabric (UNF)[8].

La imagen representa la UNF de *Nokia Nuage Networks*[9] donde se aprecia claramente la federación de controladores de área de servicio gestionadas desde una cabecera principal[10] desde donde se configuran las políticas de acceso a todos los recursos de la red.

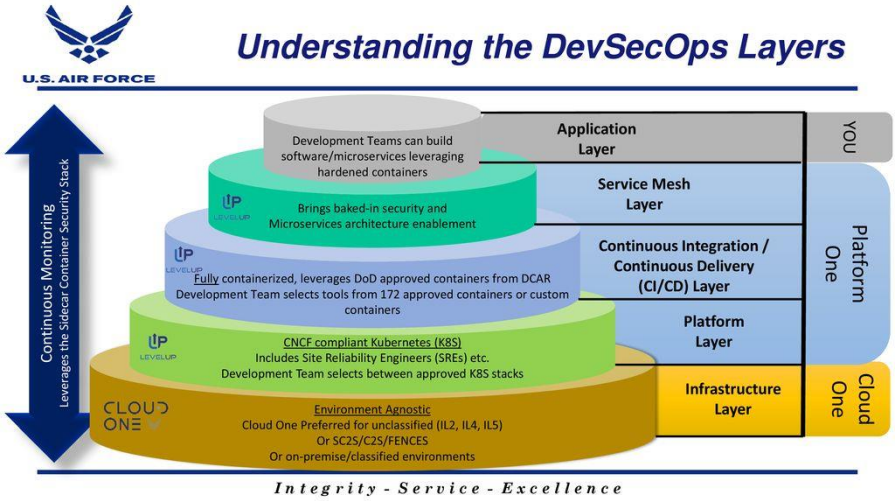
FIGURE 1. Nuage Networks Virtualized Services Platform

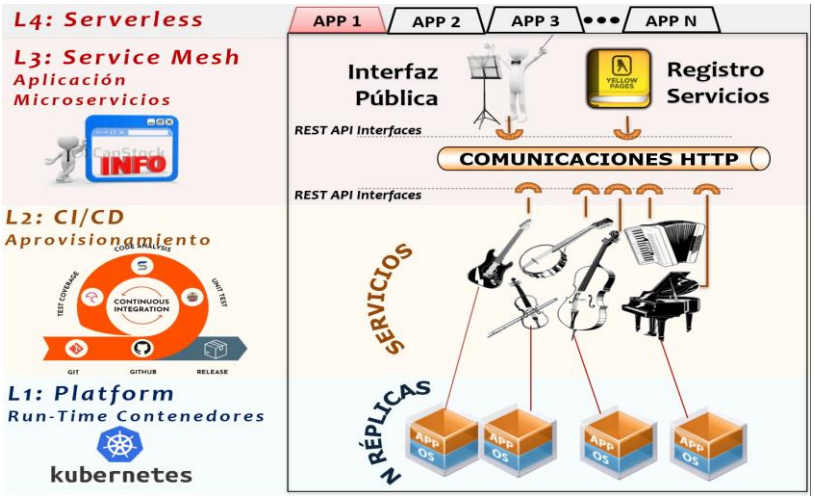


[7] ***OpenFabrics Alliance:*** *https://en.wikipedia.org/wiki/OpenFabrics_Alliance*
[8] ***UNF, Controladores de SDN:*** *https://en.wikipedia.org/wiki/List_of_SDN_controller_software*
[9] ***Nokia, The Universal Networking Fabric:*** *https://onestore.nokia.com/asset/212701*
[10] ***OVH Installs Nuage SDN for OpenStack as a Service,*** *https://convergedigest.com/ovh-installs-nuage-sdn-for-openstack-as/*

3.3.- ARQUITECTURA DEL CENTRO DE DATOS.

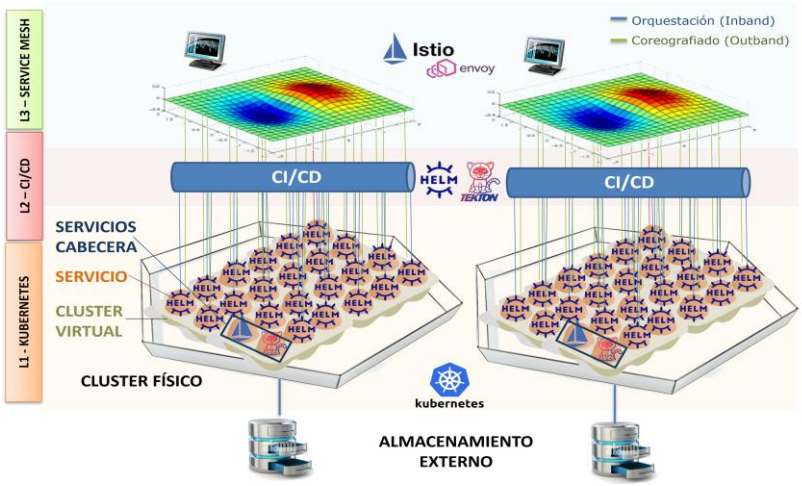
3.3.1.- CAPAS DE OPERACIÓN: DESPLIEGUE APLICACIONES.





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.	• OpenFabrics Alliance • Cisco Application Centric Infrastructure (ACI) • Juniper Apstra • Arista CloudVision • Nokia Data-Center Fabric • 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 • Novell Rancher • Canonical Charmed Kubernetes • 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 • RedHat OpenShift Pipelines • Tekton • Jenkins, Jenkins X • 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 • Istio • 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 • Knative

3.3.2.- 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 el *"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).	• Dynatrace • Datalog • SolarWinds • IBM Instana • Sidecar Container Security Stack
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 • Open Cluster Management • D2IQ

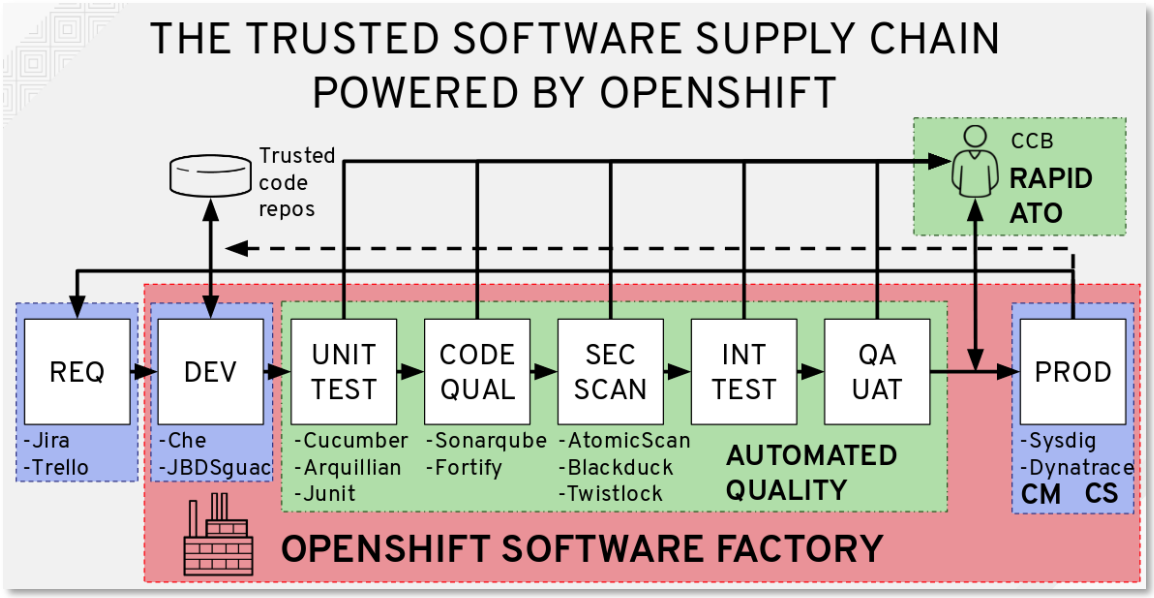
4.- FACTORÍA: AUTOMATIZANDO LA PRODUCCIÓN DE APLICACIONES.

4.1.- ARQUITECTURA DE PROCESOS EN LA FABRICACIÓN DE APLICACIONES.

El punto de partida consistiría en **normalizar la estructura de procesos de una factoría[11] DevSecOps a través de instituciones europeas** como el ETSI.

A partir de una estructura de responsabilidades bien perfilada, surgen las herramientas[12] que cada proceso necesita para realizar satisfactoriamente sus funciones. *Las herramientas que cada factoría va a necesitar para cumplir con esas funciones variarán según el tipo de aplicaciones que deba producir*.

En la imagen, un resumen de las herramientas más comunes en cada etapa del ciclo de vida de producción de aplicaciones.



La seguridad[13] debe estar presente en cada etapa del ciclo de vida DevOps que aplican las factorías software, sin embargo, debido a la necesidad de un enfoque holístico de toda cadena de suministro, tanto la toma de decisiones sobre medidas a aplicar en cada etapa por las distintas factorías, como la evaluación del rendimiento de esas medidas de seguridad y los correctivos asociados, se realizan en un proceso paralelo al de producción… especializado en mejorar la seguridad informática de cada una de las aplicaciones de manera independiente, y conjunta dentro del ecosistema de aplicaciones donde vaya a integrarse.

[11] ***IBM RedHat Secure Software Factory:*** http://redhatgov.io/workshops/secure_software_factory/
[12] ***Michael Bryzek, Design Microservices the Right Way:*** https://youtu.be/j6ow-UemzBc
[13] ***Nokia Berlin Security Centre****, análisis y mejora continua de la seguridad en aplicaciones informáticas:* https://youtu.be/JIEoRChIus8

4.2.- HERRAMIENTAS PARA CADA PROCESO: REDHAT CODE READY PORTAFOLIO.

En la imagen la Suite integrada para desarrollo de aplicaciones para una metodología DevOps que está desarrollando RedHat, cuyo nombre comercial es RedHat Code Ready[14].

La suite no es completa, y requiere ser ampliada con otras herramientas, especialmente validación de APIs[15], análisis de dependencias[16] y microsegmentación. Esto implica un complejo proceso de evaluación hasta lograr integrar satisfactoriamente todas estas herramientas en una solución final de la que inferir una metodología única de trabajo para toda la factoría (similar a Métrica v3[17] en administraciones del Estado):

- **Red Hat CodeReady Workspaces & Eclipse Che**: IDE basada en Eclipse para trabajar con Kubernetes.
- **Red Hat CodeReady Containers**: despliegue local de clusteres OpenShift.
- **Odo**: CLI para automatizar despliegues abstrayendo todos los aspectos técnicos de Kubernetes. Puede integrarse en Eclipse.
- **Red Hat OpenShift developer console**.
- **OpenShift Pipelines and Tekton** for CI/CD.
- **OpenShift Serverless** and Knative.
- **VS Code / IntelliJ**: IDEs alternativos.
- **Red Hat CodeReady analytics**: análisis de dependencias.
- **Red Hat CodeReady toolchain**.

[14] ***Developer Tools, RedHat Code Ready Roadmap:*** *https://developers.redhat.com/summit/2020/developer-tools-codeready-roadmap*

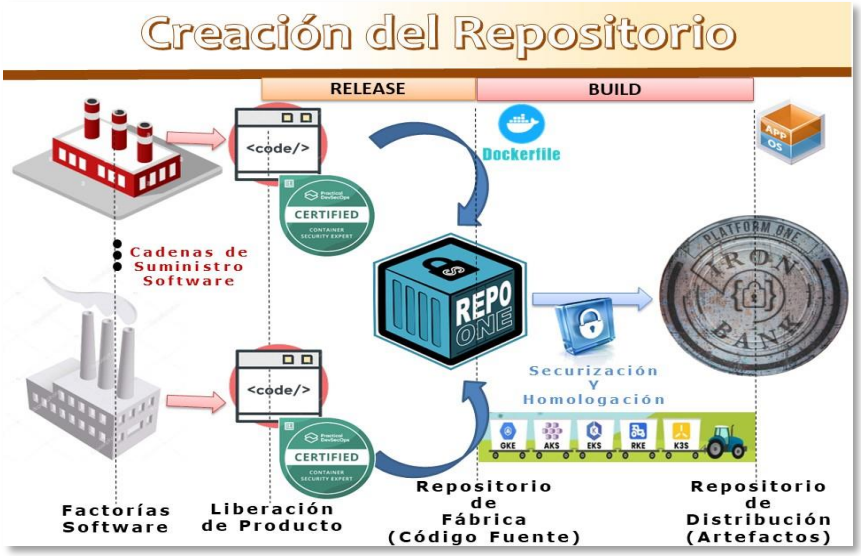
[15] ***API Builder:*** *https://www.apibuilder.io/*

[16] ***Endor Labs, gestion de dependencias:*** *https://www.endorlabs.com/*

[17] ***Métrica v3:*** *https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html*

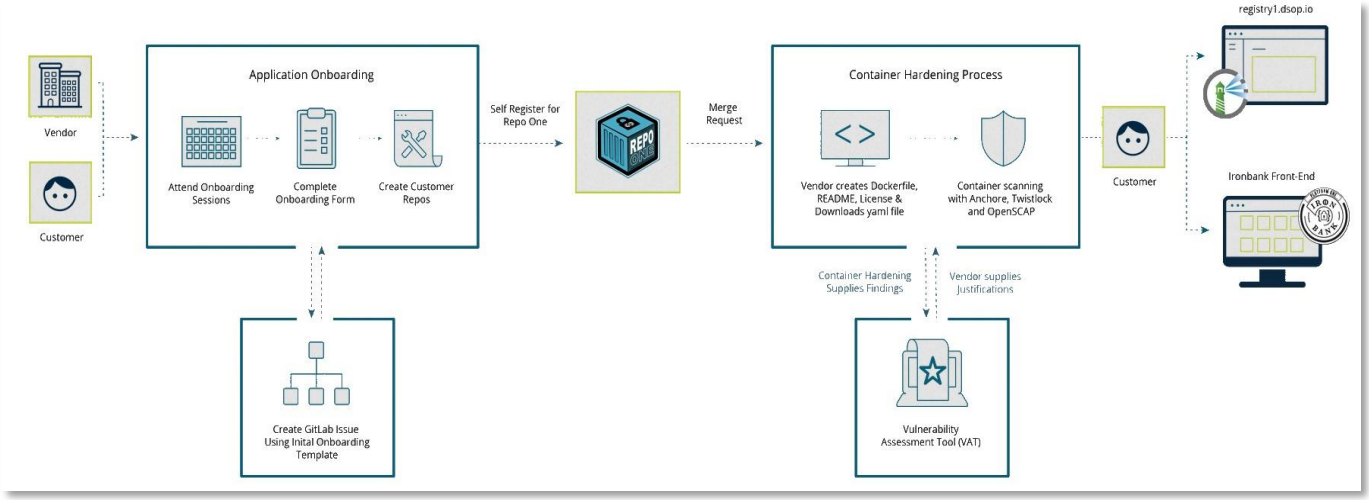
4.3.- LIBERANDO APLICACIONES: REPOSITORIO CENTRALIZADO DE ARTEFACTOS.

La imagen representa cómo el Departamento de Defensa de Estados Unidos distribuye servicios en todo su ecosistema de factorías software a través de los repositorios de código fuente RepoOne[18] y artefactos IronBank[19].



Las fábricas liberan un código fuente validado por el sistema de autorización continua. A continuación, un proceso de homologación (imagen de abajo) construye, a partir del código fuente, los artefactos que finalmente van distribuirse y desplegarse en los distintos clústeres. En entornos de desarrollo, no hay homologación, sino que se automatiza el proceso: se concatena un pipeline CI/CD de build (construcción de artefactos a partir del código fuente) con uno GitOps de deploy (instanciación automática de esos artefactos en los distintos clústeres). Para poder automatizar el proceso, se limita y estandariza el abanico de artefactos que manejan los pipelines GitOps de despliegue.

RELEASE… LIBERACIÓN CÓDIGO FUENTE | **BUILD… CONSTRUCCIÓN ARTEFACTOS**



[18] ***Repo One,*** *DoD Centralized Source Code Repository (DCCSCR):* https://repo1.dso.mil/dsop/dccscr

[19] ***Iron Bank,*** *DoD Centralized Artifacts Repository (DCAR):* https://docs-ironbank.dso.mil/overview/

5.- SUMINISTRO DE MEDIOS DE PRODUCCIÓN.

5.1.- LAS PLATAFORMAS DE ENTREGA CONTINUA.

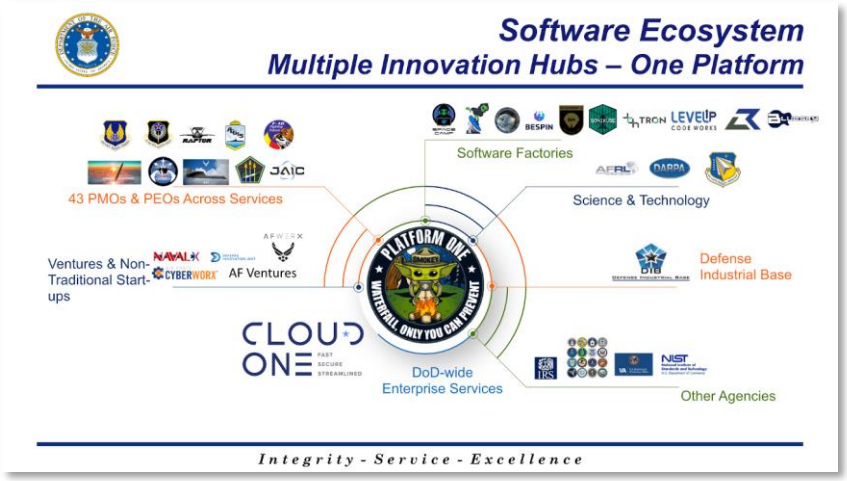
Las factorías de todas las industrias requieren de una sofisticada maquinaria para poder producir aquello que deben suministrar a la sociedad. Para el caso de factorías de aplicaciones, se trata de plataformas de entrega continua que permitan desplegar aplicaciones orientadas a servicios.

En la computación se da la anomalía de que las factorías de aplicaciones tienen la titánica labor de ensamblar sus propias plataformas DevSecOps, es decir, su propia maquinaria de producción. Tarea que abordan sin guía alguna y a partir de toda la tornillería que suministra el código abierto. Tanto operadoras de centros de datos como las factorías de aplicaciones tienen dos posibilidades: bien suscribirse a plataformas de grandes capacidades (como Amazon); bien montar sus propias plataformas propietarias de bajo rendimiento y dudosa viabilidad futura.

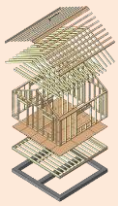
Alquilar computación compartida por millones de usuarios (como Amazon) para alojar lógica crítica de negocio no es una práctica segura. Así que para reducir costes, las operadoras barajan complejos equilibrios entre qué parte queda alojada en servidores externos (tipo Amazon), y qué parte en plataforma privada más segura, pero de bajas prestaciones y alto coste.

El resultado final de estas estructuras híbridas, compuestas en base retales no concebidos para integrarse en una estructura final (y en muchas ocasiones, incompatibles entre sí y/o inviables a largo plazo) son plataformas difíciles de operar y mantener, con serios problemas de seguridad y costes desorbitados.

Surge la necesidad de establecer una cadena de valor capaz de suministrar este tipo de plataformas, tanto a factorías de aplicaciones, como a operadoras de centros de datos, evitando todos los riesgos de seguridad que implica alquilar computación, además de simplificar la operativa de estas plataformas con diseños especializados, reduciendo enormemente sus costes de operación y mantenimiento. En el sector de la aeronáutica se da la excepcional condición de diseñar de manera conjunta tanto entorno de fábrica como el de operadora de centros de datos, lo que lo transforma en privilegiado para la integración de una solución final capaz de resolver todas las cuestiones de ciberseguridad, sirviendo así de referencia para un nuevo tejido industrial de suministro de aplicaciones software, la única forma de abordar el dilema de la soberanía digital europea.



5.2.- LA ESTRUCTURA DE LA CADENA DE VALOR.

FASE	OBJETIVO	DESCRIPCIÓN
1	 ARQUITECTURA	• **Arquitectura - Modelo de Sistema**: instituciones de normalización, como ETSI, coordinan todo el ecosistema productivo gracias a un único modelo de sistema para la plataforma, tomando como punto de partida las especificaciones de fabricación de las plataformas Cloud One y Platform One del Departamento de Defensa de Estados Unidos, disponibles al público en internet.
2	 DISEÑO	• **Diseño - Factorías de Plataforma y Componentes**: dos piezas claramente diferenciadas: o L0 – NetOps - Software Define Data-Center: la infraestructura física de estas plataformas, son mallas, ora de máquinas virtuales, ora de máquinas física. Para máquinas físicas, la única propuesta abierta es OpenFabrics Alliance; para máquinas virtuales OpenStack/CloudStack. o L1-L2-L3-L4 – GitOps - Plataforma de entrega continua: solo existe en el mercado una solución que contemple las cuatro capas de la entrega continua (Kubernetes, CI/CD, Malla de Servicios y Serverless): RedHat OpenShift.
3	 PRUEBAS	• **Pruebas - Homologación de Plataforma**: los andamiajes de pruebas de certificación evalúan las diferentes opciones tecnológicas, estableciendo modelos de infraestructura para cada caso de uso que permitan versionar cada evolución. OPNFV certifica núcleos de red 5G sobre Telco Clouds, siendo el instituto Fraunhofer su representante más destacado.
4	 DESPLIEGUE	• **Clientes – Sistema de Necesidades**: la evolución depende de las directrices provenientes del sistema de necesidades: las factorías de aplicaciones y los operadores de centros de datos de las distintas actividades económicas. Es necesaria la colaboración de sectores estratégicos, como la banca, las telecomunicaciones o la aeronáutica.

5.3.- MITIGACIÓN DE RIESGOS.

Empresas individuales que han intentado resolver este desafío, como *Sun Microsystems*, han desaparecido por el alto riesgo que implica una inversión de estas características: el umbral hasta lograr un producto viable comercialmente es muy alto, es fácil quedarse en el camino. Se trata de datos críticos de negocio, con una natural inercia al cambio.

Tal vez sea este el motivo por el cual la inversión actual se dirige a establecer distintos parques temáticos donde la publicidad masiva garantiza retorno rápido a la inversión, en detrimento de inversiones en el legítimo uso de la computación, que no es otro más que aliviar las tareas administrativas.

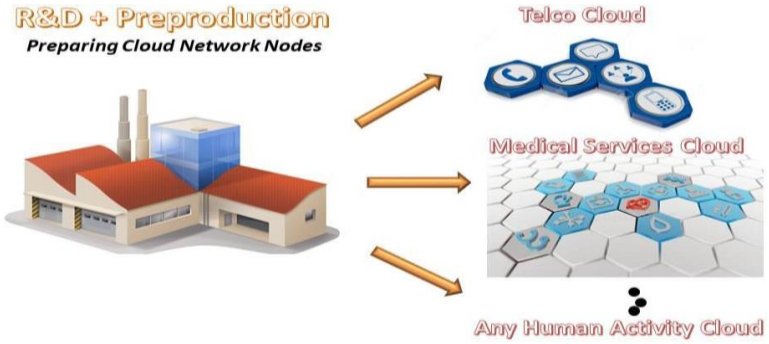
Se torna vital, pues, localizar una metodología que sortee todas las dificultades que entraña la producción de esta vital maquinaria. Un riesgo similar al que asumió IBM a la hora de miniaturizar los primeros ordenadores, pero que le otorgó un 90% de penetración de mercado.

Para este caso, se parte de una base ya establecida: el sistema de normas elaborado por el Departamento de Defensa de Estados Unidos para todas sus factorías de aplicaciones (Cloud One y Platform One). La superficie de investigación es mucho menor respecto al caso de IBM y existen sectores económicos que se ven abocados a seguir el mismo camino que las Fuerzas Aéreas de Defensa de Estados Unidos, por motivos de seguridad nacional.

Localizar una metodología que mitigue los riesgos implica analizar el punto de vista de cada agente involucrado en este proceso productivo:

- **Operadores de centros de datos – Las necesidades**: debido a responsabilizarse de datos críticos de negocio, solo invertirán en adoptar nuevos sistemas si presentan ventajas muy contundentes que compensen el esfuerzo de la adopción. Tal vez un proceso abierto (similar al *Java Community Process*) sobre una infraestructura piloto, donde las operadoras puedan evaluar los prototipos además de manifestar sus necesidades para la mejora de los mismos, pueda agilizar los tiempos de aceptación de producto.
- **Ecosistema de fabricación – Los intereses**: la computación es un sector reciente, sin consolidar, como las telecomunicaciones o la aeronáutica. En otras palabras, no hay una tradición de coordinación, no existe un modelo que garantice beneficios superiores por el hecho de cooperar que trabajando en competición. Tan solo sectores industrializados y obligados a una modernización radical de su infraestructura de computación pueden ser un punto de partida hacia una futura diversificación y miniaturización de esos centros de datos, la única vía efectiva para su democratización.
- **Instituciones de normalización – Los costes**: las operadoras de centros de datos padecen una determinada sintomatología. Sin embargo, sólo una visión de conjunto de todo el sistema productivo es capaz de diagnosticar las causas de esos síntomas de manera certera, lo que se traduce en minimizar los costes de resolución de las necesidades planteadas, garantizando viabilidad futura a todo el proceso productivo. Una financiación pública da la estabilidad necesaria a este proceso de normalización de la estructura, reduciendo los riesgos de una falta de modelo de gobierno.

6.- BIBLIOGRAFÍA.



ESTADO DEL ARTE	
IBM Secure Software Factory	http://redhatgov.io/workshops/secure_software_factory/
Thomal Erl, SOA: Analysis and Design for Services and Microservices	https://www.arcitura.com/books/
Universal Networking Fabric, Lista Controladores SDN	https://en.wikipedia.org/wiki/List_of_SDN_controller_software
MuleSoft Microservices	https://youtu.be/SouNISAnXlo
Cloud LandScape	https://landscape.cncf.io/
IDC, Cloud Centric Infrastructures	https://info.idc.com/cloud-centric-digital-infrastructure-infographic.html
David Cheriton: Arista/Apstra OS	https://youtu.be/LA_LEdV8Cq4
Nokia, The Universal Networking Fabric	https://onestore.nokia.com/asset/212701
Dimitri Stiliadis, arquitecto Nokia Nuage Networks	https://youtu.be/O7UrGrjnYV4?t=88
Arquitectura Microservicios	https://youtu.be/j6ow-UemzBc

RETOS QUE ENFRENTAR	
Stanford, estrategias para la nube	http://web.stanford.edu/class/cs349d/
Stanford, Zero Trust Discussion	https://youtu.be/ooAPzzYkyaE?t=3593
VM Ware, Rawlinson Ribera, Fragmentación Datos	https://youtu.be/dFySwm2bKTg?t=220

EUROPA, PROBLEMA SOBERANÍA DIGITAL	
GAIA-X	https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
Oliver Wyman	https://www.expansion.com/economia-digital/2020/11/22/5fba2e48e5fdea66688b458c.html

PROYECTOS DE REFERENCIA	
OpenFabrics Alliance	https://en.wikipedia.org/wiki/OpenFabrics_Alliance
Platform One, Air Force	https://p1.dso.mil/#/
Karl Isenberg, D2IQ	https://www.youtube.com/watch?v=qku6ilFG5RM
Java Community Process	https://www.jcp.org/en/home/index
Data-Center OS	https://cs.stanford.edu/~matei/papers/2011/hotcloud_datacenter_os.pdf

TELCO CLOUD	
OSM ETSI	https://osm.etsi.org
OPNFV Pharos Lab	https://www.opnfv.org/community/projects/pharos
Enterprise Cloud Simulation	https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1493-2

LÍNEAS DE INVESTIGACIÓN	
Single Unix Specification	https://es.wikipedia.org/wiki/Single_Unix_Specification
Constellation System	https://en.wikipedia.org/wiki/Sun_Constellation_System
INCOSE, International Council for Systems Engineering	https://www.incose.org/