INFRAESTRUCTURAS CRÍTICAS

Modernizando la Producción de Aplicaciones

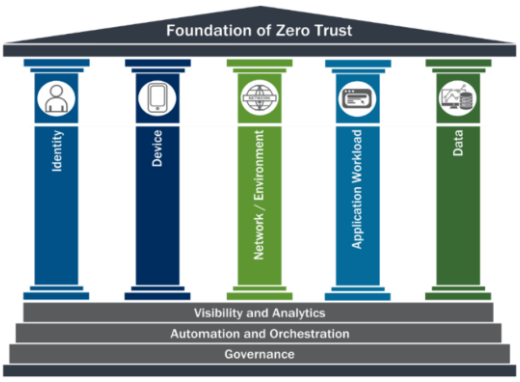
INDEX

1.- MODERNIZACIÓN DE INFRAESTRUCTURAS CRÍTICAS.

1.1.- MOTIVACIÓN: EL MODELO DE CIBERSEGURIDAD ZERO-TRUST (CONFIANZA CERO).

1.1.1.- LA MODERNIZACIÓN: EL NUEVO MODELO DE PRODUCCIÓN DE APLICACIONES.

El primer principio de seguridad es la gobernanza de los entornos que se quieren proteger, una derrama heterogénea de entornos es ingobernable. En consecuencia, el plan de maduración de las infraestructuras de Seguridad Nacional de USA hacia principios Zero-Trust[1] de ciberseguridad comienza **por *unificar y estabilizar el modelo de producción de aplicaciones frente a la evolución tecnológica mediante la estandarización; tanto de los entornos de ejecución (Platform One) como el formato de entrega de las aplicaciones (Iron Bank)***, superando todas las limitaciones de modelos de producción anteriores que vienen lastrando la evolución del sector… y así poder estar a la altura de los tiempos, de hoy y de mañana. Esto implica *reestructurar la cadena de valor del software para lograr tanto aislar la evolución de las aplicaciones respecto de la plataforma donde se ejecutan* (gracias a la entrega de aplicación en un repositorio contenedores); *como desacoplar la evolución de la plataforma de ejecución respecto del hardware* donde se despliega:



- **Operadora de Centro de Datos**: la estandarización de la plataforma de ejecución aísla su evolución del hardware donde se despliega. Un único plano de control para la red de entornos con un sistema de identidades permite la gestión centralizada, ubicua y extremo a extremo de todos los recursos de computación:
- **Fábrica de aplicaciones** responsable de suministrar aplicaciones seguras de fábrica controlando tanto el diseño del plano de datos, como las dependencias de la lógica (SBOM=Software Bill Of Materials). Clave es un diseño orientado a Servicios/uServicios[2] para acelerar entregas.

[1] ***CISA Zero-Trust Maturity Model***: https://www.cisa.gov/zero-trust-maturity-model
[2] ***How Department of Defense moved to Kubernetes and Istio***: https://youtu.be/YjZ4AZ7hRM0

1.1.2.- EL PROBLEMA: SUMINISTRO DE HERRAMIENTAS ESTANDARIZADAS.

Sin herramientas, ni un tornillo se es capaz de desatornillar. Las tecnologías de nube donde diseñar y ejecutar esas aplicaciones evolucionan vertiginosamente[3] sin ninguna normativa, sin ningún plan a largo plazo, centrados exclusivamente en alquiler de maquinaria virtualizada, dejando fuera de la ecuación otros casos de uso como el de infraestructura crítica, que requiere de sus propias nubes privadas.

La estrategia de seguridad nacional de Estados Unidos apuesta por industrializar la producción de aplicaciones de infraestructuras de Seguridad Nacional. **Suministrando de manera gratuita unos medios de producción estandarizados hacen posible lo imposible**… que se animen a adoptar los principios Zero-Trust que conllevan un costosísimo rediseño de toda la cadena de valor del software, incluyendo **refactorización de aplicaciones y entornos donde se ejecutan**. La modernización de infraestructuras ha de hacerse una sola vez, a una plataforma de ejecución DevSecOps estable en el tiempo tanto en fábrica como operadora, es decir, con una normativa clara.

Comienza la modernización en las infraestructuras de Defensa con fecha límite 2027, siguen las gubernamentales para terminar incluyendo todas las infraestructuras del país. *No es posible aplicar reglas de juego internacionales al mundo del dato sin antes universalizar la calidad a todos los procesos de fabricación de aplicaciones, gracias a democratizar el acceso a unas herramientas adecuadas para lograrlo*.

1.1.3.- LA CREACIÓN DE COMUNIDAD DE FABRICANTES

Para la creación de comunidad de fabricantes de Seguridad Nacional tres son los elementos que han sido establecidos:

- **Sistema de normas de fabricación**, estructura de procesos de producción que permite visualizar el grado de seguridad de las aplicaciones liberadas. Procesos descritos en su documentación de referencia *"DevSecOps Reference Design"* : https://p1.dso.mil/resources/platform-one.
- **Plan de modernización**, incorporación gradual de nuevas metodologías y herramientas de trabajo, con las dinámicas de formación de personal requeridas. La comunidad Catalyst es responsable de catalizar la incorporación de nuevos fabricantes al ecosistema de Seguridad Nacional: https://catalystcampus.org/ecosystem-overview/.
- **Suministro de medios de producción estandarizados**, para agilizar la puesta en funcionamiento de las nuevas factorías… una serie de vendedores se ocupan de comercializar infraestructuras de fabricación que garanticen cumplir con la rigurosa normativa de Seguridad Nacional de Estados Unidos en materia de aplicaciones informáticas: https://catalystcampus.org/platform-one-commercialization/.

[3] ***Mapa de Tecnologías de Nube:*** https://landscape.cncf.io/

Existen servicios de consultoría que pueden ser una puerta de entrada a este ecosistema de fabricantes vinculados a la Seguridad Nacional de USA:

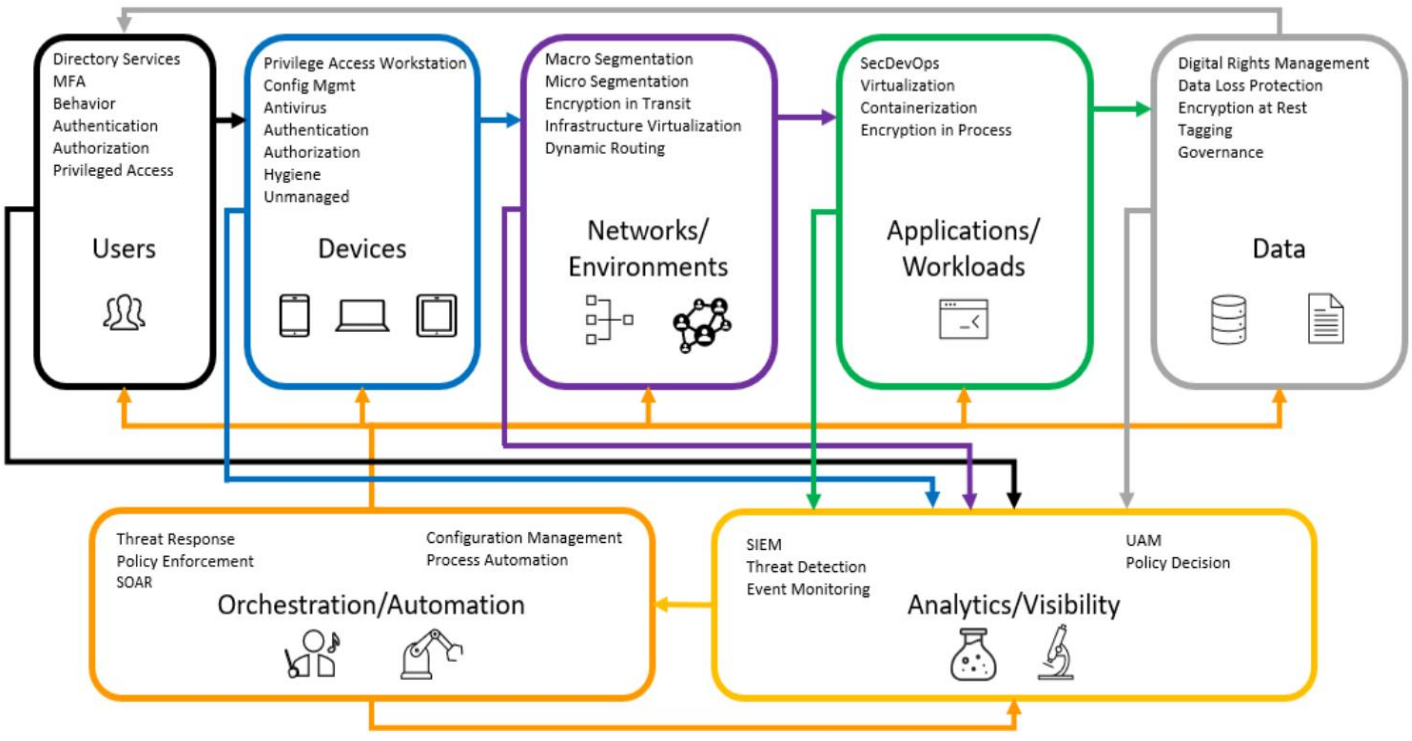
How can I effectively modernize my legacy system, both hardware and software?
By using modern design patterns, modularization, microservices,
and translation tools,
Seed designs an effective, efficient plan to move your mission system forward.
https://www.seed-innovations.com

1.1.4.- IMPORTANDO EL MODELO DE PRODUCCIÓN DE USA A EUROPA

Un trabajo mancomunado con otros fabricantes que compartan la misma problemática tal vez redunde en una significativa reducción de costes de la modernización y una mayor compatibilidad con **estándares comunes que mantienen un plan de evolución estable en el tiempo**, evitando la vorágine incontrolada de líneas de evolución que terminan muriendo. Además, *la estandarización independiza las infraestructuras críticas de los fabricantes*.

- Tecnologías probadas por una gran comunidad de fabricantes
- Consultorías y servicios de soporte disponibles.

En definitiva, importar este nuevo modelo de producción software (basado en la distribución centralizada de contenedores) de USA a Europa. La comunidad Catalyst tiene procesos de formación intensivos de 6 meses[4] en USA, donde se aprende todo este universo de la Seguridad Nacional, además de establecer conexiones que van a facilitar todos los procesos de comercialización. De hecho, la creación de comunidad de fabricantes es el motivo de la existencia de esta comunidad, o sea, facilitar la contratación.



[4] ***Programas formativos 6 meses***: https://p1.dso.mil/residency

1.2.- ARQUITECTURA DEL CENTRO DE DATOS.

1.2.1.- CLOUD ONE Y PLATFORM ONE.

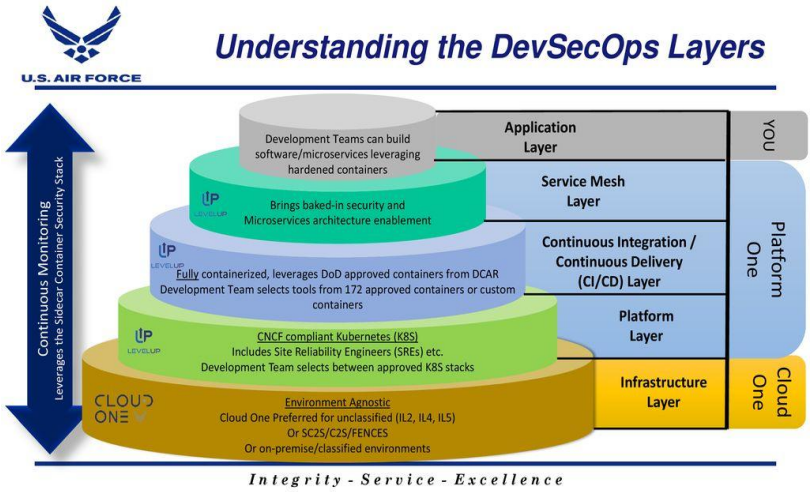
A la hora de administrar infraestructuras de centro de datos, aparecen dos capas, la undercloud (Defensa USA la llama Cloud One) y la Plataforma DevSecOps (Defensa USA la llama Platform One[5]), que no es más que una forma de inicializar los clústeres, es decir, un Helm Chart[6] que define las herramientas que ha de tener el clúster. *Esta arquitectura de dos capas desacopla la plataforma DevSecOps software, del undercloud hardware, permitiendo una evolución constante del entorno de ejecución de aplicaciones al margen del hardware donde se despliegue la plataforma*.

PLATFORM ONE BIG BANG UNIVERSE

https://p1.dso.mil/services/big-bang

VivSoft ENBUILD

https://www.vivsoft.io/post/big-bang-deployment-simplified-with-enbuild



Inicialización Clústeres

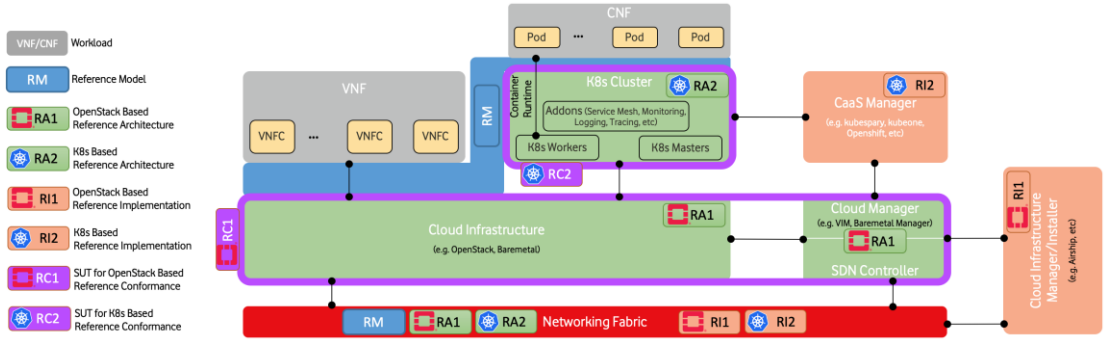
https://p1.dso.mil

(herramientas Open Source para evitar vendor lock-in)

On Premise: normas Telco Cloud

Anuket(https://anuket.io/) = CNTT(https://cntt.readthedocs.io) + OPNFV (https://www.opnfv.org/)

Normativa estable en el tiempo, con un modelo de gobierno[7] que establece ciclos de pruebas y entrega[8].



On Cloud: Normas de cada Proveedor de Nube.

CLOUD ONE FAST SECURE STREAMLINED

UnderCloud

https://www.cloud.mil/

[5] ***Estructura de Capas de Platform One***: https://csrc.nist.gov/csrc/media/Presentations/2022/oscal-mini-workshop-1-P1_DoD%2BNIST/P1%20OSCAL%20PA%20Approved.pdf

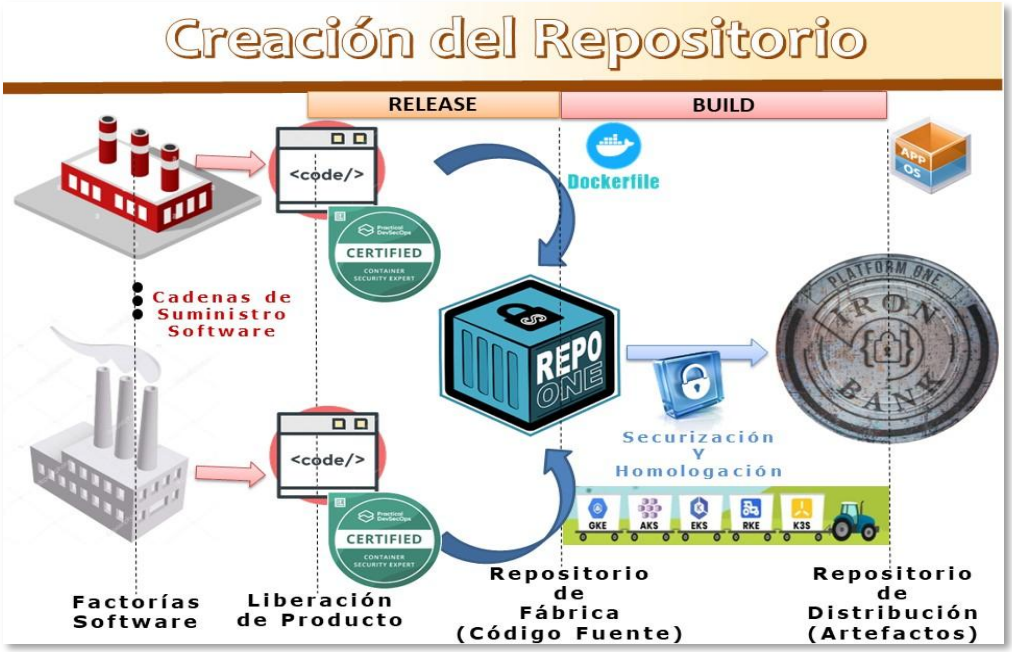
[6] ***Demo BigBang***, *Helm Chart configurable para desplegar distintas herramientas sobre un clúster según su rol dentro de un pipeline de construcción DevSecOps:* https://www.youtube.com/watch?v=rfufvM3ktYE&t=1047s

[7] ***Modelo de Gobierno Telco Cloud:*** https://osm-download.etsi.org/ftp/osm-7.0-seven/OSM9-hackfest/presentations/OSM%239%20Hackfest%20-%20HD0.0%20Introduction%20to%20NFV%20and%20OSM.pptx.pdf

[8] ***Telefónica Única,*** *pionera en Telco Cloud:* https://youtu.be/npYqd_l5YjY?si=XqJC2ElZnnJjqE01

1.3.- USOS DEL CENTRO DE DATOS

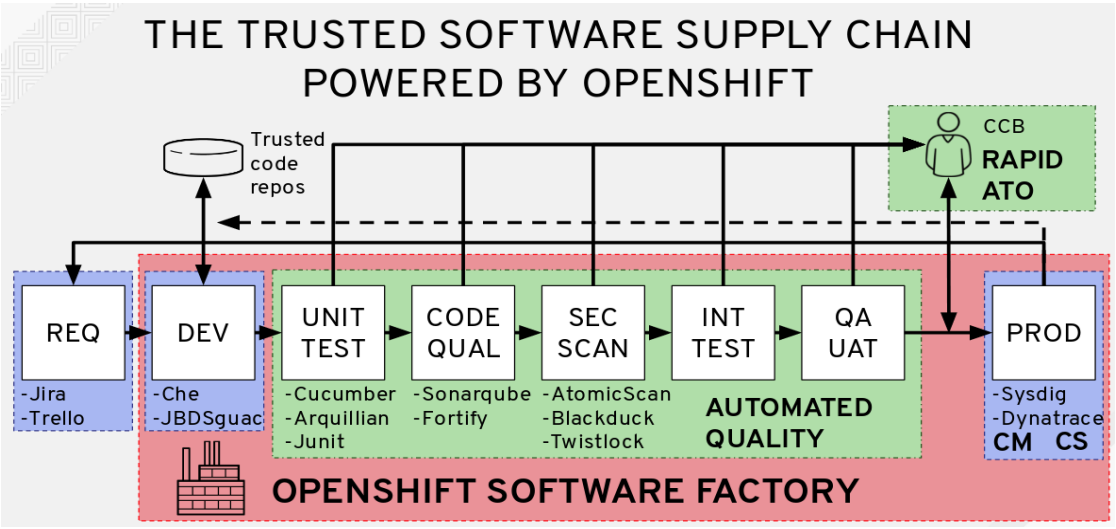
1.3.1.- DISTRIBUCIÓN DE APLICACIONES: EL REPOSITORIO



El repositorio de distribución software[9] **juega un papel crítico dentro de modelo de producción de aplicaciones de Seguridad Nacional USA**. El repositorio[10] de contenedores compartido por todas las factorías con procesos de homologación de sus contenedores para su ejecución sobre una plataforma estandarizada (equiparable a un distribuidor de paquetes Linux) desacopla la evolución de las factorías de aplicaciones respecto de las operadoras de centros de datos.

1.3.2.- FACTORÍAS SOFTWARE: METODOLOGÍA DEVSECOPS

1.3.2.1 ESTRUCTURA DE UNA FACTORÍA[11]

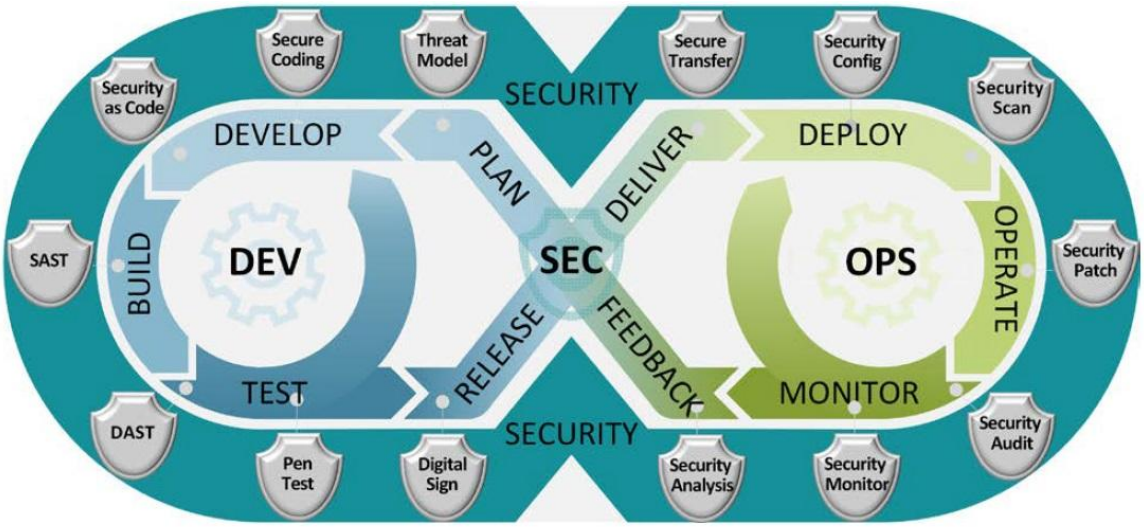


[9] ***Repo One - DCCSCR,*** *DoD Centralized Container Source Code Repository:* https://repo1.dso.mil/dsop/dccscr

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

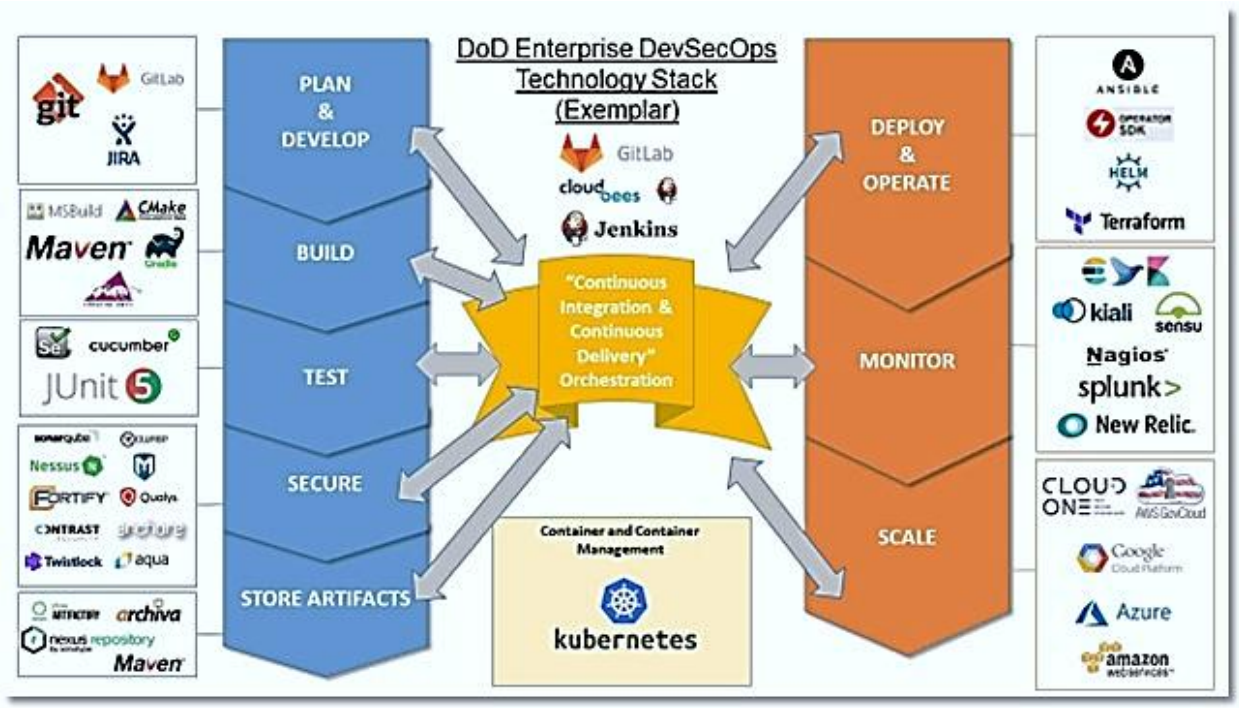
[11] ***IBM RedHat Secure Software Factory:*** http://redhatgov.io/workshops/secure_software_factory/

1.3.2.2 ETAPAS DEL PROCESO DE PRODUCCIÓN SOFTWARE



Uno de los factores decisivos para agilizar los procesos de entrega, es el sistema de puntos de autorización (gates) distribuidos en esta secuencia de procesos de fabricación, cuyo resultado recibe el nombre de cATO (Continuous Authorization to Operate)[12].

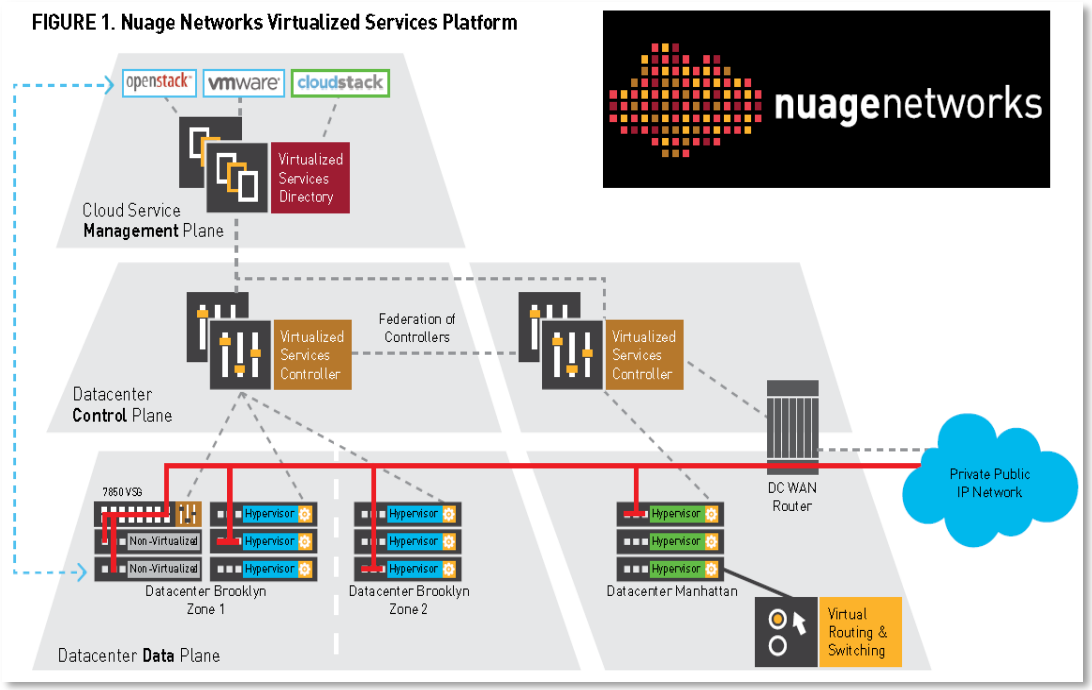
1.3.2.3 HERRAMIENTAS PARA LA FABRICACIÓN DE APLICACIONES



[12] *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*

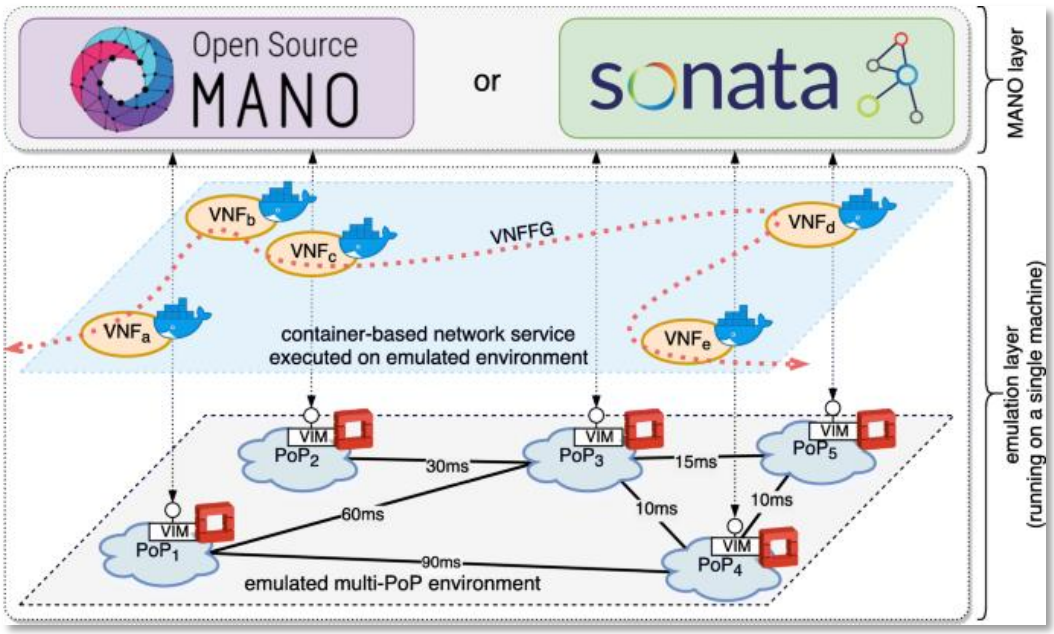
1.3.3.- OPERADORAS: SOFTWARE DEFINED PERIMETER

1.3.3.1 ESCALABILIDAD: SOFTWARE DEFINED NETWORK



Sobre estas líneas, la estructura que permite la gestión centralizada de políticas de red a lo largo de toda la red de centros de datos.

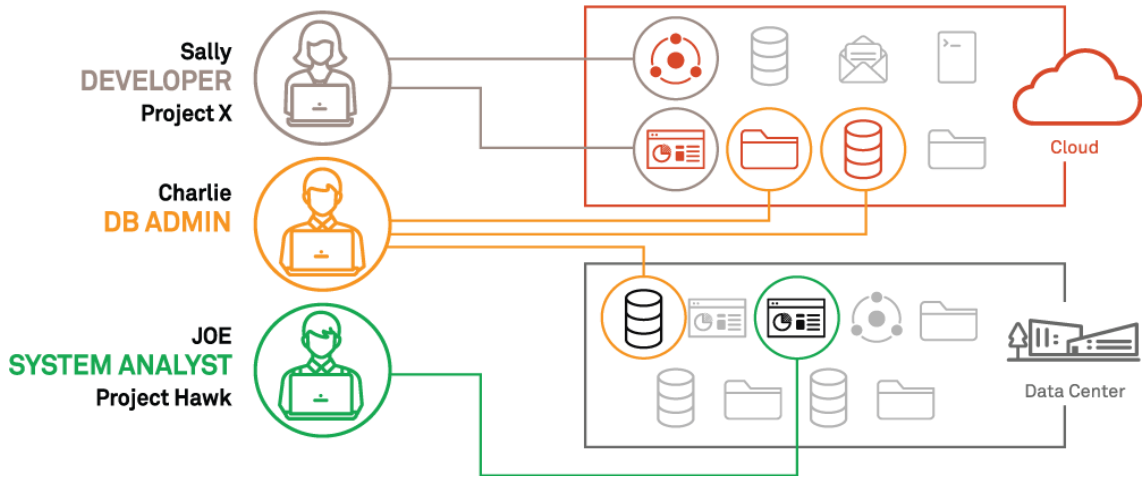
Bajo estas líneas, un entorno de simulación[13] para comprobar la escalabilidad.



[13] ***Simulación orquestadores NVFs*** *en escenarios con múltiples puntos de presencia (PoP):* https://www.researchgate.net/publication/334046310_Automated_testing_of_NFV_orchestrators_against_carrier-grade_multi-PoP_scenarios_using_emulation-based_smoke_testing

1.3.3.2 SEGURIDAD: CNAP – CLOUD NATIVE ACCESS POINT

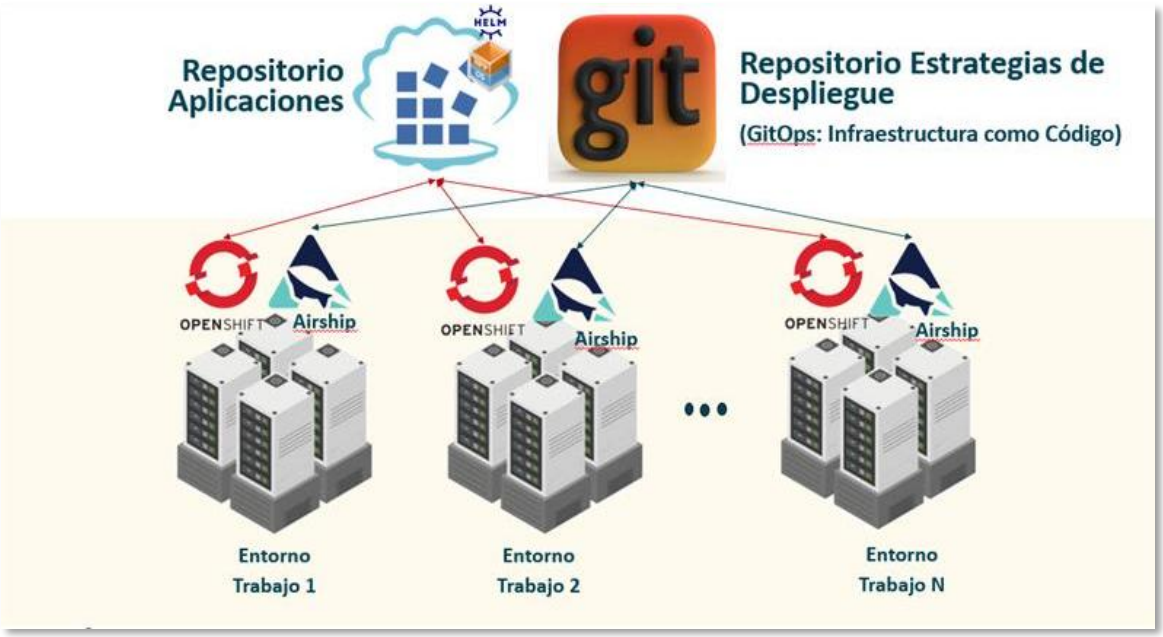
Tal como muestra la imagen, Cloud Native Access Point[14] consiste en desplegar una red definida por software por cada acceso de usuario (también llamado 'segmento de uno'), que solo le da visibilidad a los recursos sobre los que tiene permisos ese usuario, en función de su rol en el sistema, el dispositivo que usa para acceder y su localización geográfica. Un proceso se ocupa de continuamente escanear si cambian las condiciones de acceso de cada conexión, para reconfigurar la red definida por software de las conexiones para las que cambian sus condiciones.



1.4.- EL ENTORNO DE PRUEBAS I+D.

1.4.1.- ARQUITECTURA DEL ENTORNO.

En las instalaciones I+D se despliegan estructuras de trabajo como las indicadas en la imagen, sirviendo de extensa batería de pruebas para los futuros entornos de producción



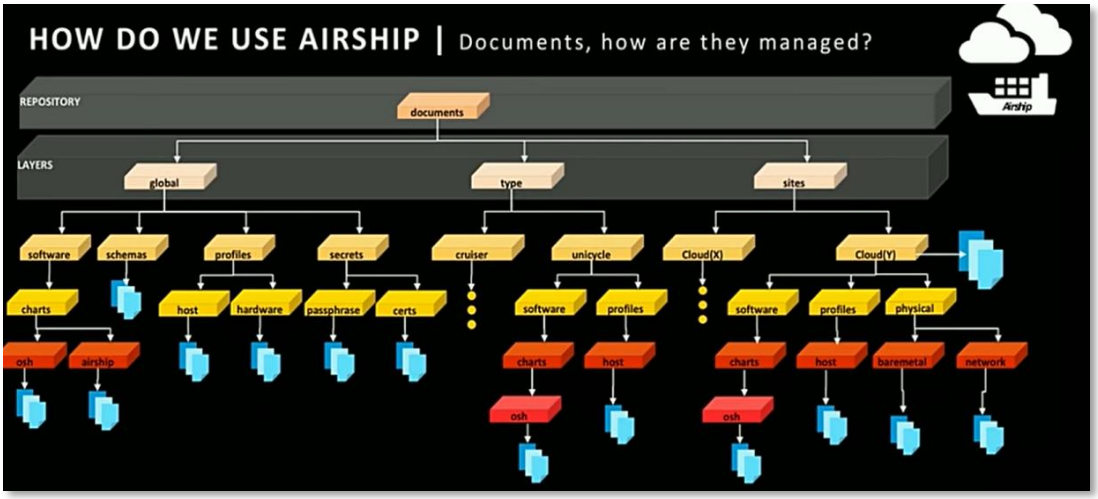
[14] ***Cloud Native Access Point***: https://www.youtube.com/watch?v=15KlsxFxkxo

1.4.2.- APLICATIVO: LOS REPOSITORIOS, INTERFAZ ENTRE APLICACIÓN Y PLATAFORMA.

La clave del diseño, radica en la estructura de repositorios que desacopla la evolución de aplicativo, de la evolución de plataforma. Se pueden aplicar procesos de mejora continua en los entornos de ejecución hacia principios Zero-Trust si se aísla la evolución de la plataforma del desarrollo de aplicaciones a través de una interfaz estable: contenedores e infraestructura como código. Aparecen dos repositorios:

- **Repositorio de Aplicación**: se almacenan las aplicaciones en forma de contenedores. Los contenedores se crean a través de un proceso de homologación[15] y securización[16] a partir de un repositorio de código fuente. Estas aplicaciones se desplegarán en plataformas Zero-Trust, que son clústeres kubernetes (por ejemplo, RedHat OpenShift) ya inicializados con herramientas de monitorización continua, aprovisionamiento e identificación de usuarios.
- **Repositorio de Estrategias de Despliegue**: colecciones de documentos YAML que definen todas las configuraciones necesarias para desplegar cada centro de datos de manera totalmente automatizada. El centro de datos, descarga su estrategia de despliegue del repositorio y a partir de ahí se autoinstala. Estas estrategias tienen tres elementos:
  - *Descripción de la Infraestructura*: ejm., sectorización en clústeres k8s para controlar el ciclo de vida de aplicaciones Helm, como Helm OpenStack. Las herramientas para resolver este problema están en el mundo de la Telco Cloud[17], como por ejemplo AirShip[18] de AT&T.
  - *Descripción de Entornos de Ejecución*: ejm., inicialización de clústeres con las herramientas necesarias en cada etapa de un pipeline DevSecOps. BigBang de Defensa USA sería una de las herramientas para resolver este problema.
  - *Configuraciones de cada Entorno de Ejecución*: ejm., personalizar cada entorno de trabajo de una factoría Software.

En la imagen, el aspecto de las estrategias de despliegue en AirShip:



[15] ***Homologación Debian*** *para repositorios .deb:* https://www.debian.org/doc/manuals/developers-reference/index.en.html

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

[17] ***CNTT-RI2, Kubernetes Installer Comparison:*** https://lf-networking.atlassian.net/wiki/spaces/LN/pages/15653770/Kubernetes+Installer+Comparison

[18] ***Airship****:* https://www.airshipit.org/

1.4.3.- PLATAFORMA: ENSAMBLADA EN FÁBRICA SIGUIENDO ESTÁNDARES CNTT.

En el sector Telco, los centros de datos se ensamblan en factoría[19], para luego ser ubicado en su emplazamiento final. A partir de ahí, el centro de datos se conecta a la cabecera de región desde la que se descarga las configuraciones que deben aplicarse en ese sitio.

En Brasil, una estimación sería 50.000 controladores de antena en emplazamientos recónditos, sin este grado de automatización, no sería posible ni la puesta en marcha, ni la actualización de todo el parque de centros de datos.

Empleando esta misma maquinaria, bajo la estandarización CNTT supone establecer una línea de evolución clara y estable en el tiempo para la plataforma de nube. Adicionalmente, el sector Telco cuenta con centros especializados en investigar los problemas de ciberseguridad[20], lo que garantiza una mejora continua de la plataforma Zero-Trust en cuestiones de seguridad informática.

TRANSPORTE AL EMPLAZAMIENTO	AUTOINSTALACIÓN
	

1.4.4.- CIBERSEGURIDAD: LA GOBERNANZA DE LOS ENTORNOS DE EJECUCIÓN.

El primer principio de seguridad es la gobernanza de los entornos que se quieren proteger. *Este principio aplicado a la informática implica el uso de plataformas de ejecución de aplicaciones diseñadas bajo un único estándar*, con procesos de mejora continua. Una derrama heterogénea de entornos de ejecución es ingobernable, al margen de las inversiones en distintas herramientas tecnológicas para la seguridad informática.

El uso de un único entorno de ejecución estandarizado 'urbi et orbi', obliga a sistematizar[21] la producción del software[22] estandarizando tanto la plataforma[23] de ejecución, como los repositorios de entrega de aplicaciones. *Abstrayendo la compleja problemática de los entornos de ejecución y su evolución, las fábricas de aplicaciones ahora pueden centrarse en mejorar el diseño de sus aplicaciones*, incorporando nuevos aspectos de seguridad, como estructuras para la gobernanza del dato, que evita problemas de fragmentación gracias a establecer esquemas de crecimiento para los datos.

---

[19] ***Nokia Datacenter Delivery Service***: https://youtu.be/nCKNIYdp7_Y?si=prtsqq8MqZyuTU2z

[20] ***Nokia Berlín Security Centre***, *análisis y mejora continua de la seguridad en aplicaciones informáticas:* https://youtu.be/LNR-0Q4FUVY?si=brk9rZeyuVjVKxdc

[21] ***Modelo Producción Software*** *de Seguridad Nacional USA:* https://media.dau.edu/playlist/details/1_wwqs338p

[22] ***Refactorización de Aplicaciones*** *de Seguridad Nacional USA:* https://media.dau.edu/playlist/details/1_0kko71p1

[23] ***Plataforma DevSecOps*** *de Seguridad Nacional USA:* https://media.dau.edu/playlist/details/1_iu6ulm7r

2.- LA SOCIEDAD DE LA INFORMACIÓN.

Por doquier apreciamos cómo las aplicaciones informáticas infiltran cada intersticio de nuestras vidas cotidianas. En el coche guían nuestra ruta, en el móvil nos mantienen conectados a toda hora, en el trabajo preparando informes u organizando la agenda de eventos. Ningún espacio, ni ninguna actividad se escapa a su influjo, un fenómeno que hemos acordado llamar "la transformación digital".

Sin darnos cuenta, somos cada vez más dependientes de un mundo virtual del que poco sabemos. Desde las corporaciones más grandes hasta cada uno de nosotros -a título individual-, nadie es capaz de sustraerse a esta poderosa influencia… estamos todos a merced de estas aplicaciones informáticas, cual boyas a la deriva de corrientes oceánicas.

¿A dónde nos arrastran las corrientes de este océano digital? El cine recurrentemente evoca el miedo a ser dominados por unas máquinas que nosotros mismos hemos creado. Sentimos que esa nueva realidad nos arrastra a un futuro incierto, sacrificando el tesoro de nuestra intimidad por el camino.

Sin embargo, todo este universo virtual que nos envuelve se reduce a aplicaciones informáticas: en todo su amplio espectro de objetivos y tecnologías de construcción… desde sistemas de control de vuelo, pasando por la robótica de las fábricas, inteligencia artificial, big data, hasta las aplicaciones de nuestros ordenadores personales o teléfonos móviles.

En el ADN encontramos codificados los esquemas organizativos de todos los sistemas que forman un organismo vivo. La información existe para organizar y coordinar la vida, es decir, para el orden y buen compás que rige este Cosmos. Las sociedades humanas no escapan a esta ley, por eso nos vemos rodeados de todas esas herramientas informáticas que sirven para organizarnos mejor como sociedad, en eso que rotulan como "sociedad de la información". Se torna vital, pues, no dejar la producción de esas aplicaciones que organizan todas nuestras vidas en manos de miopes designios comerciales, que nos atrapan en experiencias virtuales con inciertas intenciones y dudosa utilidad.

Tal vez sea nuestra incapacidad para organizar y gobernar la producción de esas aplicaciones que controlan nuestras vidas la que realmente nos infunde esa sensación de estar a merced de esas tecnologías, en lugar de ponerlas a nuestro servicio. ¿Es la inteligencia artificial el problema, o los datos de los que se alimentan esos algoritmos que corren sobre una maquinaria al alcance de muy pocos bolsillos, originando el problema de la soberanía digital? Nuestros datos concentrados y hacinados de una manera antihigiénica en nubes sobre las que no tenemos ningún control, al no ser nosotros sus dueños… con una alta fragmentación, gestionados por algoritmos de una trazabilidad muy pobre, que no suelen ajustarse a ninguna norma de calidad. Cuando hay mucha hojarasca, es fácil que una pequeña chispa detone un imparable incendio, ¿será este nuestro verdadero temor, simplemente no atinamos a cristalizarlo en palabras?