

¿Listos para empezar?

true

Si

DevOps

Devops

Luis Salas Sysadmin



¡Bienvenidos y bienvenidas!

Comunidad
DevOps + Cloud Native

Costa Rica



Leonardo Murillo

Organizador de la Comunidad

CTO @ Qwinix, Inc.
Fundador @ Cloud Native Architects



/in/leonardomurillo/



/murillodigital



/murillodigital

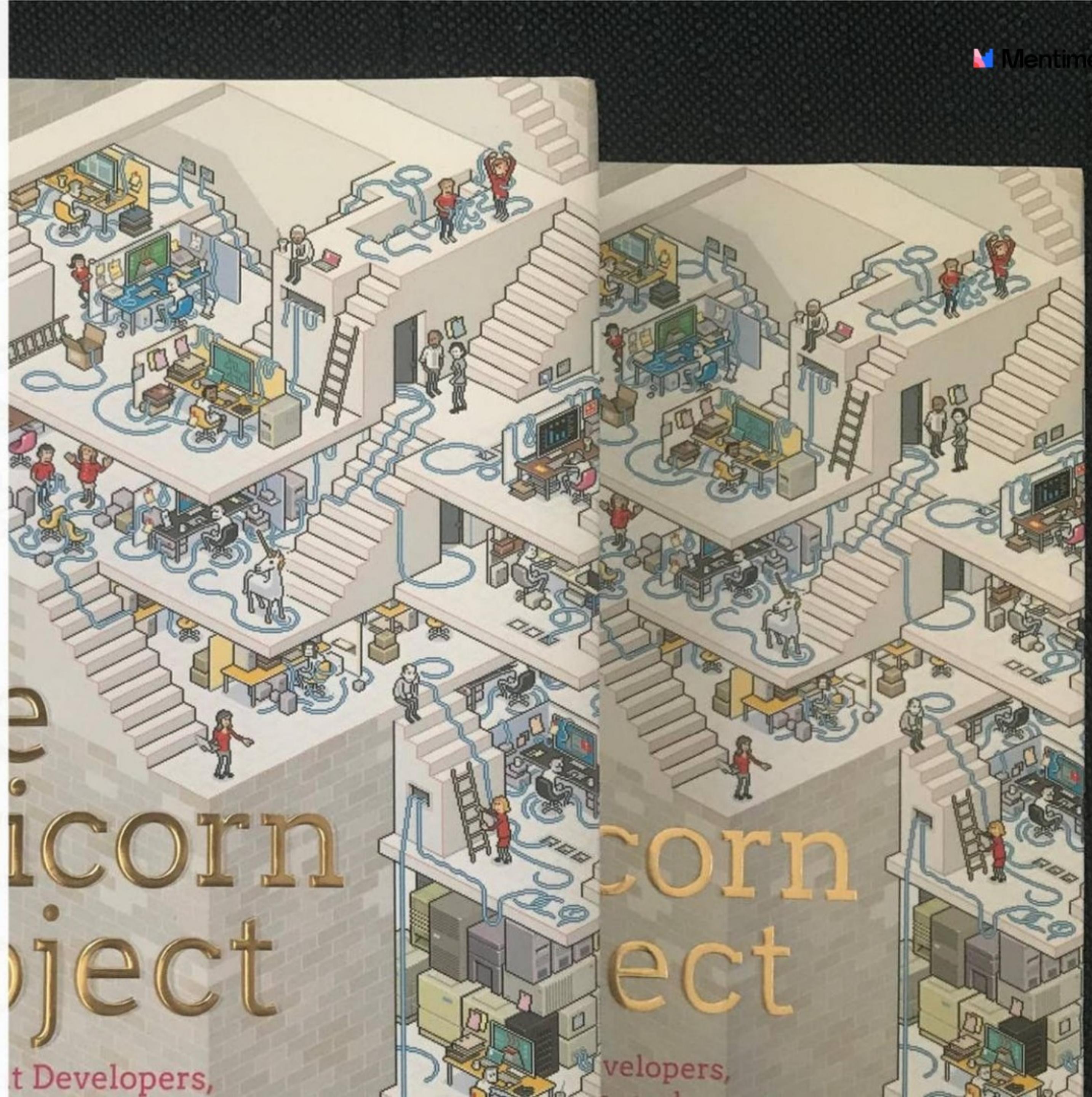


<https://murillodigital.com>

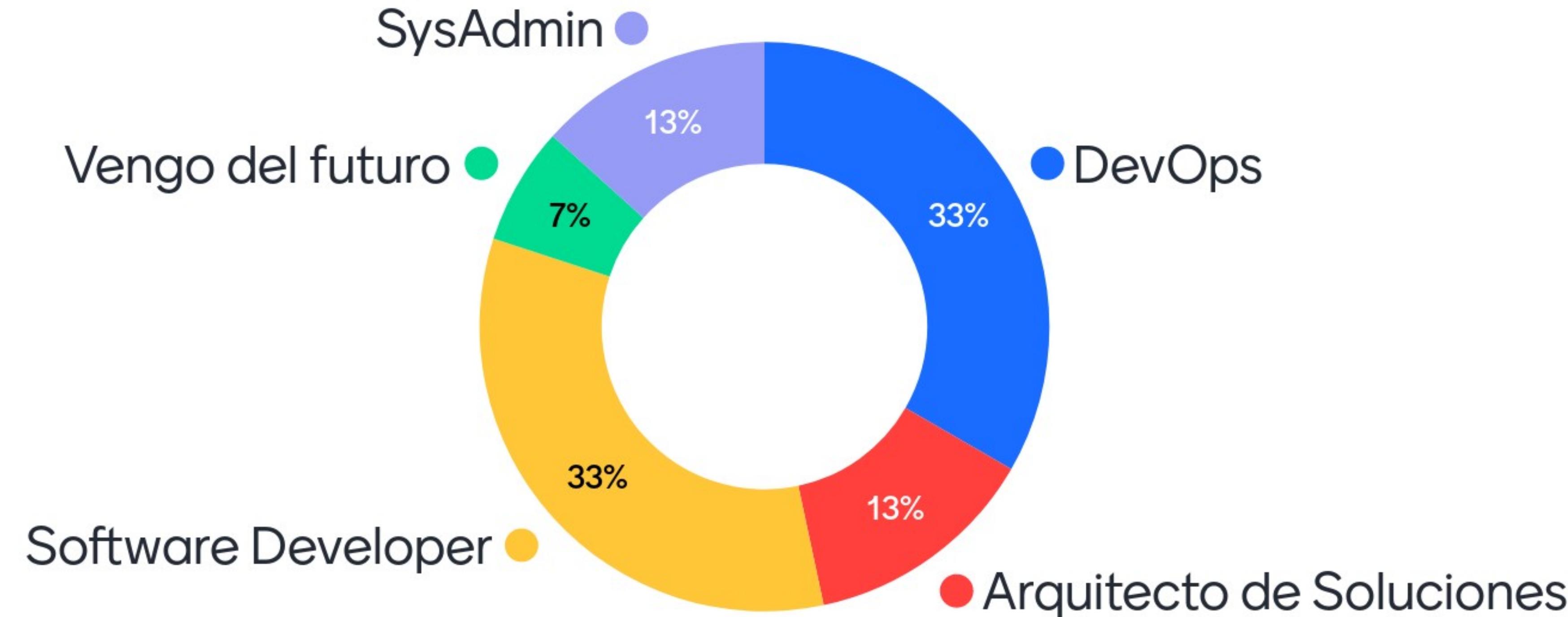


¡Tres !

1. Entre todos y todas las participantes (asistencia hasta el final del evento)
2. El que más votos tenga de “peor pelada en producción”
3. Entre los y las que tengan la cuenta correcta de cuantas veces aparece la palabra “Kubernetes” en esta presentación.



¿Con cual función te identificás más?



¿Cuál es tu nivel de experiencia?



Empezando a explorar



DevOps y/o Cloud Native es parte de mi trabajo cotidiano

0

Soy pro y la próxima charla la doy yo

1

Vengo del futuro y tengo una advertencia



Objetivos de la comunidad

Networking y Desarrollo Profesional



Slack Workspace

<https://crdevopscloudnative.slack.com>



Charlas, Webinars, etc

<https://www.meetup.com/devops-cloudnative-costarica/>



Web y Directorio Profesional

<https://comunidad.cloudnative.cr>



Conocimiento y colaboración

Workshops

Aprendizaje interactivo de tecnologías, herramientas, mejores prácticas de gestión de talento y procesos

Charlas

Representantes y líderes de pensamiento de la comunidad global de DevOps y Cloud Native exponiendo sus ideas y avances en la industria.

Reunión de la comunidad

Reunión abierta para comunicar propuestas, iniciativas y planeamiento, una oportunidad abierta para que miembros expongan sus expectativas, retos e historias.

Eventos conjuntos

Hackathons, proyectos conjuntos y “guest speakers” en coordinación con otras comunidades.



Participación Global



Explore by Region

North America Central and South America Europe Africa Asia Virtual

BELO HORIZONTE, MG
Brazil

CAMPINAS, SP
Brazil

MEDELLÍN
Colombia

RECIFE
Brazil

BOGOTÁ
Colombia

GUATEMALA
Guatemala

MENDOZA, MENDOZA
PROVINCE
Argentina

SAN SALVADOR, SAN
SALVADOR DEPARTMENT
El Salvador

BRASÍLIA
Brazil

JOÃO PESSOA, PB
Brazil

PANAMÁ
Panama

SANTIAGO
Chile

BUENOS AIRES
Argentina

LIMA
Peru

PORTO ALEGRE
Brazil

SÃO PAULO
Brazil



SKIL^{up}Chapters
by DevOps Institute
LATAM



Ops

Nuestra industria nos ofrece muchos privilegios

Hemos esquivado el impacto de la pandemia relativamente bien.

Tenemos ingresos superiores al promedio.

Cada vez más el mundo depende de nuestras habilidades.

Tenemos el poder de cambiar la vida de los que sufren



Community as Code

Propuestas, colaboración y directorio



CRDevOpsCloudNative/comunidad

directorio/
eventos/
workshops/
site/





¿Cuál fue tu peor pelada en producción?

Cual fué tu mayor pelada en producción

Editar un SP en PRD. Quitando un where antes de ejecutar un job con el sp, se borraron la mayoría de los usuarios del sistema.

En una empresa de colocation realice un rm -rf / en un servidor web de produccion.... Como si eso no fuera malo, me paso lo mismo la siguiente semana :(... es que estaba en noviando

¿cuenta volarse todas las reglas de todos los security groups de una cuenta de producción de aws?

Olvide renovar el certificado digital de una tienda de venta de flores el 14 de febrero

Hice un deployment de CRD's a un cluster de un cliente en kubernetes de un cliente, pero olvide cambiar el contexto, instale el app en el cluster de otro cliente que producción tenía versiones diferentes y se You can't use 'macro parameter character #' in math mode todo





CLOUD NATIVE COMPUTING FOUNDATION



Evento anual organizado por la CNCF que reúne a DevOps, SREs, Desarrolladores, Arquitectos y muchos otros profesionales involucrados en la comunidad del software libre, modernización, arquitectura nativa para la nube, y más.



KubeCon

CI/CD

Comunidad

Kubernetes

Data y ML

Redes

Almacenamiento

Observabilidad

Rendimiento

Seguridad e Identidad

Serverless

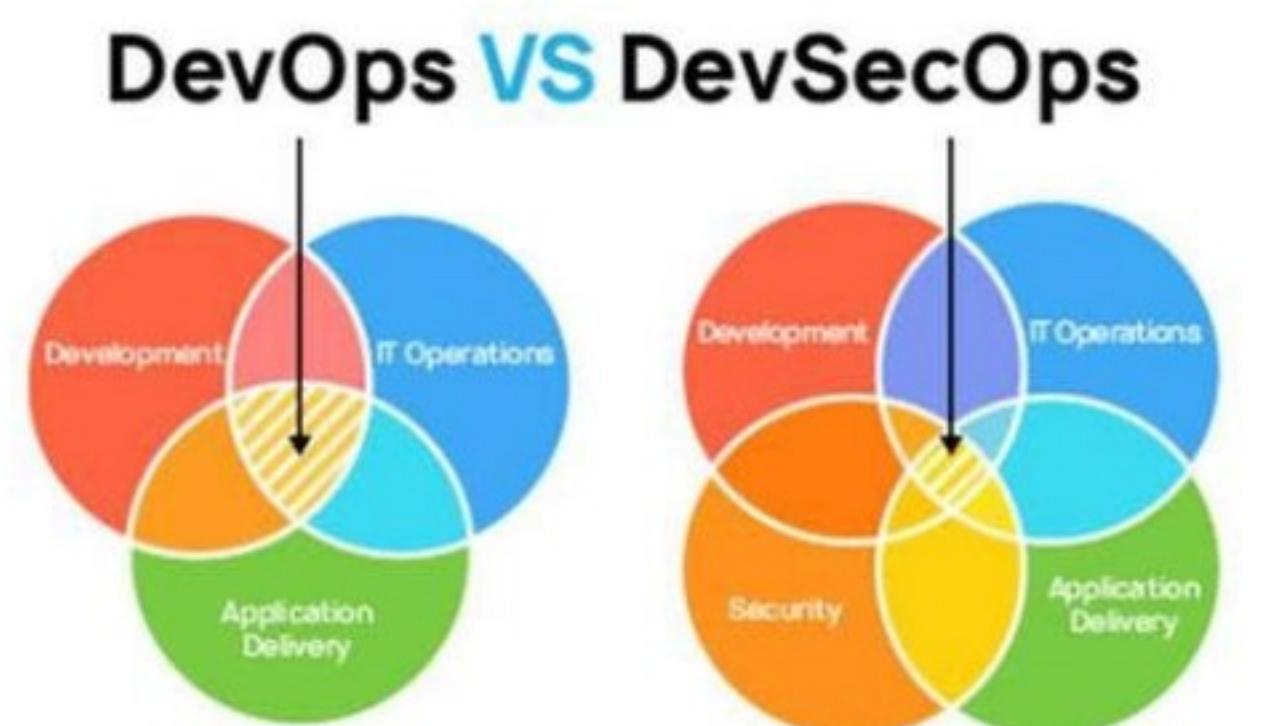
Service Mesh

Diversidad e Inclusión

DevSecOps

Extiende el concepto de responsabilidad compartida de DevOps para que incluya la seguridad.

Introduce un enfoque en seguridad a través de todo el SDLC, integrando seguridad en patrones existentes asociados a DevOps como la automatización, CI/CD, inmutabilidad, determinismo y “todo como código”





Falco utiliza reglas declaradas en yaml y monitorización constante de syscalls para identificar y alertar sobre comportamiento no deseado.

```
- rule: shell_in_container
  desc: notice shell activity within a container
  condition: container.id != host and proc.name = bash
  output: shell in a container (user=%user.name container_id=%container.id container_name=%container.name)
  priority: WARNING
```



Puede inspeccionar los audit events de Kubernetes, y puede evaluar condiciones relacionadas a entidades dentro del cluster, y retornar información específica de los objetos de Kubernetes.

Homepage:

<https://falco.org/>

Open Source:

<https://github.com/falcosecurity/falco>

Documentation:

<https://falco.org/docs/>

CNCF Status:

Incubating



Open Policy Agent

OPA desacopla la toma y enforzamiento de decisiones usando políticas declarativas, escritas en un lenguaje llamado Rego.

Homepage:

<https://www.openpolicyagent.org/>

Open Source:

<https://github.com/open-policy-agent/opa>

Documentation:

<https://www.openpolicyagent.org/docs/latest/>

CNCF Status:
Incubating

Se puede utilizar a través de todos los elementos de una arquitectura distribuida, desde usuario, redes, infraestructura, nodos y runtime, etc.

Se integra efectivamente con Kubernetes, y el proyecto OPA Gatekeeper (beta) incluye CRDs.

The Rego Playground

EVALUATE SHARE

```

1 package kubernetes.admission
2
3 deny[msg] {
4     input.request.kind.kind == "Pod"
5     image := input.request.object.spec.containers[_].image
6     not startsWith(image, "k8s.io/")
7     msg := sprintf("image '%v' comes from untrusted registry", [image])
8 }
9
10 deny[msg] {
11     some namespace, name
12     input.request.kind.kind == "Ingress"
13     newhost := input.request.object.spec.rules[_].host
14     oldhost := ingressess(namespace)[name].spec.rules[_].host
15     newhost == oldhost
16     input.request.object.metadata.namespace != namespace
17     input.request.object.metadata.name != name
18     msg := sprintf("ingress host conflicts with ingress %v/%v", [namespace, name])
19 }
20

```

INPUT

```

1 {
2     "apiVersion": "admission.k8s.io/v1beta1",
3     "kind": "AdmissionReview",
4     "request": {
5         "kind": {
6             "group": "",
7             "kind": "Pod",
8             "version": "v1"
9         },
10        "object": {
11            "metadata": {
12                "name": "myapp"
13            }
14        }
15    }
16 }

```

OUTPUT

```

Evaluated query in 64.822 µs.
1 {
2     "deny": [
3         "image 'nginx' comes from untrusted registry",
4         "image 'mysql' comes from untrusted registry"
5     ]
6 }

```

Built by styra

OPA v0.15.1-0.2019105162027-d1522c847504



DataOps

Agile + DevOps aplicado a la implementación de procesos y controles para data analytics.

Herramientas, procesos y cultura para acelerar la innovación facilitada por el creciente volumen de datos (180 Zettabytes para el 2025!)

MLOps

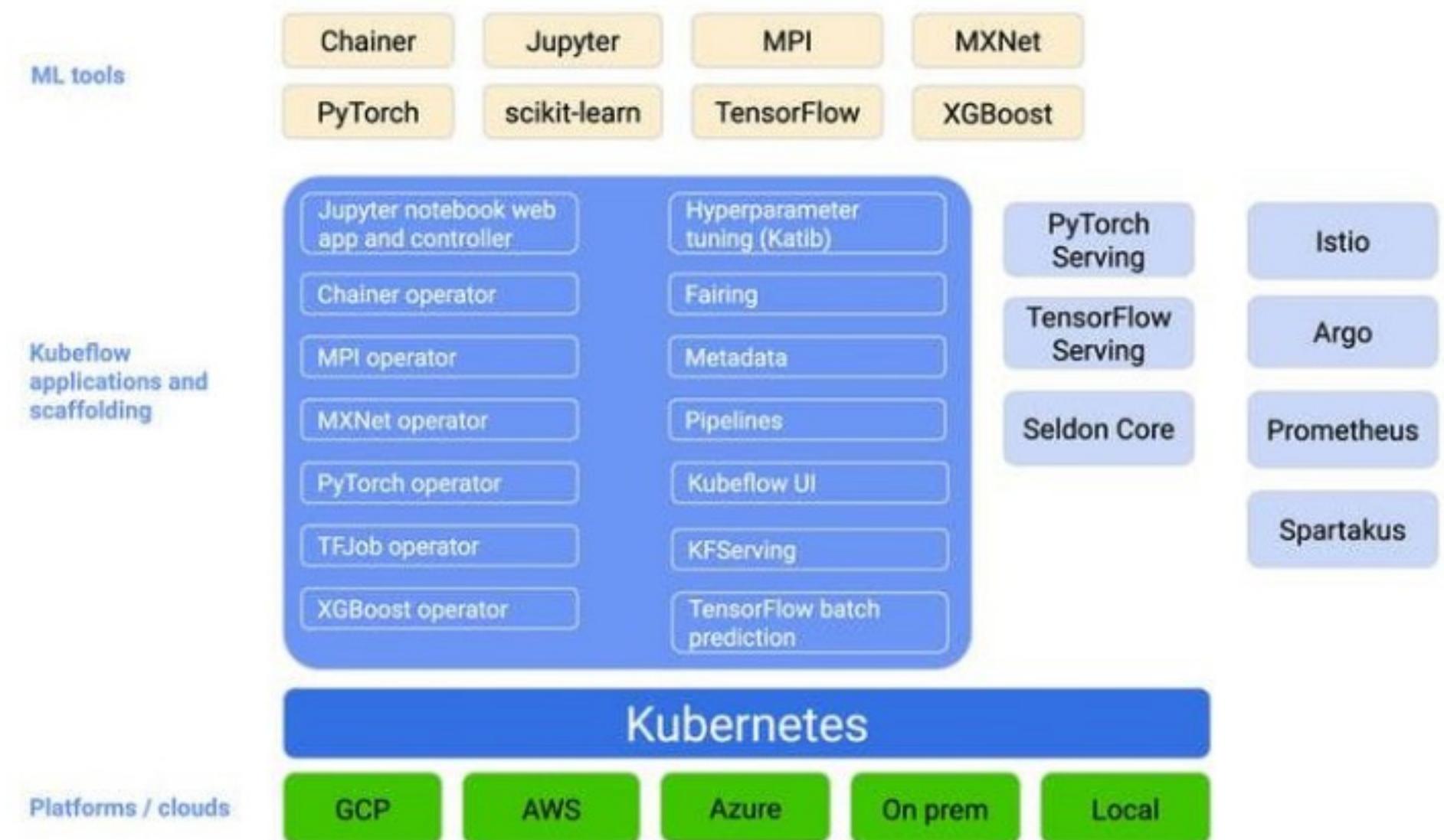
La filosofía y procesos de DevOps aplicados a llevar a producción modelos de machine learning.



Kubeflow

Un toolkit para la ejecucion de workflows para Machine Learning en un contexto nativo a Kubernetes.

Garantiza reproducibilidad y portabilidad de los complejos procesos que participan en el ciclo de vida de un modelo de Machine Learning, desde desarrollo, hasta entrenamiento e inferencia.



Homepage:

<https://www.kubeflow.org/>

Open Source:

<https://github.com/kubeflow/>

Documentation:

<https://www.kubeflow.org/docs/>

CNCF Status:

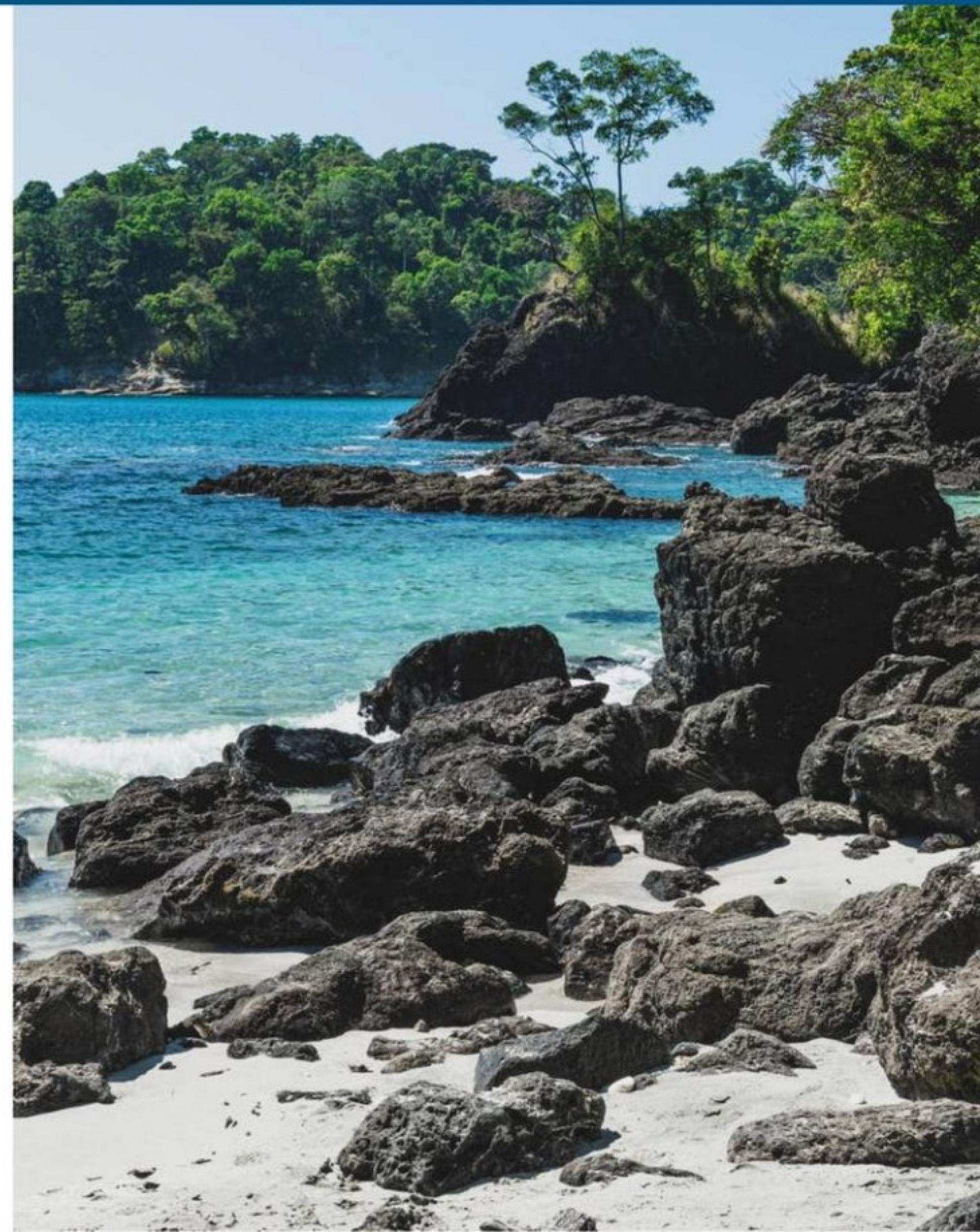
No es parte de CNCF

Service Mesh

Service Mesh

Abstracción que facilita la gestión de tráfico entre servicios, así como la seguridad, observabilidad y descubrimiento.

Facilitador de la implementación de arquitecturas multicloud y hybrid cloud.





Con un enfoque en ser de facil instalación, “security first” y súmamente liviano, Linkerd (v2) utiliza proxys transparentes para manejar todo el tráfico desde y hacia los servicios – al ser transparentes le permiten manipular el tráfico y brindar seguridad y telemetría sin impacto a la solución ni la introducción de latencia excesiva.

Incluye un UI para la gestión de la configuración y el tráfico. Permite la implementación simple de modelos de deployment progresivo y otros patrones avanzados.

A screenshot of the Linkerd UI interface. The top navigation bar has a green header with the Linkerd logo and the word "Namespaces". On the left, there's a sidebar with sections for "CLUSTER" (Namespaces selected, Control Plane), "DEFAULT" (dropdown), "WORKLOADS" (Daemon Sets, Deployments, Jobs, Pods), and a "Grafana" link. The main content area is titled "HTTP metrics" and shows a table of metrics for various namespaces. The table has columns for Namespace, Meshed, Success Rate, RPS, P50 Latency, P95 Latency, P99 Latency, and Grafana. The rows include default, kube-node-lease, kube-public, kube-system, and linkerd. The linkerd row shows values: 9/9, 100.00%, 6.7, 3 ms, 44 ms, 67 ms, and a yellow warning icon.

Homepage:

<https://linkerd.io/>

Open Source:

<https://github.com/linkerd/linkerd2>

Documentation:

<https://linkerd.io/2/overview/>

CNCF Status:

Incubating

GitOps y CI/CD



fluxcd / gitops-working-group

Mentimeter

Code Issues Pull requests Actions Projects Wiki Security Insights

Max 3 branches 0 tags

vistanprod Merge pull request #3 from todaynessesome/patch-1

ignore initial commit

CODE_OF_CONDUCT.md Add DCO, CoC, and Gov docs

DOCS Add DCO, CoC and Gov docs

GOVERNANCE.md Update GOVERNANCE.md

LICENSE Initial license

MATERIALS create materials file

README.md Fix up issue link

README.md

gitops-working-group

Announcing the GitOps Working Group

GitOps

Gestión declarativa del estado deseado de la infraestructura y la aplicación.

“Single source of truth”, todo versionado, todo en código, determinístico (declarativo, no imperativo)

GitOps Principles

To give participants in the cloud native ecosystem clarity on what GitOps means, and by extension to realize these benefits, the creators of this working group defined these five core GitOps Principles that are at the foundation of GitOps practices.

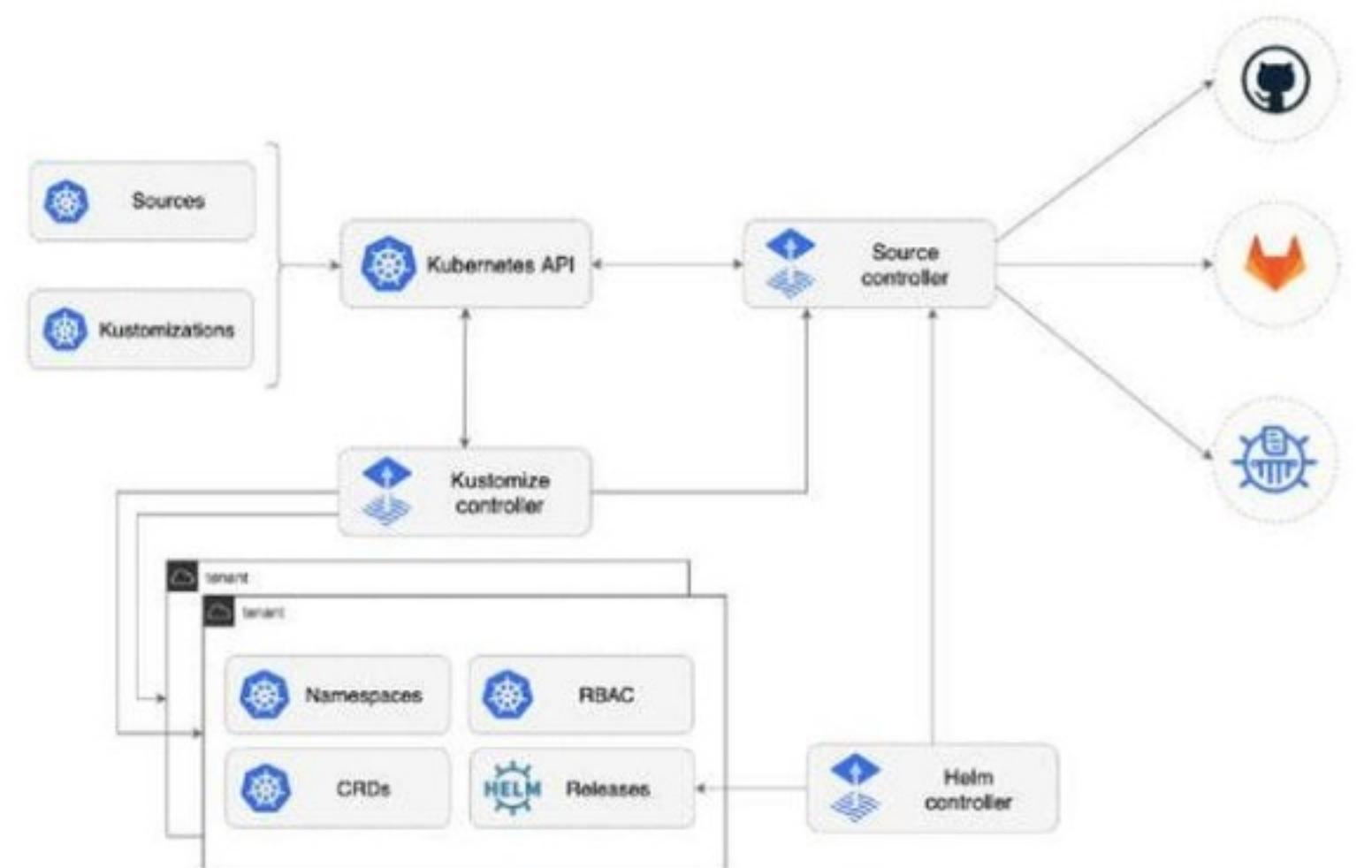
The Five GitOps Principles are as follows:

1. **Declarative Configuration:** All resources managed through a GitOps process must be completely expressed declaratively.
2. **Version controlled, immutable storage:** Declarative descriptions are stored in a repository that supports immutability, versioning and version history. For example, git.
3. **Automated delivery:** Delivery of the declarative descriptions, from the repository to runtime environment, is fully automated.
4. **Software Agents:** Reconcilers maintain system state and apply the resources described in the declarative configuration.
5. **Closed loop:** Actions are performed on divergence between the version controlled declarative configuration and the actual state of the target system.



Una herramienta para mantener Kubernetes clusters en sync con un estado deseado, almacenado declarativamente en un repositorio con control de versiones (ej. Git)

Utiliza operadores y custom resources para “deploy”, y es parte del GitOps Toolkit



Homepage:

<https://fluxcd.io/>

Open Source:

<https://github.com/fluxcd/flux2>

Documentation:

<https://toolkit.fluxcd.io/>

CNCF Status:
Sandbox



keptn

Homepage:

<https://keptn.sh/>

Open Source:

<https://github.com/keptn/keptn>

Documentation:

<https://keptn.sh/docs/>

CNCF Status:

Sandbox

Control plane para continuous delivery basada en eventos y operaciones automatizadas para aplicaciones nativas para la nube.

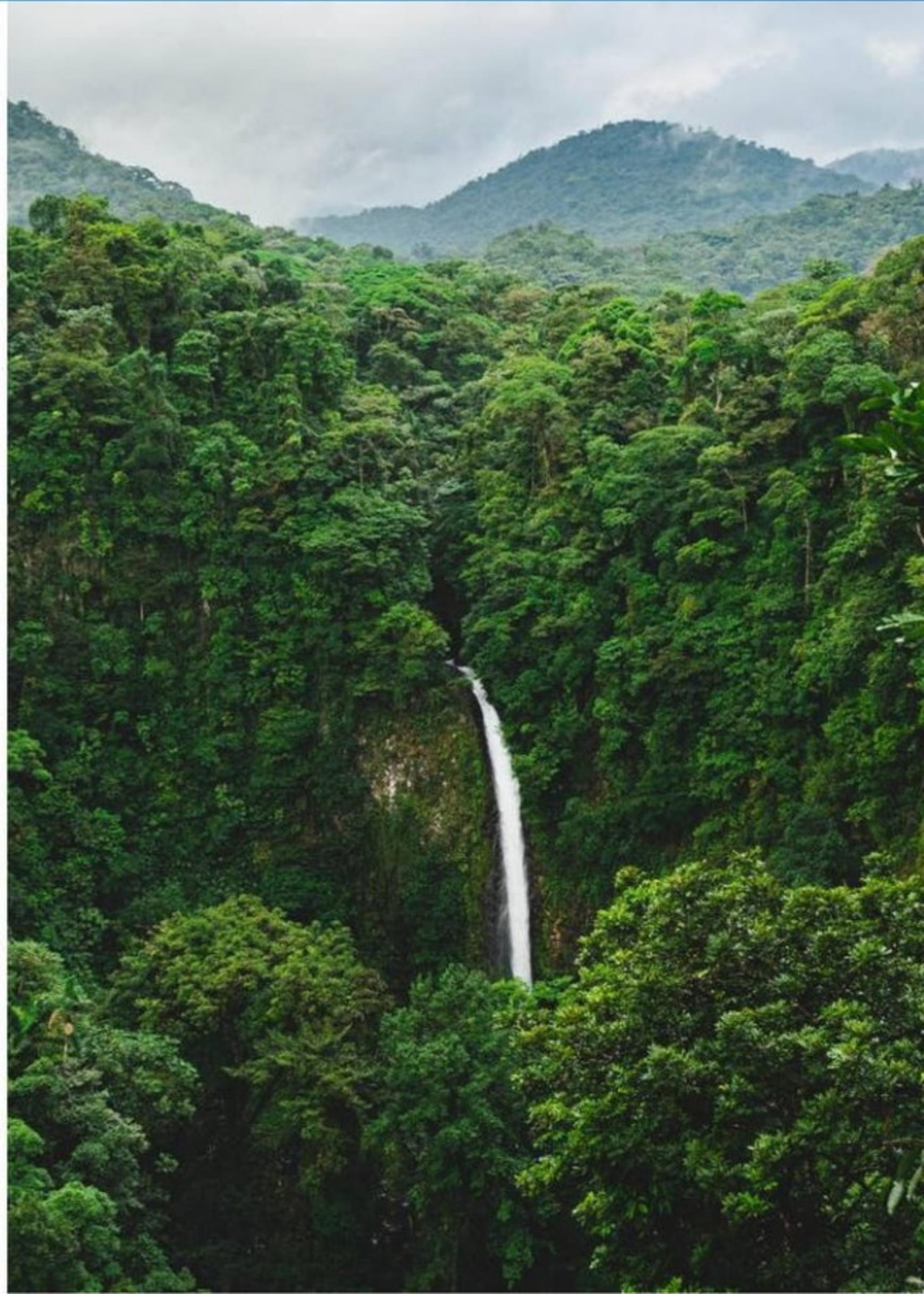
Plataforma súmamente flexible, nativa para Kubernetes, con soporte para progressive delivery usando quality gates, verificación continua de rendimiento, gestión de deployment automatizado multi-stage, automatización de operaciones y otros muchos casos de uso.

Infrastructure as Code -> Infrastructure as Software

Programando infraestructura para la nube

Gestión de infraestructura usando lenguajes conocidos e integrado de manera directa al SDLC del producto.

Enfoque en static analysis y seguridad del código de infraestructura





Creación, despliegue y gestión de infraestructura en cualquier nube, usando lenguajes de programación y herramientas existentes.

Reduce las barreras entre Ops y Development.

Gestiona secretos, y funciona tanto con nubes públicas como con Kubernetes.

Incorpora herramientas de auditoria y “Policy as Code”

Downside: Community edition no va más allá que para Desarrollo individual.

Homepage:

<https://www.pulumi.com/>

Open Source:

<https://github.com/pulumi>

Documentation:

<https://www.pulumi.com/docs/>

CNCF Status:

No es parte de CNCF

checkov

by bridgecrew

Homepage:

<https://www.checkov.io/>

Open Source:

<https://github.com/bridgecrewio/checkov>

Documentation:

<https://www.checkov.io/documentation.html>

CNCF Status:

No es parte de CNCF

Herramienta para static analysis de Infrastructure as Code con soporte para muchos frameworks, incluyendo:

Terraform

Cloudformation

Kubernetes

Arm

Serverless

Detecta errores de configuración usando policies escritas usando python – incluye muchos policies listos para usar.

¿De los temas que vimos, cuales son los tres que más te interesarian para un futuro workshop?

A word cloud visualization showing the popularity of various DevOps and infrastructure topics. The words are arranged in a cluster, with their sizes and colors representing the number of votes they received.

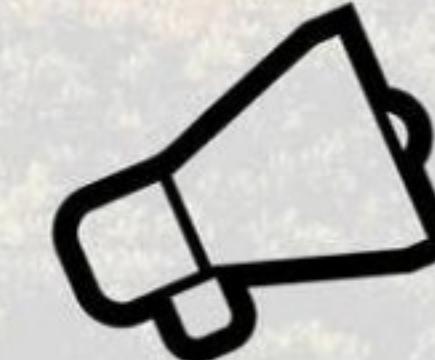
- service mesh (red)
- gitops (blue)
- devsecops (pink)
- infrastructure as software (yellow)
- infrastructure as code (blue)
- kubernetes (pink)
- cicd (purple)
- pulumi (green)
- kustomize (orange)
- k8s 4 the edge (orange)
- k3 microk8 (orange)
- ci cd (light blue)
- dataops (green)
- devsecoos (red)
- iac (orange)

¿Y ahora qué?



Participen en
Slack

Compartan el
Meetup!



Apúntense en
eventos y reuniones



Y traigan a alguien 😊