



DevSecOps

¿Qué es DevSecOps?
¿Por qué es tan importante?
y
¿Cómo protegerse?



Karen Mena - Palo Alto Networks

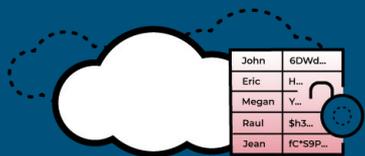
Solutions Architect - Prisma Cloud

<https://www.linkedin.com/in/karen-mena-4ba38810b/>

klugo@paloaltonetworks.com



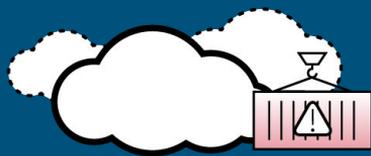
El riesgo se presenta en entornos y aplicaciones en la nube



Riesgos de Cumplimiento

43%

de las bases de datos en la nube no están cifradas



Vulnerabilidades en contenedores

91%

de las imágenes contienen al menos una vulnerabilidad crítica o de alta gravedad



Redes Inseguras

60%

de las organizaciones a nivel mundial tienen configuraciones de red inseguras



Credenciales IAM Inseguras

66%

de las organizaciones en todo el mundo utilizan claves de acceso durante más de 90 días

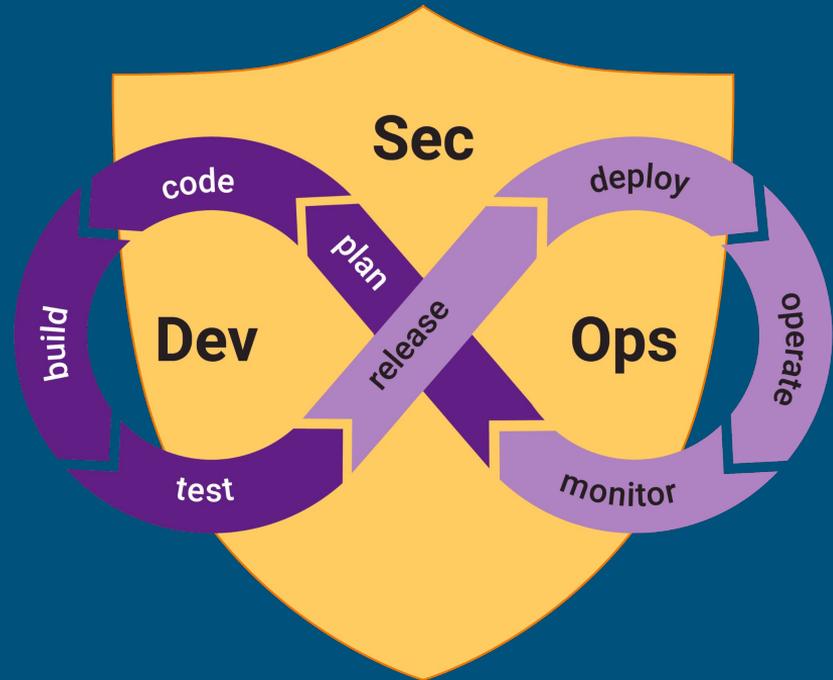
Pero ¿Qué es exactamente DevSecOps?

DevSecOps significa Desarrollo, Seguridad y Operaciones.

Se trata de implementar la seguridad desde la fase inicial del desarrollo de la aplicación hasta la entrega del producto final.

¿Como Funciona?

1. **Code.** En el primer paso, un desarrollador crea un código en el sistema de gestión de control de versiones, todos los cambios se ven y se hacen en el mismo sistema.
2. **Code Analysis.** Después, otro desarrollador toma el código del mismo sistema, lo analiza e identifica los errores o brechas de seguridad en el código.
3. **Build.** Una vez que el desarrollador rectifica el error, se compila el código.
4. **Test.** En el siguiente paso se llevan a cabo pruebas de seguridad, interfaz de usuario, integración y API.
5. **Release y Deploy.** Una vez que la aplicación supera estas pruebas, es apta para el paso a producción, se crea el artefacto y se coloca en el entorno correspondiente.
6. **Monitor.** Una vez ya desplegada la aplicación, se realiza una supervisión continua para identificar y rectificar las amenazas a la seguridad.

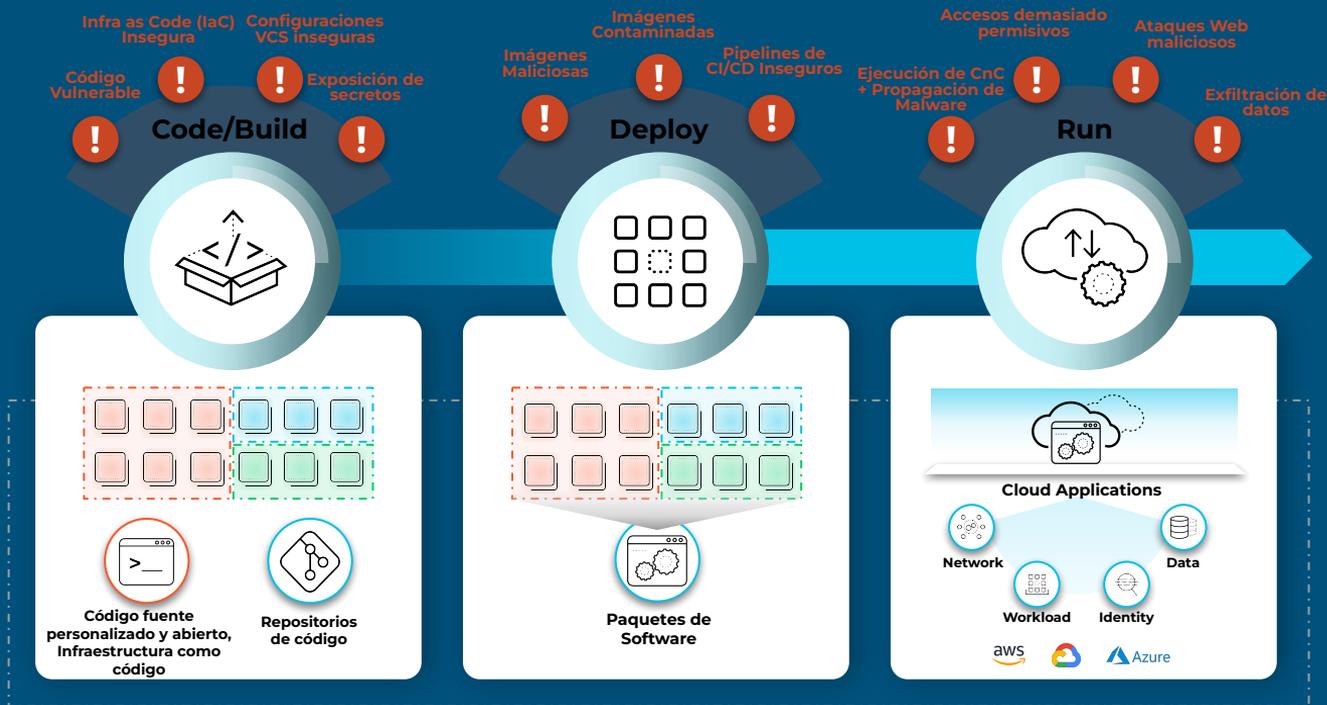


¿Cual es su objetivo?

- Garantizar que se detecten todas brechas de seguridad y se reduzcan las vulnerabilidades.
- Durante el proceso todo mundo es responsable de la seguridad, desde el desarrollador hasta el departamento de operaciones.
- DevSecOps garantiza la seguridad en cada nivel del desarrollo.

¿Por qué es tan importante?

Las aplicaciones en la nube están sujetas a varios riesgos y vulnerabilidades en cada etapa del ciclo de vida del desarrollo, desde el código hasta el tiempo de ejecución (runtime).



Buenas prácticas en DevSecOps

1. Codificación segura y protegida
2. Implementar Automatización
3. Implementar Seguridad desde el principio
4. ShiftLeft:

"Desplazamiento a la izquierda" que es mover la seguridad al punto más temprano posible en el Pipeline de DevOps:

- Escaneo de Vulnerabilidades en herramientas de CI, IDE y SCM
- Checks de Seguridad dentro de los flujos de CD
- Visibilidad, cumplimiento y protección en runtime

¿Cómo podemos protegernos?

PRISMA CLOUD nos ayuda a...

- Identificar y prevenir las vulnerabilidades en todo el ciclo de vida de las aplicaciones.
- Integrar la gestión de vulnerabilidades en cualquier proceso de CI, mientras monitorea, identifica y previene continuamente los riesgos para todos los hosts, imágenes y funciones del entorno.

Prisma Cloud combina la detección de vulnerabilidades con un feed de amenazas .

The screenshot shows the Jenkins 'Image Vulnerabilities' page for the 'Incident-Lateral-Movement-Image' project. It displays a total of 13 vulnerabilities. A table lists vulnerabilities with columns for Image, Image ID, Type, Severity, CVSS, CVE, Package Name, and Package Version. Two vulnerabilities are shown: one with a severity of 'Critical' (CVSS 9.8, CVE-2022-22965) and another with a severity of 'High' (CVSS 7.5, CVE-2025-28831). A detailed view of the 'critical' CVE-2022-22965 is shown below, including its description and affected versions.

Image	Image ID	Type	Severity	CVSS	CVE	Package Name	Package Version
it_demo/incident-lateral-movement...	sha256:1e192co...	Product	Critical	9.8	CVE-2022-28391	busybox	1.32.0
it_demo/incident-lateral-movement...	sha256:1e192co...	Product	High	7.5	CVE-2025-28831	busybox	1.32.0

Severity	Package	CVE	Fix Status	Grace period	Risk factors	Description	Tags
critical	spring-beans_sp...	CVE-2022-22965	Fixed In: 5.2.20, 5.3.18	16 days ago		Impacted versions: <5.2.20 Discovered: 18 days ago Published: 18 days ago A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application	Add Tags to CVE

Hosts	Image	Severity	CVSS	Count	Score
3 hosts	eks-demo-karen, ridiculous-s...	Critical	9.8	2 28 47 41	10
master-selfhosted-pphonpas...	phimm-demo-cluster	Critical	9.8	98 633 180 37	11
node-selfhosted-pphonpas...	phimm-demo-cluster	Critical	9.8	106 66 91 37	11
3 hosts	eks-demo-karen, ridiculous-s...	High	7.5	1 21 40 37	10
3 hosts	eks-demo-karen, ridiculous-s...	High	7.5	19 34 35	10
3 hosts	eks-demo-karen, ridiculous-s...	High	7.5	19 34 35	10



DEMO

¡EN ACCIÓN!

