1° Estudio del estado del arte de DevSecOps en Latinoamérica

2020

Una iniciativa de:

DEVSECOPS Latinoamérica

COORDINADORES:

- Luciano Moreira
- Christian Ibiri

ANALISTAS:

- Julio Balderrama
- Leonardo Rosso
- Ruben Aybar
- Walter Darda
- Santiago Fernandez
- Eric Balderrama
- Elvin Mollinedo
- Luis Araujo
- Alessandra Martins
- Guto Carvalho
- Carlos Allendes
- Jaime Restrepo
- Jhon Edison Sánchez
- Michael Hidalgo
- Ramiro Pulgar
- Daniel Suarez
- Daniel Monzon
- Raúl Medina
- Ronen Riesenfeld
- Rubén Cárdenas Saavedra
- Erick Delgadillo
- Davis Porras
- Diego González Arango
- Hubert Demercado
- José Moreno
- Marcelo Galvan
- Diego García
- Nicolas Valcarcel
- John vargas
- Saira Isaac
- Mateo Martinez
- Luis Alejandro Martinez
- Mary Cruz Rosas

¿Que veremos?

- Resumen ejecutivo
- Objetivos y Ámbito del Estudio
- ¿Quién participó?
- Madurez DevOps
- Motivaciones, Cultura e interés
- Practicas y tools
- Open Source Governance
- Brechas, respuestas y registros
- Desafíos principales

Imágenes creadas por dooder

Resumen Ejecutivo

Imágenes creadas por dooder

Resumen Ejecutivo

Bienvenidos a nuestro 1° Estudio del estado del arte de DevSecOps en Latinoamérica, representa la voz de 1.264 profesionales de las tecnologías de la información, en 20 países de habla hispana y portuguesa de la industria de Latinoamérica.

La encuesta nos evidencia que las prácticas de DevOps están madurando rápidamente, pero que la seguridad no se está automatizando en una fase temprana del ciclo de vida del desarrollo y que la seguridad en las cadenas de suministro de Software todavía no es tomado como un diferenciador crítico.

Al mismo tiempo que las prácticas de DevSecOps están fomentando las prácticas de codificación segura y la mejora de la higiene de la ciberseguridad, seguimos siendo testigos de un creciente volumen de infracciones que afectan a la confianza de los clientes y reflejan los avances de nuestros adversarios.

Si bien algunos resultados de nuestra encuesta pueden sorprenderle, esperamos que también le animen a iniciar nuevas conversaciones con sus compañeros y en toda su industria. Compartir estos resultados puede ayudar a motivarnos a todos a madurar aún más las prácticas de DevSecOps en todas partes y a establecer nuevos puntos de referencia para la velocidad, la calidad y la seguridad.

Gracias a todos los que participaron en la encuesta y a nuestros Squads lideres de cada país que forman parte de la comunidad DevSecOps Latinoamérica por ayudarnos a construir la encuesta y promoverla.

Luciano Moreira y Christian Ibiri
Co-Fundadores & Tribe leader DevSecOps Latinoamérica

DEVSECOPS
Latinoamérica

Objetivos Y Ámbitos de Estudio

Imágenes creadas por dooder

Objetivos y Ámbitos de Estudio

El objetivo de la presente estudio fue abrir la serie para explorar y conocer el Estado del Arte de DevSecOps en la región de Latinoamérica, tiene como objetivo investigar para conocer la adopción de las practicas de DevSecOps, y el papel que juega este cambio cultural en la seguridad de las organizaciones, desde el punto de vista académico y sumando todos los roles involucrados desde la necesidad del cliente hasta la puesta en producción.

Este análisis se realizo tanto para la situación existente a la realización del mismo, como desde un punto de vista histórico para futuros estudios. En base a todo ello, el presente estudio combina varios ejes de análisis de los datos recopilados de las personas e industrias.

Esta es la primer encuesta de este tipo realizada en la región, centrada en el desarrollo de aplicaciones y prácticas de seguridad que ahora llamamos DevSecOps. Los resultados reportados en la encuesta vinieron en respuesta a 35 preguntas hechas por DevSecOps Latinoamérica .

La encuesta en línea se llevó a cabo entre el 20 de junio y el 18 de julio del 2020.

Objetivos y Ámbitos de Estudio

Los datos reunidos en la encuesta de la comunidad de DevSecOps proporcionan resultados estadísticamente representativos sobre la adopción, las prácticas y los desafíos de la gestión de las prácticas de DevOps en lo que respecta a los requisitos de seguridad.

Para este primer interacción, 1264 profesionales de la tecnología de la información respondieron a la encuesta y (98%) completaron en su totalidad.

En algunos casos en los que buscábamos el conocimiento definitivo de los participantes, optamos por no incluir respuestas de "no lo sé" o "no estoy seguro" en los resultados finales, con el fin de establecer las tendencias históricas.

Todavía es muy temprano para definir el margen de error de la encuesta y definir puntos porcentuales para el muestreo de 1264 profesionales de la TI. Pero con el pasar de los años y nuevas interacciones ampliando la cobertura de muestra, tenemos un objetivo de confianza del 97%.

En total, participaron profesionales de la tecnología de la información de más de 18 países.

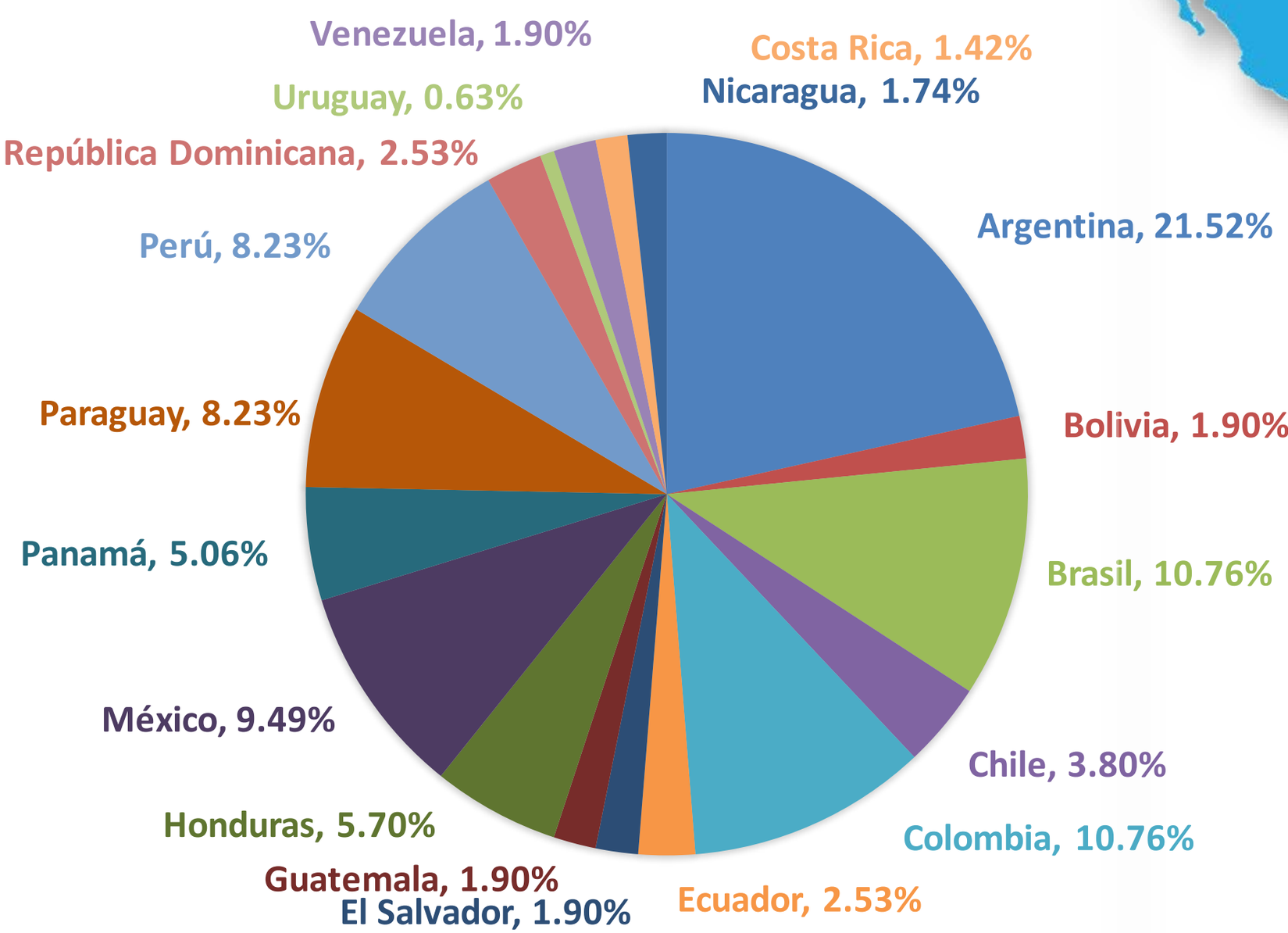
¿Quién participó?

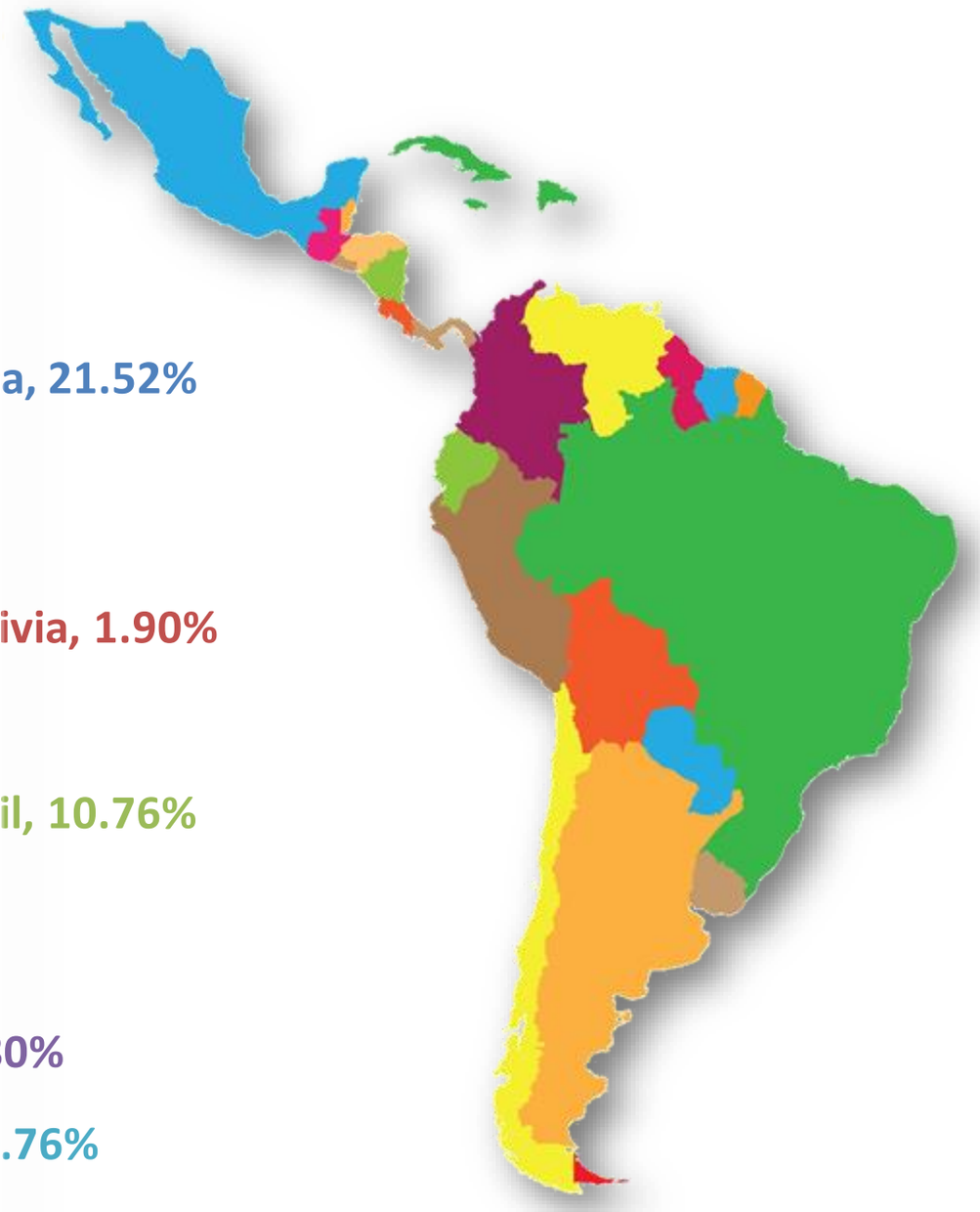
Imágenes creadas por dooder

Respuestas totales

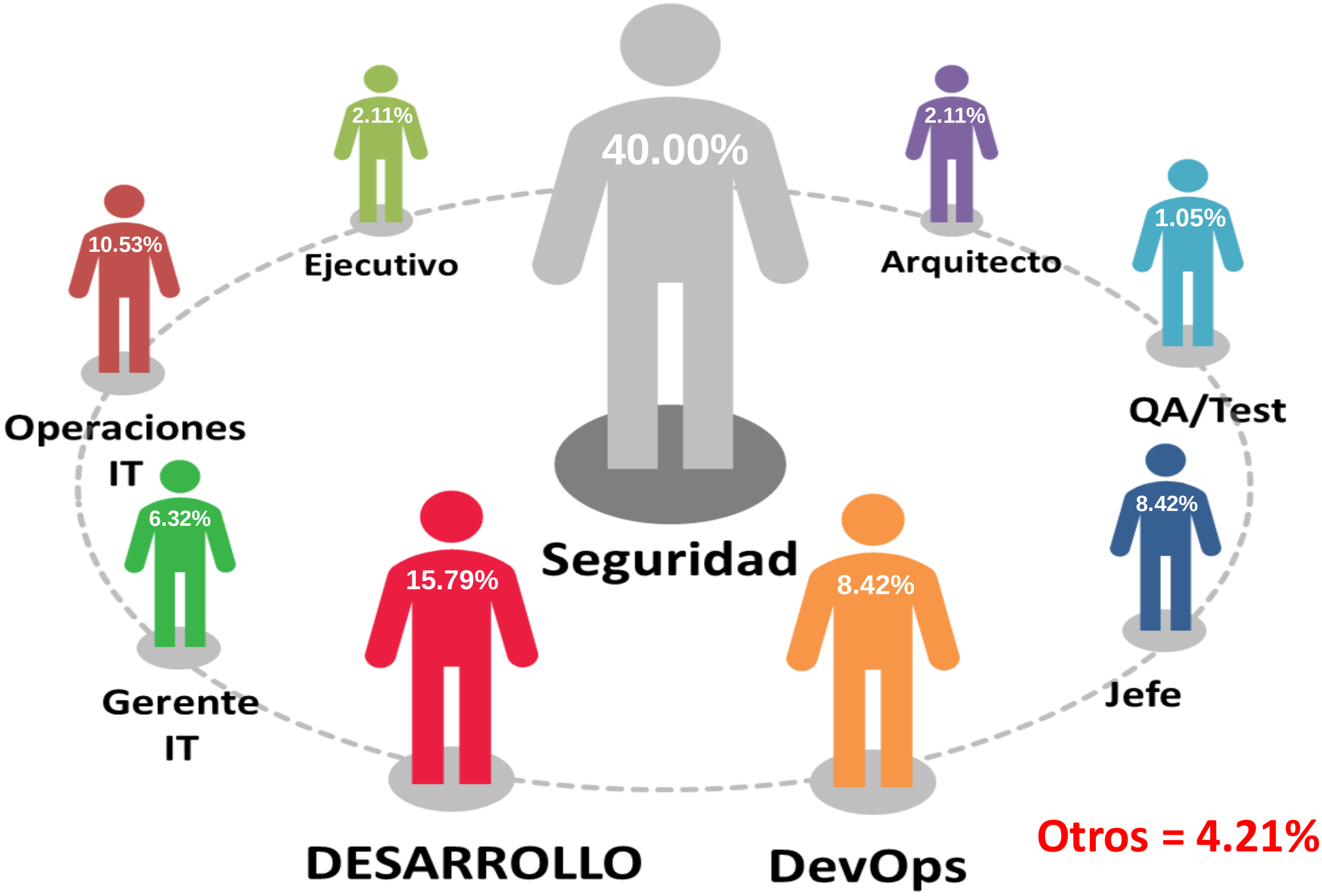
1264 **Personas de 18 países compartieron su punto de vista**

% de respuestas por país





¿Que título coincide mejor con su rol dentro de su organización?



% de Diversidad

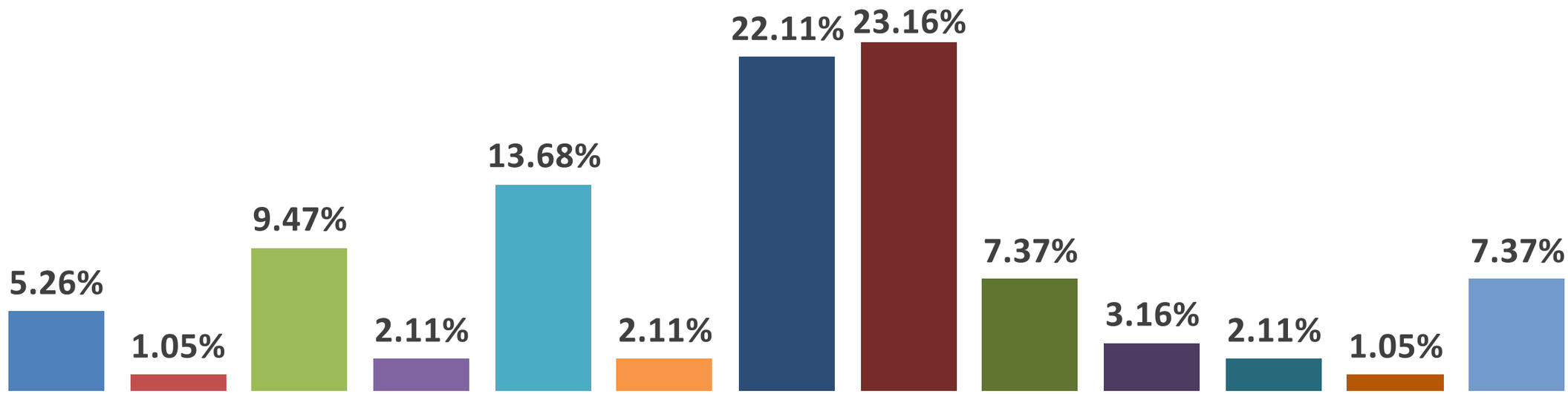
69% Hombres

31% Mujeres

Las nuevas generaciones de mujeres en IT nos evidencian estar cada día mas presentes y esta encuesta no es la excepción. Para nosotros este indicador (% de diversidad), si bien no hace parte de las preguntas de la encuesta, año tras año va ser muy importante para tener una grafica evolutiva en lo que respecta a diversidad e inclusión.

Imágenes creadas por dooder

¿En qué industria está su organización?

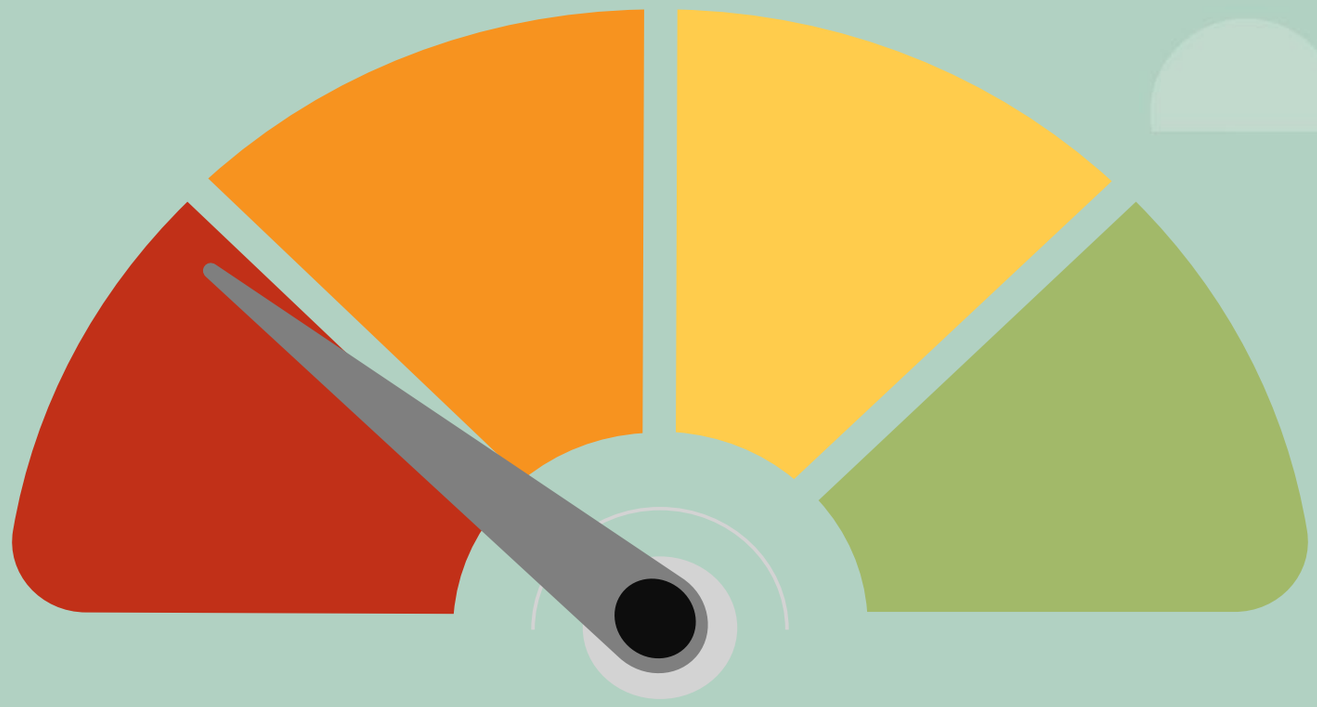


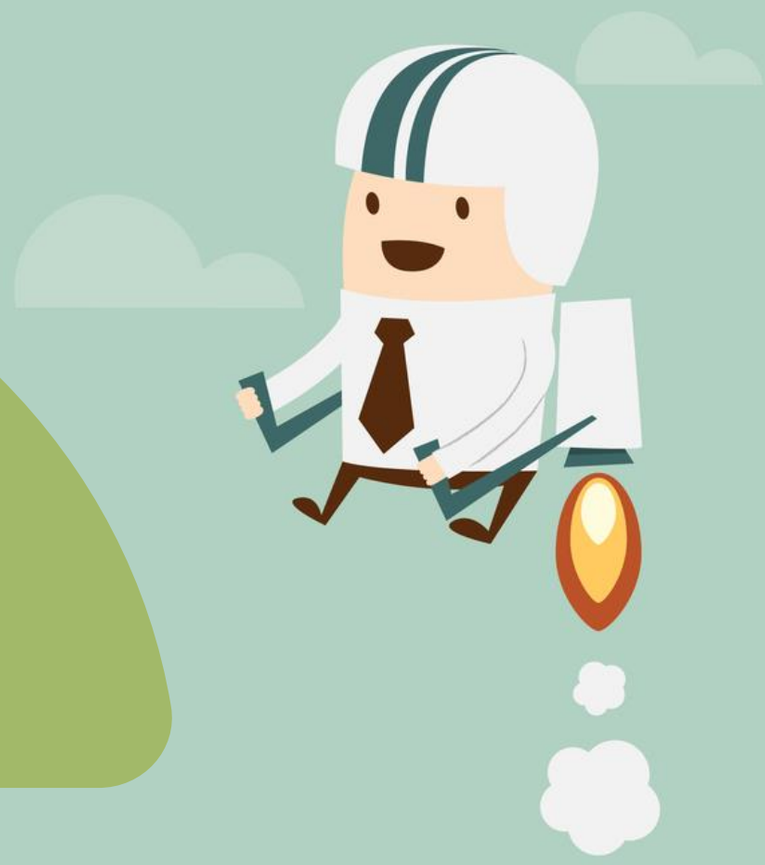
- Medios de comunicación y telecomunicaciones
- Entretenimiento
- Servicios de consultoría
- Venta al por menor
- Gobierno
- Salud
- Banca y Finanzas
- Servicios de Tecnología
- Recursos naturales (Oil & Gas etc..)
- Educación
- Seguros
- Manufactura
- Otro

Madurez DevOps

Imágenes creadas por dooder

¿Qué tan madura es la adopción de prácticas de DevOps en su organización?





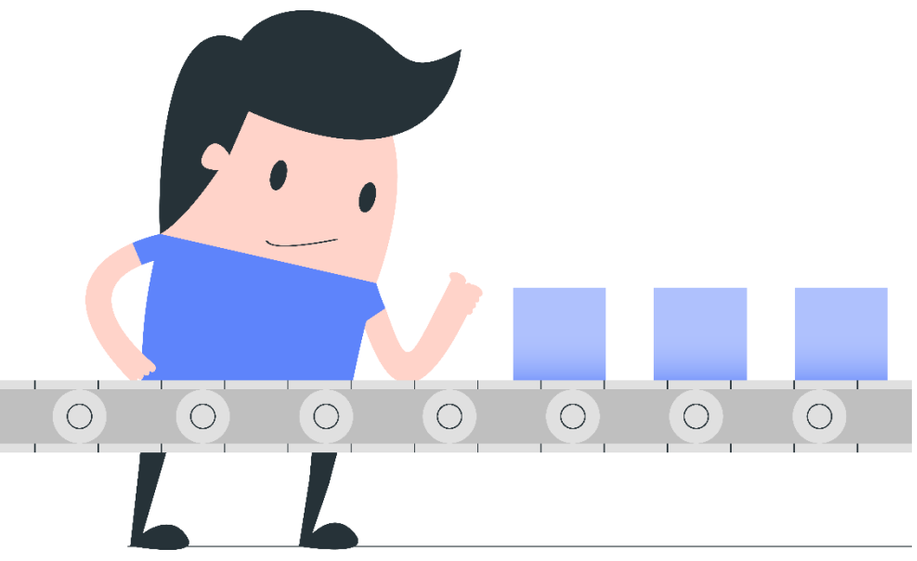
Maduro	18.95%
Improvisado	37.89%
Inmaduro	43.16%

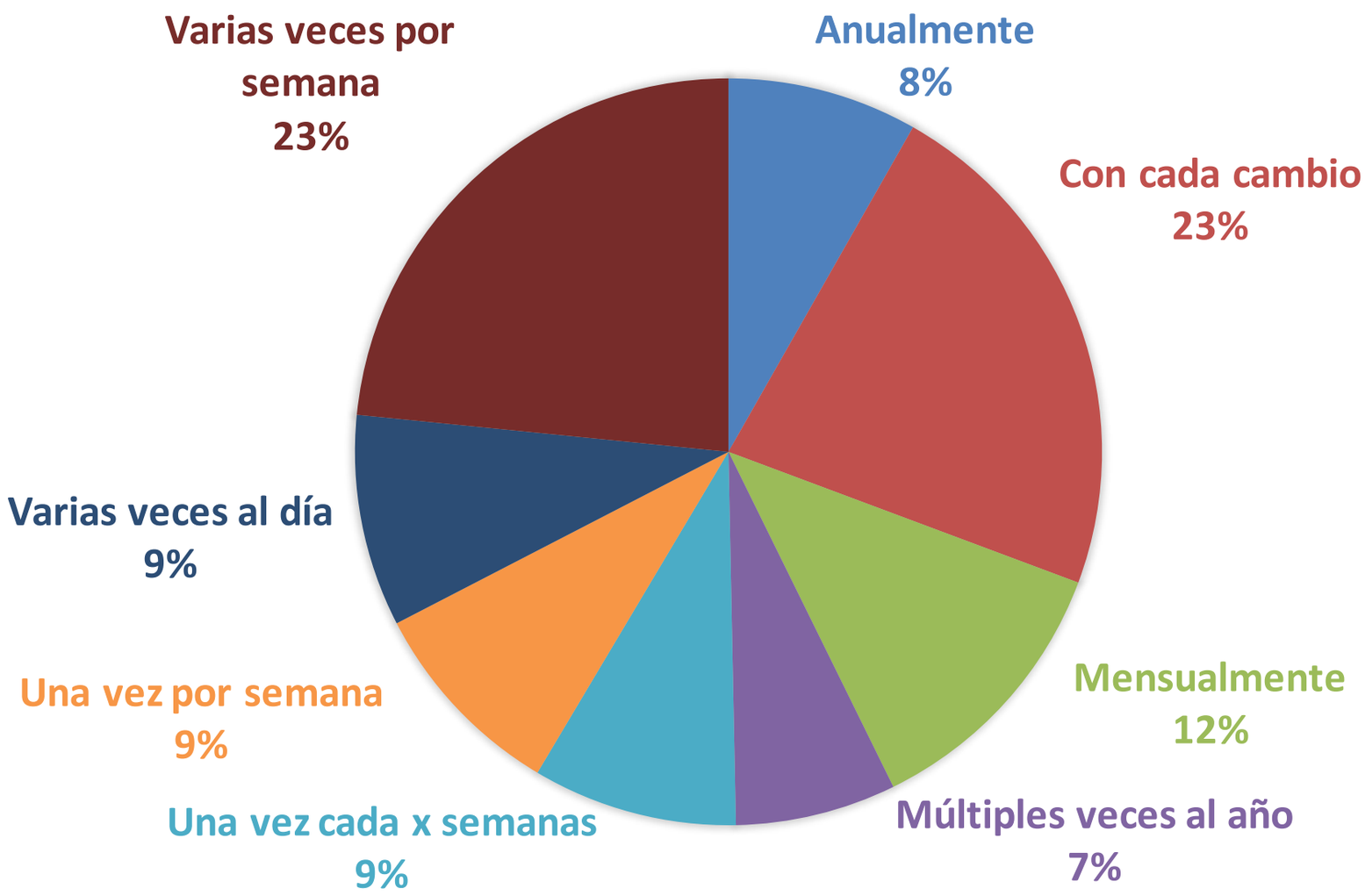
Una de las preguntas clave que vamos a realizar cada año es sobre el nivel de madurez de DevOps de una organización y la percepción del encuestado.

Imágenes creadas por dooder

¿Con qué frecuencia hacen Deploy en producción?

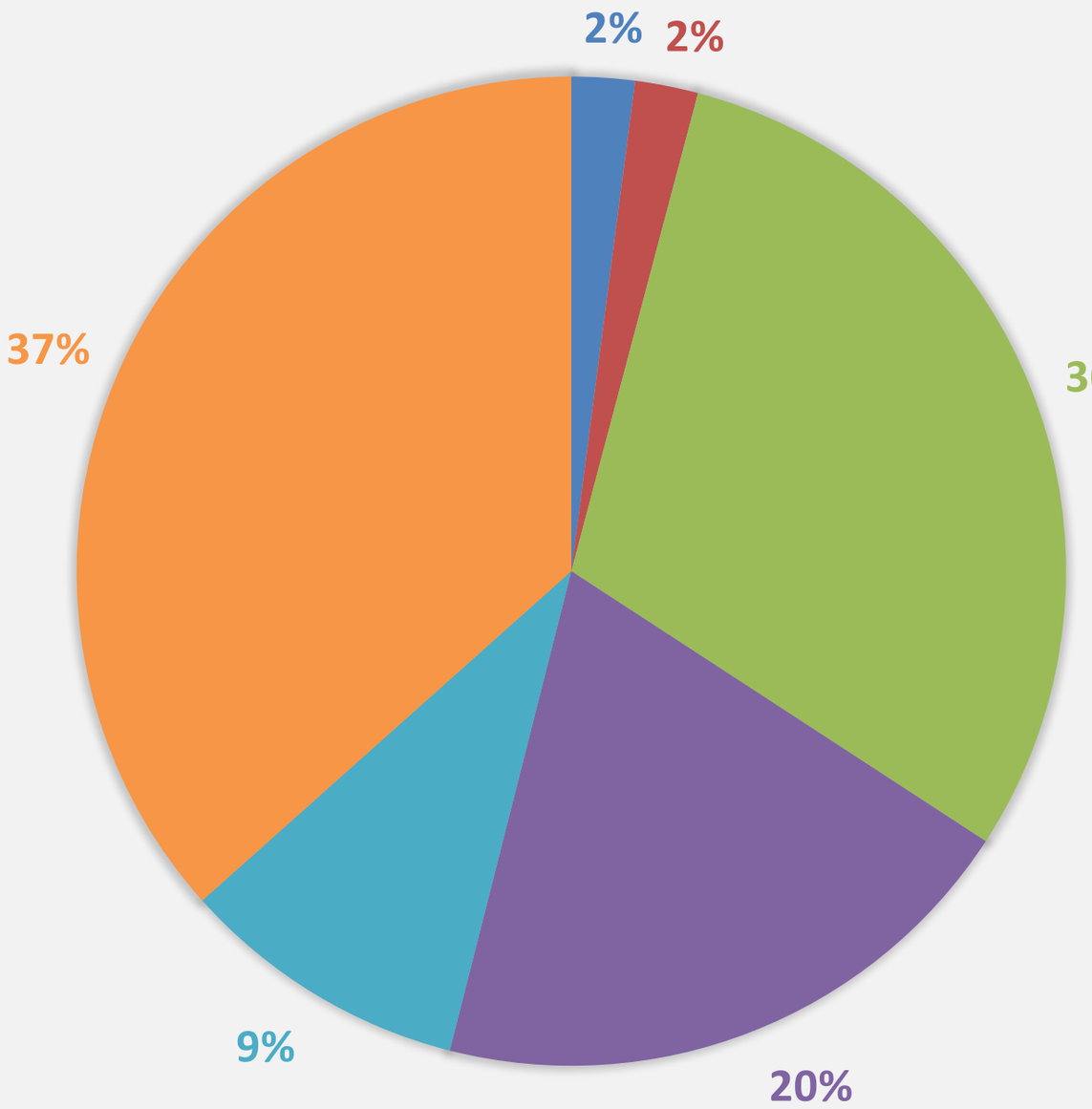
+64% de los encuestados despliegan como mínimo una vez por semana





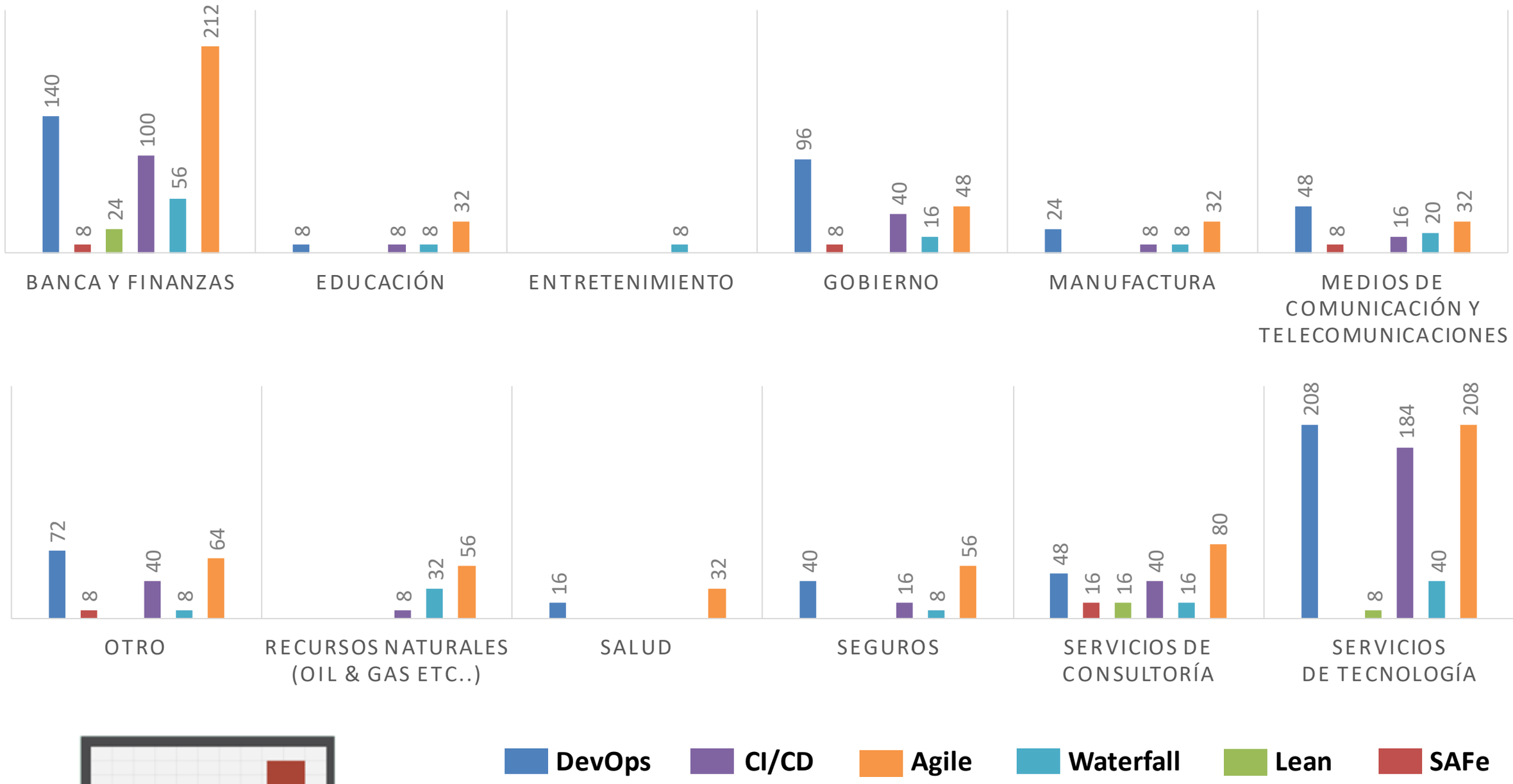
“La seguridad es súper importante para las demandas del negocio, pero si tomamos un enfoque de seguridad tradicional la velocidad de desarrollo se ve severamente frenada. Necesitamos estar seguros pero movernos rápido".

¿Qué tipo de prácticas de desarrollo/implementación se utilizan en su empresa?



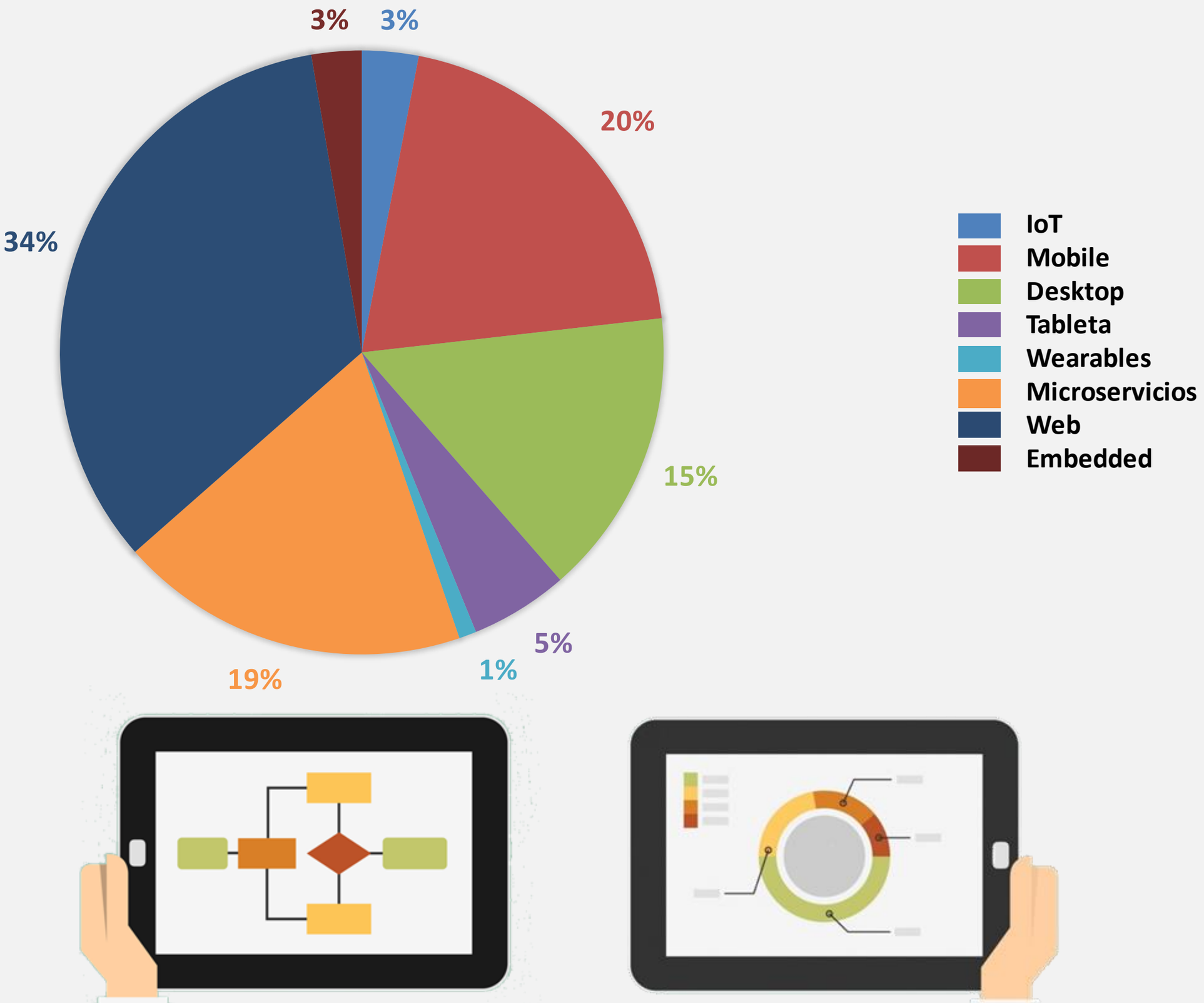
DevOps CI/CD Agile Waterfall Lean SAFe

¿Qué tipo de prácticas de desarrollo/implementación se utilizan en su empresa?



Doble clic: DevOps muestra fuerte adopción en la Banca, Gobierno, comunicaciones y servicios de tecnología.

¿Qué tipo de aplicaciones crean en su empresa?

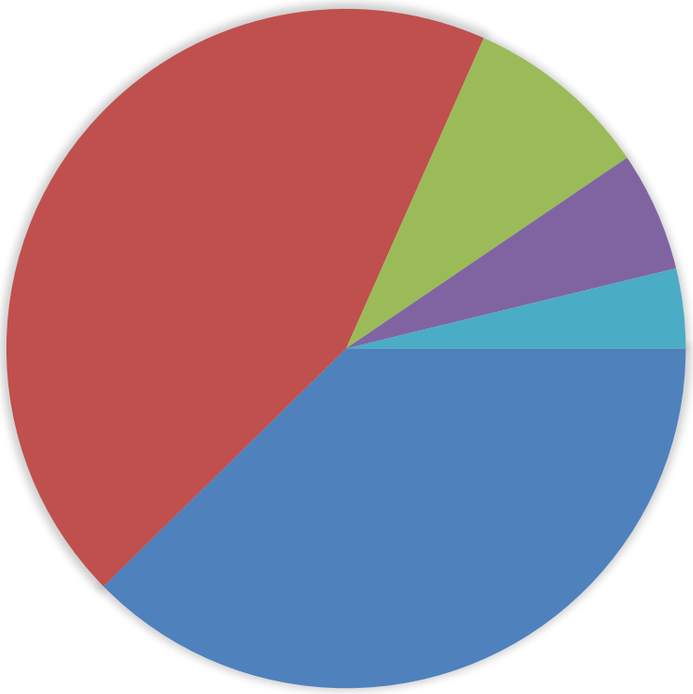


Motivaciones e Interés

Imágenes creadas por dooder

¿Cuál es su principal motivación para implementar seguridad a lo largo del ciclo de vida del desarrollo?

Mejorar la calidad del código / aplicación
44%



Requisitos de cumplimiento
9%

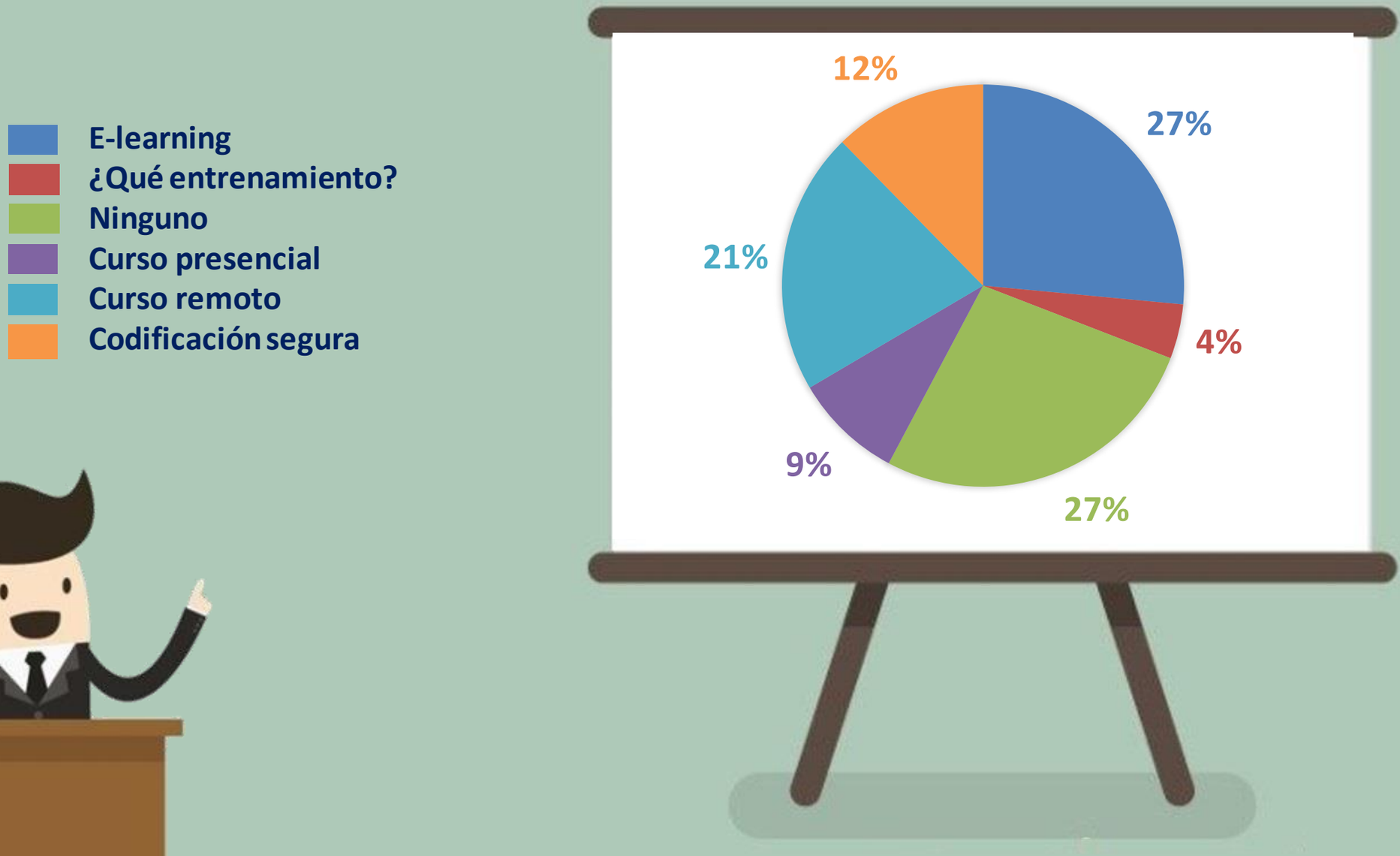
Requisitos del cliente
6%

Ventaja competitiva
4%

Gestión de riesgos
37%

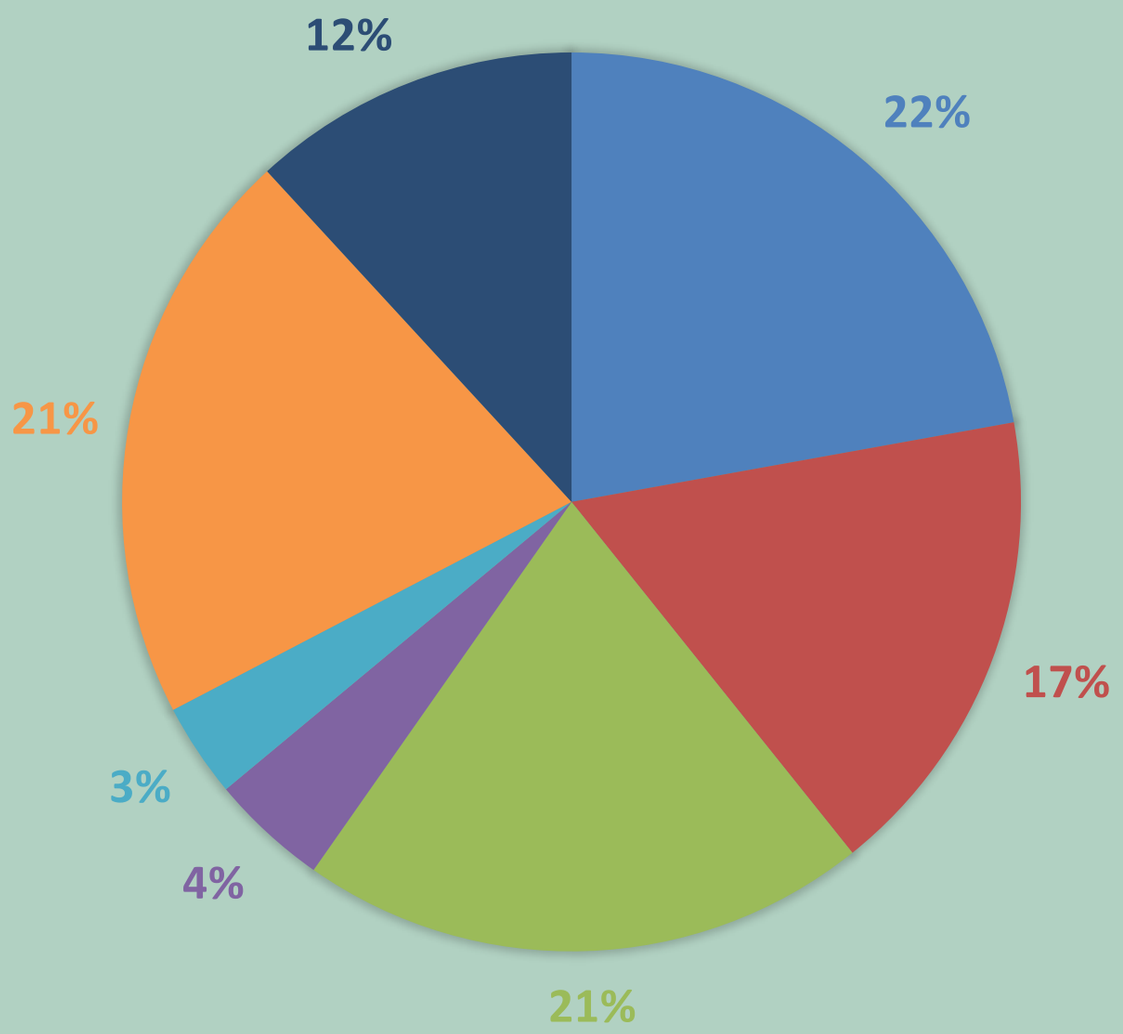
Casi la mitad de los encuestados cree que "seguridad" es sinónimo de "calidad"...

¿Qué capacitación en seguridad de aplicaciones está disponible para usted en su entorno de trabajo?



El 31% y principalmente la práctica Waterfall no recibieron ninguna formación en materia de seguridad.

¿Cómo se le informa de los problemas de InfoSec y AppSec?



- Herramientas internas
- Los clientes nos informan de los problemas
- Correo electrónico/chat
- Integración IDE
- Gerente/Jefe
- Equipo de seguridad
- Transmisión de correo electrónico

**“Las prácticas maduras son 4 veces menos propensas a depender de rumores cuando se trata de incidentes de seguridad.
En su lugar, se centran en la evidencia empírica de herramientas y equipos de seguridad mejor integrados.”**

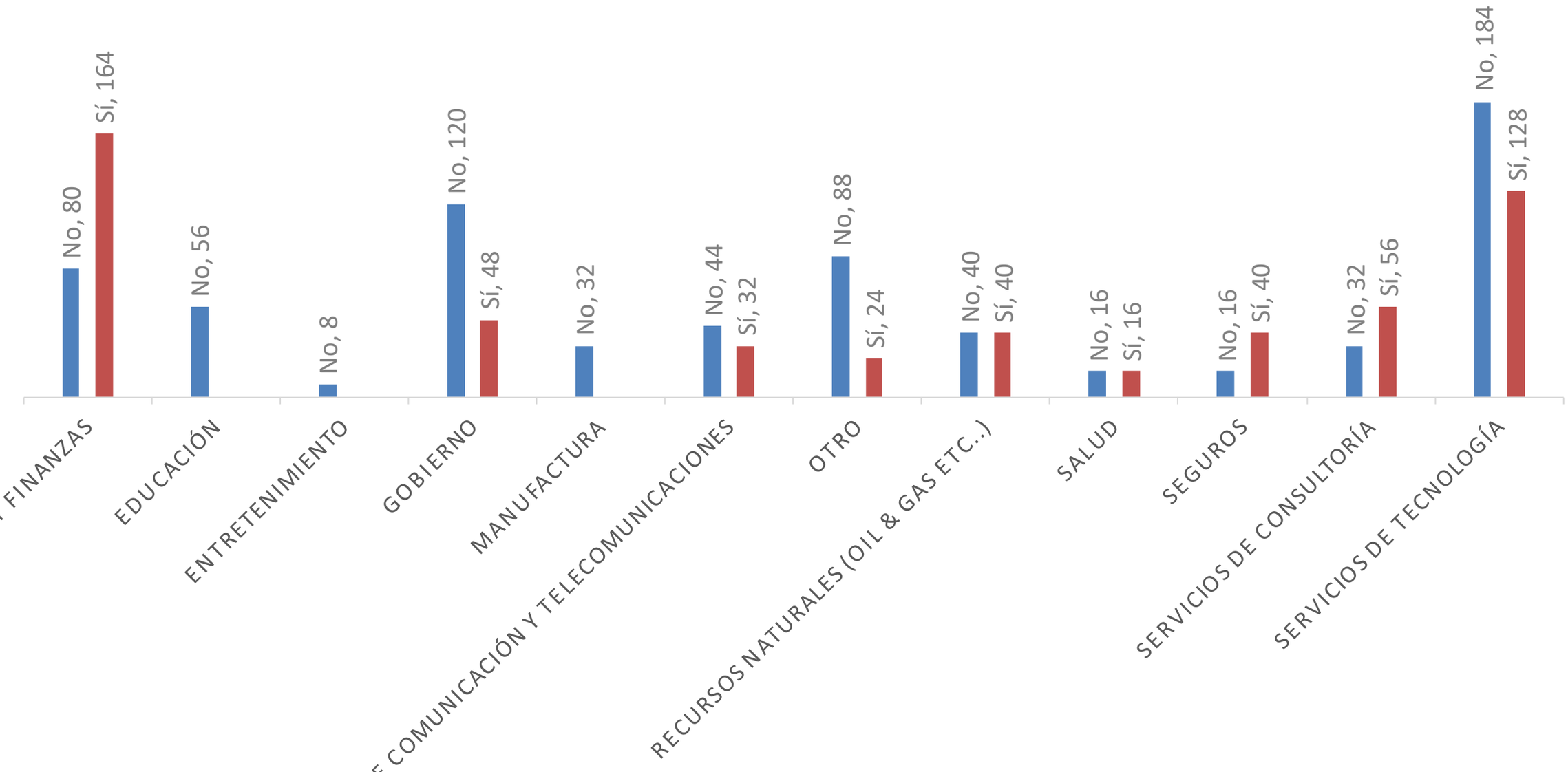
Imágenes creadas por dooder

¿Su empresa tiene un programa de seguridad en aplicaciones?

No importa cuán rápido sea la velocidad de una organización en desplegar con DevOps, si lo que producen no contempla la confidencialidad, integridad y disponibilidad entonces han fallado en entregar un producto de calidad.

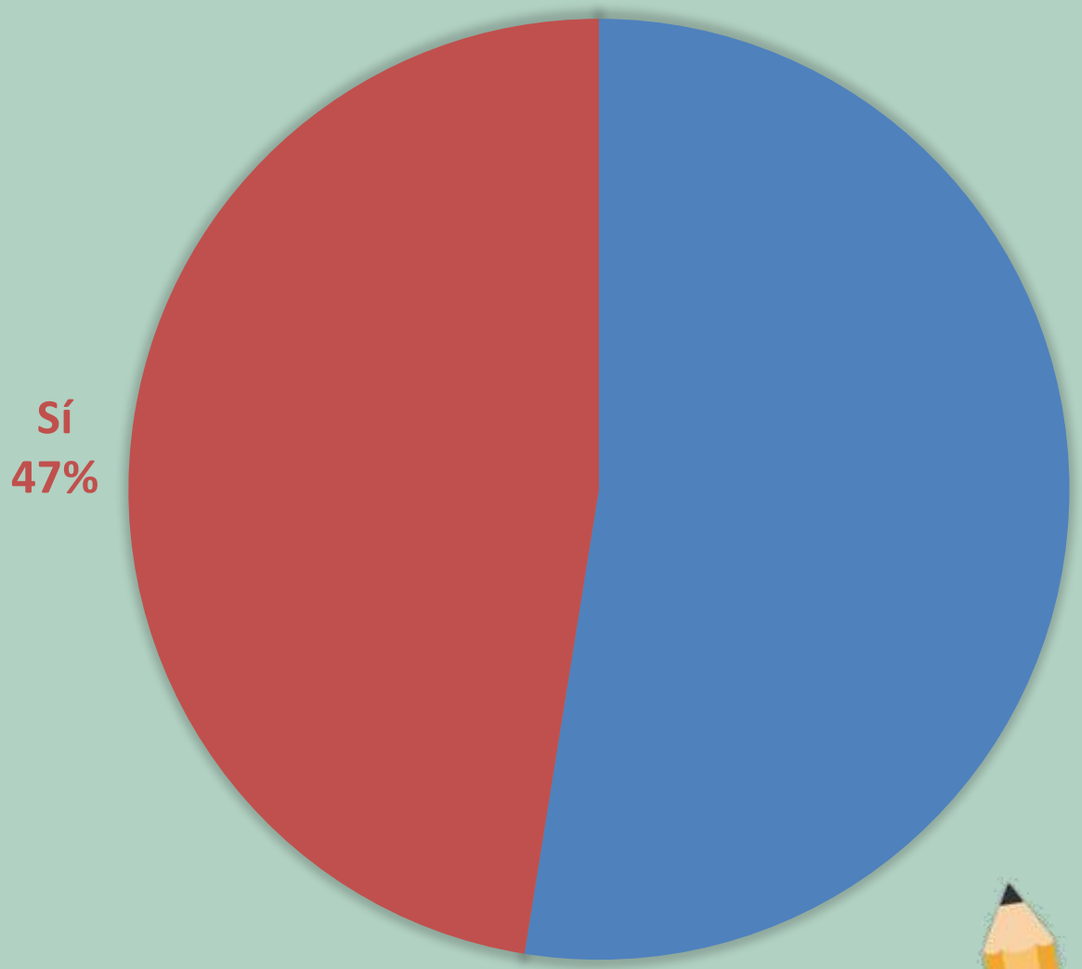
Imágenes creadas por dooder

¿Su empresa tiene un programa de seguridad en aplicaciones?

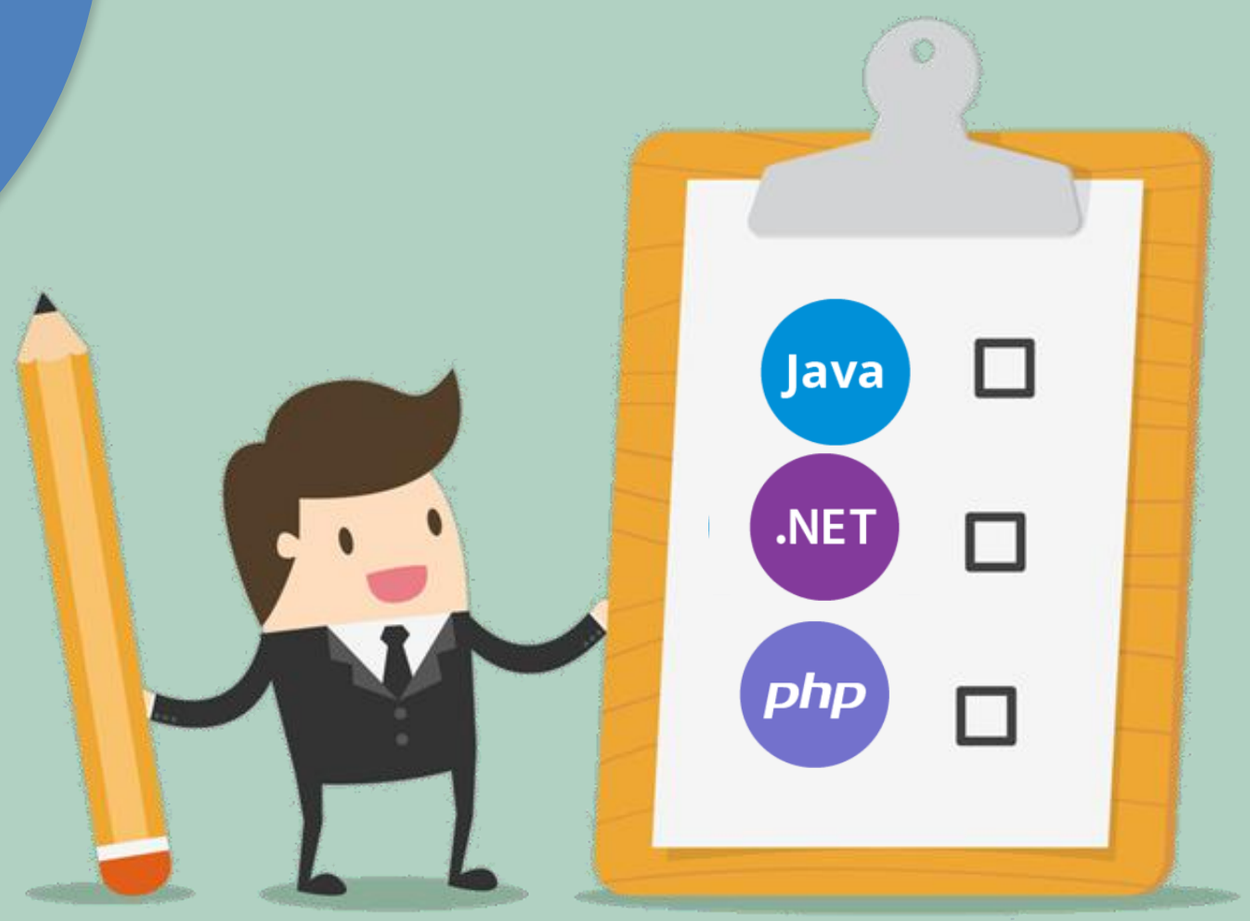


Doble clic: “es normal ver que muchas de las empresas de servicios de tecnología ofrezcan servicios de seguridad en aplicaciones a sus clientes. ¿Pero como están puertas adentro? **Hay que comer lo que uno cocina….**

¿Su equipo realiza análisis de seguridad de su código?

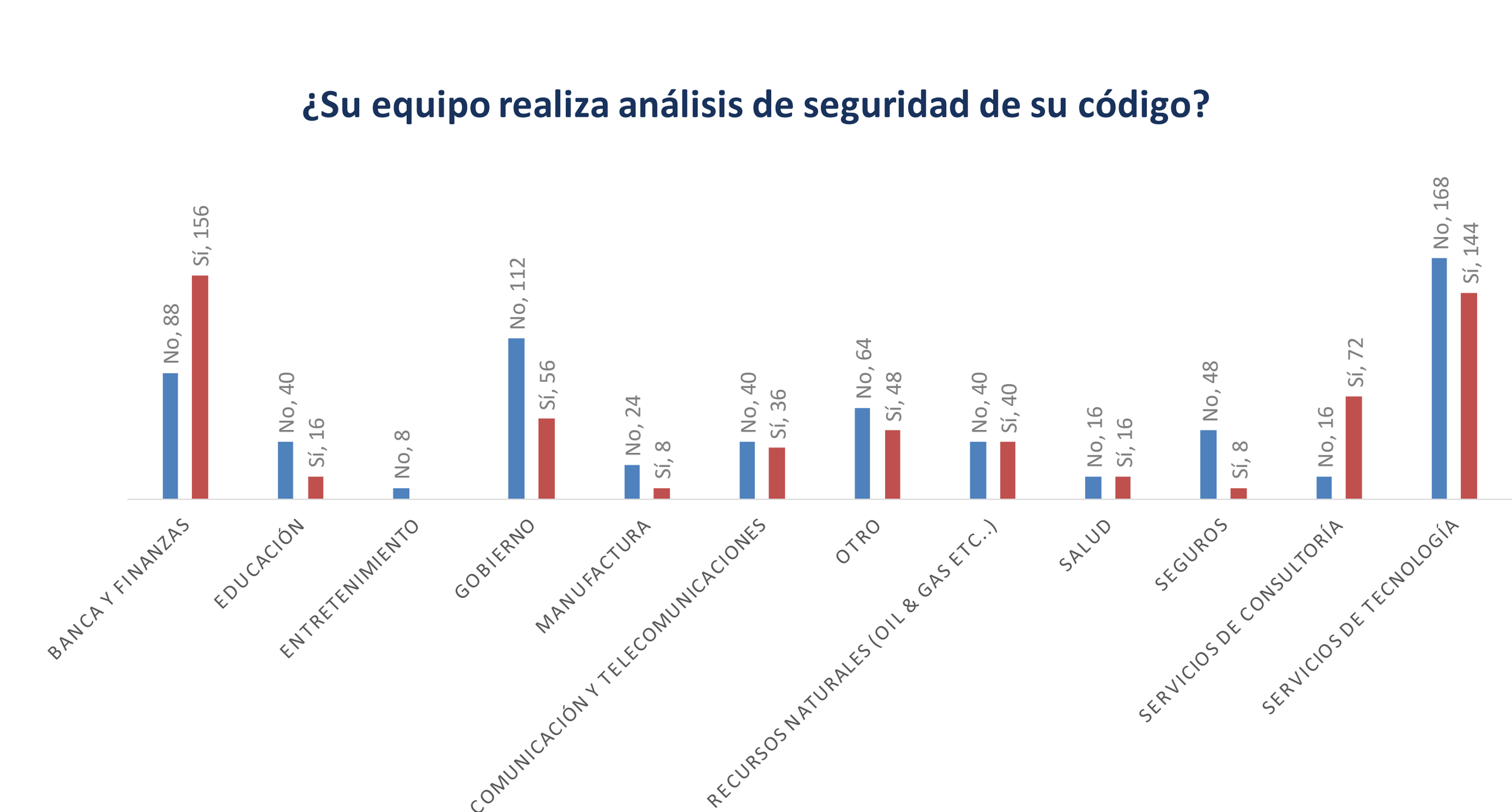


“No reconocer la importancia de la seguridad en una estrategia de DevOps es una receta para el desastre”



Imágenes creadas por dooder

¿Su equipo realiza análisis de seguridad de su código?

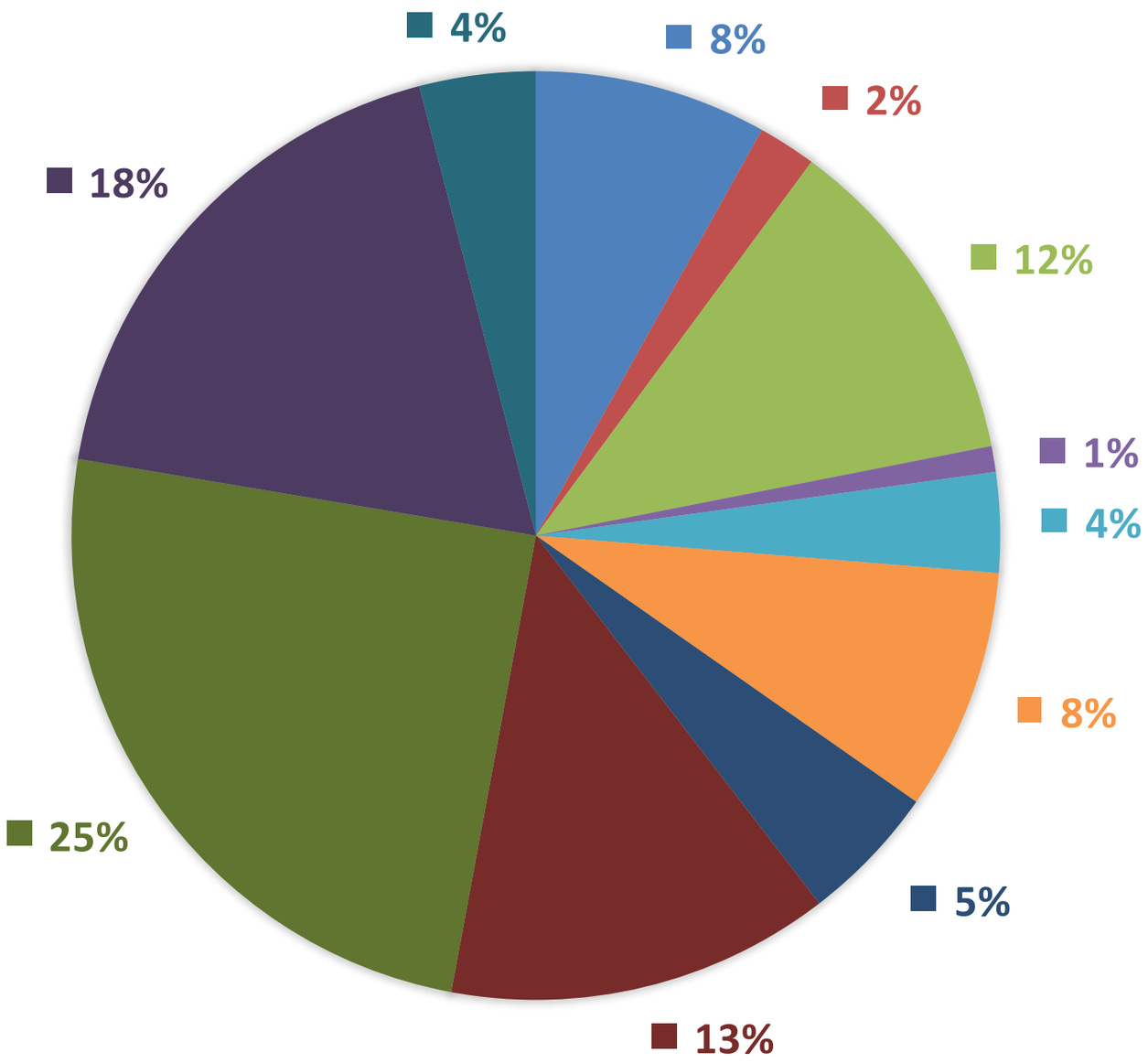


Doble clic: Los desarrolladores saben que la seguridad es importante, pero no tienen suficiente tiempo para dedicarle.

Practicas y Herramientas

Imágenes creadas por dooder

¿Qué herramientas de seguridad utiliza usted o su equipo?



- OSS - Open Source Security
- RASP - Runtime Application Self-Protection
- SAST - Static Application Security testing
- ASTO - Application Security testing Orchestration
- IAST - Interactive Application Security testing
- DAST - Dynamic Application Security testing
- CSA - Container Secure Application
- DLP - Data Loss Prevention
- WAF - Web Application Firewall
- IDS/IPS
- SCA - Software Composition Analysis

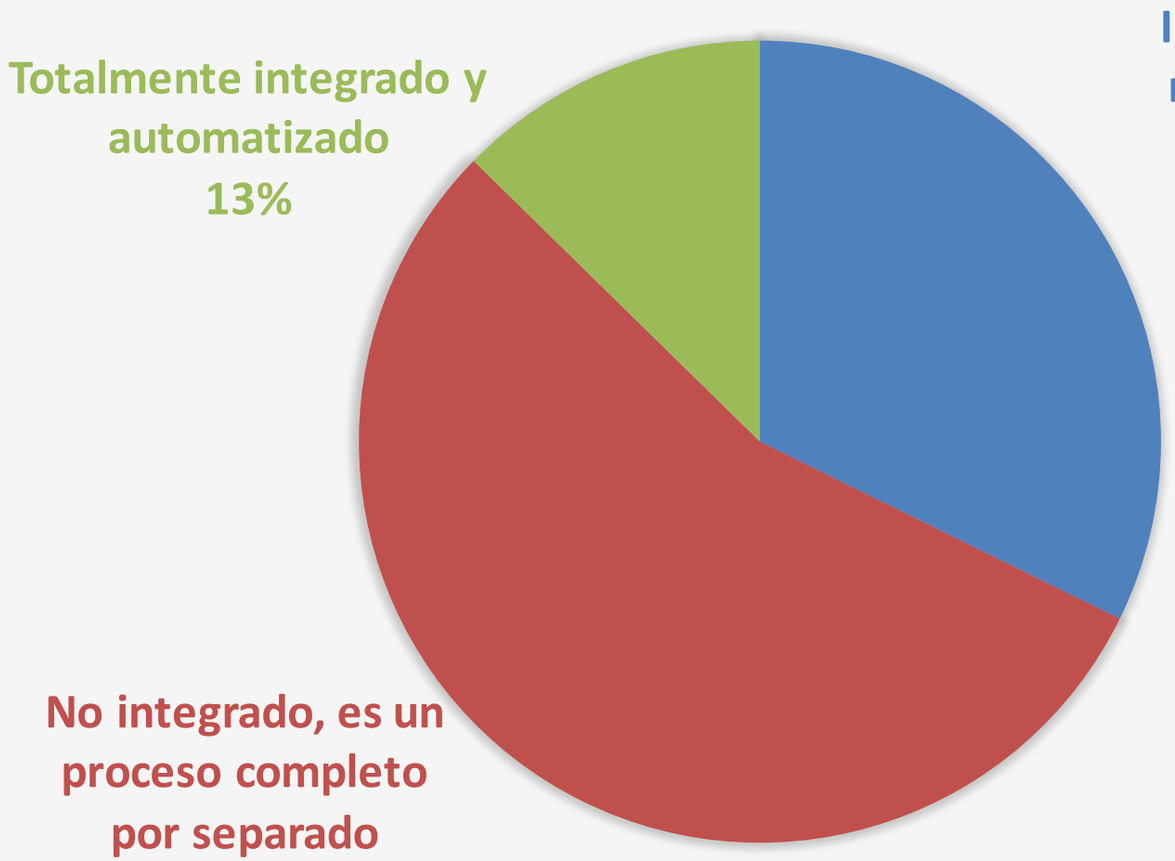
En la mayoría de las organizaciones, vemos que los WAF (Web Application Firewall), los sistemas de detección de intrusos y DLP constituyen los tres principales controles de seguridad aplicados.

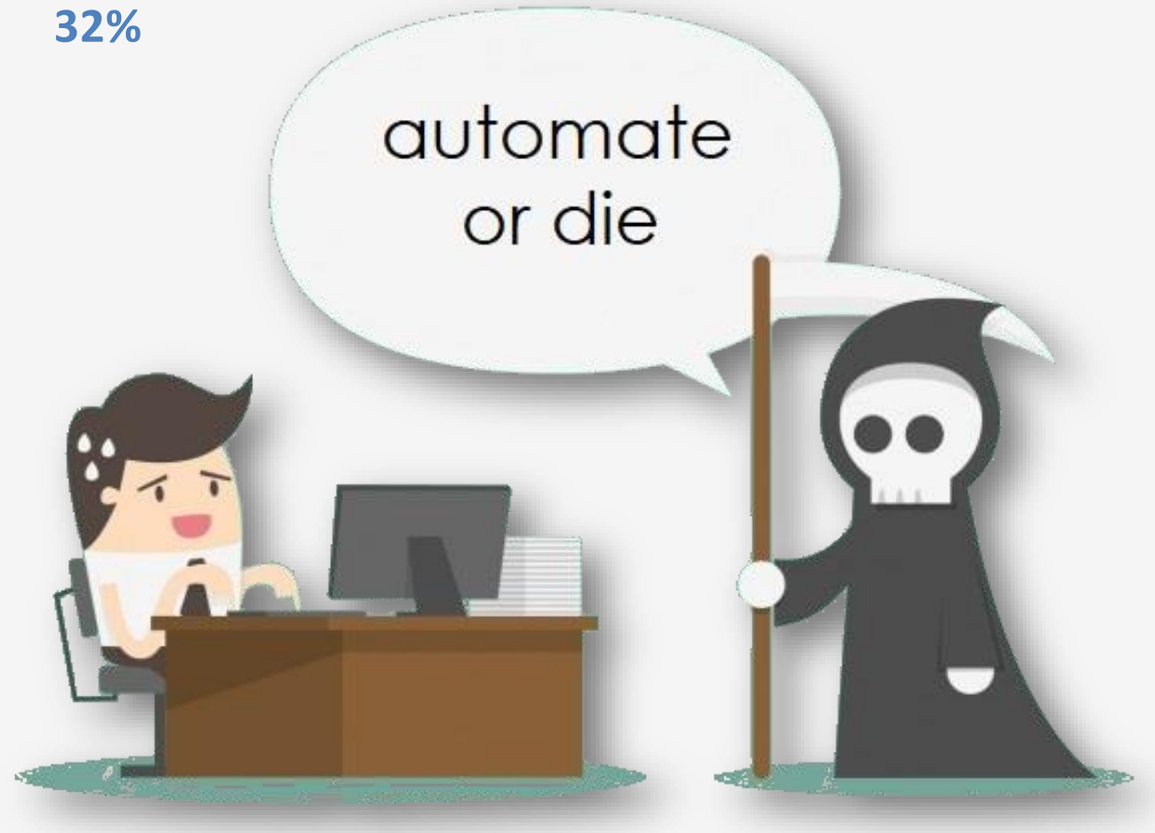
Las prácticas de DevSecOps maduras priorizan WAF, OSS Governance e IDS/IPS. ¿que nivel tiene tu organización? (Inmadura | Intermedia | Madura)

	Inmadura	Intermedia	Madura
WAF - Web Application Firewall	31.46%	38.20%	30.34%
OSS - Open Source Security	47.50%	43.75%	8.75%
IDS/IPS	29.41%	40.00%	30.59%
CSA - Container Secure Application	64.10%	29.49%	6.41%
DLP - Data Loss Prevention	44.58%	37.35%	18.07%
SCA - Software Composition Analysis	73.33%	18.67%	8.00%
DAST - Dynamic Application Security testing	64.56%	21.52%	13.92%
SAST - Static Application Security testing	55.00%	25.00%	20.00%
IAST - Interactive Application Security testing	80.82%	12.33%	6.85%
RASP - Runtime Application Self-Protection	78.08%	13.70%	8.22%
ASTO - Application Security testing Orchestration	82.67%	9.33%	8.00%

Podemos observar que de las AST (Application Security testing tools) SAST es la que tiene una nivel mayor nivel de madurez, seguido de DAST.

En general, ¿qué descripción se ajusta mejor a la integración de las herramientas de seguridad dentro del pipeline de DevOps?





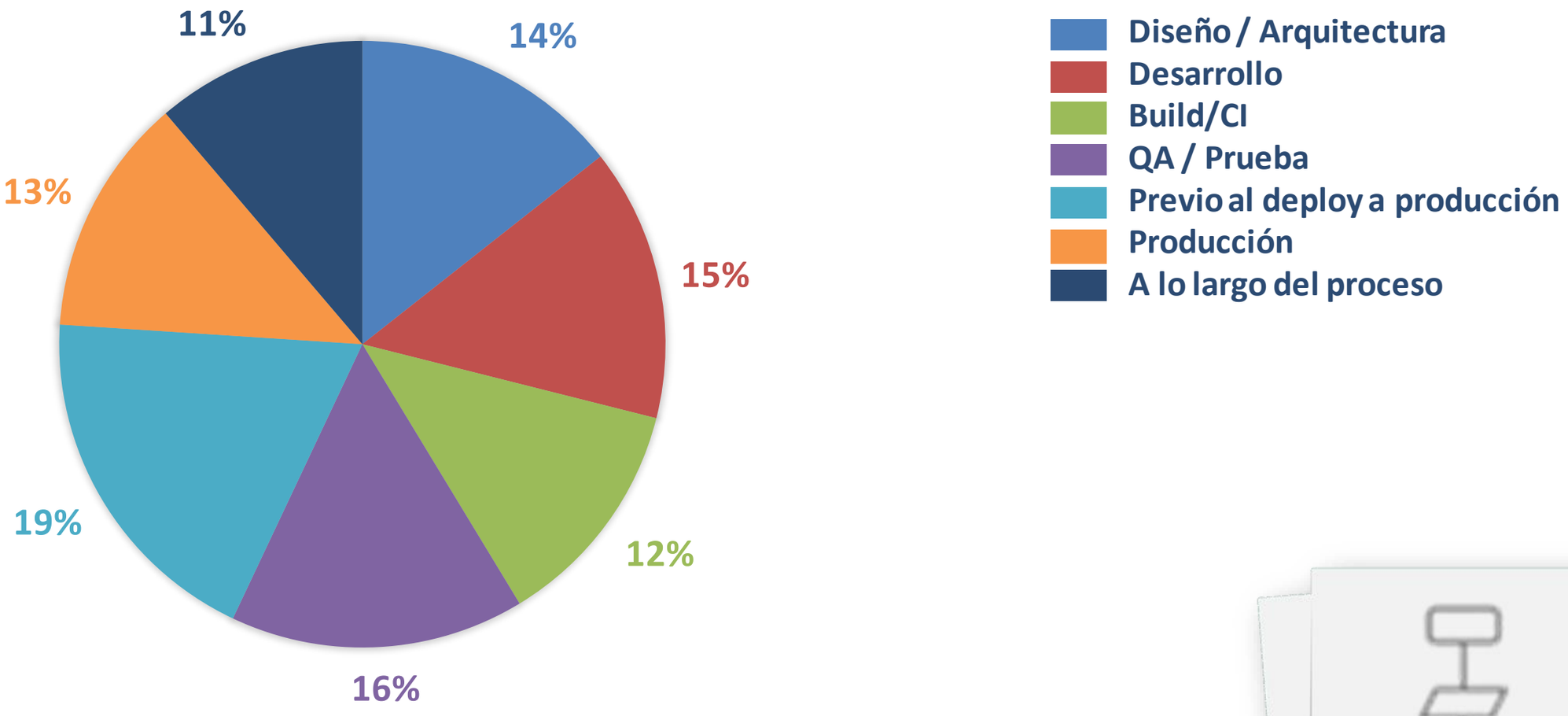
La integración de los controles de seguridad en pipelines automatizados sigue siendo más fuerte en las prácticas maduras, aunque las prácticas inmaduras y en evolución de DevOps siguen integrando cada vez más estos controles de seguridad.

¿Las herramientas de seguridad están correctamente integradas en el pipeline de desarrollo de su equipo?

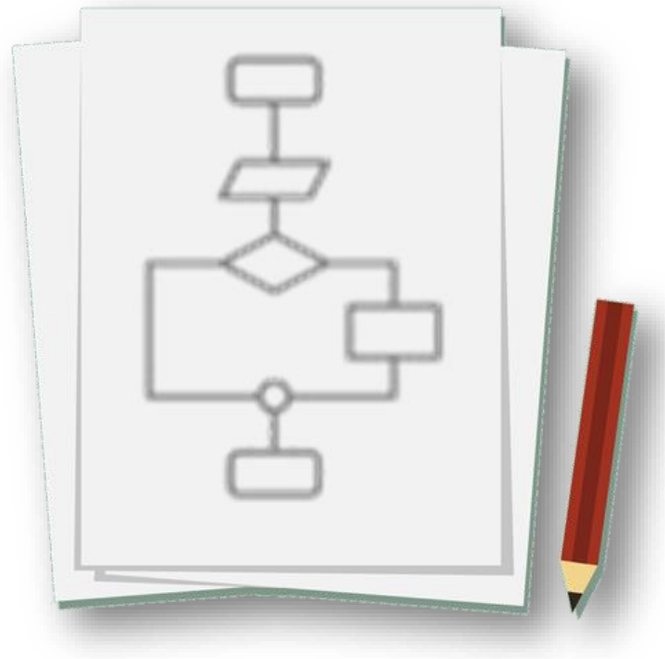
	Integrado	Semi integrado	Se ejecuta Manualmente
WAF - Web Application Firewall	14.29%	35.71%	50.00%
OSS - Open Source Security	6.85%	35.62%	57.53%
IDS/IPS	16.05%	39.51%	44.44%
CSA - Container Secure Application	9.09%	24.24%	66.67%
DLP - Data Loss Prevention	13.89%	30.56%	55.56%
SCA - Software Composition Analysis	5.00%	23.33%	71.67%
DAST - Dynamic Application Security testing	12.12%	24.24%	63.64%
SAST - Static Application Security testing	17.39%	23.19%	59.42%
IAST - Interactive Application Security testing	8.47%	20.34%	71.19%
RASP - Runtime Application Self-Protection	8.62%	17.24%	74.14%
ASTO - Application Security testing Orchestration	10.00%	21.67%	68.33%

Pudimos observar que los equipos de DevOps maduros integran adecuadamente las herramientas de seguridad automatizadas a menudo a diferencia de las prácticas de desarrollo inmaduras.

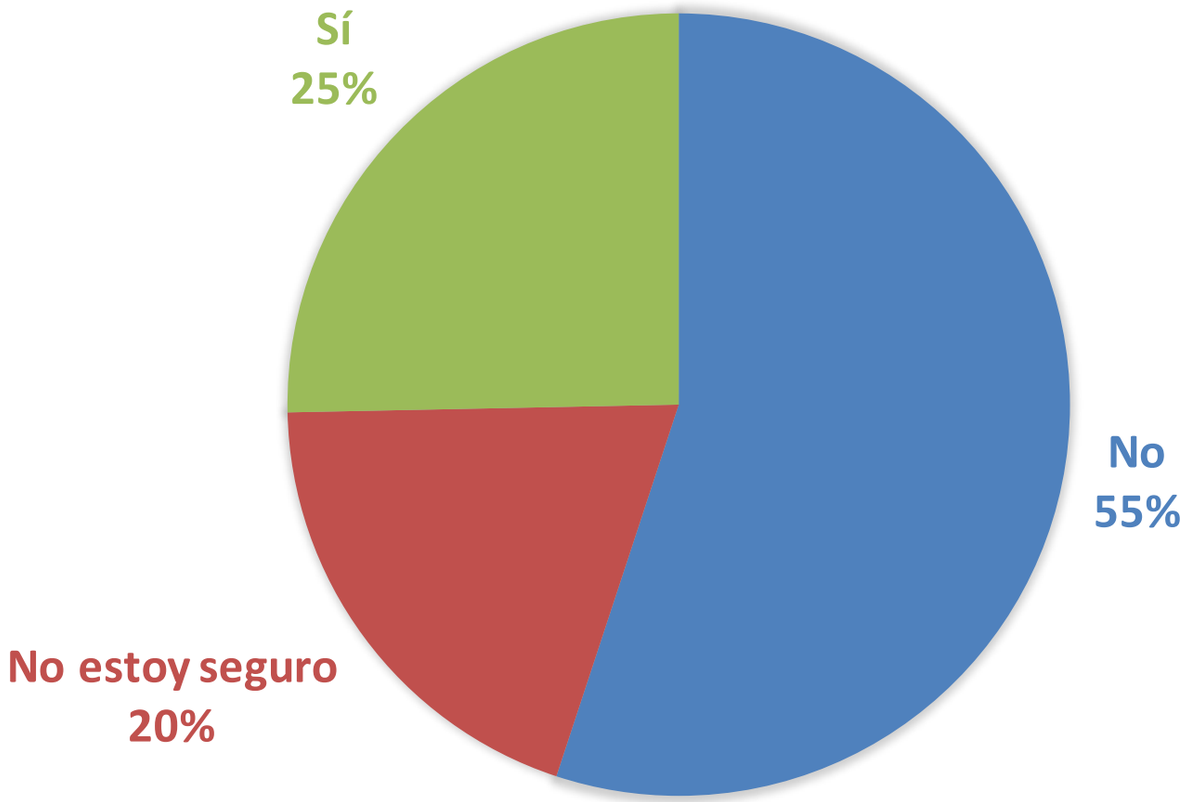
¿En qué momento del proceso de desarrollo realiza su organización el análisis automatizado de seguridad de aplicaciones?



No se trata sólo de dónde haces algo, sino de cómo lo haces. Pero mientras que la seguridad introducida al principio del ciclo de vida del desarrollo reduce el temido retrabajo y acelera los bucles de retroalimentación de DevOps, está claro que más organizaciones han puesto valor en la distribución de la seguridad a través del SDLC.



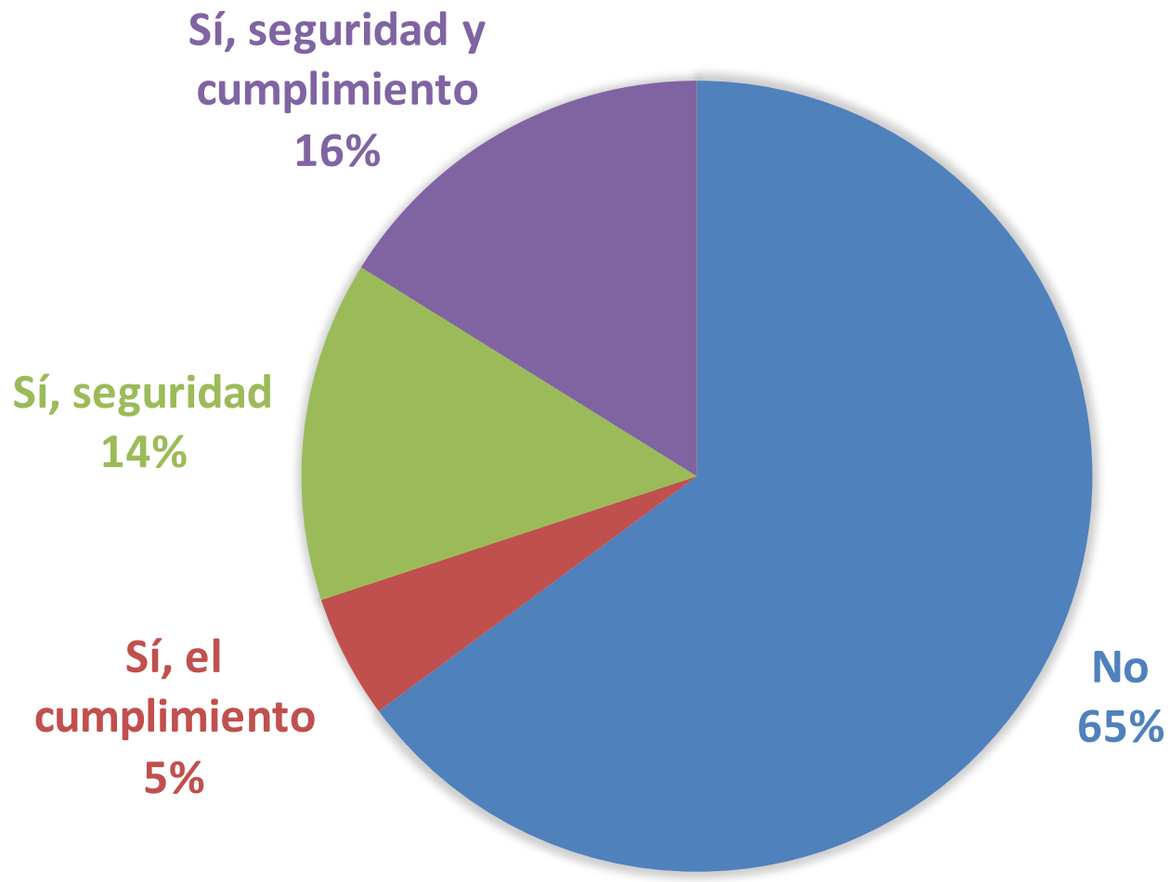
¿Tienen una solución de seguridad específica para Container (Docker, etc...)?

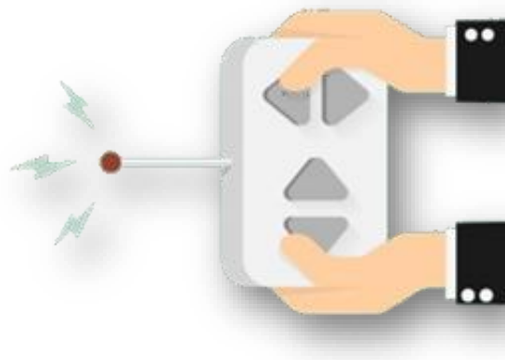


Para los que evaluamos niveles de madurez de los DevOps, las tecnologías de contenedores y de nubes vienen casi como ambientes mandatorios.

Las eficiencias obtenidas mediante estas tecnologías han acelerado la integración de las prácticas de Dev y Ops. Pero también vienen con sus propios requisitos de seguridad y exposiciones.

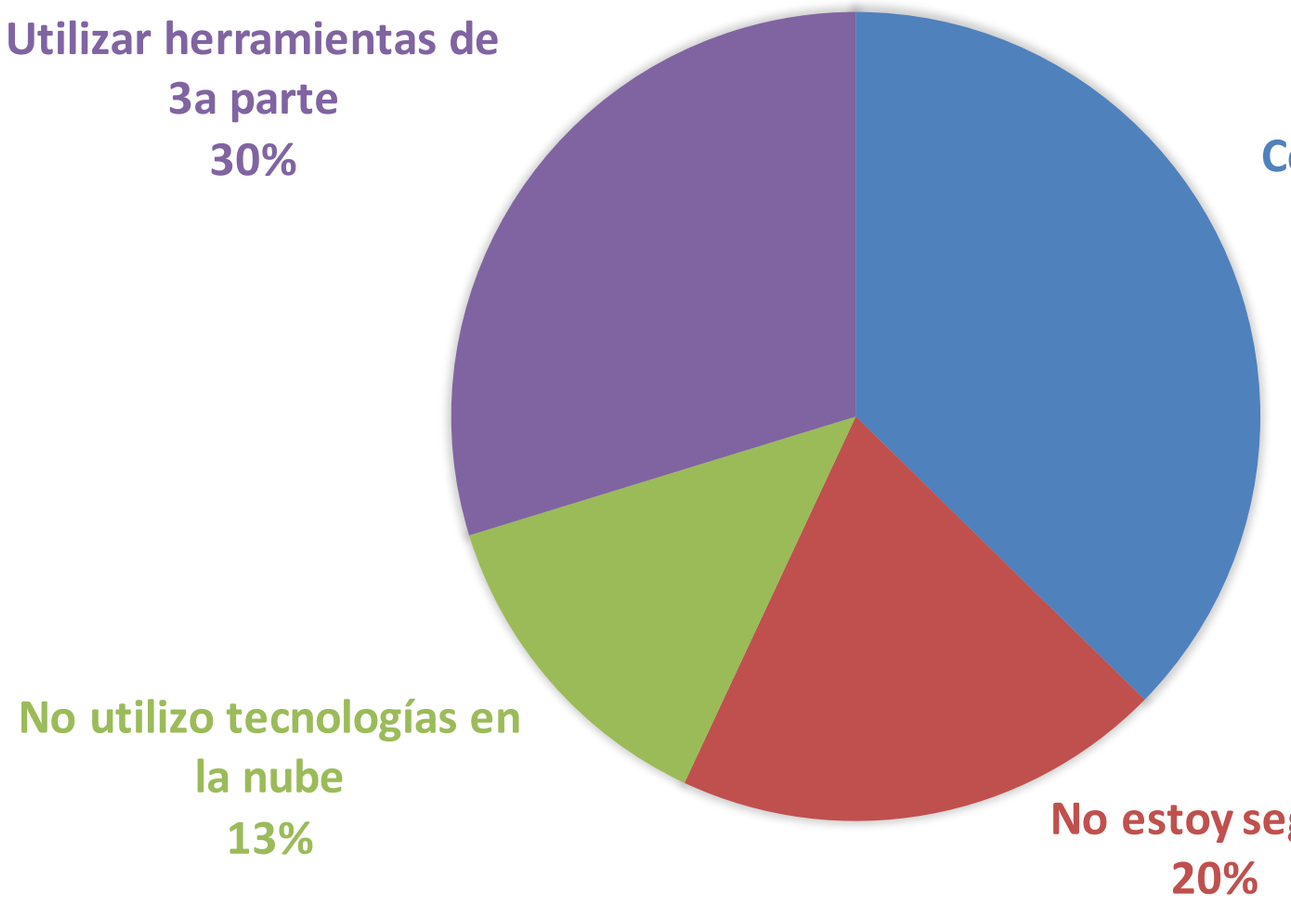
¿Tienen comprobaciones automatizadas de seguridad y cumplimiento para la herramienta de organización de clústeres?





Se puede decir que Docker vino a resolver el problema de “it works on my machine” Pero no podemos olvidar de los controles de seguridad sobre las herramienta de administración y gestión de clústeres, como por ejemplo Seguridad nativa de Kubernetes

¿Qué protección de seguridad en la nube utiliza?

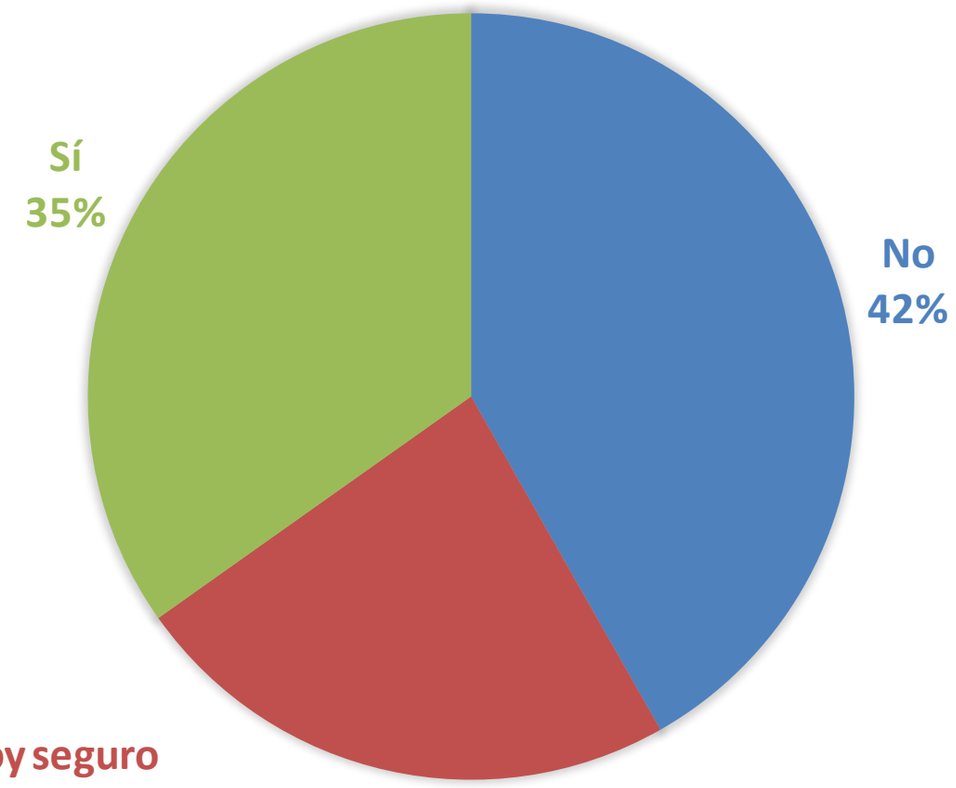


Vemos mucha tercerización o confianza en el proveedor de nube, pero recuerden cuando la infraestructura se migra a la nube, nuestras obligaciones y requisitos de seguridad también migran ahí.

Open Source Governance

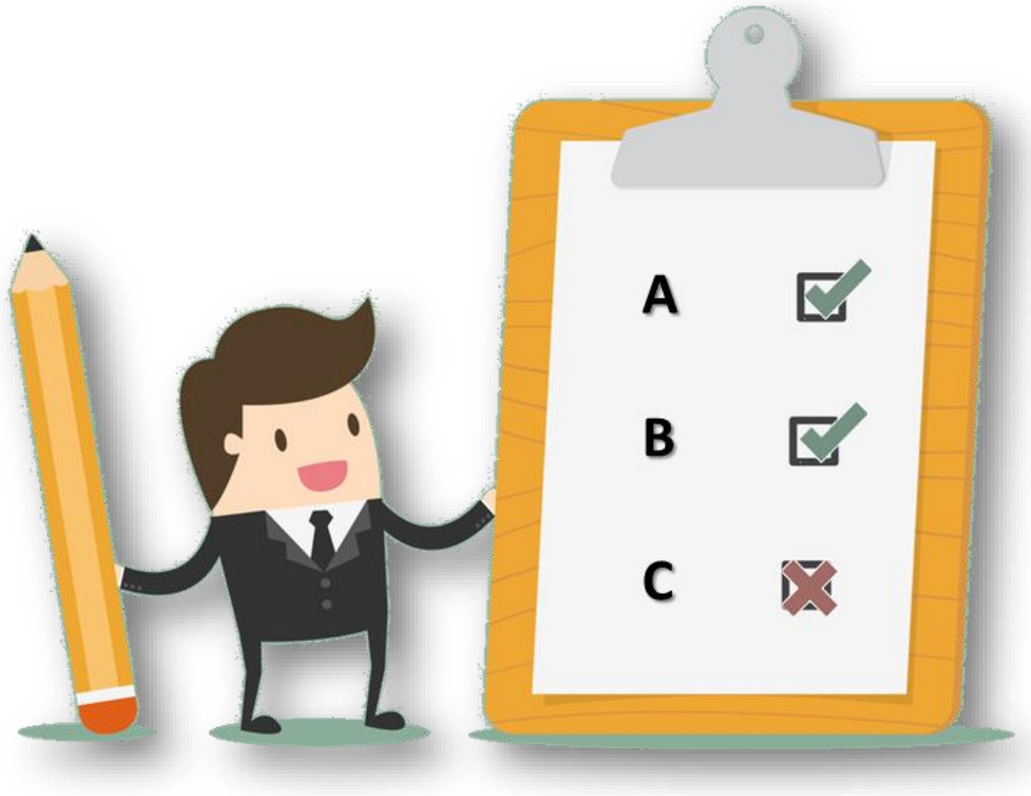
Imágenes creadas por dooder

¿Mantiene su organización un inventario de componentes Open Source utilizados en aplicaciones de producción?

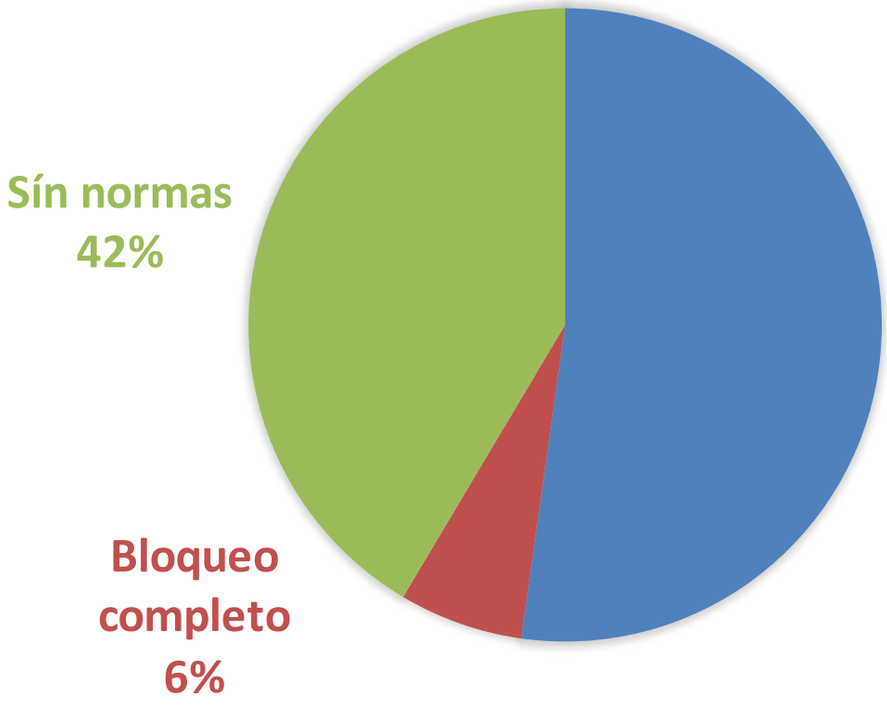


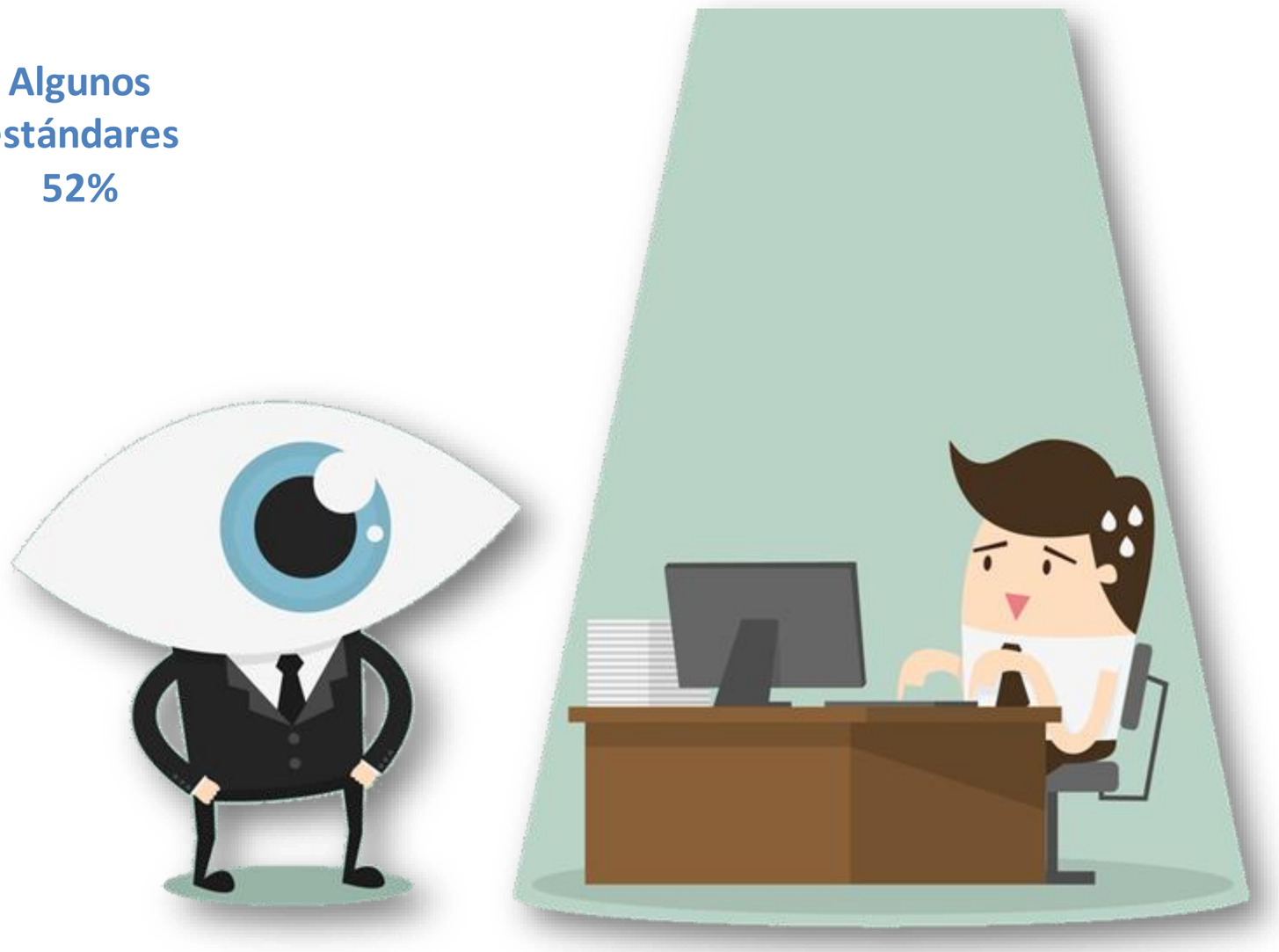
Como se ha visto anteriormente la gobernanza del código abierto empieza ser utilizada por equipos de desarrollo tanto maduros como inmaduros, pero el hecho de que existan herramientas y políticas no significa que se cumpla.

Hoy en día, más del 85 % de una aplicación moderna se construye a partir de componentes de código abierto, ya que los desarrolladores eligen descargar en un segundo lo que puede llevar días o semanas para escribir desde cero.



¿Qué tan bien controla su organización qué componentes/bibliotecas/binarios de código abierto y de terceros se utilizan en el desarrollo?



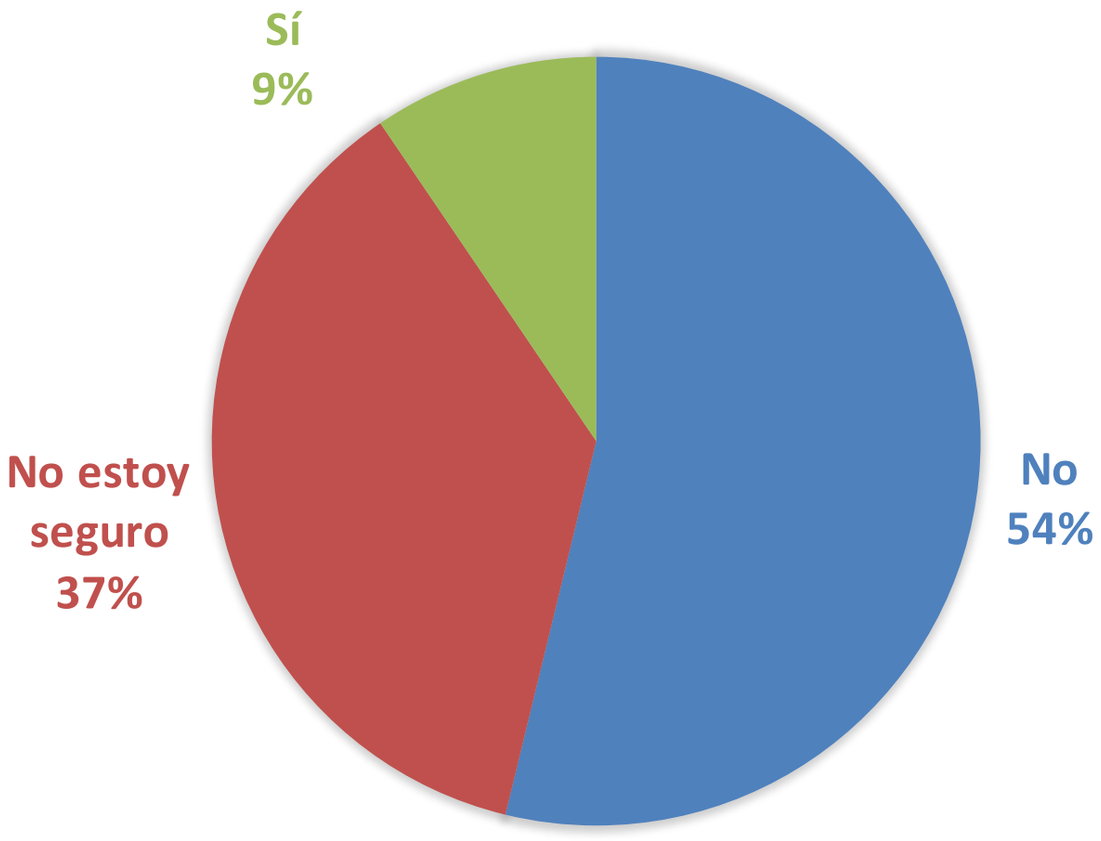


Mientras que los desarrolladores de software han aumentado exponencialmente su confianza en los componentes de software de código abierto, hemos aprendido que no todos los componentes son creados igual. Desde Heartbleed de OpenSSL, pasando por Poodle, Bash, hasta Struts2, las brechas relacionadas con el código abierto están en aumento.

Brechas, respuestas y registros

Imágenes creadas por dooder

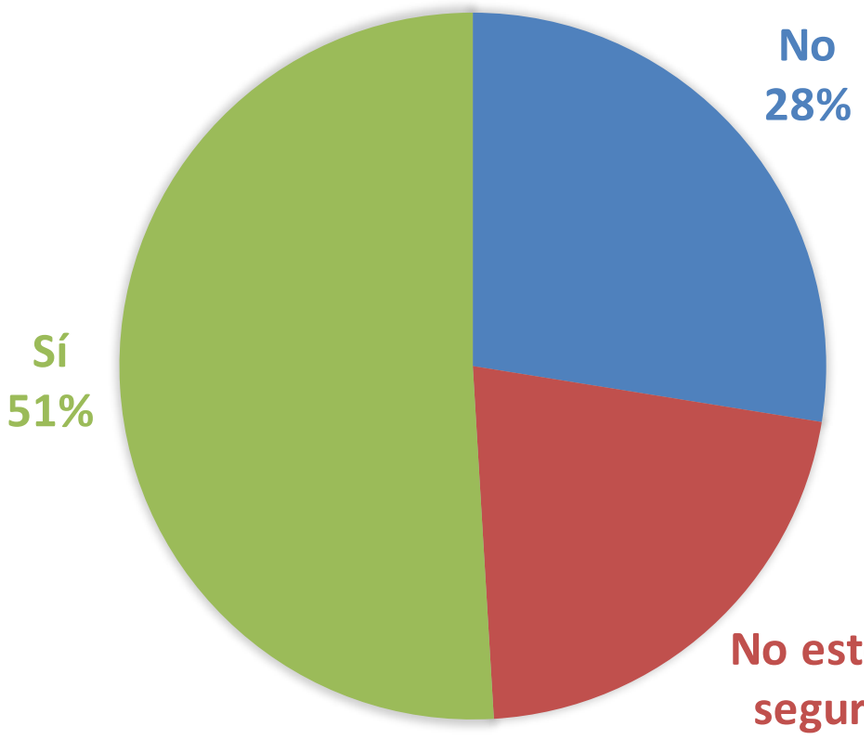
¿Ha tenido su organización una infracción que se puede atribuir a una vulnerabilidad en un componente o dependencia de código abierto en los últimos 12 meses?



Todos debemos reconocer que la seguridad es algo vivo y las organizaciones deben estar preparadas para prevenir y responder a las violaciones en cualquier momento dentro del ciclo de vida de su aplicaciones.

“Con la demanda de velocidad del negocio es difícil imaginar una higiene de ciberseguridad adecuada y suficientes preparativos para una infracción sin que existan DevSecOps".

¿Mantiene un registro de auditoría de quién cambia qué y cuándo?

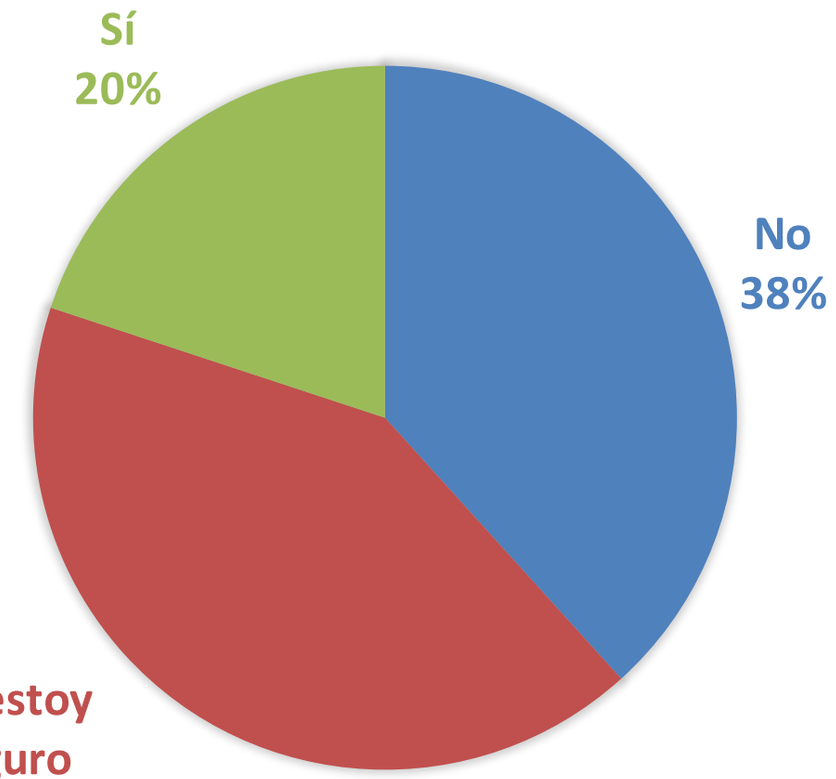


Muchas prácticas de DevOps se esfuerzan por lograr el "cumplimiento como código".

La creación de políticas de cumplimiento codificadas y pistas de auditoría en el desarrollo y las operaciones permite que estas importantes barreras de seguridad se conviertan en una parte integral de la forma en que los equipos de DevOps trabajan en el día a día.

¿Tiene una estrategia de Triaje?

DevSecOps busca insertar seguridad en un pipeline de DevOps sin ralentizarlo. Esto requiere mucha más precisión y velocidad que la que proporcionan los métodos tradicionales de seguridad de aplicación.



Dado que los ciclos de liberación de DevOps son rápidos, la cantidad de tiempo disponible para triaje y remediar las vulnerabilidades se reduce en gran medida. Por lo tanto, la gestión y la priorización de las vulnerabilidades son primordiales pero vemos en esta métrica que solo 20% cuanta con una estrategia de triaje.

¿Qué métricas utilizan para evaluar su implementación de DevSecOps? nombrar las mas significantes.

El 44% dicen no contar con métricas

Cuantos issues de seguridad se detectan luego de la implantación

Cobertura; Eficacia; Agilidad

Cantidad de Errores de Vulnerabilidad, Errores de Seguridad Reportados por Clientes Finales, Resultados de Penetration Testing

seguimiento de la frecuencia de implementación del código para tener una idea clara de la rapidez con que se implementan las nuevas características y capacidades

Calidad y frecuencia de liberaciones, cantidad de aplicaciones bajo CI/CD

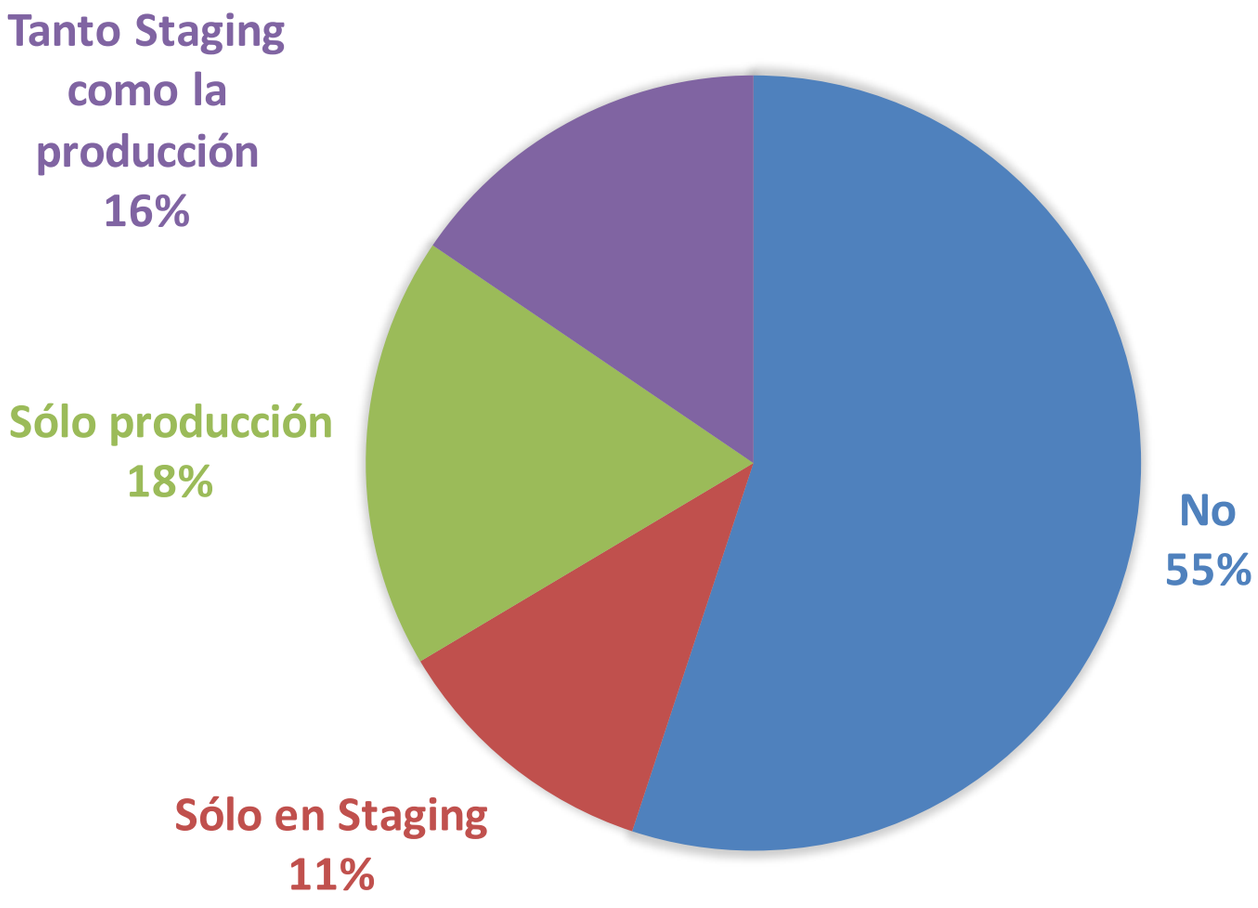
Pre-Commit Checks, Commit Checks, Test time Checks, Deploy Time checks

Total de Vulnerabilidades por Repositorio / Tiempo de Reparación (MTTR)

Frecuencia de despliegue, cantidad de smell code, paquetes no actualizados

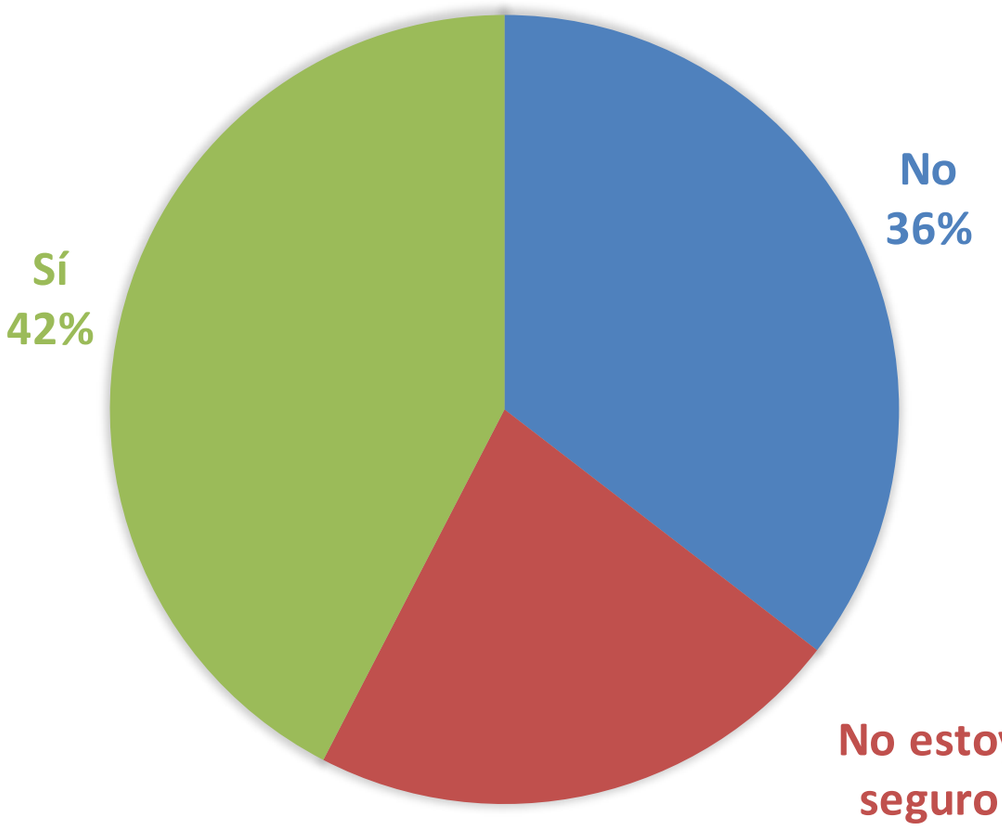
Medición de eficiencia en codificación segura (acierto y error), Medición del conocimiento en codificación segura, Medición de la gestión de vulnerabilidades por ciclos de pruebas, Medición de vulnerabilidades en función al riesgo crítico.

¿Tiene una directiva de retención de artefactos implementados en ensayo y producción?



Las políticas de retención le permiten establecer cuánto tiempo se deben mantener las ejecuciones, las pruebas y las versiones almacenadas en el sistema. Para ahorrar espacio de almacenamiento, desea eliminar ejecuciones, pruebas y versiones anteriores.

¿Tiene todas las credenciales y secretos a nivel de aplicación custodiadas y cifradas?



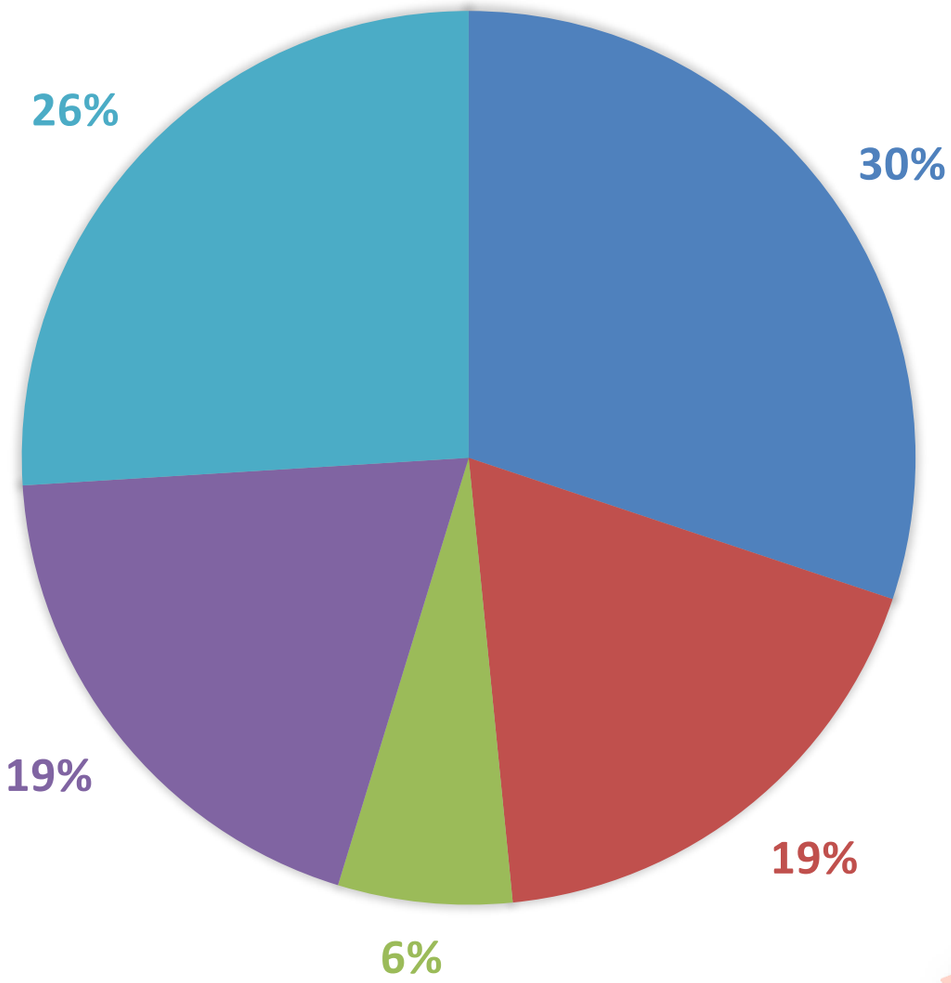
Committing contraseñas o claves para codificar dentro de cualquier repo es una mala práctica.

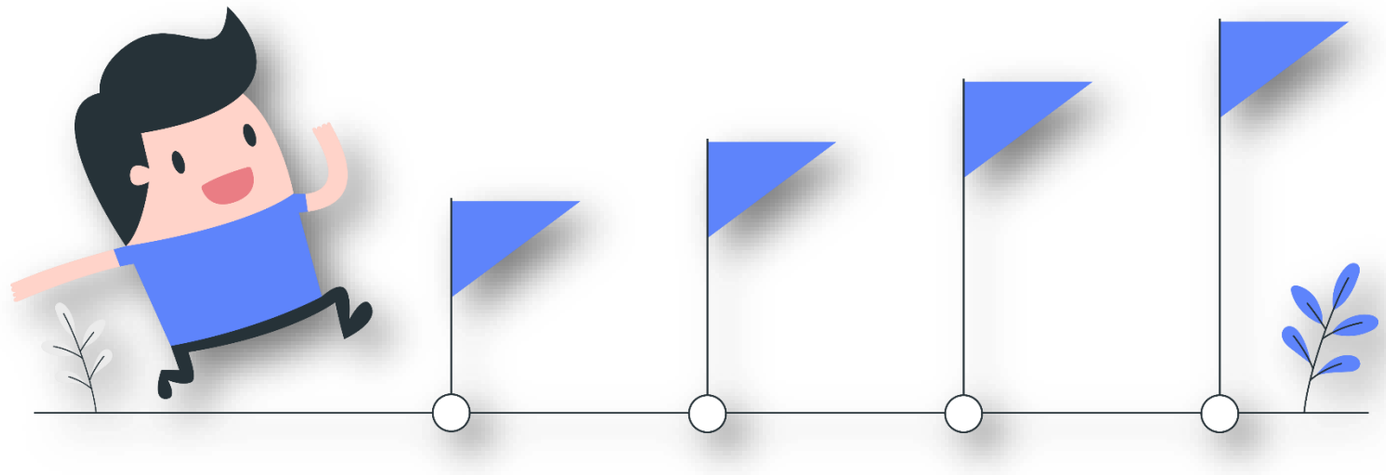
Sin embargo, durante años, los desarrolladores han publicado electivamente credenciales desprotegidas a bases de datos, cuentas y aplicaciones críticas para el negocio en sus repositorios internos, o peor aún, repositorios públicos como GitHub.

Desafíos principales

Imágenes creadas por dooder

Cuáles son los principales desafíos con los procesos de seguridad de sus aplicaciones.

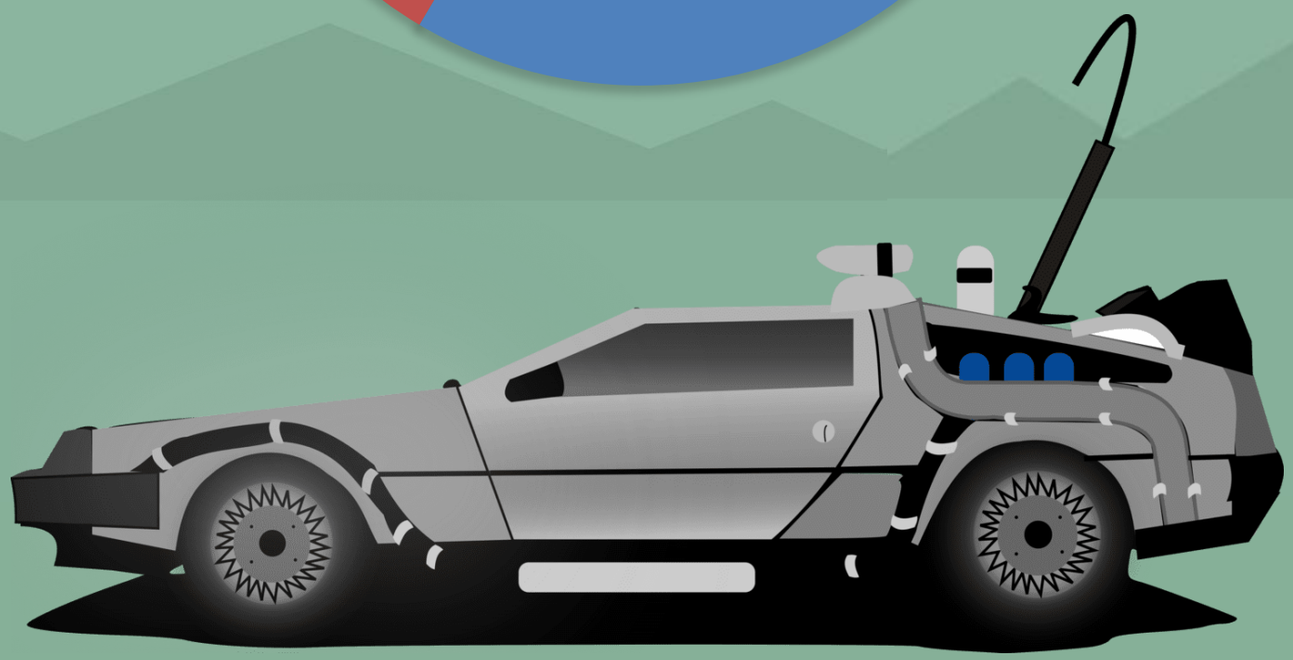




Mientras que los desarrolladores señalaron que la seguridad es importante, la encuesta nos revelo los retos a los que se enfrentan los desarrolladores cuando se les entrega información de seguridad en una fase tardía del proceso, introduciendo temidas regresiones no deseadas y disminuyendo la velocidad.

¿Cree que sus políticas/equipos de seguridad de la información están ralentizando a los equipos de desarrollo de software?

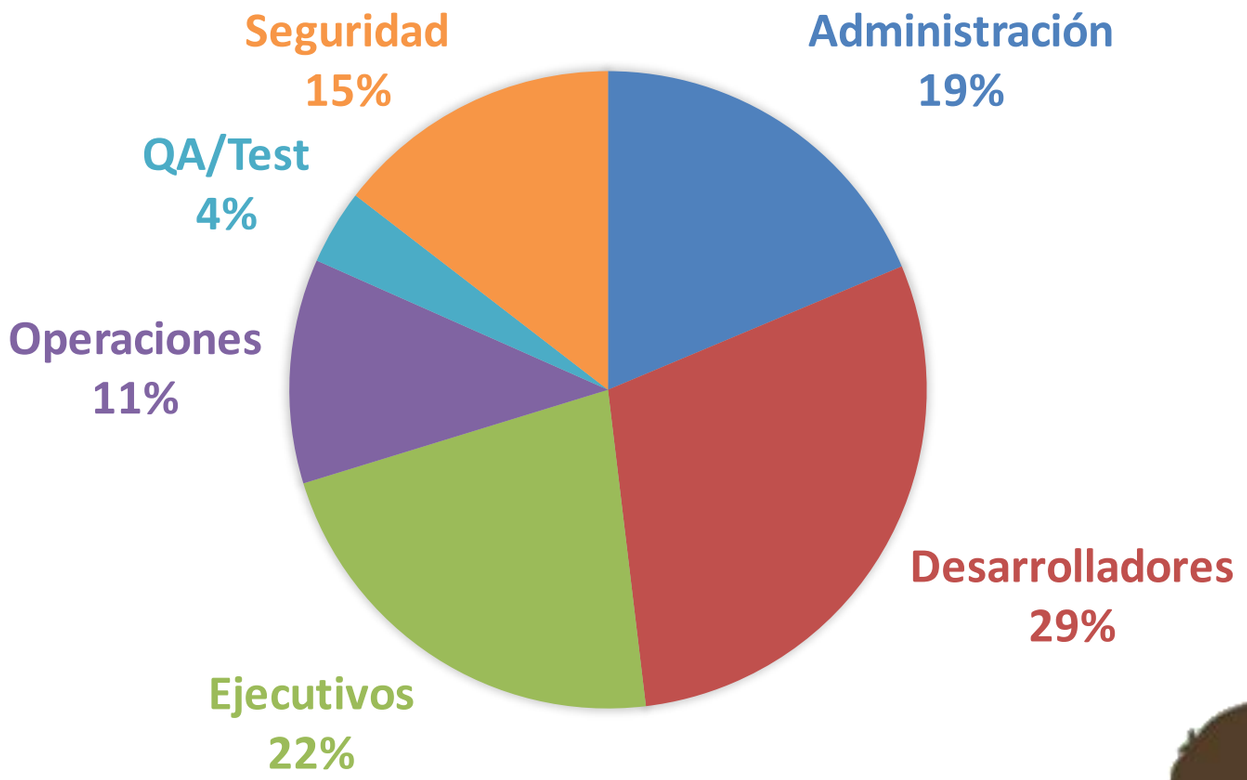
El “time to market” es cada año más corto y las prácticas de seguridad más antiguas frenan el desarrollo. Si analizamos las respuestas de los perfiles no SecOps casi el 80% respondió que “Sí”



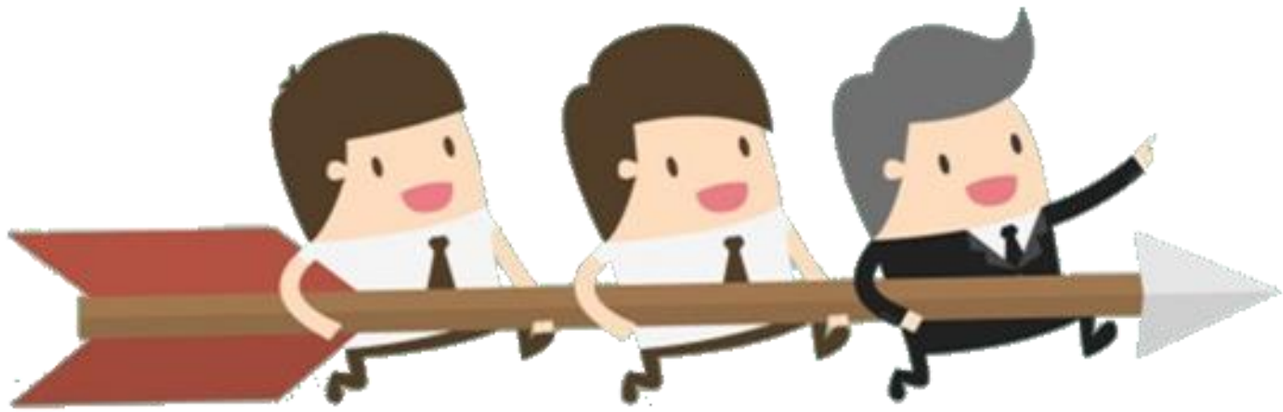
“Suban, los clientes quieren otro servicio para ayer”

Imágenes creadas por dooder

¿Quién causa más fricción en tu equipo?



Una pregunta que originalmente pretendimos que fuera humorística "Resultó que la pregunta era muy relevante para la cultura"



Vimos que en las prácticas maduras de DevOps, los desarrolladores dijeron abrumadoramente que no había fricción en sus equipos, mientras que en las prácticas inmaduras se identificó a lo Desarrolladores como la fuente clave de fricción"

¿Cuál es su interés en la seguridad de las aplicaciones?

8 de cada 10 desarrolladores consideran que la seguridad de las aplicaciones es una de las preocupaciones principales, pero no tienen suficiente tiempo para dedicarle

Conclusiones

Imágenes creadas por dooder

Conclusiones

A medida que las tecnologías avanzan y aumenta el valor del dato, nos encontramos en un terreno en el que la seguridad se convierte no solo en un valor añadido, sino en una parte esencial del diseño, tanto como puede serlo el rendimiento.

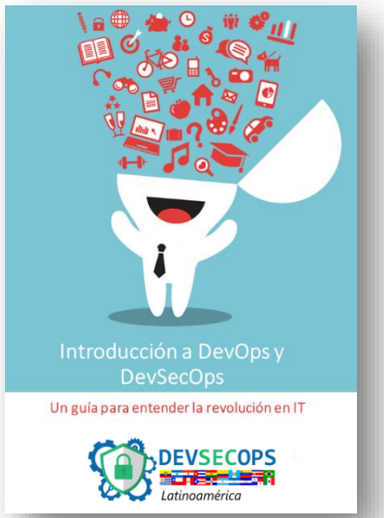
Esta filosofía no es nada nuevo y se basa en la adaptabilidad. Como dijo el célebre Bruce Lee:

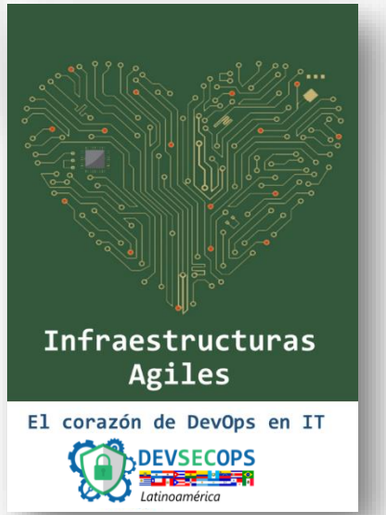
No te establezcas en una forma, adáptala y construye la tuya propia, y déjala crecer, sé como el agua. Vacía tu mente, sé amorfo, moldeable, como el agua. Si pones agua en una taza se convierte en la taza, si pones agua en una botella se convierte en la botella, si la pones en una tetera se convierte en la tetera. El agua puede fluir o puede aplastar. Sé como el agua, amigo, el agua que corre nunca se estanca; así es que hay que seguir fluyendo.

Bruce Lee

Lectura recomendada

Para profundizar los principios y la temática en DevSecOps, súmate a **DevSecOps Latinoamérica**





Próximamente

https://devsecops-latam.org

https://twitter.com/devsecops_latam

comunidaddevs-hdc8687.slack.com

https://www.linkedin.com/groups/12033278/

https://t.me/DevSecOpsLatam/

https://www.twitch.tv/devsecops_latam

Imágenes creadas por dooder