TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 1 – UNIDAD 1

Universidad Tecnológica de Pereira

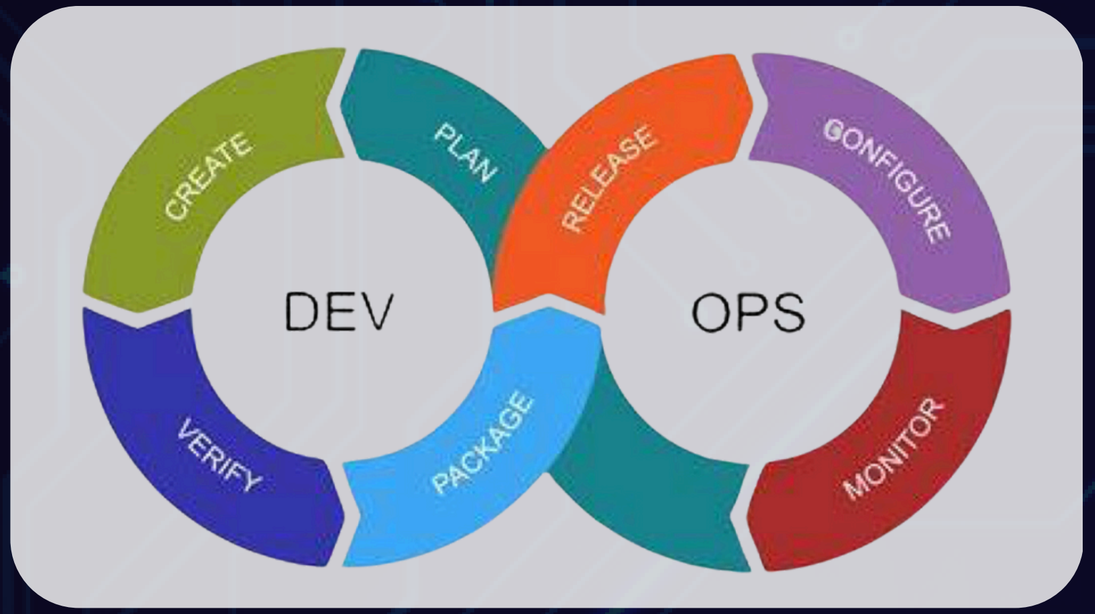
faceIT

DevOps, una combinación de las palabras "Desarrollo" y "Operaciones", es una metodología que busca eliminar las barreras entre los equipos de desarrollo de software y los equipos de operaciones. El objetivo principal de DevOps es facilitar una colaboración continua entre estos equipos para entregar software de manera más rápida, eficiente y con mayor calidad.

El concepto de devops se acuña desde el enfoque del agilismo, en donde se busca un proceso de desarrollo incremental y despliegue continuo de componentes de una aplicación.

Las metodologías ágiles buscan evitar que el proceso de desarrollo y entrega de software deje de ser lineal, liberando partes que pueden no responder a una necesidad. Por el contrario, se incluye al dueño de las aplicaciones para que éste valide cada componente y su integración con el resto de un proyecto de software.

La forma de automatizar el proceso iterativo de mejora y de incremento en la funcionalidad de un proyecto es conocida como DevOps.



Imaginemos una empresa que desarrolla una aplicación de comercio electrónico. Sin un enfoque DevOps, el equipo de desarrollo podría crear nuevas funciones sin considerar las dificultades que el equipo de operaciones enfrentará al implementarlas en producción. Por ejemplo, una nueva función puede consumir demasiados recursos del servidor, lo que provoca lentitud en el sistema. Con DevOps, ambos equipos trabajan juntos desde el inicio para garantizar que las funciones sean viables tanto en desarrollo como en producción.

Las prácticas de DevOps incluyen:

Integración continua (CI): Automatizar la fusión de cambios de código en un repositorio central varias veces al día.

Entrega continua (CD): Asegurar que el software esté siempre listo para desplegarse en producción.

Monitorización continua: Supervisar el rendimiento de las aplicaciones en tiempo real para detectar y resolver problemas rápidamente.

Por ejemplo, una empresa de streaming como Netflix utiliza DevOps para lanzar actualizaciones frecuentes sin interrumpir la experiencia del usuario, garantizando que los errores se detecten y corrijan antes de llegar al cliente.

Al proceso de Devops se han integrado todas las características de validación de brechas de seguridad, análisis de código y planes de mitigación de riesgo sobre la custodia de la información, es decir, así como se integró el proceso de despliegue al proceso de desarrollo de software (devops) también se han creado reglas y estándares para integrar la seguridad informática. Al proceso integrado de equipos dedespliegue, desarrollo de software y seguridad informática se conoce como DevSecOps.

Con este nombre se destaca la necesidad de que existan un proceso iterativo con un componente que vigile y mejora la seguridad informática en el contexto del software a desarrollar.

Por ejemplo, en el caso de una aplicación bancaria, lanzar nuevas funciones rápidamente sin evaluar adecuadamente los riesgos de seguridad puede abrir puertas a ataques como el robo de datos. Con DevSecOps, la seguridad está integrada desde el inicio, utilizando herramientas como análisis estáticos de código y pruebas de penetración automatizadas para identificar problemas antes de que lleguen a producción.

Dentro de las mejoras que tiene DevSecOps se encuentra la automatización de la seguridad por medio de herramientas de escaneo de vulnerabilidades y análisis de dependencias aseguran que se identifiquen riesgos automáticamente durante el desarrollo y despliegue. El proceso de DevSecOps busca que todos los actores (desarrolladores, encargados de infraestructura y administrativos) estén encargados también de vigilar la seguridad informática.

Un ejemplo práctico es el uso de pipelines de CI/CD seguros. Supongamos que una empresa usa un pipeline para lanzar actualizaciones de una aplicación de mensajería. Con DevSecOps, antes de cada despliegue, el pipeline ejecuta un análisis de vulnerabilidades en el código, verifica que no haya dependencias inseguras y simula ataques para comprobar la robustez de las funciones. Esto reduce la probabilidad de lanzar código inseguro a producción.

Vulnerabilidades que se detectan en el proceso:

Con todos los retos en los diferentes niveles de seguridad, todo software necesita incorporar la gestión del riesgo informático. Hay muchos métodos que un atacante puede emplear a nivel de aplicación para causar daños, por lo que es necesario comprenderlos e integrarlos al proceso iterativo de entrega. Revisaremos algunos ataques y la forma en la que DevSecOps puede ayudar a prevenirlos.

Ataque por inyección de código SQL

SQL es un estándar para la gestión de información en motores de bases de datos. Un atacante puede inyectar instrucciones de SQL simplemente usando los campos que existen en un formulario. Al inyectar SQL se vulnera por completo una base de datos, ya que el atacante puede solicitar todos los registros, así como agregar y cambiar información.

Este tipo de ataque puede afectar a cualquier aplicación que tenga un motor de bases de datos (mysql, mariaDB, sql sever, Oracle, postgres y cualquier otro).
Una inyección SQL es un ataque frecuente y altamente peligroso, a tal punto que está en la lista OWASP top 10.

Un dato que reveló Microsoft sobre un estudio de seguridad de la información llevado a cabo en 2018 revela que más del 7% de las aplicaciones de almacenamiento de software como servicio no cifran sus datos. Esto es preocupante ya que el 86% de aplicaciones colaboran con esas aplicaciones.

Así mismo, pocas implementaciones de software son compatibles con protecciones de sesión a través del protocolo HTTP seguro, se calcula que es alrededor de un 4%.

Antes de un proceso de DevOps las aplicaciones tenían prácticas de seguridad basadas en control de acceso, seguridad en el entorno y protección perimetral.

Con la implementación del secure DevOps la seguridad informática consiste en ir agregando los elementos a las canalizaciones de compilación y revisión y obteniendo los beneficios de la velocidad de desarrollo y despliegue de DevOps.

En el proceso DevSecOps lo primero que se intenta responder antes de desplegar una función de código es:

¿Mi aplicación utiliza o consume software de terceros? ¿Ese software es seguro?
¿Hay vulnerabilidades conocidas en cualquier del software de terceros que se utiliza?
¿Con qué rapidez se pueden detectar vulnerabilidades?
¿Con qué rapidez se pueden corregir vulnerabilidades detectadas?