DevSecOps, Estado del Arte en el Contexto Boliviano

Maribel Pachacuti Blanco
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
maribel.pachacuti.blanco@gmail.com

***Resumen*—Incorporar prácticas de seguridad en el flujo DevOps ha sido un desafío porque representa un esfuerzo adicional. El propósito de este artículo es dar una visión general de lo que es DevSecOps, lo que implica implementar este enfoque, los beneficios y dificultades; para luego presentar el estado del arte en el contexto boliviano de la seguridad en el desarrollo de software. Al ser esta investigación de carácter exploratorio se concluye que, en Bolivia, la cultura DevOps está en desarrollo, e incorporar prácticas de seguridad involucra grandes desafíos para los profesionales de TI.**

Palabras clave—DevOps, DevSecOps, Security, Bolivia.

I. Introducción

En los últimos años, muchas empresas de desarrollo de software han cambiado su enfoque de desarrollar software como producto (SaaP, del inglés Software as a Product) para desarrollar software como servicio (SaaS, del inglés Software as a Service). En SaaP se desarrollaba el software, se entrega al cliente quien lo instalaba y lo ejecutaba localmente. En SaaS el software se aloja en alguna infraestructura, usualmente en la nube y se accede mediante un canal, a través de la web, por ejemplo. Con SaaS los clientes no controlan la infraestructura de nube ni la funcionalidad del software, como lo hace el proveedor. Facilitando al proveedor la mejora y entrega continua sin tener que redistribuirlo a todos sus clientes, ya que solo basta con actualizar el software en su propia infraestructura en la nube. El uso de SaaS puede ser mediante suscripciones o licencias. En este enfoque de desarrollo de software complejo se integra cambios y entrega continuamente, surgiendo nuevos procesos tales como: integración continua, entrega continua, despliegue continuo, que requieren herramientas y desafíos. Los intentos de superar estos desafíos dan como resultado al concepto denominado DevOps.

DevOps es la fusión conceptual y operativa de las necesidades, equipos y tecnologías de desarrollo y operaciones [1]. Esta fusión significa alinear las prioridades de los equipos de desarrollo y equipos de operaciones para que trabajen juntos hacia un objetivo común de ejecución exitosa de proyectos cooperando en el desarrollo de software y desplegando ese software en producción [2]. DevOps posee cuatro principios principales, que son: cultura, automatización, medición y uso compartido [3].

A medida que DevOps se ha vuelto popular, las empresas de desarrollo de software adoptan practicas asociadas a DevOps. Desde las pruebas de concepto, pruebas, entornos de prueba, hasta el despliegue se requiere máxima agilidad posible y eso pasa porque en la mayoría de los equipos de desarrollo se adopta metodologías agiles para obtener mayores resultados, facilidad ante el cambio entre otros. DevOps ofrece marco para el despliegue rápido y eficiente de código a ambientes de producción, el objetivo es la agilidad y la mejora continua del software.

Por otro lado, la seguridad no es algo que muchos programas DevOps hayan incluido como parte de su proceso. La seguridad de software para muchos desarrolladores y personal de operaciones implica esfuerzos adicionales, tiempo y costo de desarrollo. Existe una incertidumbre de lograr objetivos o metas en el desarrollo ágil y el ciclo de lanzamiento cuando se habla de integrar seguridad, lo que provoca temor y dudas.

DevSecOps satisface la necesidad de seguridad en DevOps. Este concepto está diseñado para crear e incluir prácticas de seguridad que puedan incorporarse en el mundo rápido y ágil de DevOps. Promueve una extensión al objetivo de DevOps de promover la colaboración entre desarrolladores y operadores al involucrar también a expertos en seguridad desde el principio.

A. Antecedentes

El movimiento DevOps ha impulsado y logrado romper barreras dentro de las organizaciones que dividen los equipos en funciones especializadas de desarrollo y operaciones. DevOps permite que las organizaciones que adoptan el movimiento y la cultura sean más competitivas al permitir lanzamientos de software más rápidos y confiables al aprovechar la automatización para reemplazar los procesos manuales involucrados en el envío de software.

Un efecto secundario de esta velocidad es que las herramientas y procesos de seguridad deben moverse al mismo ritmo para mantenerse al día. La idea que impulsa DevSecOps, DevOpsSec o Security DevOps es realizar las pruebas de seguridad de la aplicación en desarrollo en el proceso utilizado para enviarla.

Hace algunos años la seguridad de software se centraba en la naturaleza y el origen de los ataques, así como en las medidas para prevenirlos. Sin embargo, dado a la evolución de los ataques que cada vez son más sofisticados es difícil anticipar los ataques. La incapacidad de anticipar ataques es la razón por la que surgen parches en respuesta a las nuevas vulnerabilidades de día cero. Los DevSecOps tienen el propósito de hacer un software que pueda absorber los ataques y continúe funcionando, es decir, el software debe tener la capacidad de resistir, pero no romperse, para lograr este propósito se requiere un cambio de mentalidad en la forma de enfrentar los ataques.

Para referenciar este artículo (IEEE):

[N] M. Pachacuti, «DevSecOps, Estado del Arte en el Contexto Boliviano» *Revista PGI. Investigación, Ciencia y Tecnología en Informática,* nº 7, pp. 72-75, 2020.

Según una encuesta realizada por HPE Security Fortifyteam del 2016 muestra que, si bien muchos creen que la seguridad debería ser parte de DevOps, la seguridad no es un factor importante para DevOps [4]. Gartner estima en que menos del 20% de los arquitectos de seguridad empresarial se han comprometido con sus iniciativas DevOps para incorporar de forma activa y sistemática la seguridad de la información en sus iniciativas DevOps [5].

B. Referencia teórica

1) DevOps

Es una metodología de trabajo basada en el desarrollo de código que usa nuevas herramientas y prácticas para reducir la tradicional distancia entre desarrollo y operaciones. Este nuevo enfoque de colaboración que es DevOps permite a los equipos trabajar de forma más cercana, aportando mayor agilidad al negocio y notables incrementos de productividad. Adoptando el cambio cultural que es DevOps, las empresas pueden acelerar el ciclo de vida de sus aplicaciones [5].

2) DevSecOps

DevSecOps, es una extensión de la mentalidad de DevOps a seguridad, es decir, incorporar seguridad en todo el proceso de DevOps. No existe un consenso en el campo sobre el orden de las palabras, por lo que los términos de búsqueda deben abarcar posibles permutaciones, por ejemplo: devsecops, secdevops, devopsec entre otros [6].

3) Principios DevSecOps

Los principios que caracterizan a DevSecOps se basan en los principios DevOps: cultura, automatización, medición y el compartir, pero con la adición de la seguridad desde el principio del flujo de trabajo DevOps.

a) Cultura

Una cultura DevOps promueve la colaboración entre los equipos de desarrollo y los equipos de operación, donde todos aceptan que son responsables de entregar el software a un usuario final. DevSecOps significa incluir la colaboración con el equipo de seguridad, así como promover una cultura donde las operaciones y el desarrollo también trabajen para integrar la seguridad en su trabajo. Eso significa involucrar al equipo de seguridad desde las etapas de planificación, y hacer que todos se pongan de acuerdo en que la seguridad es responsabilidad de todos [6].

b) Automatización

En DevOps, la automatización de la compilación, la implementación y las pruebas es importante para lograr un rápido desarrollo e implementación. DevSecOps también promueve un enfoque en la automatización de la seguridad, para poder mantenerse al día con la velocidad y la escala logradas por DevOps. El objetivo debe ser la automatización al 100% de los controles de seguridad, donde los controles se pueden implementar y administrar sin interferencia manual [4].

c) Medición

Las mediciones incluyen el monitoreo de métricas comerciales, como los ingresos y los indicadores clave de rendimiento, como el efecto que las nuevas versiones tienen sobre la estabilidad de un sistema, para conocer el estado actual y encontrar la forma de mejorarlo. DevSecOps promueve el uso y el desarrollo de métricas que rastrean amenazas y vulnerabilidades en todo el proceso de desarrollo de software [4]. Los controles de seguridad automáticos en todo el proceso de desarrollo de software significan que las métricas están disponibles para rastrear amenazas y vulnerabilidades en tiempo real y eso permite a la organización verificar qué tan buena es una aplicación bajo demanda [6].

d) Compartir

Los desarrolladores y operadores comparten conocimientos, herramientas de desarrollo y técnicas para gestionar el proceso. DevSecOps promueve la inclusión del equipo de seguridad en el intercambio promovido en un entorno DevOps. Al informar a los equipos de seguridad sobre los desafíos que enfrentan los operadores y desarrolladores, y viceversa, se mejorarán los procesos de seguridad que desarrollan [6].

e) Desplazar la seguridad hacia la izquierda

En el proceso tradicional de desarrollo de software, la seguridad es un paso cercano al final del proceso. DevSecOps promueve un cambio hacia la izquierda por seguridad, donde debe incluirse en cada parte del proceso de desarrollo de software. Esto significa que los equipos de seguridad están involucrados desde el primer paso de planificación y es parte de la planificación de cada iteración del ciclo de desarrollo.

4) Buenas prácticas

Las prácticas de seguridad en DevOps significan que las organizaciones deben desarrollar experiencia y procesos para descubrir, proteger y encontrar mejores soluciones a las amenazas y los riesgos, preferiblemente con anticipación [5]. Realizar evaluaciones de riesgos desde la primera etapa de planificación y continuamente antes de cada iteración es importante como una forma de priorizar los riesgos, examinar los controles ya establecidos y decidir cuáles son necesarios en el futuro.

a) Pruebas continuas

Los controles de seguridad automáticos en cada parte del proceso de desarrollo del software son importantes para garantizar la seguridad y permiten que las pruebas escaneen continuamente el código en busca de cambios, detecten continuamente anomalías y reviertan el código automáticamente cuando sea necesario.

b) Monitoreo y registro

Al automatizar los controles de seguridad a lo largo del proceso de desarrollo de software, es importante que los involucrados puedan generar evidencia a demanda de que los controles están funcionando y que son efectivos.

c) Seguridad como código

Esto significa definir políticas de seguridad, por ejemplo, pruebas de integración y configuración y acceso a la red, y escribir plantillas con guiones o archivos de configuración que se puedan implementar en el proceso de desarrollo desde el inicio del proyecto.

d) Equipo rojo y simulacros de seguridad

Para adelantarse a los posibles atacantes, los practicantes de DevSecOps crean un equipo rojo que ejecuta simulacros de seguridad en el software implementado. Tienen la tarea de encontrar y explotar vulnerabilidades en el sistema. Esto no solo ayuda a encontrar fallas de seguridad, sino que mejora las mediciones y ayuda a la organización a encontrar soluciones. El objetivo del Equipo Rojo es tener personas que nunca afirman que algo no puede suceder [6].

II. MÉTODOS

La presente investigación es de nivel exploratorio. Es retrospectivo, ya que la información analizada fue tomada de los bancos de datos de acceso abierto, ofrecidos por instituciones del sector público boliviano [7]. Se utilizaron técnicas de investigación documental y encuestas. Se elaboro una encuesta para determinar el estado actual de DevOps en Bolivia.

La investigación exploratoria, inicia el proceso investigativo, se caracteriza por ser más cualitativo que cuantitativo, con un enfoque constructivista para caracterizar los fenómenos de estudio; aquí, generalmente hacen su aparición las variables de estudio, que luego serán operativizadas en los niveles de investigación descriptivo, relacional, explicativo, predictivo y aplicativo, que le preceden en ese orden [8].

III. RESULTADOS

A. *Material bibliográfico accesible sobre el tema*

Actualmente, si bien el termino DevSecOps es relativamente nueva ya existen libros y guías sobre la seguridad en DevOps, sin embargo, aún el tema es nuevo y se ven más formas de profundizar el tema estableciendo más mecanismos de seguridad. A continuación, se formula reseña de los trabajos más relevantes y que pueden conseguirse en el medio.

1) *DevOpsSec*

Este informe muestra cómo examinar los desafíos de seguridad y cumplimiento que DevOps plantea en su organización, aprovechar las prácticas y flujos de trabajo clave de DevOps, crear seguridad como código asignando controles y controles de seguridad en los flujos de trabajo de DevOps, desarrollar el cumplimiento en DevOps y conectar las políticas de cumplimiento, las verificaciones y auditorías a la Entrega continua entre otros [5].

2) *Securing DevOps*

En este libro se enseña las técnicas esenciales para proteger sus servicios en la nube. Usando estudios de casos convincentes, le muestra cómo incorporar la seguridad en pruebas automatizadas, entrega continua y otros procesos centrales de DevOps. También enseña a identificar, evaluar y asegurar las vulnerabilidades únicas que presentan las implementaciones en la nube y las herramientas de automatización comúnmente utilizadas en las infraestructuras modernas [6].

B. *Iniciativa boliviana sobre DevSecOps*

En Bolivia el termino DevOps recién está tomando importancia. Por otro lado, las empresas del sector público todavía no tienen un proceso de desarrollo seguro. Sin embargo, de acuerdo a los lineamientos y estándares para el desarrollo de software de alta calidad para entidades del sector público se va introduciendo términos de DevOps y seguridad. Estos lineamientos han sido desarrollados por el grupo de trabajo de desarrollo de software del consejo para las tecnologías de información y comunicación del estado plurinacional de Bolivia. Aún están en proceso de aprobación por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) y el Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB), luego de su aprobación pasara a una segunda evaluación por las entidades públicas para finalmente ser publicado y todas las entidades públicas deberán cumplir con dichos lineamientos.

En estos lineamientos, dentro de la sección de despliegue continuo se habla sobre algunos procesos del flujo de trabajo de DevOps como integración continua, entrega continua y despliegue continuo. Por tanto, es importante integrar la seguridad en cada una de las fases de DevOps para lograr un desarrollo de software seguro.

C. *Cultura DevSecOps en Bolivia*

Se elaboro una encuesta de investigación para determinar el estado actual de DevOps y las prácticas de seguridad en el desarrollo de software en Bolivia. Seis instituciones públicas contestaron a la encuesta realizada. Las instituciones públicas encuestadas fueron: SEDES, INSO, AGEMED, AGETIC, COMIBOL y la Dirección de Sistemas del Ministerio de economía. Las personas que ayudaron con la encuesta fueron desarrolladores, responsables de desarrollo, personal de control de calidad de las instituciones anteriormente mencionadas.

La primera pregunta realizada fue si el área de desarrollo cuenta con algún rol de DevOps. Obteniendo como resultado que ninguna institución de las encuestadas tiene el rol DevOps. Ver Figura 1.

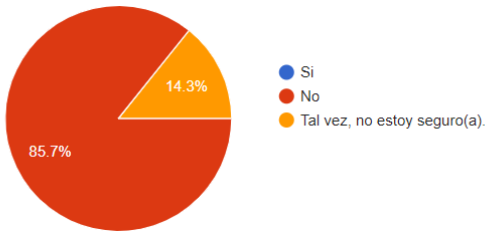

Fig. 1. Rol de DevOps en equipos de desarrollo.

En el caso de contar con DevOps, se ha preguntado si se integran principios de seguridad en el flujo de trabajo de DevOps, como la mayoría de las instituciones encuestadas no cuentan con el rol de DevOps se obtuvo como resultado que no se tiene DevOps. Ver figura 2.

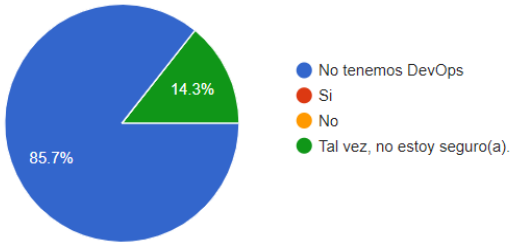

Fig. 2. Seguridad en el flujo de trabajo de DevOps

Acerca el despliegue, se ha preguntado: ¿Quién realiza el despliegue a producción? Obteniendo como resultado que los encargados de infraestructura IT y desarrolladores son los que realizan el despliegue del software a producción. Ver Figura 3.

Fig. 3. Encargado del despliegue de software a producción.

También se preguntó: ¿Cuentan con procedimientos para el control de cambios, uso de repositorios seguros, documentar cambios funcionales y de seguridad a producción?, obteniendo como resultado que, si existen procedimientos para el control de cambios, uso de repositorios seguros y documentación, lo que indica que pese a que no se cuenta con una cultura DevOps existe un flujo para el despliegue a producción que cuenta con mecanismos básicos de seguridad.

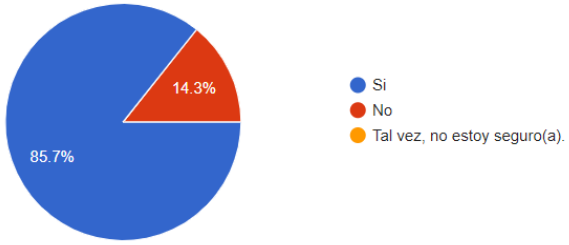

Fig. 4. Procedimientos para el despliegue

En la mayoría de las instituciones encuestadas los encargados de las pruebas de seguridad al software son los mismos desarrolladores de software lo que es preocupante por el sesgo que puede existir, lo ideal es que se cuente con un personal dedicado a las pruebas de seguridad al software.

D. Beneficios de adoptar DevSecOps

Adoptar una cultura DevSecOps en una organización será un gran desafío para los equipos de desarrollo, operaciones y seguridad, pero no por la tecnología sino por la cultura. Alcanzar una cultura de DevSecOps podría traer muchos beneficios a la hora de crear código seguro, como ser:

- Mayor velocidad y agilidad para los equipos de seguridad.
- Capacidad para responder al cambio y las necesidades rápidamente. DevSecOps permite una cultura de mejoras iterativas constantes.
- Mejor colaboración y comunicación entre los equipos de operaciones, desarrollo y seguridad.
- Más oportunidades para compilaciones automatizadas y pruebas de control de calidad.
- Identificación temprana de vulnerabilidades en el código.
- El principio de 'seguridad por diseño' se garantiza mediante el uso de la revisión de seguridad automatizada del código, las pruebas de seguridad de aplicaciones automatizadas, la educación y el empoderamiento de los desarrolladores para utilizar patrones de diseño seguros.
- La reducción de costos se logra detectando y solucionando problemas de seguridad durante las fases de desarrollo, lo que también aumenta la velocidad de entrega.

IV. Discusión

DevSecOps se ha convertido en una de las palabras de moda en el ecosistema DevOps en los últimos años. Es fácil entender qué significa DevSecOps y por qué las personas se preocupan por él, ya que es una estrategia que extiende la eficiencia de DevOps a la seguridad del software. Pero cuando se pretende implementar DevSecOps, puede transformarse en una tarea complicada. No existe un mecanismo ni fórmula para lograr DevSecOps, tampoco hay una herramienta específica que se pueda adquirir, o incluso un proceso particular a seguir. La implementación de DevSecOps requiere que se realice una evaluación amplia de sus recursos de TI existentes y procesos de DevOps, luego crear una estrategia holística que integre seguridad en todos ellos.

En Bolivia, tras los resultados encontrados podemos observar que aún falta mejorar el proceso de desarrollo de software y adoptar una cultura DevOps para un despliegue automatizado y seguro a producción.

Referencias

[1] J. Yankel C. A. Cois and A. Connell. "Modern devops: Optimizing software development through effective system interactions". 2014.

[2] Fitzgerald and K. J. Stol. “Continuous software engineering: A roadmap and agenda”. USA, 2017

[3] J. Humble and M. Joanne. “Why enterprises must adopt devops to enable continuous delivery”. 2011.

[4] Hewlett Packard Enterprise. “Application security and devops. Technical report”, 2016.

[5] Bird J., “DevOpsSec”, United States, 2016

[6] Vehent J. “Securing DevOps”, 2018

[7] Centro de gestión de incidentes informáticos, “Estadísticas de incidentes de seguridad al primer semestre 2018”, 27 de julio del 2018 , [En línea]: https://www.cgii.gob.bo/es/noticias/estadistica-de-incidentes-de-seguridad-al-primer-semestre-2018

[8] J. Supo, “Evidencia de aprendizaje en metodología de la investigación científica”, 2018, [En línea]: http://bioestadisticomasterclass.com/

Breve CV de la autora

Maribel Pachacuti Blanco es Licenciada en Informática por la Universidad Mayor de San Andrés Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoria Informática en el Postgrado en Informática UMSA. Con experiencia como QA engineer, QA automation y Project manager. Sus intereses investigativos son la ciberseguridad y seguridad informática. Email: maribel.pachacuti.blanco@gmail.com.