DevOps: optimizando el rendimiento de los entornos de TI

gmv
INNOVATING SOLUTIONS

DevOps: optimizando el rendimiento de los entornos de TI

Uno de los términos con los que nos hemos familiarizado en los últimos 10 años ha sido el de DevOps, que proviene de unir dos palabras en inglés, development y operations, lo que ya nos permite hacernos una idea de lo que esconde. Sin embargo, ¿por qué es algo que necesitan las empresas? ¿Qué beneficios ofrece? ¿Cómo puede implementarse en las organizaciones? ¿Incrementa los niveles de inseguridad? En estas páginas queremos resolver estas dudas.

A falta de una definición consensuada, podríamos decir que DevOps es una práctica de ingeniería de software que tiene como objetivo unificar el desarrollo (Dev) y la operación del software (Ops). La principal característica del movimiento DevOps es apostar por la automatización y la gestión constante en todos los pasos de la construcción del software, desde la integración, las pruebas, y la liberación, hasta la implementación y la administración de la infraestructura. DevOps apunta a ciclos de desarrollo más cortos, mayor frecuencia de implementación y lanzamientos más confiables, en estrecha alineación con los objetivos comerciales. Resumiendo, DevOps es una metodología para creación de software basada en la integración entre desarrolladores de software y administradores de sistemas, que permite crear software más rápidamente, con mayor calidad, y menor coste, así como elevada frecuencia de actualización.

¿QUÉ APORTA DEVOPS?

El término surge en la conferencia Agile'08, y se populariza desde el principio gracias a los DevOps Days que se fueron celebrando desde entonces en diferentes ciudades. Y surgió a la sombra del desarrollo de software ágil (Agile), que permitía a las empresas un desarrollo que les capacitaba para realizar actualizaciones más rápidas y frecuentes, en vez de esperar a tener grandes paquetes de actualizaciones que implementar, como se ha venido haciendo tradicionalmente.

Pero esta evolución requería cierta adaptación para poder cambiar sus procesos de gestión de versiones, introduciendo elementos como la automatización, las herramientas de integración continua, así como los procesos de control y las entregas de mejoras también de forma constante.

DevSecOps, el camino seguro hacia la transformación digital

Roberto Galán Martín, Chief Software Architect de Secure e-Solutions de GMV

La carrera por la digitalización de las empresas y las necesidades del mercado actual, demandan a la industria del desarrollo software mayor agilidad en la construcción de aplicaciones, y una reducción del "time-to-market" sin mermar en la calidad. Para alcanzar esta meta, aparte de implantar nuevas arquitecturas, infraestructuras de despliegue y herramientas, se ha demostrado que es fundamental integrar los procesos y equipos de desarrollo junto con los de operaciones, siguiendo una metodología DevOps. Las diferentes actividades que se realizan en el ámbito DevOps, como la integración continua, los controles de calidad, los despliegues automáticos, o la definición de la infraestructura como código, han permitido disminuir los riesgos que producen los cambios en el software, y reducir los tiempos de entrega y actualización.

No cabe duda de que DevOps se ha convertido en una herramienta fundamental que las compañías deben implantar para alcanzar el éxito en el contexto de la transformación digital. Sin embargo, el éxito de cualquier producto o servicio software puede verse truncado rápidamente si aparece una vulnerabilidad o brecha de seguridad que comprometa el sistema. Tómense como ejemplo la pérdida de usuarios y caída en bolsa que sufrió Facebook tras el ataque cibernético de finales de 2018, o el cierre de Google+ tras un bug que comprometió información de más de 52 millones de usuarios. Las nuevas tecnologías que aceleran la transformación digital como la nube, los contenedores, la orientación a APIs o las arquitecturas serverless añaden nuevas amenazas de seguridad que hay que tener en cuenta. La seguridad perimetral no es suficiente para combatir este crecimiento en alza de las ciberamenazas, y por ello es necesario trabajar en la seguridad desde dentro del desarrollo de las aplicaciones. En un ciclo de vida tradicional, lo más habitual es abordar la seguridad en la etapa final de implantación, delegando esta tarea en un equipo especialista de ciberseguridad que está aislado del resto de actividades del proyecto. Siguiendo esta aproximación se pierde la agilidad y rapidez conseguida con la metodología DevOps, debido a que los problemas de seguridad detectados imponen retroceder a fases tempranas del ciclo de desarrollo. La solución al problema es la misma: cambio cultural para integrar los equipos de seguridad con el resto, automatización, monitorización y procesos bien definidos. Con este nuevo planteamiento, conocido como DevSecOps, la seguridad debe ser una responsabilidad compartida por todos los miembros del equipo e integrada desde principio a fin. En las etapas iniciales debe definirse un modelo de amenazas que permita a posteriori aplicar controles, pruebas y verificaciones de seguridad de forma automática y transparente tanto en el desarrollo como en la entrega y la operativa de las aplicaciones.

En GMV siempre hemos apostado por el cumplimiento de la seguridad en el ciclo de desarrollo. Es una de nuestras señas de identidad, y por ello, a medida que hemos implantado DevOps en nuestra organización, nos hemos movido de manera natural hacia un planteamiento DevSecOps. Para nosotros la seguridad no resta agilidad sino que aporta valor en todas y cada una de las fases del ciclo de vida de un proyecto.

Los **beneficios** de DevOps abarcan todo el proceso de entrega e incluyen:

- Entrega y frecuencia de despliegue mejorada.
- Llegada más rápida al mercado, lo que reduce el Time to Market de los desarrollos, acortando los plazos entre versiones, y posibilitando un tiempo de recuperación menor en caso de que algo falle al implementarlo.
- Fiabilidad, reduciendo la tasa de errores de nuevas versiones.
- Escalabilidad.
- Colaboración mejorada, acercando el desarrollo a la operación de las aplicaciones.
- Seguridad.

Resumiendo, los procesos simples se vuelven cada vez más programables y dinámicos, utilizando un enfoque DevOps. DevOps tiene como objetivo maximizar la previsibilidad, eficiencia, seguridad y mantenimiento de los procesos operativos, algo que se ve reforzado por la automatización.

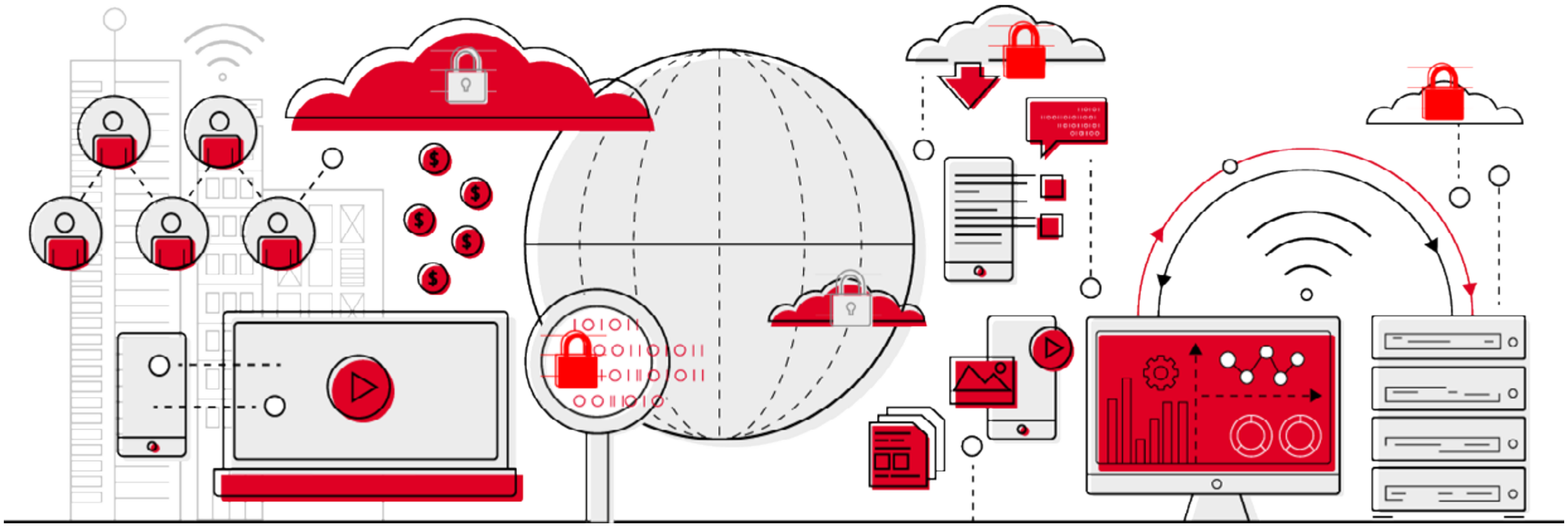
PILARES BÁSICOS DE DEVOPS

Los **4 pilares básicos** de DevOps son cultura, automatización, medición y compartición. Y pueden desglosarse en cinco ámbitos diferentes:

- Cultura y Organización
- Diseño y Arquitectura
- Construcción y Despliegue
- Operación y Monitorización
- Seguridad y Verificación

Pero pese a las ventajas comentadas, un recientes estudio, realizado en 6 países, entre los que se encuentra España, refleja que entre antes de finales de 2019 sólo un 45% de empresas han establecido o van a establecer DevOps. De éstas, son una de cada cinco las que consideran que está plenamente establecido o en fase de madurez, mientras que un 25% dice tenerlo establecido.

Algo más optimista es otro estudio publicado recientemente que señala que de cara a 2021 más del 80 por ciento de las empresas podría haber realizado una aproximación a DevOps. Este informe indica que los principales retos a los que se enfrentará esta evolución están en la parte cultural, no en la tecnológica.



Para afrontar estos retos, los responsables de TI deben aumentar sus esfuerzos en automatizar aplicaciones y procesos, así como fomentar un cambio cultural gradual con el que todos los miembros del departamento de TI puedan unirse a este cambio.

DEVOPS EN LA ESTRATEGIA DE DYNATRACE

Hace cinco años, Dynatrace desarrolló una nueva plataforma de Software Intelligence que se apoyaba en un motor de Inteligencia Artificial. Se trataba de una arquitectura basada en un agente único (OneAgent), con la automatización como elemento principal y diferenciador (despliegues, auto-descubrimiento de relaciones y dependencias, identificación de problemas y causa raíz, análisis de impacto e incluso actualizaciones automáticas...), altamente escalable en entornos Multi-Cloud (plataformas cloud, contenedores, microservicios...), y con foco en la satisfacción y experiencia de usuarios.

Así, Dynatrace ingiere e integra datos End-to-End a lo largo de la cadena de herramientas DevOps, incluyendo Continuous Integration (CI), Continuos Delivery (CD), así como métricas de las plataformas Cloud donde las aplicaciones funcionan, para automatizar la resolución de problemas y optimización del rendimiento de aplicaciones.

Dynatrace ayuda a las compañías a acelerar y optimizar procesos y aplicaciones DevOps en Cloud centrándose en las diferentes áreas de actuación:

- **MultiCloud o Cloud Híbrida.** Dynatrace permite mejorar los procesos de evaluación y definición de planes de acción (break, Shift re-platform) para la plataformas Cloud de los clientes, con el objetivo de sacar el máximo partido a los entornos Cloud.
- **Colaboración DevOps.** Se trata de un cambio de mentalidad, en primer lugar, que permita la colaboración entre Desarrollo y Operaciones. Dynatrace soporta estrategias Shift-Left, que permiten envolver conceptos relacionados con el rendimiento en etapas tempranas del desarrollo, automatizando procesos, mejorando la calidad de los ciclos de pruebas, para asegurar que las aplicaciones llegar a producción de forma madura y con código probado y analizado en detalle. Todo esto permitiendo integraciones con las herramientas utilizadas

DEVOPS: OPTIMIZANDO EL RENDIMIENTO DE LOS ENTORNOS DE TI

por los desarrolladores (Jenkins, Eclipse, JUnit, Ansible, Chef, Selenium...)

❖ **Shift-Right y Self-Healing.** Utilizando Dynatrace para realizar una monitorización integral y Full-Stack en entornos productivos, integrándose incluso con otras tecnologías, con el fin de una vez detectados los problemas y su causa raíz de forma automática por nuestro motor de Inteligencia Artificial, se permite, incluso, definir sincronizaciones y resoluciones automáticas para conseguir un MTTR mucho más rápido, reduciendo así el riesgo para operaciones, Negocio y los usuarios finales.

❖ **Webscale y Production grade.** La idea es utilizar la plataforma Dynatrace, junto con las integraciones y sincronizaciones mencionadas anteriormente, con el objetivo final de convertir los tradicionales NOC en sistemas totalmente automatizados, sin un cuadro de mandos impulsado por el motor de IA de Dynatrace, con el objetivo de ir del mundo DevOps al mundo NoOps.

DEVOPS EN LA ESTRATEGIA DE GMV

Dentro de la propuesta de ayuda a la Transformación Digital de las empresas, GMV trabaja con Dynatrace de diferentes maneras. Una de ellas, y quizá la más evidente, es monitorizando el propio ecosistema para analizar problemas de rendimiento y cuellos de botella, de modo que podamos garantizar a nuestros equipos de desarrollo una plataforma robusta sobre la que trabajar.

La segunda es incorporando Dynatrace como un nodo más en el pipeline automatizado de despliegue, analizando el comportamiento de entornos pre-productivos y aportando feedback real de usuarios durante la fase de operación. Con todo esto, se integran datos de monitorización valiosos para el desarrollo, y se diseñan testeos E2E basados en uso real de las plataformas monitorizadas.

Todo esto, sin olvidar la seguridad, dado que como señalan desde la propia compañía, "la seguridad es el aspecto más importante, ya que está en nuestro ADN, y por eso queremos focalizar nuestra propuesta también en este pilar básico, no solo en la automatización o la monitorización".

De hecho, de la integración de DevOps con una aproximación con la seguridad en mente, surge el término de DevSecOps.

La seguridad efectiva de DevOps precisa no sólo de nuevas herramientas, sino de cambios culturales para integrar la seguridad lo antes posible en estos flujos de trabajo.

En el caso de la propuesta de GMV, además de un análisis estático del código fuente, se analizan los potenciales riesgos de seguridad en la fase de desarrollo, con buenas prácticas de desarrollo seguro, escaneo estático de seguridad como parte de la integración continua, escáner de vulnerabilidades para con-

Optimizando el rendimiento de los entornos TI

Las soluciones que aporta GMV en este terreno para la Transformación Digital son:

❖ <u>Soporte del ciclo de vida de las aplicaciones</u>. Soluciones que unifican el desarrollo y las operaciones para acelerar la innovación empresarial y satisfacer las demandas del cliente:

➔ DEV: Integración dentro del ecosistema de software. Herramienta QA dando soporte a pruebas automáticas, de carga…

➔ OPS: Monitorización Full Stack y de experiencia de usuario durante la fase de explotación.

❖ <u>Optimización de aplicaciones:</u> Se detectan, diagnostican y solucionan los problemas de rendimiento así como de disponibilidad de aplicaciones:

➔ Soporte (experto arquitecto): Informes periódicos de análisis de rendimiento de aplicaciones.

➔ Asistencia 24x7.

❖ <u>Misión crítica (training):</u> Se detecta y diagnostica la causa raíz de un problema de rendimiento:

➔ Implantación y Consultoría.

➔ Respuesta a problemas.

tenedores, modelado de amenazas en base a la arquitectura definida para la aplicación, test de intrusión en entornos previos, o automatización de la configuración de la infraestructura y estandarización de los entornos, entre otros aspectos. Asimismo, también estas prácticas afectan a la fase de operación del entorno productivo, con automatización de la instalación de parches de seguridad, cifrado de conexiones y mecanismos de autenticación y autorización centralizados, seguridad perimetral, auditorias, o hacking ético, por poner algunos ejemplos.

EL FUTURO DE DEVOPS, DE LA MANO DE DYNATRACE

Una vez consolidada la plataforma, Dynatrace trabaja en una metodología que permita transformar la forma en la que software se entrega y gestiona, denominada Autonomous Cloud Management (ACM). Esta metodología busca que Desarrollo pueda crear software de calidad mucho más rápido, que Operaciones se oriente a una automatización completa, y que Negocio tenga una orientación completa en sus clientes.

Para ello, han definido esta metodología alrededor de su plataforma para ofrecer un camino integrado en sus procesos de Transformación Digital, contemplando aspectos como:

❖ **Monitoring as a Service:** una monitorización como Servicio para tener una visibilidad completa de las aplicaciones, procesos e infraestructuras.

❖ **Performance as a Service:** incorporando Dynatrace como herramienta de monitorización en fases de desarrollo y pruebas.

❖ **Unbreakable Pipeline:** construyendo un ciclo continuo de innovación de las aplicaciones, con despliegues mucho más rápidos, colaboración entre equipos, integración con procesos CI/CD, resolución rápida de problemas en producción...

❖ **Self-Healing:** con definición de guías para mecanismos de solución automáticos en base a los problemas identificados por la plataforma Dynatrace y su motor de Inteligencia Artificial.

Pero, además, y según se pudo ver en el reciente Perform Summit que la firma celebró en Barcelona, en los próximos meses puede llegar a la plataforma de la compañía:

✱ **Dynatrace Cloud Application Security:** extendiendo las capacidades de OneAgent en el mundo de la seguridad para ayudar en la inmunización de código, prevención de ataques, análisis de vulnerabilidades y fraude.

✱ **Dynatrace Apps:** permitiendo a los clientes/partners de Dynatrace el desarrollo de aplicaciones de negocio directamente sobre la plataforma, en base a llamadas a funciones gestionadas por Dynatrace (FaaS, Function as a Service) e incluyendo la monitorización de dichas llamadas en la propia plataforma. ■

MÁS INFORMACIÓN

- GMV
- GMV en Dynatrace Perform Madrid
- AIOps done right
- 5 key considerations for Enterprise Cloud Monitoring
- Captura íntegramente la experiencia de tus clientes
- Monitorización de microservicios y contenedores
- Dynatrace software intelligence for the enterprise cloud