Deloitte. Insights

EDICIÓN DEL 10º ANIVERSARIO

Tendencias tecnológicas 2019

Más allá de la frontera digital.

DeVSecOps y el imperativo cibernético.

Págs. 102 -117

DeVSecOps y el imperativo cibernético

Elevar, incrustar, y evolucionar su respuesta frente al riesgo

PARA MEJORAR SUS ENFOQUES ANTE EL RIESGO CIBERNÉTICO Y OTROS RIESGOS, las organizaciones de pensamiento prospectivo están incrustando seguridad, privacidad, política, y controles, en su cultura, procesos, y herramientas de DevOps. En la medida en que DevSecOps gane impulso, más compañías probablemente harán que la automatización de la modelación de amenaza, la valoración del riesgo, y la seguridad de la tarea sean componentes fundamentales de las iniciativas de desarrollo de producto, desde generación de ideas hasta la iteración para lanzar y hasta operaciones. DevSecOps de manera fundamental transforma la administración cibernética y del riesgo desde ser actividades basadas-en-cumplimiento – típicamente realizadas más tarde en el ciclo de vida del desarrollo. Por otra parte, DevSecOps codifica las políticas y las mejores prácticas en las herramientas y plataformas subyacentes, permitiendo que la seguridad se convierta en una responsabilidad compartida de toda la organización de TI.

Las tácticas y herramientas de DevOps están cambiando dramáticamente la manera como las organizaciones de TI innovan. Y en medio de esta transformación, los líderes de TI están encontrando que los enfoques de larga data para la integración de la seguridad en productos nuevos no están siguiendo el ritmo del desarrollo de software de alta velocidad, entrega continua. Además, en la arena de DevOps, las técnicas tradicionales de seguridad "atornilladas" y los controles manuales en que han confiado las prácticas heredadas a menudo son percibidas como impedimentos para velocidad, transparencia, y la efectividad general de la seguridad.

En una tendencia creciente, algunas compañías han comenzado a incrustar la cultura, las prácticas y las herramientas de la seguridad en cada fase la secuencia de sus DevOps, un enfoque conocido como *DevSecOps*. Desplegado estratégicamente, DevSecOps puede ayudar a mejorar los niveles de seguridad y madurez del cumplimiento en la secuencia de DevOps de una compañía, al tiempo que impulsan la calidad y la productividad y reducen el tiempo-al-mercado. ¿Cómo? Las herramientas de automatización ejecutan tareas uniforme y consistentemente, mientras que los humanos usando controles manuales pueden y cometen errores. Al mismo tiempo, con DevSecOps, el flujo de la aplicación cambia libremente a través de las secuencias de DevOps, dándoles a los desarrolladores más autonomía y autoridad sin comprometer la seguridad o elevar el riesgo.

Para estar claros, DevSecOps es una evolución de la cultura y el pensamiento de DevOps. Más que generar disrupción en su agenda cibernética actual, incrusta en sus plataformas y cadenas de herramientas

subyacentes, muchos de los procesos, capacidades e inteligencia de seguridad aprendidos con los años. Construida en su experiencia de desarrollar y aplicar operaciones, DevSecOps permite a usted automatizar las buenas prácticas de seguridad cibernética en su cadena de herramientas de manera que sean utilizadas consistentemente.

La tendencia de *DevSecOps* solamente está comenzando a tomar impulso. Para su *2018 DevOps Pulse Report*, Logz.uo encuestó más de 1,000 profesionales de TI de todo el mundo acerca del estado de DevOps en sus industrias. Aproximadamente el 24 por ciento de quienes respondieron señaló que sus organizaciones de TI estaban practicando algunos elementos de DevSecOps. El otro 76 por ciento dijo que sus organizaciones ya sea no practican DevSecOps o todavía están en el proceso de implementación.[1]

Construida en su experiencia de desarrollar y aplicar operaciones, DevSecOps permite a usted automatizar las buenas prácticas de seguridad cibernética en su cadena de herramientas de manera que sean utilizadas consistentemente.

Notablemente, el 71 por ciento de quienes respondieron sintió que sus equipos actualmente carecen del conocimiento adecuado del trabajo de las prácticas de DevSecOps.[2] Durante los próximos 18 a 24 meses, esperan que el conocimiento de trabajo crezca marcadamente en la medida en que más CIO y líderes del desarrollo exploren las oportunidades de DevSecOps. De igual manera, quienes tienen en funcionamiento programas más avanzados de DevOps pueden comenzar a implementar el gobierno, maximizar la automatización, y realizar entrenamiento cruzado de especialistas tanto en DevOps como en seguridad cibernética, con nuevos procesos y herramientas.

El valor fundamental de DevOps es la velocidad al mercado.[3] Las organizaciones que no incorporen seguridad en cada fase de sus secuencias de desarrollo y operaciones corren el riesgo de dejar mucho de su valor en la mesa. Cada producto que usted levante debe ser una entidad conocida – probada, segura, y confiable. Los usuarios internos y externos no tienen que perder tiempo lidiando con sorpresas cibernéticas, y tampoco usted.

Es tiempo de dejar de jugar con la seguridad el juego de la administración de parches.

En una mentalidad de DevSecOps

Aun cuando las organizaciones de TI comenzaron en la última década a acoger las prácticas del desarrollo ágil, luchas continuaron enfocando los problemas de seguridad de la misma manera incremental, por silos, que tenían en cascada.[4] Construido en un enfoque ágil, basado-en-equipo, para el desarrollo, DevOps ahora está orientando incrementos dramáticos en la velocidad de principio-a-fin. Aun con su fuerte dependencia de los procesos heredados y los controles manuales, la seguridad permanece siendo un desafío. En muchas secuencias de DevOps, la seguridad todavía es tratada como atornillada, más que como una característica de diseño. Esto puede crear cuellos de botella en la secuencia, en parte porque pocos desarrolladores y operadores del sistema tienen experticia cibernética y aún más, muy pocos especialistas poseen un entendimiento profundo de desarrollo y operaciones. Como resultado, los equipos de DevOps y los especialistas cibernéticos continúan trabajando por separado en la secuencia, a menudo haciendo que el progreso sea lento.

De manera creciente, los CIO y los líderes de DevOps entienden que a menos que esos grupos trabajen como un equipo unificado para hornear la seguridad en los productos a través de los ciclos de desarrollo y operaciones, sus compañías pueden nunca realizar la promesa plena de DevOps.[5]

DevSecOps no es una tendencia de seguridad en y por sí misma sino, más aún, un aspecto de la revolución continua de DevOps que *Tech Trends* ha realizado la crónica en ediciones pasadas.[6] También es más una mentalidad que un conjunto formal de reglas y

herramientas. DevSecOps les ofrece a las compañías practicar DevOps como una *manera diferente de pensar acerca de la seguridad*. Considere las siguientes características de DevSecOps, y cómo difieren de la manera como usted está enfocando la seguridad en su secuencia de desarrollo hoy:

- **Colaboración abierta en objetivos compartidos.** DevSecOps crea expectativas y métricas compartidas para la medición del éxito. Alinea los arquitectos de la seguridad y centra las actividades con base en las prioridades del negocio.
- **Seguridad en la fuente.** DevSecOps destaca capacidades de seguridad consumibles, de auto-servicio, establece barandillas de seguridad, y hace posible que los equipos monitoreen los resultados y proporcionen retroalimentación específica. Puede encontrar vulnerabilidades cibernéticas temprano en el ciclo de desarrollo de la aplicación, reduciendo la necesidad de reproceso justo antes o después del despliegue.
- **Refuerza y eleva mediante automatización.** Mediante la automatización de tareas recurrentes, DevSecOps hace posible orquestar un flujo integrado de los procesos, insertar controles operacionales preventivos, y crear rastras continuas de auditoría.
- **Operaciones orientadas-al-riesgo y perspectivas que se pueden llevar a la acción**. Las organizaciones que incorporan DevSecOps en sus secuencias de desarrollo pueden utilizar perspectivas operacionales e inteligencia de amenazas para orientar el flujo de los procesos, la priorización, y las recomendaciones de remediación. Ya no se tienen que basar solamente en exploraciones del código y pueden tomar un enfoque más basado-en-el-riesgo para la prueba.
- **Enfoque holístico para los objetivos de seguridad**. Las estructuras integradas ayudan a asegurar tanto la secuencia como la aplicación. Esto ayuda a crear un entorno más comprensivo, de defensa de principio-a-fin a través de la producción.
- **Monitoreo proactivo y retroalimentación recursiva**. La prueba continua, automatizada, ayuda a identificar problemas antes que surjan. Los desarrolladores también pueden aprovechar el inicio de sesiones y la telemetría para orientar el aprendizaje y la innovación.
- **Seguridad automatizada de las operaciones**. Dado que la visibilidad en algunos aspectos de la seguridad de las operaciones puede ser limitada, los CIO que vigilan las auditorías de la seguridad a menudo se han encontrado a sí mismos en una posición de tener que *asumir* (esperanza) que varios administradores de seguridad han realizado sus trabajos de la manera correcta. La seguridad-como-código puede ofrecer un enfoque más efectivo. Nuevas técnicas en contenedorización y automatización de la infraestructura de la nube pública ahora hacen posible auditar la seguridad y el cumplimiento en las operaciones confiable y consistentemente, con menos esfuerzo.
- **Ingeniería de las operaciones**. Con menos humanos como parte del lazo, el proceso de detectar una intrusión y actuar puede conllevar horas preciosas e incluso días. Sin embargo, en entornos seguros de infraestructura-como-código en contenedores o en entornos públicos nube/contenedorizados, las capacidades diseñadas de respuesta pueden automática e instantáneamente redirigir el tráfico, congelar nodos para inspección posterior, notificar operadores, y girar casos frescos – todo ello automáticamente.

Tomados juntos, esos elementos de DevSecOps pueden ayudar a mejorar la calidad general de la seguridad, impulsar la productividad, y reducir los problemas de cumplimiento. Muy importante, pueden romper el cuello de botella que la seguridad tradicional crea en entornos de desarrollo de velocidad alta, desencadenando entonces el potencial pleno de DevOps.

DevSecOps en cuatro partes

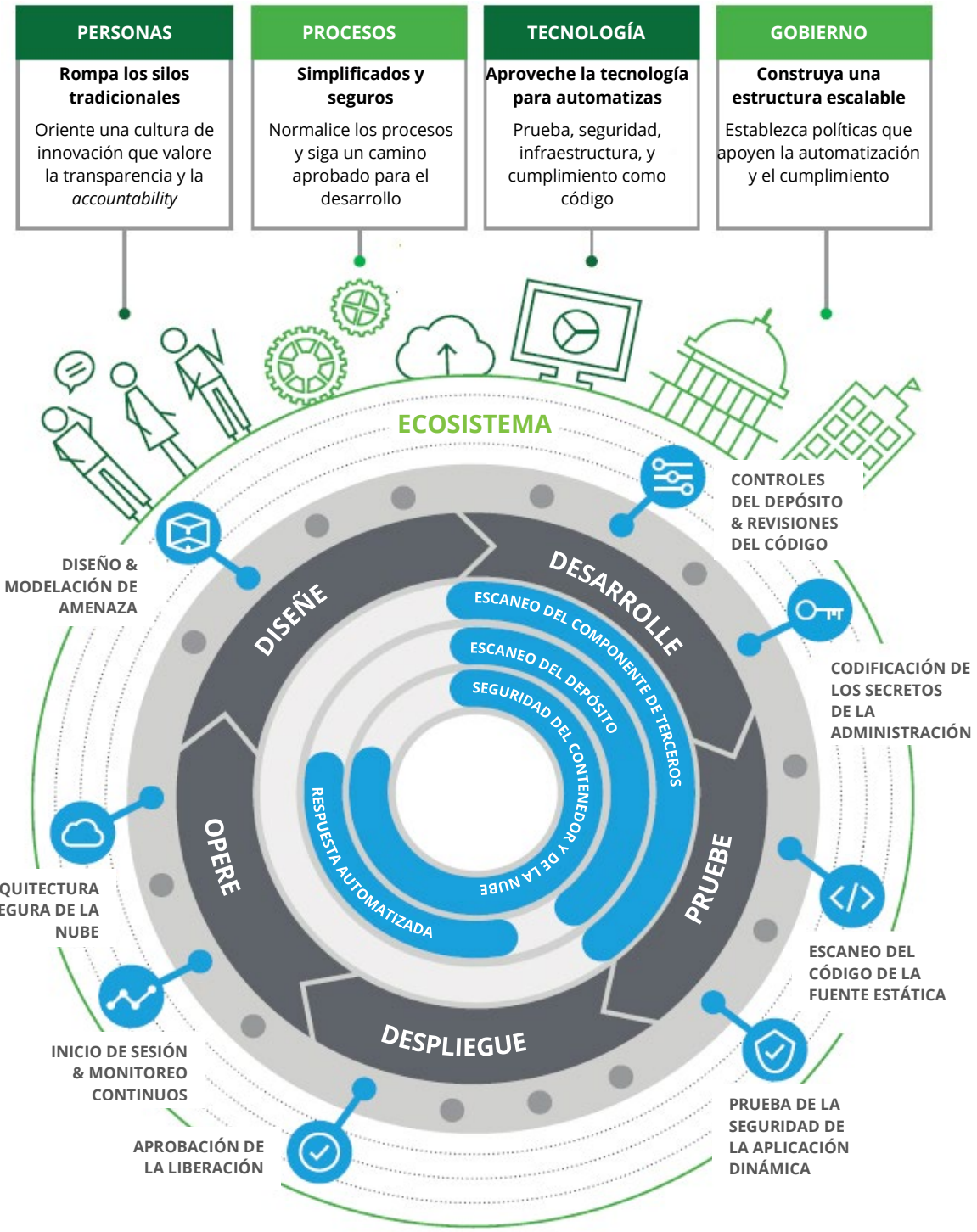
DecSecOps incorpora cultura, prácticas, y herramientas de seguridad para orientar visibilidad, colaboración, y agilidad en cada fase de la secuencia de DevOps. Si bien las compañías pueden personalizar sus enfoques de seguridad para respaldar sus propias agendas cibernéticas y sus propias necesidades de producto, las iniciativas de DevSecOps típicamente recaen en cuatro pilares fundamentales:

- **Personas.** Cuando usted integre la seguridad en su secuencia de DevOps, recuerde que las personas son todavía su mayor activo de eficiencia (o ineficiencia). En el modelo tradicional de cascada, los equipos de

FIGURA 1

¿Qué es DevSecOps?

Es un cambio transformacional que incorpora cultura, prácticas, y herramientas **seguras** en cada fase del proceso de DevOps.



Fuente: Análisis de Deloitte.

desarrollo, seguridad, y operaciones trabajan por silos. En la medida en que usted se mueva en el mundo de DevOps, los equipos todavía pueden operar de esa manera por un momento; romper esas barreras tradicionales puede ser la primera y más importante catálisis para su camino de DevSecOps. Intente identificar y remediar esos silos rápidamente, cree metas compartidas en los equipos de DevSecOps, y oriente una cultura de innovación que consista en apertura, transparencia, propiedad, y *accountability*. Si bien la jerarquía del recurso humano puede permanecer separada, la cultura de desarrollo debe estar basada-en-el-producto y por consiguiente liderada por los *equipos del producto*. Cada parte responsable (dev, sec, opc) posee una porción del éxito del producto.

Un sub-producto positivo de DevSecOps es que los especialistas en seguridad cibernética a menudo desarrollan un mayor entendimiento de las presiones del desarrollo y por consiguiente orientan la automatización final de las funciones de seguridad.

También es importante comenzar pequeño. Los equipos pequeños gradualmente se cohesionan; si son exitosos, más y más equipos de producto pueden comenzar la auto-adopción de las prácticas de DevSecOps a través de la empresa. En la medida en que usted escale DevSecOps, los equipos de producto probablemente se volverán aún más auto-suficientes, identificarán sus propios desafíos de seguridad, y automáticamente corregirán el curso para beneficio de la entrega segura del producto. Un sub-producto positivo de DevSecOps es que los especialistas en seguridad cibernética a menudo desarrollan un mayor entendimiento de las presiones del desarrollo y por consiguiente orientan la automatización final de las funciones de seguridad. De igual manera, los equipos de desarrollo con un entendimiento más profundo de los enfoques de seguridad cibernética probablemente pueden adoptar prácticas seguras de codificación. El resultado neto en ambos casos es eficiencia incrementada.

- **Procesos.** Tenga en mente que velocidad y calidad son clave para DevSecOps, intente simplificar los procesos manuales tanto como sea posible sin sacrificar las necesidades de la seguridad cibernética. Dado que el desarrollo y el despliegue ahora son acelerados mucho más rápido que antes, los procesos de desarrollo de seguridad del software deben volverse más como-fábrica. De otra manera, los esfuerzos para acelerar exponencialmente desarrollos seguros del software pueden ser insostenibles.

  Considere crear procesos normalizados de desarrollo que sigan enfoques consistentes. Aquí es donde el concepto del proceso de seguridad de "cambiar-a-la-izquierda" se vuelve importante.[7] Por ejemplo, intente incorporar el pensamiento del diseño para entender las necesidades de seguridad de los clientes. Implemente guiones gráficos para la modelación de amenazas en los cambios del software para construir capacidad de recuperación cibernética en la aplicación incluso antes que se escriba la primera línea de código. E incorpore escaneo incremental del código estático en el entorno integrado de desarrollo antes que la aplicación sea empaquetada. Si, la mentalidad de cambiar-a-la-izquierda tiene un poco más de esfuerzo extra por delante, pero puede ayudar a prevenir muchas más violaciones esperando que ocurra – y una cantidad de reproceso del producto. En una palabra, considere inmediatamente sus requerimientos de seguridad cibernética e intente moverlos tan pronto como se pueda en la etapa de diseño, intentando eliminar más tardes las demoras del "guardián" de la seguridad manual.

- **Tecnología.** La introducción de DevOps ha creado una plétora de soluciones basadas-en-la-nube que los equipos de desarrollo están usando para acelerar la entrega. Afortunadamente, el software de seguridad cibernética ahora está comenzando a mantener el ritmo. Por ejemplo, la secuencia clasificada de herramientas – prueba-como-código, cumplimiento-como-código, y otras – pueden eliminar la necesidad de algunas actividades manuales de seguridad, impulsando por lo tanto la velocidad. Cuando herramientas tales como esas son implementadas en los procesos correctos, los equipos de desarrollo y seguridad pueden unificarse más, los costos de defectos pueden caer en picada, y la calidad puede volverse consistente a través de la secuencia. Considere asumir un enfoque incremental para el despliegue de la tecnología, probando esas nuevas herramientas de seguridad con equipos específicos de producto antes de liberarlas para la empresa.
- **Gobierno.** El término *gobierno* es amplio por diseño, pero hay dos tipos de pensamiento acerca del gobierno de la seguridad cibernética en el mundo de DevSecOps:

    - **A nivel micro (el mundo que se resuelve alrededor de los equipos del producto).** Incrustar la seguridad cibernética en DevOps puede impulsar la eficiencia en el gobierno. ¿Cómo? DevSecOps, por diseño, requiere un proceso altamente consistente que usa un conjunto uniforme de herramientas y controles automatizados. Esto ayuda a simplificar el monitoreo y la prueba de los controles requeridos. De hecho, mediante diseñar procesos de DevSecOps para ajustar las necesidades de los equipos de cumplimiento y control, usted puede ser capaz de gradualmente automatizar los procesos de prueba y liberar recursos del desarrollador. El proceso de sacar una lista de tiquetes, seleccionar muestras, e identificar todos los rastros de auditoría relevantes provenientes de múltiples sistemas puede haber tomado *días* del tiempo del desarrollador. Usando cumplimiento-como-código, ello se puede lograr en minutos.

    - **A nivel macro.** DevOps ha transformado cómo las organizaciones de TI trabajan. En algunas compañías, las operaciones de TI – que tradicionalmente comprenden una mezcla de administración senior, administración, e ingenieros – se está moviendo hacia una jerarquía más plana conformada por pocas posiciones de administración apoyadas por arquitectos e ingenieros. Al mismo tiempo, han crecido las sanciones por operar entornos de TI insuficientemente gobernados. Esto significa que el gobierno general del panorama de TI *proyectado* es más importante que nunca antes. El éxito de la marca de su compañía crecientemente depende de productos desarrollados usando DevOps.

Al igual que cualquier otro programa de TI, DevSecOps debe estar directamente vinculada con su estrategia más amplia de TI – la cual, a su vez, debe estar orientada por su estrategia de negocios. Si el programa de DevOps apoya sus estrategias de TI y de negocios, entonces al mismo tiempo incruste la “Sec.” En corto plazo, puede ayudarle a reforzar su postura de madurez cibernética y ahorrarle tener que reprocesar más tarde su programa de DevOps cuando sea mucho más difícil hacerlo.

LECCIONES DE LAS LÍNEAS DEL FRENTE

NADA PARA ESTORNUDAR: NIAID PRIORIZA EL CAMBIO DE CULTURA EN SU TRANSFORMACIÓN DE DEVSECCOPS

LECCIÓN UNO

El National Institute of Allergy and Infectious Diseases (NIAISD) trabaja para mantenernos seguros a todos mediante dirigir y apoyar investigación para prevenir enfermedades infecciosas, inmunológicas, y alérgicas. En NIAID, la organización de TI está trabajando para la "prueba de futuro" de sí misma y proporciona apoyo oportuno y seguro a los investigadores y al personal que dirigen proyectos de investigación claves. Si bien la agencia ha usado Dev Ops para asegurar la entrega más rápida de sus soluciones de software, necesita proteger datos sensibles de salud, lo cual ha resultado en una visión para la seguridad automatizada en todos los lugares y llevó a DevSecOps – el siguiente paso lógico para DevOps-

"Pienso de DevSecOps como las tres patas de un taburete: prácticas de administración, prácticas tecnológicas, y prácticas culturales," dice Joe Croghan, jefe de la marca de ingeniería de software de NIAIS.[8] "La parte cultural es la más desafiante: usted les pide a los equipos transparencia, que admitan equivocaciones, y que cambien continuamente; puede ser mucho para las personas poner sus brazos alrededor." Croghan considera que el cambio es vital para asegurar la productividad continuada de cara al cambio rápido, y que ello ha permitido que su equipo continúe respondiendo rápidamente a las solicitudes de productos seguros.

Los ciclos largos de liberación de software estuvieron causando cuellos de botella en la entrega de soluciones de tecnología en NIAID, combinados con los desafíos existentes del panorama rápidamente cambiante de la seguridad. La implementación de prácticas de DevOps – integración continua y entrega continua, prueba automatizada, e infraestructura-como-código – ha ayudado a reducir el tiempo de espera para la entrega de software y para el parcheo de defectos críticos. Las prácticas de infraestructura-como-código reducen las vulnerabilidades mediante hacer que se puedan inspeccionar algunos aspectos de la seguridad tales como configuraciones de la aplicación y del servidor. E integrar herramientas de escaneo de la seguridad tales como Fortify en la secuencia de DevSecOps detiene que las vulnerabilidades de la codificación lleguen a producción en primer lugar.

"Los desafíos que siempre hemos tenido con la seguridad son consistencia, previsibilidad, y poner las políticas de seguridad en una estructura sistemática," dice Croghan. "Mediante la implementación del enfoque de DevSecOps, podemos realizar y poner en funcionamiento protocolos de seguridad consistentes, específicos. Cuando estamos usando esas técnicas, podemos estar muy confiados en que nuestros servidores lo estarán, y si hay un problema, podemos ajustarlo consistentemente mediante cambiar el código."

En el próximo año, Croghan espera abordar algunos de los cambios culturales y de administración que son cruciales para sostener el impulso de DevSecOps que tiene el equipo. El personal y los clientes ahora ven el valor del nuevo enfoque y les ha gustado la aplicación del nuevo despliegue de la aplicación, con el equipo de ingeniería de software completando en un mes más de 250 despliegues automatizados. Pero Croghan aspira a cambiar la cultura y mucho más. "Pienso que dentro de un año continuaremos adoptando nuevas metodologías," dice, "pero necesitamos cambiar la manera como trabajamos. La cultura de DevSecOps es continuamente medir, reevaluar, y cambiar." Esos cambios incluyen la alineación de comportamientos mediante la educación de su personal en la entrega de código seguro dentro de la estructura de DevSecOps y exceder las expectativas de sus clientes respecto de entrega, seguridad, velocidad del software.

LOS SUEÑOS DE LA SECUENCIA DE LA FDA

LECCIÓN DOS

Seguridad y protección radican en el corazón de cada cosa que hace la US Food and Drug Administration. Cada día, los 17,500 empleados de la agencia trabajan diligentemente para asegurar la seguridad y la eficacia del suministro de alimentos de los Estados Unidos, farmacéuticos, dispositivos médicos, cosméticos, y más. En medio de los recientes pedidos para que la agencia acelere el proceso mediante el cual se dan las aprobaciones, los equipos de la agencia están trabajando para lograr el balance correcto entre velocidad y seguridad.

Dado lo crítico de esta misión, la FDA necesita respaldar con velocidad la seguridad, privacidad, y estabilidad de sus sistemas de TI. Para este fin, el Center for Biologics Evaluation and Research (CBER) ha lanzado una ambiciosa iniciativa de DevSecOps para hacer reingeniería de su enfoque para la seguridad a través del proceso de desarrollo del producto. Si bien el proyecto todavía está en las primeras etapas, sus metas son claras: 1) construir en seguridad por adelantado, más que tratarla después de los hechos, 2) automatizar tanto como sea posible, y 3) transformar la cultura de desarrollo de la agencia en una que enfatice agilidad y velocidad.

De acuerdo con el gerente senior del proyecto de TI Christopher Kiem, DevSecOps representa una oportunidad importante para conseguir que todos trabajen en la misma página desde el comienzo de cada proyecto. "En el día uno, queremos que el talento de nuestras operaciones proporcione perspectivas y orientación sobre seguridad para nuestros desarrolladores en lo que esperamos se convertirá en un lazo de conversación continua en la cual todos están aprendiendo unos de otros," dice.

Este lazo del proyecto también incluirá inputs provenientes de las herramientas de automatización de la seguridad. Una herramienta estática de análisis de código escaneará el código fuente por problemas de seguridad. Los escáneres de aplicación revisarán los archivos de librería de fuente abierta por problemas de seguridad. A partir de la detección de problemas, todas esas herramientas abrirán problemas para que los desarrolladores y los ingenieros de DevSecOps valoren y resuelvan.

Esas y otras herramientas de DevSecOps facilitarán el proceso general de desarrollo y acelerarán la secuencia. "Cuando los gerentes de proyecto vienen con nuevos requerimientos del sistema, ya estarán en funcionamiento las herramientas, los procesos, y la automatización críticos para el desarrollo," dice Kiem. "Esto hará posible que los gerentes de proyecto tomen decisiones rápidamente. Nuestra meta es eliminar las reuniones, correos electrónicos, y las idas-y-vueltas que frenan a las personas.

Actualmente, el CBER está realizando una modernización del análisis para identificar las diferentes piezas y partes – estándares de datos, reglas regulatorias, tipos de presentación, *stakeholders*, entre otros –para incluirlos en un plan de juego formal. Este plan también identificará los elementos de DevOps ya en funcionamiento que puedan ser aprovechados. En los próximos meses, el liderazgo de TI de CBER presentará el plan a la administración del Center para solicitar su input y asegurar su patrocinio. "Una vez que tengamos respaldo para el proyecto, comenzaremos a valorar nuestras necesidades de tecnología y a desarrollar planes para poner una secuencia en funcionamiento," dice Kiem. "También estaremos trabajando estrechamente con los socios de TI de nuestra empresa para diseñar la arquitectura de DevSecOps que llene cualesquiera brechas de infraestructura y respalde nuestras prioridades."

Las prioridades a las cuales Kiem se refiere no están limitadas a desarrollo de software y seguridad mejorada del producto. Demás, con DevSecOps él ve una oportunidad tangencial para hacer reingeniería de sistemas centrales y, al hacerlo, mantener los costos de la agencia bajo control. "Pienso que, a través de los sectores público y privado, hay oportunidades para disminuir el desembolso en TI. Cuando usted hace reingeniería de los procesos de desarrollo para mejorar seguridad y calidad, usted puede usar esta oportunidad para consolidar la huella de su tecnología. Cuando las cosas están zumbando a lo largo de una secuencia bien desarrollado y usted está liberando los productos que sus usuarios quieren, usted ya no debe necesitar sus menos seguros sistemas heredados, los conjuntos masivos de herramientas, y el tiempo requerido para poder deshacerse de todas esas cosas – y de los costos relacionados con ellas."[9]

MI PARTE

ADAM BANKS, DIRECTOR DE TECNOLOGÍA E INFORMACIÓN JEFE Y DIRECTOR DIGITAL JEFE, MAERSK

Maersk, al igual que muchas otras organizaciones industriales, se ha vuelto digitalmente dependiente – por eficiencia operacional y como el orientador en nuevos productos, ofertas, y mercados. Maersk siempre ha sido un negocio prospectivo, pero hoy tenemos un centro de atención fortalecido en parte a causa de un ciberataque global en 2017 que infectó nuestra red a través de puertos y oficinas y a través de docenas de países. Como parte de la recuperación, reconstruimos nuestra capacidad central de TI, incluyendo la reconstrucción de la infraestructura de servidor y red, moviendo más de 60,000 dispositivos a un nuevo estándar común, desplegando actualizaciones globales del sistema de operación, restaurando toda nuestra pila de aplicaciones, y re-estableciendo la terminal más automatizada del mundo, todo ello en asunto de semanas. Ahora tenemos uno de los entornos más estandarizados de cualquier compañía en la industria – un fundamento que nos permite entregar cambio al ritmo de los negocios digitales.

Dado el siempre cambiante panorama cibernético, estamos construyendo una infraestructura aún más segura y confiable que pueda respaldar el crecimiento futuro de Maersk. Nos estamos centrando en cadenas de herramientas automatizadas, construyendo procesos de escaneo relevantes estáticos y dinámicos en nuestros procesos continuos de integración y despliegue. Hemos adoptado monitoreo posterior-al-despliegue a través de la producción, y hemos podido avanzar desde escribir una línea de costo hasta desplegarla en producción sin contacto humano. Ello presenta algunos desafíos interesantes a través de la organización: ¿Cuándo usted libera un producto? Con tal agitación rápida y cambiante, ¿en qué punto declara usted que es una versión nueva? Actualmente, estamos gastando una buena cantidad de tiempo explorando esos conceptos, haciendo que DevSecOps sea un área central de interés.

Les hemos pedido a nuestros CISO que identifiquen las brechas que tenemos en nuestra infraestructura, así como también los controles de compensación disponibles para abordar esas brechas. Una de las principales cosas que hemos hecho en los últimos dos años es mover el gobierno del riesgo desde una función corporativa central hacia una función del CISO, de manera que el CISO elabore la política y también haga forzoso su cumplimiento. Yo espero que ellos derriben la puerta donde haya un área del negocio que "no tenga riesgo alguno," porque ello no es posible. Los CISO trabajan con los propietarios de negocio para tomar decisiones deliberadas, y los propietarios de negocio pueden decidir cómo abordar los riesgos existentes cuando estén contenidos en su geografía funcional. Es un enfoque de consulta, pero consulta con dientes.

Para ese fin, nuestro CISO puede no ser un miembro permanente, pero no hay reunión trimestral del comité de auditoría donde no esté en la agenda. En nuestra junta de supervisión, cada uno actualiza al otro que tenga algún tema cibernético asociado con él. Nosotros le mostramos a la junta un diagrama concentrado que represente el número de ataques en la superficie externa, las penetraciones, todos los incidentes, y luego los incidentes importamos – no les mostramos lo que estamos haciendo, sino más aún, demostramos que nuestros procesos están funcionando. Queremos que ellos entiendan que, si los ataques de superficie externa vienen de 200 a 800 por semana, deben estar haciéndonos preguntas; si ven un incremento en los que están penetrando, queremos un diálogo acerca de cómo seguir el desmarcado. Queremos que los no-tecnólogos, así como también los líderes de TI, entiendan que hay un nivel mínimo de control y capacidad de recuperación que debe estar en funcionamiento si y cuando nosotros fallamos en detener un futuro ataque. Con su apoyo, podemos controlar la cantidad del daño hecho y la velocidad de nuestra recuperación.

En este entorno, no pienso que sea un enfoque de cualquiera/o cuando se trate del desarrollo tradicional de cascada, DevOps, cadenas de herramientas integradas, y entrega ágil. Nosotros todavía organizamos nuestras personas según las estructuras tradicionales de planee-construya-opere, con sedes funcionales organizadas alrededor de las capacidades de tecnología o del ciclo de vida de TI. Esto les permite a todas las áreas del negocio ganar a partir de los mejoramientos en cualquier área, a través de todas las actividades. Sin una sede funcional

a la cual las personas vuelvan, usted constantemente está agitando personas y procesos, lo cual significa que usted está fallando en mejorarlos cada vez. Por ejemplo, yo no quiero que cada uno de mis equipos globales resuelvan la prueba automatizada de regresión.

De manera que implementamos un centro de excelencia que les proporciona a los miembros de equipo las herramientas, el pensamiento, y los modelos que necesitan para completar sus tareas. Este modelo nos ha permitido incrementar en madurez y capacidad, al tiempo que desplegamos aplicaciones de una manera más moderna, diversa.

Sin embargo, este modelo solo funciona si todos quienes están alrededor de la mesa de liderazgo entienden el valor inherente contenido en la organización de tecnología. Maersk es un negocio digital, y somos incapaces de operar si la tecnología no funciona correctamente, de manera que los líderes de nuestro negocio necesitan entender lo que está en juego. Yo sabía lo que habíamos logrado en Maersk cuando propuse una reducción del presupuesto de tecnología y mis pares argumentaron contra ello, temiendo que perdiéramos demasiado valor. Yo pienso que ese el objetivo que todos estamos intentando lograr: entendimiento completo de cómo seguridad y DevSecOps pueden impactar los resultados de negocio.

Mi meta es tener alguien en la mesa ejecutiva capaz de liderar la función de tecnología en pocos años. Esto reflejaría que las operaciones y la pila de la tecnología subyacente se han estabilizado, y que los líderes de negocio tienen suficiente comprensión de la tecnología para dar el paso y liderar el cargo. Pero la prueba real será si se esfuerzan en tomar roles en los cuales las responsabilidades de facilitación de la tecnología sean tan reconocidas y tan importantes como liderar las ventas o una línea del negocio. Estamos bien en nuestro camino.

MI PARTE

WES HUMMEL, VP DE INGENIERIA DE LA CONFIABILIDAD DEL SITIO, PAYPAL

Para PayPal, con más de 254 millones de tenedores de cuentas activos y cerca de 7.5 billones de transacciones de pago en 2017, seguridad y confianza son centrales para todo lo que hacemos y lo que nuestros clientes esperan. Como tal, tratamos la seguridad como una prioridad estratégica de negocios y una parte fundamental de cómo desarrollamos, liberamos, y mantenemos nuestro código de producto, integrándolo por defecto en cada nivel, a través de todo el ciclo de vida del desarrollo.

Para mí, DevSecOps significa no solo empoderar a nuestros desarrolladores con las herramientas necesarias para desarrollar software seguro, de alta calidad, sino también crear una cultura que construya productos seguros por defecto. Con nuestra compañía, nuestra base de clientes, y nuestro volumen de transacciones creciendo tan rápido, necesitamos seguridad a escala: a partir de 2017, PayPal tenía 4,500 desarrolladores, 50 millones de líneas de código, 1 millón construidas por mes, 2,600 aplicaciones, nueve zonas de disponibilidad, 230 billones de golpes, y 42,000 ejecuciones de lote por día. Nosotros les dimos a los desarrolladores tanto control como fuera posible sobre su código y sus resultados para ayudarles a lograr esta escala. Cuando usted les ofrece a los desarrolladores flexibilidad y autonomía, es importante construir una base de talento que viva y respire su mantra de seguridad. Hemos trabajado para crear una cultura en la cual los desarrolladores entiendan que los productos exitosos requieren una apreciación igual de desarrollo, seguridad, y operaciones. Esta ha sido nuestro camino: satisfacer necesidades de seguridad, disponibilidad, y calidad al tiempo que facilitamos liberaciones de código a velocidad alta.

Al inicio de nuestro camino hemos adoptado una metodología ágil, y actualmente estamos haciendo la transición hacia DevSecOps. Intentamos encontrar un balance entre desarrollo y operaciones mediante proporcionar las herramientas que hagan que cada paso – desde generación de ideas hasta liberación del código – carezca de fricción para los desarrolladores. Nosotros los empoderamos con la libertad de usar nuestro conjunto recomendado de herramientas, el "camino opinado," que incluye prueba de seguridad de penetración, controles de seguridad auto-facilitados, modelación de amenaza, escaneo automatizado, y otras características. Pero también consideramos que los desarrolladores no deben ser forzados a usar un conjunto específico de herramientas, de manera que les damos autonomía para seguir un camino sin-opinión y llevarlo a nuestra pila. Nosotros proporcionamos las herramientas y los procesos que necesitan para desplegar código al tiempo que satisfacen nuestros estándares de seguridad, disponibilidad, y calidad. Esta manera de trabajar según una estructura de DevSecOps está resultando en mejores desempeño y productividad para nuestros desarrolladores. También estamos viendo una reducción en las potenciales vulnerabilidades y mejoramientos en el mantenimiento de nuestros estándares de seguridad del producto – un resultado de arraigar pensamiento y procesos basados-en-riesgo dentro de la secuencia de DevOps.

Nuestro principal centro de atención ahora es levantar una flota autónoma de herramientas de desarrollo, operaciones, y seguridad que podamos mantener virtualmente libres de manos. Hay tremendo valor en ser capaces de operar escáneres y pruebas de principio-a-fin sobre una base de minuto-por-minuto, desplegar parches a través de la automatización, identificar potenciales vulnerabilidades a intervalos regulares, y asegurar que las aplicaciones están satisfaciendo los estándares, incluyendo los cambios de configuración o las actualizaciones de la interfaz del vendedor en producción. La automatización de esos procesos es clave para escalar una flota de más de 200,000 nodos con velocidad y consistencia al tiempo que tiene todos los despliegues y desarrollos con los mismos estándares de seguridad y calidad.

La automatización de nuestra seguridad y de nuestro cumplimiento también han sido útiles en áreas relacionadas. Nuestro centro de atención puesto en la automatización ha hecho más fácil abordar las complejidades de las obligaciones y políticas legales y de cumplimiento, dado que operamos en más de 200 mercados globales. Con la naturaleza de nuestro negocio, la seguridad y la confianza permanecerán siendo una capacidad central y una prioridad para PayPal. No importa el tamaño de la compañía en la cual usted esté – si usted construye seguridad en su núcleo, servirá bien a sus negocios.

¿ESTÁ USTED PREPARADO?

Incrustar seguridad en la secuencia de DevOps inicialmente puede parecer una propuesta sencilla. Después de todo, si DevSecOps es solo una manera de pensar acerca de seguridad, entonces desplegarla en su fábrica de DevOps debe ser un ascenso suave, ¿cierto? Quizás para los pocos que tienen maestría plena en DevOps. Para todos los demás – y ello incluye la mayoría de las organizaciones – desarrollar prácticas de DevSecOps probablemente será otro componente en las iniciativas de DevOps que todavía están en etapas tempranas. Por ejemplo, en su *2018 Global Developer Report*, GitLab encuestó cerca de 5,300 profesionales de TI acerca de sus experiencias con DevOps. El treinta y cinco por ciento de quienes respondieron dijo que la cultura DevOps en sus compañías estaba "de alguna manera establecida." Solo el 23 por ciento de los encuestados iría más lejos para describir su método de desarrollo como DevOps.[10]

Cuando usted explore oportunidades de DevSecOps, hágase a usted mismo las siguientes preguntas no solo acerca de seguridad sino acerca de cómo ellas pueden afectar sus esfuerzos actuales de DevOps.

- **¿Tendré que contratar desarrolladores con experticia en seguridad?**

  No necesariamente. Primero, trabaje para convertir en código el conocimiento combinado del experto en seguridad y del desarrollar. Luego, mejorar las habilidades del talento existente puede ser la única opción viable para el personal en la medida en que la tendencia de *DevSecOps* progrese, pero permite que usted retenga importante conocimiento del negocio ganado durante los años desde cada área respectiva. Además, los desarrolladores con experticia en seguridad (y viceversa) ahora están en alta demanda y crecientemente son difíciles de reclutar (y mantener).[11]

- **¿DevSecOps haría que mi secuencia vaya más despacio?**

  Probablemente no. Concedido, si usted no tenía controles de seguridad antes para DevSecOps, siempre habrá algún intercambio de eficiencia, pero DevSecOps proporciona dos beneficios importantes de eficiencia: 1) La incorporación de seguridad en la secuencia de DevSecOps resultará en una secuencia más rápida que el método de cascada, y 2) DevSecOps consigue tiempo más rápido cuando se mueve adelante porque las vulnerabilidades son mitigadas con el tiempo y la eficiencia se incrementa. Los desarrolladores también gradualmente ganan más libertad y autonomía para avanzar el producto a través de la secuencia a causa de controles automatizados.

- **¿Puede DevSecOps ser compatible con mi requerimiento de cumplimiento?**

  Sí – si algo, ayuda a facilitar la carga del mantenimiento del cumplimiento. En un estado ideal de DevSecOps, seguridad, auditoría, monitoreo, y notificación están plenamente automatizados y monitoreados continuamente, mejorando el cumplimiento.

Mi proceso DevOps todavía es inmaduro. ¿Cómo puedo asegurar que mi gobierno de DevSecOps es escalable?

Planee, elabore guiones gráficos, y comience pequeño. Los modelos sostenibles y escalables de gobierno de DevSecOps típicamente caracterizan los siguientes componentes:

- Roles y responsabilidades claramente definidos en todos los equipos *multifuncionales.*
- Políticas y procedimientos específicos de DevSecOps que permiten que las organizaciones mantengan el ritmo del desarrollo de la aplicación en un entorno de DevOps.
- Herramientas automatizadas de seguridad a través de la secuencia que reducen vulnerabilidades y hacen que sea menor la frecuencia del error humano
- Sistemas de monitoreo y notificación de la seguridad en DevSecOps que crean rastros de auditoría automatizados a través del ciclo de vida de desarrollo del software – lo cual, a su vez, facilita la presentación de reportes de cumplimiento
- Monitoreo continuo de métricas de seguridad, lo cual ayuda a que los equipos de DevOps constantemente mejores su toma de decisiones de seguridad

LÍNEA DE RESULTADOS

La necesidad siempre creciente de llevar productos de calidad fuera de la puerta más rápido ha elevado las prácticas de DevOps a la posibilidad de tenerlas en la arena del desarrollo de software. En una extensión natural de la evolución de DevOps, la tendencia DevSecOps ofrece a los CIO y a sus equipos de desarrollo una nueva mezcla de herramientas, prácticas, y automatización que, desplegadas en concierto, pueden ayudar a asegurar el desarrollo y las operaciones.

Autores

VIKRAM KUNCHALA es directivo de la práctica Cyber Risk Services de Deloitte & Touche LLP y líder de la solución US Application Security. Con cerca de 21 años en diseño e implementación de soluciones de seguridad y programas de administración del riesgo cibernético, tiene experiencia en seguridad de aplicación, identidad y administración de acceso, y administración de amenaza y vulnerabilidad cibernética. Kunchala tiene amplia experiencia ayudando a que organizaciones técnicas y de negocio logren objetivos estratégicos y tácticos. También lidera la práctica de Travel, Hospitality, and Leisure Cyber Risk, de Deloitte.

KIRAN NORTON es directivo de la práctica Cyber Risk Services de Deloitte & Touche LLP y tiene más de 20 años de experiencia de industria. También lidera la oferta de infraestructura de seguridad, de Deloitte, donde les ayuda a clientes a transformar sus enfoques tradicionales de seguridad en orden a permitir transformación digital, modernización de la cadena de suministro, velocidad al mercado, reducción de costos, y otras prioridades del negocio.

MICHELLE SHUTTLEWORTH es directora administrativa del grupo Methods & Tools de Deloitte Consulting LLP. Es responsable por consistencia, confiabilidad, y eficiencia en la entrega global de servicio al cliente mediante métodos y herramientas innovadores. Shuttleworh se vinculó a Deloitte Consulting LLP en 1997 luego de comenzar su carrera en la industria minorista. Exitosamente ha liderado muchas implementaciones grandes de tecnología centrándose en transformación mediante tecnología y administración del cambio organizacional.

DYLAN HACK es gerente senior de Cyber Risk Services de Deloitte & Touche LLP. Tiene 20 años de experiencia en administración de proyectos de seguridad cibernética con clientes globales centrándose en ciencias de la vida. Hack lidera implementaciones de DevSecOps, lo cual incluye selección de herramientas, endurecimiento de la secuencia, e incorporación de prácticas seguras de desarrollo de software. Fuera de DevSecOps, ha tenido varios roles, incluyendo programación, administración de sistemas, planeación de la continuidad del negocio, cumplimiento, y auditoría.

CONTRIBUYENTES SENIOR

Arti Balakrishnan
Director
Deloitte MCS Limited

Alex Cacchi
Senior manager
Deloitte LLP

Doug Scheinder
Managing director
Deloitte Consulting LLP

Will Rockfall
Partner
Deloitte LLP

Notas finales

[1] Logz.io, "The 2018 DevOps pulse," 2018.

[2] Ibid.

[3] DevOps Research and Assessment, *Accelerate: 2018 State of DevOps,* August 29, 2018.

[4] Mark White et al., *Right-speed IT*, Deloitte University Press, February 24, 2016.

[5] Warwick Ashford, "Firms need to move from DevOps to DevSecOps, says expert," *Computer Weekly,* March 20, 2018.

[6] Ayan Chatterjee and Alejandro Danylyszyn, *Real-time DevOps,* Deloitte University Press, February 21, 2014.

[7] Chris Riley, "The how and why of shift-left security," Twistlock, May 31, 2017.

[8] Interview with Joe Croghan, chief of NIAID's software engineering branch, November 14, 2018.

[9] Interview with Christopher Kiem, senior IT project manager, US Food and Drug Administration, November 19, 2018.

[10] GitLab, "2018 global developer report," March 7, 2018.

[11] Ashford, "Firms need to move from DevOps to DevSecOps, says expert."

Documento original:
Chapter: ***DeVSecOps and the cyber imperative. Elevating, embedding, and evolving your risk response*** – Pgs. 102 – 116.
On: ***Tech Trends 2019. Beyond the digital frontier -*** Deloitte Insights, January 2019.
https://www2.deloitte.com/insights/us/en/focus/tech-trends/2019/embedding-security-devops-pipelines-devsecops.html.
Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.