ágoraSIC Centro de Conocimiento en Ciberseguridad

Revolución SecDevOps

Así están cambiando las reglas del juego

Amazon, Google, BBVA o Microsoft, entre otras, ponen en marcha miles de aplicaciones cada año. Y lo hacen de forma continua y automatizada bajo el concepto 'DevOps'. El problema es que no todas las empresas incorporan en este proceso la ciberseguridad, lo que provoca pérdidas millonarias por materialización de amenazas o por intentar a posteriori gestionar las vulnerabilidades en el código y, por ende, en los procesos de negocio. La más reciente 'víctima' de este tipo de fallos de seguridad ha sido Alphabet que cerrará su red social Google+ tras detectar un error de programación que podría haber dado acceso a datos de miles de usuarios desde 2015. Equifax, Sony o Uber… también forman parte de una larga lista conocida de compañías con vulnerabilidades en sus aplicaciones y que han sido objeto de notable alcance mediático por la importancia de los incidentes. Para evitarlo se está abriendo camino una cultura colaborativa, bautizada como SecDevOps, que supone integrar la seguridad en los equipos de desarrollo y operaciones (DevOps), aplicando la protección 'por defecto' y automatizando todo tipo de test desde el principio. Como dice Gartner: "DevOps es bueno, SecDevOps es mejor". En las páginas de este especial, SIC se adentra en sus interioridades.

Por **José Manuel Vera**

SUMARIO

* Es posible obtener una versión en pdf de este especial rellenando el formulario disponible en www.revistasic.com

1 El poder de las aplicaciones (y cómo SecDevOps está cambiando el mundo)

Automatizar los análisis de seguridad, crear cultura entre desarrolladores, equipos de negocio y hacer que la protección esté 'por defecto', desde que se idea una aplicación hasta que se despliega, es el objetivo del concepto SecDevOps. No es una 'bala de plata' de la seguridad, pero las empresas que lo usan parchean vulnerabilidades en horas o días... y las ponen en funcionamiento con un 50% menos de problemas de seguridad. Amazon WS, Apple, Microsoft, Nexflix, BBVA, Grupo Santander, Telefónica, Inditex o Microsoft son algunas de las empresas que ya han apostado por ella. Se trata de la siguiente ola 'ciber' para hacer seguras, automatizándolo todo, millones aplicaciones que conectan a personas, empresas y dispositivos. Supone un cambio cultural que permite ver la seguridad como una mejora continua, en vez de un freno permanente. Muchos de los referentes mundiales explican aquí cómo empezar...

En cada minuto, en el mundo, se usan millones de aplicaciones para comprar, reservar hoteles y restaurantes, controlar el coche, gestionar empresas (y atender a miles de clientes 'a un click') o, simplemente, acceder a gigantescos videoclubs virtuales. Las aplicaciones se han convertido en la llave de acceso a un mundo lleno de tecnología pero también en la mejor 'tarjeta de visita' de bancos, marcas de ropa, firmas de automóviles, aseguradoras, servicios de ocio... En 2017 se crearon hasta un 380% más y tuvieron 175.000 millones de descargas. Se calcula que, para 2020, este mercado moverá cerca de 165.000 millones de euros.

Y solo es el principio porque no hay sector que pueda escapar a la fiebre digital de relacionarse con el cliente y gestionar los procesos de una compañía a través de aplicaciones. Es lo que tiene un mundo hiperconectado. Pero ello también supone que, sin importar lo que se fabrique o se ofrezca, todas las empresas, por encima de cualquier cosa, son compañías de software y por eso su objetivo es desarrollar y poner en marcha cada año, en tiempo récord, cientos e, incluso, miles de aplicaciones y mejoras.

Se trata de una carrera frenética que ya lideran las compañías del 'Top 10' mundial en cada campo: Google, Microsoft, IBM, Netflix, BBVA o Inditex y que marcará la diferencia entre los ganadores y perdedores en pocos años –el llamado 'Kodak'–. El reto es ofrecer más y mejores aplicaciones que la competencia y eliminar en ellas cualquier tecnología que no aporte valor. "Las empresas más innovadoras y punteras son capaces de desarrollar y desplegar aplicaciones hasta 200 veces más rápido que sus competidores y las nativas digitales tienen hasta ocho veces más oportunidades de triunfar", explica el Responsable de AppDev de **Red Hat**, **Miguel Ángel Díaz**.

Por eso, tanto los consejos de administración como los CEO, presionan cada día a los responsables de TI para poner en marcha todo tipo de aplicaciones, en muchos casos, "sin priorizar la seguridad", recuerda **Swapnil Deshmukh,** Experto en Seguridad de Aplicaciones de **Visa.** Así, se calcula que el 80% de los riesgos ciber-

Un viaje por la seguridad de las aplicaciones...

Todo empezó con el modelo en cascada

Por los años 50 del siglo XX nació la metodología en cascada como un avance crucial a la hora de sistematizar la producción de software. Funcionaba muy bien (y lo sigue haciendo para algunos tipos de aplicaciones), sobre todo en proyectos grandes con una elevada carga en la especificación de requisitos que no varía con el tiempo (es el caso habitual en la industria militar, del espacio y, posteriormente, de la banca). Durante unos 40 años el desarrollo en cascada fue casi un estándar a nivel empresarial; en aquellos momentos la seguridad simplemente no era parte de la ecuación.

Pero llegó la necesidad de hacerlo todo más rápido...

A finales de los años 90, nació la 'metodología Ágil' de desarrollo. Se centraba en resolver la rigidez del modelo en cascada cuando la especificación de requisitos era incompleta. Comenzó a usar un modelo de desarrollo iterativo, que era más eficiente a la hora de gestionar los requisitos cambiantes necesarios para optimizar el *time to market* de un producto o servicio. Sin embargo, el desarrollo ágil quedaba limitado por la velocidad del equipo de operaciones a la hora de desplegar y gestionar los artefactos en los diferentes entornos.

Nace el concepto DevOps

El movimiento DevOps surge como una solución a este problema, unificando la cultura de desarrollo –Dev– con la de operaciones –Ops– y fomentando la automatización y la autonomía entre ambos equipos. Además, las aplicaciones ya no vivían únicamente en los CPDs de los clientes: la ubicuidad y la autoprovisión de los servicios también eran empujados por la democratización del *cloud computing*.

Pero ¿era seguro?

Como casi siempre, la seguridad se fue incorporando a remolque. Insertarla en una metodología en cascada era más o menos fácil. Al principio se añadió al final del proceso, como unas pruebas que tenían lugar cuando la aplicación llegaba a producción. Por entonces, se seguía confiando únicamente en los dispositivos de seguridad perimetrales (cortafuegos y sistemas de prevención de intrusos) para proteger las aplicaciones. Con Internet y la interconectividad este modelo fue cada vez menos sostenible, ya que la seguridad era un proceso caro y poco eficiente.

Empujando la seguridad a la izquierda (el principio)

Uno de los primeros intentos para hacerlo fue adelantar las pruebas de seguridad al entorno de preproduc-

néticos para una empresa ya vienen de sus aplicaciones. Pero no es un problema nuevo: en 2003, el conocido criptógrafo, **Bruce Schneier**, alertó de que "el mercado, a menudo, premia el software de baja calidad, apostando más porque sea funcional y se comercialice lo antes posible que por su calidad o seguridad".

En este maratón en el que se ha convertido la transformación digital los responsables de la seguridad de la información, los CISO, ven como, con reducidos presupuestos y equipos mínimos, tienen que hacer seguras miles de aplicaciones que han sido concebidas sin pensar en ello."Se están contratando ejércitos de desarrolladores de software y consumiendo cantidades sin precedentes de componentes de código abierto para automatizar y optimizar todo el ciclo de vida del desarrollo del software", explica el director ejecutivo de **Sonatype**, **Wayne Jackson.**

Qué aporta DevOps... y porqué se integra Sec

Para lograr esta entrega contra reloj, DevOps se ha convertido desde hace una década en uno de los términos de moda. Se trata de un cambio cultural que aglutina los conceptos anglosajones de DEVelopment–desarrollo– y OPerationS –operaciones–. La idea es romper los departamentos estancos y crear una cultura colaborativa entre equipos de desarrollo y operaciones de TI que permita acelerar el desarrollo y el despliegue de cualquier proyecto. Su éxito es tal que las empresas que lo han puesto en marcha aseguran ser capaces de desplegar aplicaciones o modificarlas 46 veces más rápido que su competencia, con una tasa de fallos hasta cinco veces menor, según explica el

Lo han dicho...

"Dame seis horas para cortar un árbol y pasaré las primeras cuatro afilando el hacha". Abraham Lincoln (sobre la necesidad de hacer bien las cosas desde cero)

"Apueste por el rendimiento de todo el sistema y nunca pase un defecto al siguiente paso". Gene Kim, The Phoenix Proyect

"Las empresas deciden dónde y cómo invertir en seguridad cibernética basándose en una evaluación de coste-beneficio pero, en última instancia, son las responsables de la protección de sus datos y sistemas". Estrategia de Ciberseguridad Nacional de Reino Unido, 2016-2021

"Lo mejor es enemigo de lo bien hecho". Voltaire

"La gente está anclada a incentivos a corto plazo sin tener una visión de las grandes transformaciones que están viviéndose". Sacha Labourey, CEO, CloudBees (sobre por qué no todos adoptan DevOps y SevDevOps)

"Esta es mi regla de oro: por cada 1.000 líneas de código, de media, hay un error en código. Por cada 20 errores de código, al menos, uno es una vulnerabilidad de seguridad. Por cada 10 vulnerabilidades, al menos, una se puede explotar". J. **Wolfgang Goerlich,** Vicepresidente de Programas Estratégicos, CBI (sobre el problema de no aportar seguridad a DevOps)

"DevOpsSec, SecDevOps, DevSecOps... son lo mismo: la integración de las prácticas de seguridad con DevOps. Podría decirse que DevOps incorpora, por defecto, la seguridad con control de calidad (QA) en el desarrollo y las operaciones; lo que está claro es que 'Sec', la seguridad, siempre debe estar presente". Comunidad DecSecOps

"Explora la forma de aplicar la inteligencia artificial y la automatización para mejorar el trabajo de las personas... y no como una forma de reemplazarlas". David W. Cearley, vicepresidente y Gartner Fellow en Gartner Research

"Con demasiada frecuencia abordamos las pruebas de seguridad al final del proceso de entrega. Ello supone descubrir problemas importantes, costosos y difíciles de solucionar tras el desarrollo. Una situación que se podría evitar si los expertos en seguridad hubieran trabajado con los equipos de entrega... durante el proceso de entrega". Jeremy Foote, asesor administrativo de ECS Security

"Los equipos de DevOps están entregando aplicaciones a una velocidad que los de seguridad no pueden cubrir cada día. Con DevSecOps, al ser 'dueños' del problema de seguridad, los equipos de DevOps son más autosuficientes y capaces de ofrecer productos robustos a gran velocidad". Jeremy Foote, asesor administrativo de ECS Security

"El coste medio de un fallo de seguridad, por aplicación, ronda los 40.000 euros mientras que la mayor brecha de seguridad detectada ha supuesto más de 3,5 millones de euros". Revista Business Matters, 2016

"La automatización de los procesos de seguridad en DevOps permite que decubrir fallos importantes, durante el desarrollo, incluidos los de arquitectura, no sean costosos y difícil de solucionar después". Puppet Estado de DevOps Report 2016

"Solo necesitamos tener suerte una vez. Vosotros necesitáis tener suerte siempre". El **IRA** a Margaret Tatcher, tras un atentado fallido.

ción. Seguridad solía trabajar en ese momento, antes de dar el visto bueno para el pase a producción de una aplicación. Con la llegada de las metodologías ágiles y DevOps este modelo también se fue quedando caduco. El número de aplicaciones crecía a un ritmo muy elevado y el equipo de seguridad no podía revisarlas todas. Así que acabó convirtiéndose en el cuello de botella del proceso ágil. El, a veces, llamado "departamento del no". Además, el foco de los atacantes se había centrado en la capa de aplicación, tras ver que era rentable el coste/beneficio a la hora de robar información.

Llega DevSecOps

En este contexto nace el movimiento DevSecOps. El creador del concepto fue un analista de la consultora **Gartner**, **Neil MacDonald**, que en un artículo de 2012, da nombre a la necesidad de crear cultura de seguridad en DevOps. Se trataba de ofrecer una iniciativa para intentar empujar la seguridad más a la izquierda dentro del proceso de desarrollo de una forma escalable (mucha gente usa SecDev–Ops, pero quizá sea más precisa la forma anglosajona, DevSecOps, ya que refleja mejor el papel de la seguridad como un 'punto de unión' entre el desarrollo y las operaciones).

El objetivo es sacar las herramientas de seguridad del equipo de seguridad para ponerlas en manos de los desarrolladores y de operaciones. Y para ello es necesario crear el cambio cultural inculcando la seguridad como un indicador más de la calidad del software. Y para reducir su dependencia del equipo de seguridad hay que confiar en una estrategia de automatización y autonomía. Por eso, ahora, muchos equipos están intentando incorporar las pruebas de seguridad en sus ciclos de integración continua. Sin embargo, las herramientas de análisis estático (SAST) y dinámico (DAST) no son suficientes para detectar errores de diseño en las aplicaciones.

Estos fallos, en promedio, constituyen algo más del 50% de los fallos de seguridad detectados cuando una aplicación llega a producción, y suelen ser los más caros de corregir. Por eso, durante los últimos años, muchos equipos de seguridad están intentando llevar la seguridad hacia la fase de diseño, sirviéndose del modelado de amenazas, una herramienta que puede ayudar mucho en este proceso. Se centra en usar abstracciones para ayudar a pensar y evaluar los riesgos de forma efectiva. Te permite definir una estrategia de seguridad dentro del ciclo de desarrollo que sea compatible con tu 'apetito al riesgo'. Y ser SecDevOps por defecto.

Jorge Esperón
Arquitecto de Seguridad
Continuum Security

estudio **'Estado de DevOps en 2017'** de **Dora** y **Puppet.** Gracias a ello, en 2011, Amazon aseguraba ser capaz de realizar actualizaciones y mejores en miles de aplicaciones… en un solo día.

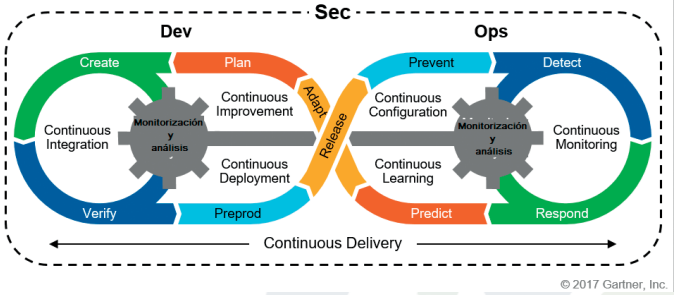
Confiar en las máquinas lo que no puede ver la persona

Gracias a la automatización de procesos se pueden detectar errores más rápido, en cualquier fase del ciclo de vida de un proyecto y solucionarlos antes de su puesta en funcionamiento. "Ninguna persona puede ofrecer la seguridad que una máquina corriendo, por ejemplo, código inseguro", destaca **Fran Ramírez**, coautor del libro **'Docker: SecDevOps'**. Con ello se gana tiempo y se evitan pérdidas millonarias para corregir problemas que se podrían haber evitado desde el diseño. Curiosamente, se calcula que más del 20% de las compañías desconocen si el código fuente de sus aplicaciones es seguro o si ha sido vulnerado.

Por eso, a DevOps se sumó, en 2012, el concepto 'Sec' –SecDevOps o DevSecOps, su acepción anglosajona–,que supone integrar la cultura de la seguridad en las buenas prácticas y metodologías de desarrollo y operaciones. Y se hace con dos enfoques. Por un lado el que considera la seguridad como código (Security as Code, SaC), implementando la seguridad en las herramientas del flujo DevOps. Se trata de priorizar la automatización sobre los procesos manuales, por lo que se basa en software de análisis estático, que analiza los cambios en partes concretas del código en lugar de explorarlo por completo. Y por otro, el que ve la infraestructura como código (Infraestructure as Code, IaC), por lo que utiliza el conjunto de herramientas DevOps para configurar y actualizar los componentes más básicos de forma rápida y automática.

El concepto SecDevops va ligado a desarrollo Agile, a ser capaces de ser más rápidos que los demás en pasar del concepto a la implantación y ello obliga a interrelacionar los departamentos de desarrollo, operaciones y seguridad. Algo complejo pero vital para el negocio. La razón es sencilla: los fallos de seguridad son detectados durante el desarrollo y se corrigen de forma rápida. Así se consiguen aplicaciones robustas en semanas o días cuando antes se tardaban meses y semanas en parchear vulnerabilidades o defectos de código inseguros. Amazon realiza más de 50 millones de cambios al año en sus aplicaciones y en cada uno de ellos invierte minutos, horas… un tiempo mínimo en comparación con la forma de trabajo clásica en la que se corrigen al cabo de uno o varios días.

Así se integra la seguridad en el proceso DevOps

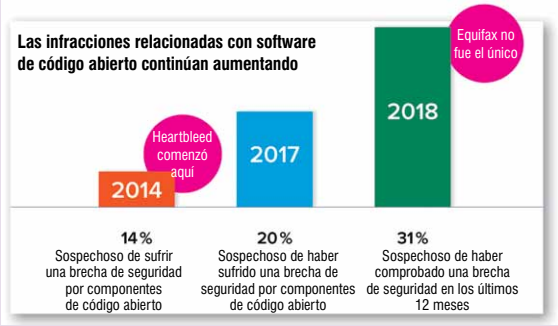


¿Qué papel juegan CIOs y CISOS en SecDevOps?

El CIO es el nexo entre negocio, gobierno y arquitectura. El concepto de SecDevOps intenta evitar gastar dinero 'en grapas' para remediar problemas de seguridad al usar la aplicación... que se podían haber detectado en el desarrollo. "Es un error pensar en SecDevOps como un trabajo extra para el responsable de seguridad. La seguridad debe ser el trabajo de todos y cuando esto es así… da menos trabajo. Eso sí, es importante tener claro que si esta no está implementada directamente en el ciclo de desarrollo de software puede suponer un retardo a la hora de desplegarlo. Por eso es importante tener un programa de 'campeones de seguridad' –líderes formados– que desarrollen una labor 'táctica' en cada nivel. Ello permitirá a los desarrolladores comprender más sobre los riesgos que supone no hacerlo de forma segura", explica **Peter Chestna**, de **CA Technologies**. "Si se implementa una cultura SecDevOps el CISO comprobará que las alertas por problemas de seguridad descenderán, ya que ésta se habrá desplazado' hacia la izquierda', hacia los desarrolladores. Pero esto es un proceso que lleva tiempo", añade.

"La influencia que un CISO o CIO tiene sobre la introducción de la seguridad en DevOps depende de cada compañía, pero estamos descubriendo que los desarrolladores tienen más influencia de lo que la mayoría de la gente piensa. Una razón es porque tienen sus manos en los teclados y seleccionan muchas de las herramientas y procesos de DevOps que se utilizan, mientras que muchos CISOs están empezando a entender qué está pasando en su propia empresa. La introducción de la seguridad no debe significar más trabajo para los desarrolladores, ya que reducir la productividad de los desarrolladores no es necesario y los desarrolladores lo rechazarán o eludirán", añade **John Walsh,** DevOps Evangelista & Community Manager en **CyberArk Conjur.**

"Lo que tienen que tener claro CISOs, CIOs, CTOs... es que este concepto plantea soluciones. SecDevOps establece unos mecanismos que permiten recuperar una visión clara sobre el software y establecer los controles necesarios para que sean seguras. La seguridad es algo transversal y el reto debería ser el mismo para cualquier responsable", comentan desde **BBVA Next Technologies**. "Además, plantea para todo el 'C-level' usar la tecnología como un impulso para ser rápidos y acompañar el negocio con la seguridad al mismo ritmo, reduciendo el coste de oportunidad que un enfoque de desarrollo clásico, con pruebas al final del ciclo, plantea".



Incremento de las inversiones en seguridad automatizada

La encuesta de la comunidad DevSecOps confirmó la apuesta de las empresas por introducir controles de seguridad automatizados a lo largo del ciclo de vida del desarrollo de software en 2018 en comparación con el año anterior. Para las organizaciones de DevOps maduras, la encuesta observó un aumento del 15% al 57% en seguridad automatizada, que se implementó en cada etapa del ciclo de vida del desarrollo de software. Las tres principales inversiones en seguridad automatizada que han destacado los participantes en el estudio fueron en cortafuegos de aplicaciones web, la seguridad de contenedores y la gestión de código abierto.

Coste de incorporar DevOps y SecDevOps

Hay dos aspectos que pueden ayudar a entender los ahorros que se obtienen al implantar DevOps: ahorro de costes en horas de trabajo y de reducción de 'caídas' del sistema. En el informe **"Puppet State of DevOps Report"** de 2016**,** se plantea la siguiente formula para calcular el exceso de coste que supone el trabajo no planificado ni automatizado. Coste del exceso de trabajo = Personas x Salario medio x Beneficios x Porcentaje de tiempo dedicado a trabajo extra.

Ir más rápido, ir más seguro... o las dos

El dilema de DevOps frente a SecDevOps, cuando no existe esta cultura, es el de la velocidad versus la seguridad. "SecDevOps es igual a DevOps en cuanto a filosofía, ideas y formas de trabajo. Si DevOps consiste en que sean los propios desarrolladores los que se encarguen del despliegue y las operaciones de los productos, SecDevOps es que sean los propios desarrolladores los que se encarguen de integrar seguridad en el desarrollo de los productos", explican los expertos de **BBVA Next Technologies**

Pero la clave de su éxito es que SecDevOps aplica la seguridad al código, con más frecuencia, evitando retrasos a posteriori. Hasta hace poco, para el 90% de las empresas que usan DevOps, la seguridad era una idea de último momento, según **Gartner** –en 2017 sólo la integraban un 15%–. Pero para 2021, las prácticas DevSecOps estarán presentes en el 80% de los equipos de desarrollo rápido. "La seguridad en aplicaciones debe verse como un 'activador' en vez de como un inhibidor de la expansión comercial", destaca la firma Puppet en uno de sus informes –tras preguntar a más de 3.000 profesionales técnicos de todo el mundo–.

Cambio de mentalidad para verlo todo desde la seguridad

Pero no es sencillo. "Implementar DevOps conlleva un cambio de cultura. Los desarrolladores pasan a hacer operaciones y los chicos de operaciones tienen que integrarse con los equipos de desarrollo. Y ambos tienen que pasar a entender las necesidades del otro y hablar el mismo idioma. Y en ese momento, la seguridad supone dar un paso más. "Mucha gente cree que supone que un auditor haga una serie de pruebas puntualmente, por lo que los desarrolladores no tienen por qué tener conocimientos de seguridad, ni preocuparse por ella durante la construcción", añaden desde BBVA Next Technologies. "Cambiar esta mentalidad puede ser el mayor hito de SecDevOps. Y las mayores lecciones conllevan que los especialistas en seguridad formen parte de los equipos de desarrollo para lo que hay que invertir mucho en formación de seguridad para los desarrolladores. Cosa que estamos haciendo de forma intensiva en empresas como la nuestra".

"Cuando los problemas de seguridad se encuentran al final del ciclo, hay una batalla presupuestaria que sigue y, a menudo, el tiempo para comercializar triunfa sobre la seguridad y, por lo tanto, se liberan los defectos conocidos", comenta **Peter Chestna** de **CA Technologies.**

Además, la eliminación de los silos que supone el trabajo departamental acelera el ciclo vital del desarrollo (*Systems Development Life Cycle*, SDLC), y elimina la visión de la seguridad como una barrera para la velocidad y el progreso. Pero para que este cambio sea posible, las compañías deben implementar pruebas dinámicas de seguridad de aplicaciones (o DAST), para buscar problemas más a menudo e integrar mejor sus herramientas. Se trata de detectar errores y vulnerabilidades que puedan ser vistas cuando el producto está siendo construido. "Incorporar la seguridad al desarrollo de aplicaciones –DevOps–, ya no es una opción: es una necesidad porque supone poner seguridad al comienzo de

Software de código abierto: las dos caras de una moneda

Para no perder el ritmo en la carrera por desarrollar e implementar aplicaciones en tiempo récord, el software de código abierto (en inglés *open source* software u OSS) se ha convertido en una pieza fundamental. A su favor, destaca por ser fácil de implementar, ofrecer todo tipo de funcionalidades y tener un código aceptable... en su contra, que en muchas ocasiones es vulnerable. "En este mundo, la velocidad es tan crítica, que el código abierto está en todas partes, aunque las preocupaciones por su seguridad, a veces, quede relegada 'al asiento de atrás'.

La explotación de vulnerabilidades de componentes de software de código abierto han crecido un 121%, según una encuesta de la comunidad DevSecOps de 2018. Esto supone que en sólo un año ha aumentado un 55%.

El problema es que, de momento, el 52% de los desarrolladores que usan código abierto o componentes comerciales no lo actualizan cuando se conoce una nueva vulnerabilidad, según un informe de **Vanson Bourne** –en el que se preguntó a 1.800 ejecutivos de grandes empresas de 14 países–. Con ello se dispara el riesgo de sufrir una brecha de seguridad. Precisamente evitarlo es lo que pretende DevSecOps. El reto es hacerlo sin frenar el desarrollo y siendo eficientes. El estudio muestra que el 83% de los encuestados usa componentes comerciales o de código abierto, o ambos, con un promedio de 73 componentes por aplicación. El problema es que estos son más eficientes… pero también presentan más vulnerabilidades –se calcula que unas 71 por aplicación–. Y es que sólo el 23% de los encuestados confesaron realizar pruebas de vulnerabilidades en los componentes en cada versión. De hecho, solo el 71% de las organizaciones declara contar con un programa formal de seguridad de aplicaciones (AppSec) y solo el 53% de las organizaciones mantiene un inventario de todos los componentes en sus aplicaciones".

Biblioteca mundial de vulnerabilidades

Para facilitar la identificación de fallos de seguridad en el software, el gobierno de EE.UU. dispone de un organismo, el **National Vulnerability Database (NVD)**, que registra y publica todas las vulnerabilidades conocidas. Gracias a ellas se pueden corregir en los procesos automatizados.

El problema es que el número ha llegado a ser tal que no puede seguir el ritmo y los expertos la achacan que su información es incompleta o se publica excesivamente tarde. Compañías como Sonatype han llegado a detectar hasta 1,3 millones de vulnerabilidades en componentes de código abierto que no figuran en su base de datos. Empresas como **Risk Based Security**, también especializada en bases de datos de vulnerabilidades, han llegado a denunciar que cuentan hasta con 57.000 avisos no publicados por el NVD.

En 2017, también se desveló que el organismo que registra este tipo de fallos en China, el **CNNVD**, contaba con 1.700 registros más que su homólogo estadounidense. Es más, mientras éste tarda 13 días en incluir las vulnerabilidades el segundo no lo hace hasta los 33, de media. Unos tiempos preocupantes teniendo en cuenta que los *exploit* –programas malicioso que se aprovechan de vulnerabilidades conocidas, pero no remediadas, para entrar en un sistema– tardan en aprovechar los fallos de seguridad conocidos ipoco más de tres días!

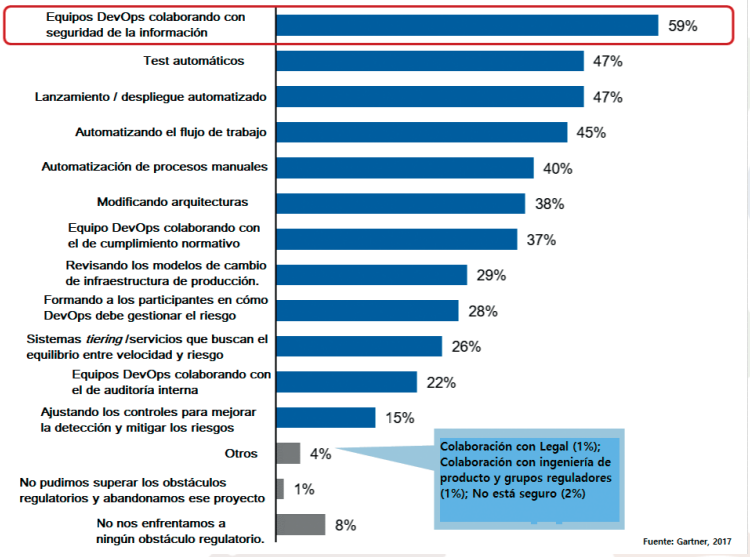
Un problema de seguridad nacional: En 2018 se ha denunciado que la CNNVD está siendo manipulada para publicar sus alertas más tarde, de forma premeditada. ¿Por qué? En 2017, publicaron una vulnerabilidad de Microsoft Office, la CVE-2017-0199, 57 días después de informar de ella la compañía. Y un grupo de APT, supuestamente con origen en el país, la explotó durante ese tiempo para atacar empresas financieras rusas y asiáticas.

la vida de cualquier aplicación evitando futuros problemas", explica el manager de Ciberseguridad en **CapGemini**, **Juan Carlos Pascual**.

Automatizar todo lo que se pueda

"El reto, con SecDevOps, es automatizar las tareas centrales de seguridad, el código y que los controles de seguridad se hagan de forma centralizada. Y estudiar la seguridad de las aplicaciones desde el principio, cuando se plantean sus requisitos, sus funcionalidades, las posibles amenazas a las que estarán sometidas… y qué nivel de riesgo queremos asumir con ellas. Una vez definidos los riesgos se pueden automatizar procesos", destaca Pascual. Los equipos de DevOps tienen un 90% más de probabilidades de cumplir con las medidas de seguridad cuando se automatizan este tipo de procesos y la seguridad automatizada en aplicaciones reduce la posibilidad de que incluya vulnerabilidades en un 50%.

Cómo se implementa la seguridad en DevOps, según Gartner



En la cabeza de un responsable de SecDevOps

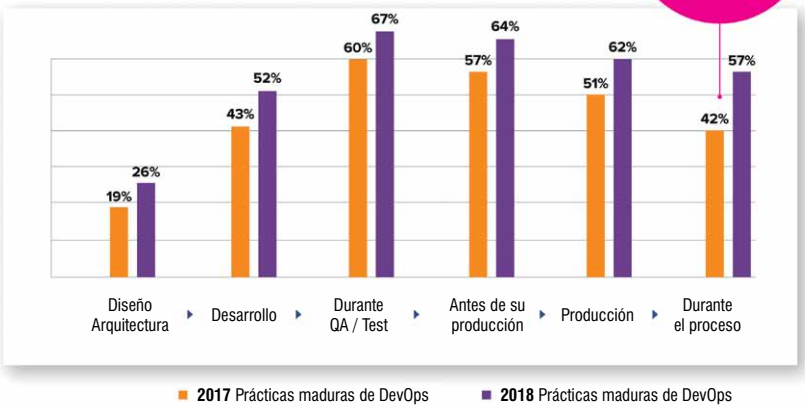
Mientras en unas empresas se está apostando por crear el puesto del SecDevOps, en otras se implementa la seguridad entre los expertos en la cultura DevOps.

A veces este cambio supone adaptar la compañía y mejorar la comunicación para aplicar esta filosofía de trabajo **(Isidro Labrador, GMV**, Revista SIC nº 125, 'DevOps y Ciberseguridad'**)**. El reto es contar con una cultura de calidad y mejora continua y conjunta, tanto en el área de desarrollo, como de operaciones y seguridad para disponer de la tecnología correcta para añadir la seguridad en el proceso –*pipeline*–.

Un responsable de SecDevOps se encarga de garantizar la seguridad de las aplicaciones en base a automatizaciones. Una vez se han implantado herramientas que revisan exhaustivamente la seguridad de lo que se construye, y se han integrado de forma que se ejecuten análisis siempre que se construye algo nuevo, los desarrolladores sólo tienen que revisar los resultados de los análisis y corregir las cuestiones de seguridad. "Para esto es necesario que tenga conocimientos de seguridad. Pero si esto se cumple y los desarrolladores adoptan la mecánica de revisar los análisis y corregir los problemas de seguridad siempre que terminan una funcionalidad, al final forma parte del día a día de los desarrolladores y les supone un impacto pequeño. De hecho, más relevante que cualquier dato es entender que la automatización de la seguridad es la única vía para escalar la función clásica de seguridad en un entorno DevOps. Si tu negocio exige cambios en producción (aunque no sea cada día), como en las empresas tecnológicas más punteras, sino, al menos, cada mes, la única forma de no retrasarlos es integrando la seguridad de forma automatizada en los procesos de desarrollo y despliegue", explican los expertos de BBVA Next Technologies, que consideran que aplicar esta nueva cultura de trabajo "no solo supone una simple mejora, sino la supervivencia: si no se integra la seguridad como parte de la filosofía DevOps es imposible aplicar la misma".

¿Dónde se incluye la seguridad automatizada en el proceso DevOps?

La inversión de seguridad en DevOPs creció un 15%



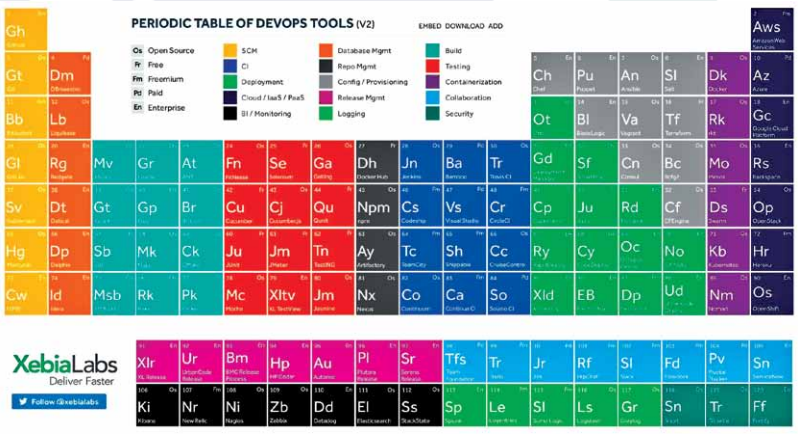
Por eso es vital incorporar la seguridad 'a medida' en cada proyecto, con ajustes continuos y adaptándose al desarrollo en un marco de tiempo razonable. Para realizar los test se apuesta más por herramientas comerciales –como las de Sonatype, CyberArk, Micro Focus, Trend Micro, entre otras– y de código abierto (*open source*) –como Jenkins o Jira– que permiten usar *fuzzers* –pruebas automatizadas para comprobar la seguridad de un software metiendo datos inválidos, inesperados o aleatorios– para identificar fallos en las API por entradas de datos erróneas o aleatorias, posibles *sqlinjections*, realizando tests de seguridad estática del código o tests de seguridad de infraestructura, entre otros.

Las compañías que aplican DevSecOps lo hacen de forma más eficente cuando, con las herramientas adecuadas, analizan la seguridad de producción –fijándose en IDS / IPS y RASP– para garantizar que cumplan las normativas de seguridad –como la GDPR– y sean robustas ante las últimas amenazas conocidas. Además, en los últimos años, muchas herramientas de desarrollo ofrecen formación a los desarrolladores en seguridad para que detecten cualquier problema que hasta ahora omitían por falta de conocimiento.

"Muchos dicen que este concepto está muy maduro y Sec ya está incluido en DevOps, pero el informe CyberArk Advanced Threat Landscape 2018 muestra que solo el 41% de los equipos de seguridad y DevOps trabajan de forma conjunta –tras preguntar a 1.300 ejecutivos de TI, DevOps y empresarios de siete países–. La seguridad no puede considerarse parte de DevOps automáticamente hasta que se incluyan los equipos de seguridad y las mejores prácticas de seguridad desde el inicio del proceso de desarrollo. Esto se

llama 'cambio de seguridad' y reduce el coste de cualquier posible problema que se encuentre más adelante en el proceso de desarrollo", resalta **John Walsh**, DevOps Evangelista & Community Manager en **CyberArk Conjur.**

Además, con la automatización de procesos, DevSecOps también consigue actualizar vulnerabilidades conocidas como la de Meltdown en sistemas Intel, destaca, **George Gerchow**, de **Sumo Logic**. "Las empresas que tienen implementada esta cultura lo hicieron de forma sencilla, rápida y sin ninguna interrupción notable para los clientes internos o externos". "En los entornos tradicionales, habría tomado semanas o meses hacer esto con el tiempo de inactividad porque las tres funciones de desarrollo, operaciones y seguridad estaban aisladas", dice Gerchow.



Aplicaciones con vulnerabilidades 'por diseño'

Un dato que resulta preocupante es cuando se conoce que los atacantes de la empresa Equifax, en 2017, usaron una vulnerabilidad conocida… ¡sólo tres días antes! De hecho, aunque menos mediático, este ataque también afectó a Alaska Airlines, Okinawa Power –Correos de Japón– y a AADHAAR (el sistema de la seguridad social de la India).

Los tiempos en los que los responsables de seguridad dejaban pasar meses antes de parchear sus sistemas tienen los días contados. Sobre todo si se trata de aplicaciones hechas con código abierto, como ocurre con la mayoría. Investigadores de la firma Sonatype han alertado de que muchos de los programas que se usan en código abierto, se descargan y usan con vulnerabilidades sin parchear –se calcula que entre 80.000 y 100.000 cada año–. Es más, la compañía incluso ha realizado un ránking con los países que más descargan software de código abierto con vulnerabilidades conocidas. El que lo hace de forma más segura es Singapur, con un 10%, mientras que Estados Unidos y China lideran este ranking con un 14.1% y 14.0% –España queda situada por la mitad–.

Ello supone que el 57% del 'Top 500' mundial de empresas tienen alguna vulnerabilidad en sus aplicaciones, aunque no lo saben. Y el tiempo medio entre la notificación de una vulnerabilidad y su explotación por parte del cibercrimen se ha reducido de 45 días en 2006 a 15 en 2015… y a sólo tres en 2018, según datos de Sonatype.

Así que cualquier alerta de seguridad en el software obliga a las empresa a analizar qué aplicaciones en producción puede ser explotables, determinar un plan de emergencia en caso de que ocurra y corregir esta vulnerabilidad en cualquier aplicación qué esté en producción en pocos días –o incluso horas–. "Una vez que se conoce un fallo de seguridad se produce un efecto como el de 'la fiebre del oro' para poderla explotar lo antes posible", recuerda el CSO de la empresa **PTC, Josh Corman.**

"La clave para aplicar Sec en DevOps es aprovechar procesos y tecnologías que ya tienen las compañías y aplicar seguridad (también formando equipos) en todos sus procesos", explica **Humbert Costas,** Responsable de Innovación (CSO) de **Ackcent.** "Por supuesto, una parte importante es monitorizarlo todo, no sólo durante el desarrollo y despligue sino también durante su uso, por ejemplo, prestando mucha atención a las APIs. Y por supuesto, hay que hacer auditorías y análisis de forma continua, no esperar al final. Esa es la clave".

En este contexto, SecDevOps se convierte en una herramienta imprescindible para parchear de forma automática vulnerabilidades que se acaban de conocer en aplicaciones en servicio –y detectarlas y corregirlas al momento en las que están en desarrollo o despliegue–.

Black SecDevOps, la nueva forma de ataque

La consultora **Forrester** ha llegado a recomendar, en marzo de 2018, "automatizar procesos más rápido que el cibercrimen. Si una empresa piensa que su equipo de ciberseguridad tiene problemas por el alto volumen de alertas y el trabajo que generan… es que no está preparada para lo que está llegando".

Aplicar el concepto DevOps, con Sec, permite a las empresas adelantarse un paso por delante del cibercrimen aplicando mejoras de seguridad de forma rápida y eficaz en todo el ciclo de vida de las aplicaciones gracias a la automatización de procesos.

Actualmente, según un estudio de Forrester, el 8% de las empresas ya son capaces de implementar mejoras en sus aplicaciones, al menos, una vez al día, el 25% lo hace cada semana y el 68% cada mes. Es más, el 7% de los equipos DevOps pueden hacerlo cada hora, según el informe **'Accelerate: State of DevOps'** de **DORA** –tras preguntar a 1.900 expertos en DevOps–, mientras que el 48% los puede aplicar entre un día y una semana y un 52% entre una semana y seis meses. Así que los que consiguen hacerlo más rápido son los que menos riesgo asumen.

El cibercrimen también apuesta por DevOps para usos maliciosos

Los atacantes están haciendo un uso intensivo de tecnologías como la Inteligencia Artificial (AI) o del procesamiento en lenguaje natural para el Aprendizaje automático (ML) y mejorando también sus procesos para que sirvan a nivel global y de forma más eficaz. Incorporar la seguridad y automatizar procesos en el desarrollo de aplicaciones también tiene un lado oscuro. Es la zona donde el cibercrimen ve un nuevo vector de ataque: inyectar vulnerabilidades, defectos y *malware* conocidos en la cadena de software y en las propias herramientas de automatización, así como aprovechar vulnerabilidades conocidas en los programas de código abierto.

En el momento presente uno de los principales objetivos de ciberataques son los contenedores. Se trata de una de las herramientas más usadas para automatizar pruebas y procesos –también de seguridad–, siendo el más conocido Docker (véase la reseña del libro **'Docker: SecDevOps'**, en la sección Bibliografía de esta edición). Éstas permiten desplegar aplicaciones en un entorno controlado –antes de su despliegue– para ver fallos de funcionalidad y de seguridad.

El problema de estas herramientas –cada dos semanas en 2018 su descarga se ha incrementado en más de 1.000 millones–, es que no suelen ser testeadas para garantizar su seguridad –sólo el 42% de las empresas confesaron hacerlo, según una encuesta a la comunidad DevSecOps, en 2018–. Así que ya no sólo cuenta aplicar la seguridad a las aplicaciones en desarrollo… sino hacerlo a las herramientas con las que se hace.

2

Mitos de DevOps a SecDevOps
QUÉ OPINAN LOS EXPERTOS

I.

"Uno de los grandes fallos, a la hora de aplicar DevSecOps, es enfocarse sólo en automatizarlo todo. Para hacerlo bien hay que mezclar ese concepto con un cambio cultural que también integre los procesos de seguidad a lo largo del ciclo de vida de desarrollo de las aplicaciones para que esté en todas las capas". Eso sí, también destaca que este concepto aún está poco maduro "para popularizarlo hace falta más inversión, más conocimiento de las prácticas de seguridad, gobernanza y estrategia", comenta **Elías Grande**, coautor del libro **'Docker: SecDevOps'**. "Por supuesto, el reto de cualquier responsable de seguridad es saber cuándo hay un fallo detectado que exige parar o no el proceso de desarrollo y despliegue. De eso depende ser eficientes aplicando esta cultura y por eso, de momento, es un concepto al que le falta mucho recorrido".

Elías Grande

John Walsh

BBVA Next Technologies

II.

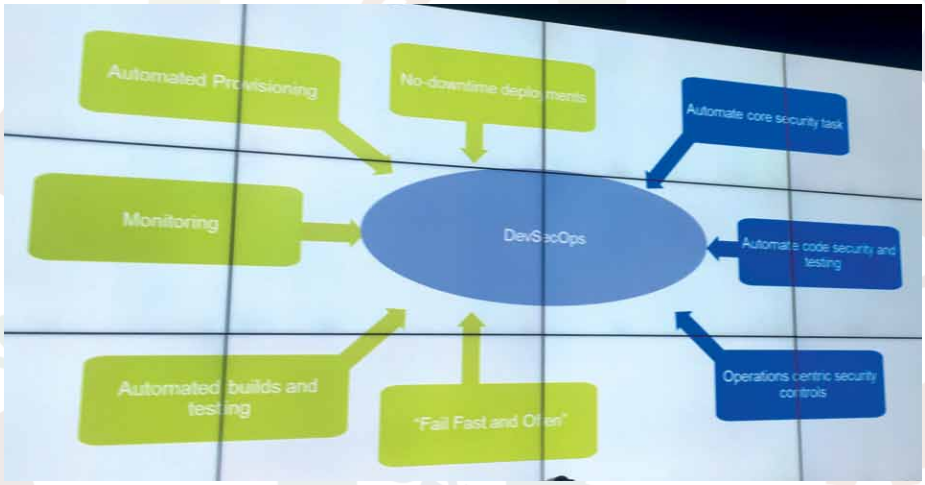
"Una situación muy común es sufrir retrasos. Cuando esto sucede, es un error muy típico empezar a dejar de lado muchas cosas para intentar acelerar la construcción. Y el resultado es que, a medio plazo, se acaba perdiendo no sólo más tiempo, sino también calidad, seguridad, etc.", resaltan desde **BBVA Next Technologies**.

"Con la mentalidad DevOps, y esto incluye la parte Sec, toda inversión de tiempo y recursos en automatizaciones, produce un retorno de inversión en un plazo muy corto".

"Al igual que ocurre en cualquier proceso de desarrollo clásico, el mayor error es acumular excesiva deuda técnica pensando que habrá tiempo en el futuro para solucionarlo. Un desarrollo que sale a producción sin el nivel de seguridad adecuado es sinónimo de problemas en el futuro, y esto no es inherente al modelo SecDevOps, sino que es el reto que hemos tenido siempre".

III.

"El mayor error al aplicar seguridad en DevOps es pensar que se limita a los análisis automáticos de vulnerabilidad del sistema. He hablado con varias personas en eventos que tienen este falso sentido de seguridad porque implementan algunos análisis automáticos para asegurar que su software esté parcheado y actualizado. Sí, se debería hacer esto y creo que mucha gente lo está aplicando, pero esto no consigue que DevOps sea lo mismo que DevSecOps", recuerda **John Walsh,** DevOps Evangelista & Community Manager en **CyberArk Conjur**. "También es necesario controlar el acceso y autenticar los contenedores de clientes, por ejemplo. En nuestro informe de 2018, 'CyberArk Advanced Threat Landscape', encontramos que casi ningún equipo de ciberseguridad ni de DevOps podía identificar todos los lugares en los podría existir una credencial o permiso de acceso. Un dato evidente de que aún queda mucho por hacer en seguridad en DevOps".



Aprendiendo de los que ya lo aplican con éxito...

3 Por qué funciona en BBVA, Microsoft y Netflix

Cualquier compañía que se plantee implantar el paradigma SecDevOps es, además de su negocio, una compañía de software. Pero en algunas el software y la seguridad tienen más relevancia que en otras. Por ejemplo, para el sector financiero, el software tiene mucha importancia y la seguridad aún más. En el mundo anglosajón se suele hablar de "bank level security" como un nivel de exigencia mayor. La clave, como siempre, es buscar el nivel de riesgo que se quiere asumir por parte del negocio.

BBVA

"Comenzamos primero a aplicar el concepto 'Sec' en el área de desarrollo de productos de seguridad (IAM, criptografía, etc.). En esta área los desarrolladores ya contaban con conocimientos de seguridad, por lo que fue más sencillo. Luego se implementó en el resto de las áreas y, en general, en aquellas partes de la organización que usaban tecnologías más modernas (contenedores, microservicios, etc.). Eran las más proclives a abrazar la seguridad como una parte más del ciclo. Lógicamente, es más costoso en las áreas más *legacy* –heredadas–, no tanto por la seguridad en sí, como también por los cambios necesarios en sus procesos de desarrollo clásicos".

"Nosotros apostamos por un modelo de desarrollo de producto. Es decir, desarrollamos nuestros productos. En cambio, otros bancos apuestan por un modelo de compra de productos. En este modelo se pierde el control de la metodología y las formas de trabajo de los equipos de desarrollo, así como la agilidad para cambiar el software a tus necesidades. Pero en realidad, esto no es SecDevOps sino más bien SecOps. En general, la filosofía SecDevOps está unificada, entre aquellos que de verdad la aplican".

"Lo mejor de nuestra filosofía es que, por un lado, los productos cuentan con unos niveles de calidad y seguridad muy elevados desde el primer momento y, por otro, los integrantes de los equipos están mucho más cerca de los productos, los entienden mejor, tienen más libertad y más conocimiento, y no gastan tanto tiempo en tareas tediosas, gracias a las automatizaciones, por lo que, por lo general, están más contentos, lo cual también implica que son más productivos y más creativos".

"¿Lo peor? la inversión inicial que exige y el esfuerzo hasta llegar a un buen nivel de madurez... Esta filosofía requiere un cambio de mentalidad en la forma de trabajar, y muchas veces ese cambio es el principal hándicap para abordarlo, por encima incluso de cualquier inversión económica".

"Uno de los productos que hemos construido está centrado en permitir escalar la filosofía SecDevOps. Lo llamamos **Chimera** porque cuando empezamos a plantearlo hace unos años nadie pensaba que sería posible. Básicamente Chimera acompaña a todos los DevOps durante el ciclo de vida de desarrollo, dando *feedback* de seguridad tanto de su código (incluida la infraestructura diseñada como código) como de sus APIs, contenedores y resto de artefactos. Se integra en los *pipelines* y las herramientas de desarrollo e incluso permite bloquear una promoción entre entornos si el nivel de seguridad no es el adecuado. Precisamente el predicar con el ejemplo de la filosofía SecDevOps con un producto software que ayuda a los desarrolladores es lo que nos hace sentirnos más orgullosos de lo conseguido".

"También nos gustaría mencionar, como uno de los principales éxitos, el cambio filosófico conseguido entre los desarrolladores. Antiguamente era impensable que un equipo de desarrollo pidiera ayuda para que la seguridad fuera parte de su ciclo de desarrollo y teníamos que actuar casi como policías. Cuando a día de hoy se nos acercan equipos que están comenzando un nuevo proyecto pidiendo integrar la seguridad desde el día uno nos hace sentir que hemos conseguido un hito muy importante".

Microsoft

"Para nosotros es una práctica que hemos tenido siempre muy desarrollada de forma interna –aunque ahora la ofrecemos a clientes–. Pero ha sido clave para nuestra transición a la nube, ya que permite poner en práctica miles de aplicaciones en entrega continua y segura, para lo que siempre se han puesto controles de calidad", explica **Santiago Núñez,** arquitecto digital de la división de Servicios Profesionales de Microsoft.

"Actualmente usamos esta cultura de seguridad en más de 1.000 suscripciones en Microsoft y más de 1.200 aplicaciones, cubriendo más de 300 controles de seguridad en 30 servicios de Azure. Ello supone que cerca de 35.000 recursos de Azure son escaneados diariamente. Además, implementamos un total de 580.000 controles de seguridad cada día. ¿El nivel mínimo? un 95% de cumplimiento".

"Estamos comprobando que si se embebe la seguridad en el propio proyecto de desarrollo, despligue y prueba se acelera la puesta en producción. Además, contamos con un *dashboard* de cumplimiento normativo que se puede actualizar y que permite incorporar cualquier cambio rápido y casi de forma automática a las aplicaciones. Nuestra forma de trabajar es crear módulos que se pueden adaptar al DevOps de cada cliente, según sus necesidades. El problema de hacer que trabajen equipos diferentes de forma conjunta y de automatizar la seguridad es que supone un choque cultural. Por eso, lo importante es implementar controles de seguridad de forma continua, pero sin parar el ciclo de desarrollo. SecDevOps no es una 'bala de plata' de la ciberseguridad pero sí permite eliminar muchas vulnerabilidades que se pueden predecir o a las que anticiparse. Además, aprendemos mucho de los errores... y eso también se incorpora al ciclo mejorando cada resultado".

Netflix

"Comenzamos a caminar a hacia este concepto en 2012 y supuso poner en marcha un servicio muy crítico y laborioso. Los despliegues de aplicaciones se hacían de forma muy cautelosa. Se desplegaban y si no se 'rompían' en una semana se ponían en funcionamiento. Fue complejo porque los problemas que surgían se intentaban resolver como si fueran una pelota entre los equipos. Era una situación que evidenciaba que hacía falta una evolución. Por ello, se rompió la separación entre departamentos (silos) y se apostó por la filosofía DevOps. Se trataba de crear equipos que pudieran desarrollar un sistema, ponerlo en marcha y mantenerlo. Y para ello se dieron responsabilidades a los equipos de desarrollo".

"También formamos equipos que crearon herramientas centralizadas que podían usar todos los equipos (por ejemplo, Cloud Platform, Performance & Reliability Engineering, Engineering Tools) para resolver problemas similares en todos ellos. Así estos equipos centralizados actuaron como multiplicadores de fuerza al convertir su conocimiento especializado en bloques de construcción reutilizables".

"Las herramientas de Netflix, a menudo, son de código abierto, y suele ser interesante probarlas antes de usarlas. Nosotros aconsejamos comenzar por el análisis del valor potencial, los costes y apostar por el cambio de mentalidad. Hay que evaluar lo que se necesita y optar por la menor complejidad necesaria".

"El camino desde 2012 hasta hoy ha estado lleno de experimentos, aprendizaje y adaptaciones pero ahora los cambios tardan horas en lugar de días y los desarrolladores pueden investigar rápidamente los problemas y realizar cambios en lugar de buscar ayuda en otros equipos. Pero aún queda mucho por evolucionar", explican **Philip Fisher-Ogden, Greg Burrell y Dianne Marsh** en el blog de la compañía.

4 Cinco casos que podrían haberse evitado...

DJI

En otoño de 2017, el investigador Kevin Finisterre encontró claves privadas para DJI, un fabricante chino de drones, dominios web y claves AWS s3 disponibles públicamente en GitHub durante

un programa de recompensas por fallos de seguridad. Usando estos datos, un atacante podría acceder a los datos del registro de vuelo de aviones no tripulados y a las imágenes que los usuarios subieron a DJI, incluidas las fotos de las identificaciones gubernamentales, las licencias de conducir y los pasaportes.

Equifax

Los mejores ejemplos de problemas de seguridad en DevOps suceden alrededor de software de código abierto (OSS).

"La violación de Equifax –que supuso el robo de datos personales de 143 millones de personas en 2017– se produjo debido a una biblioteca Struts, con una vulnerabilidad sin parchear. Es probable que no fuera un ataque dirigido y sí fruto de la oportunidad tras encontrar la brecha. Pero dando con ella fue fácil para los atacantes. Por eso, tener código implementado con seguridad desde el principio es fundamental y hay que actualizarlo lo más rápido posible", explica **Peter Chestna**, **CA Tecnologies**.

Facebook

Más de 30 millones de usuarios de Facebook, inicialmente, se vieron afectados por una filtración de datos detectada la última semana de septiembre. Los ciberdelincuentes supieron explotar

una vulnerabilidad en la función "Ver cómo" de Facebook para robar *tokens* de acceso, unas claves que permiten iniciar sesión de manera automática y no tener que volver a escribir una contraseña cada vez que se quiere acceder. Según esta red social, el problema ha sido resuelto y ya no hay peligro, pero se recomienda a todos los usuarios que cierren la sesión de sus cuentas en sus diferentes dispositivos.

Google+

Alphabet –la matriz de la multinacional estadounidense– ha anunciado en octubre que cerrará, en los próximos 10 meses, su red social Google+ tras detectar un fallo de seguridad –presente desde 2015– que podría permitir el acceso a datos personales de hasta a un millón de usuarios. La compañía destacó que

"no hemos encontrado pruebas de que algún desarrollador fuera consciente de este error o que se haya utilizado", aunque sí reconoció que este fallo de aplicación podría permitir que aplicaciones externas pudieran acceder a datos que habían compartido los usuarios –aunque sin ser públicos–.

Lexnet

En julio de 2017, el Ministerio de Justicia tuvo que interrumpir el servicio que prestaba, desde 2016, a través de esta plataforma para gestionar las notificaciones entre todos los juzgados y los profesionales, principalmente abogados

y procuradores (para los cuales es de obligado cumplimiento). Un error en el diseño técnico del sistema, en el control de acceso, permitía que abogados y procuradores accedieran, de forma

fácil –bastaba cambiar un número– a casos judiciales del resto de profesionales. El error expuso todos los casos judiciales que había en ese momento en la plataforma –e, incluso, hubo gente que descargó expedientes que no eran los suyos–.

Uber

El robo de datos a la compañía, conocido en noviembre de 2017, fue una de las violaciones de DevOps más complejas. Los delincuentes robaron los datos personales de 57 millones de clientes y conductores de Uber Technologies Inc. Pudieron violar el repositorio privado de GitHub de Uber y encontrar el código con permisos y claves. Con ellos, los atacantes se desplazaron de forma lateral desde el entorno de desarrollo de Uber a su

cuenta de producción de Amazon Web Services (AWS). Esta es la misma cuenta de AWS que usó la compañía para procesar los datos de la empresa en tiempo real, por lo que contenía una gran cantidad de información confidencial del cliente. Uber probablemente tiene DevOps muy maduros, aunque este ciberataque no fue el primero que sufrió la compañía. Lo que sí se hubiera podido mejorar fue su gestión: intentaron pagar a los atacantes 80.000 euros para mantener la brecha en secreto. Curiosamente no fue el primer caso que sufrió la compañía: en 2014, los atacantes aprovecharon sus claves y contraseñas en GitHub para robar los datos personales de 50.000 personas. Tras una negociación, las fiscalías de todos los estados de EE.UU. la empresa ha aceptado pagar 130 millones de euros en compensación por ocultar el robo masivo de datos de sus clientes desde 2016.

Las 10 vulnerabilidades más temidas en aplicaciones en 2017, según la asociación OWASP

Open Web Application Security Project, también conocido como **OWASP**, es una iniciativa, sin ánimo de lucro, que recoge las peores vulnerabilidades, además de facilitar guías para evitarlas. Cada cuatro años realiza un informe actualizado con las más preocupantes y más explotadas por el cibercrimen. Quizá lo más llamativo es que, a pesar del paso de los años, hay varias que siguen estando en el 'Top10' año tras año, sin que se remedien. Se trata de los fallos de inyección de código y los problemas en las plataformas de autenticación. En su último informe estas fueron las más preocupantes, sobre todo porque se repiten cada año:

OWASP Open Web Application Security Project

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	U	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	U	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

5 Guía para implementar SecDevOps y no morir en el intento

Para aplicar la seguridad con éxito a DevOps, Gartner recomienda hacerlo en torno a cuatro pilares para hacer aplicaciones seguras durante su desarrollo: Identificar vulnerabilidades conocidas en ellas y eliminarlas, codificar de forma segura y automatizar todos los procesos cuanto sea posible. Para ello es importante contar con herramientas de mapeo de datos, para saber dónde están los realmente críticos, de enmascaramiento (como la seudonimización, el cifrado y la anonimización) y contar con datos reales que permitan realizar simulaciones del despliegue de la aplicación lo más fidedignas posibles, para corregir posibles brechas de seguridad –por ejemplo, por no tener actualizado Java–. También hay que disponer de herramientas que permitan eliminar vulnerabilidades. La clave para acometer este proceso con éxito es saber cuándo es realmente importante frenar el desarrollo –y cuando no–.

Qué recomienda John Walsh*

1. **La 'identidad' de la máquina** es donde comienza la seguridad de DevOps; sin esto no puedes autenticar las máquinas y contenedores que solicitan acceso. Si no se es capaz de hacerlo, no se debe autorizarla ni darle acceso a nada.
2. **A continuación, autentica los contenedores** basándose en múltiples factores nativos de la plataforma de organización de contenedores que solo están disponibles para el contenedor legítimo (como los rangos de direcciones IP asignados a contenedores válidos, UUID aleatorios, nombre de rol, claves criptográficas u otros atributos generados automáticamente). Esta es la manera más segura de confirmar que la máquina es la que dice que es. De lo contrario, se puede quedar atrapado en un bucle que asegura unas claves y permisos con otras claves y permisos.
3. **Una vez que se hayan establecido** y autenticado las identidades de la máquina, se debe controlar y proteger el acceso a los sistemas y servicios importantes. Esto se hace administrando permisos de manera centralizada (como contraseñas, claves SSH, claves API, certificados y otras credenciales). Los permisos otorgan acceso, por lo que necesitan ser protegidos, cifrados, monitorizados y rotados. Si esto no se hace, un atacante puede robar secretos y provocar una brecha de seguridad que afecte a toda la empresa.
4. **Además de hacer seguro el control de acceso a través de la administración** y autenticación de claves y contraseñas, la seguridad debe ser un proceso fácil, e intuitivo, para los desarrolladores que ponen el Sec en DevOps. Se puede tener la mejor seguridad del mundo, pero si es una carga de trabajo demasiado grande, las personas inteligentes encontrarán formas de evitarla para seguir con su trabajo. Por eso desarrollamos CyberArk Conjur.

* **John Walsh** es evangelista en DevOps de **CyberArk Conjur**

...así lo ve BBVA Next Technologies

1. **Dejar de pensar en la seguridad exclusivamente** como una auditoría al finalizar el producto. La seguridad debe formar parte desde el diseño y la construcción.
2. **Dejar de creer que el conocimiento** en seguridad es exclusivo de los auditores de seguridad. Formar a los equipos de desarrollo en seguridad, ya que es una responsabilidad de todos.
3. **Poner el foco en los desarrolladores.** Hacer que se sientan libres y confortables. Implantar metodologías ágiles para aportar valor de manera iterativa y continua
4. **Automatizar todo lo que se pueda.** Invertir en herramientas y centrarse, desde el principio, en la automatización.
5. **No creer que cuando se acercan** las fechas de entrega, hay que centrarse en cubrir a corto plazo.

Buen consejo

"Hay dos cosas que creo que son las más importantes para implementar Sec a DevOps. La primera es la responsabilidad mutua. A menos que la seguridad sea tarea de todos, progresará poco en el reto de crear aplicaciones más seguras. La segunda es la educación. SI los trabajadores no están capacitados y, aunque les importe la seguridad, no saben aplicarla harán las cosas de forma incorrecta una y otra vez, sólo porque nadie les ha enseñado a hacerlo bien. A veces cuesta lo mismo aplicar la seguridad que no hacerlo… es solo cuestión de conocimiento", destaca **Peter Chestna** de **CA Technologies.**

6 Buscando a los 'campeones' del SecDevOps

Actualmente existen muchas soluciones de código abierto para aplicar este concepto –como Arachni Scanner, OWASP ZAP, Gauntlt, ThreadFix, OWASP Code Pulse, Boundry, Git, Chef o Jenkins–. Por supuesto, las compañías clásicas en el sector también ofrecen soluciones a medida –como Trend Micro con su Deep Security Smart Check y McAfee con su Cloud Workload Security, entre otras–.

En el mercado español se comercializan más de dos decenas de herramientas para implementar –y analizar– la seguridad durante el proceso de DevOps. Además, cada vez más empresas de ciberseguridad ofrecen este concepto como servicio –como es el caso, entre otras, de Ackcent, Grupo ICA, Mnemo, GMV, SIA o Tarlogic–.
Estas son algunas de las soluciones más usadas actualmente…

Aqua Security

■ Permite dar seguridad en las aplicaciones nativas de las empresas, tanto en contenedor como nube desde el desarrollo hasta su puesta en producción. Asegura todo el ciclo de desarrollo de software, incluyendo escaneo de imágenes para vulnerabilidades conocidas durante el proceso de compilación, entre otras funcionalidades.

www.aquasec.com

BeyondTrust

■ Proporciona una solución unificada para reducir el riesgo de vulnerabilidades a lo largo de la cadena de suministro de software. Entre otros, incluye detección de dispositivos automatizados, validación y gestión, así como identificación y remediación de vulnerabilidades de Docker.

www.beyondtrust.com

CA Technologies

■ Sus herramientas permiten la construcción, prueba, seguridad y despliegue de software de manera rápida y eficiente, proporcionando un software que es más resistente a los ataques de ciberdelincuentes. A través de la automatización, CA Technologies extiende la implementación más rápida con un *backend* ágil que entrega lanzamientos de código más confiables, ayudando a los equipos a trabajar en colaboración antes en el proceso DevSecOps para detectar vulnerabilidades de seguridad en cada fase, desde el diseño hasta la implementación.

www.ca.com

CloudPassage

■ Fundada en 2010, es referencia en automatización de la carga de trabajo en la nube y seguridad de contenedores. Fue la primera compañía en obtener patentes estadounidenses para la seguridad de la infraestructura universal en la nube a través de CloudPassage, automatizando la seguridad en la nube en el momento de desplegar las aplicaciones.

www.cloudpassage.com

Chef Automate

■ Es una plataforma de entrega continua que permite a los desarrolladores, operaciones e ingenieros de seguridad colaborar sin esfuerzo en la entrega de aplicaciones y cambios de infraestructura a la velocidad de los negocios.

automate.chef.io

CyberArk

■ Ofrece una de las soluciones más completas, ya que permite proteger las aplicaciones frente a la explotación de cuentas, credenciales y secretos con privilegios en cualquier lugar: en el punto final y en los entornos locales, la nube híbrida y los entornos DevOps. Por ejemplo, CyberArk Conjur es una solución de gestión de datos que protege y gestiona lo elementos críticos, usados por las identidades de las máquinas (incluidas aplicaciones, microservicios, aplicaciones, herramientas de CI / CD y API) y los usuarios de todo el canal DevOps para mitigar los riesgos sin afectar la velocidad.

www.cyberark.com

(Code)AI

■ Aplicación inteligente y automatizada de codificación segura para DevOps, que corrige las vulnerabilidades de seguridad en el código fuente de la computadora para evitar la piratería.

www.mycode.ai

Datical

■ Compañía de protección del dato que permite entregar, rápido, aplicaciones sin errores que lo pongan en peligro. Entre sus funcionalidades destaca por su automatización eliminando vulnerabilidades conocidas que supongan una posible fuga de información.

www.datical.com

Kiuwan

■ Es una de las herramientas en la lista de OWASP de herramientas de análisis estático del código fuente. Su solución es multilenguaje y se puede integrar con otras muchas herramientas –como Jenkins o Visual Studio–. Mientras su Code Security (SAST) escanea automáticamente código y detecta vulnerabilidades su Insights (SCA) permite gestionar componentes de código abierto (OS), evitar vulnerabilidades automatizar políticas de uso de OS.

www.kiuwan.com

HDiV

■ El fabricante español ofrece seguridad de aplicaciones y APIs, con tecnología de detección (IAST) y protección (RASP) usa-

das por empresas como Standard Chartered, Fidelity Investments, Walmart o Groupe Caisse des Dépôts, entre otras. Ofrece una de las pocas soluciones, a nivel internacional, que ha obtenido un 100% en el OWASP Benchmark por su fiabilidad sin generar falsos positivos permitiendo reducir los principales riesgos a nivel aplicación.

hdivsecurity.com

IBM

■ La multinacional se centra en ofrecer DevOps seguros en la nube o tras los cortafuegos a través de un conjunto de soluciones que permiten implementar la seguridad desde el proceso de producción de las aplicaciones.

www.ibm.com

Imperva

■ Su tecnología WAF –Web Application Firewall– protege contra los riesgos más importantes de las aplicaciones web (inyección SQL, *scripts* entre sitios, acceso ilegal a recursos, etc.) para evitar que estos fallos estén en las aplicaciones en su despliegue.

www.imperva.com

IriusRisk

■ Solución 'made in Spain', desarrolada por Continuum Security, que ofrece una única consola integrada para crear fácilmente modelos de amenazas y administrar el riesgo de seguridad de la aplicación durante todo el proceso de desarrollo de software. Entre sus ventajas destaca su modelado de amenazas en el proceso de desarrollo de software seguro, para anticiparse a posibles fugas de datos o ciberataques.

continuumsecurity.net

Micro Focus

■ Su plataforma Fortify ofrece visibilidad en todo el proceso DevOps implementando herramientas que permitan corregir código que plantee problemas de seguridad, implementar vulnerabilidades, incluso ofreciendo formación a desarrolladores en temas de seguridad aplicados al software.

www.microfocus.com

Microsoft.

■ A través de CSE (*Core Services Engineering*) ofrece un 'Secure DevOps Kit' para Azure para ayudar a desarrollar las mejores prácticas de seguridad en el desarrollo y las operaciones de aplicaciones empresariales en la nube. Contiene automatización, extensiones, complementos, plantillas, módulos y otras herramientas que agregan seguridad a las aplicaciones en la nube durante el proceso de desarrollo.

www.microsoft.com

Sonatype

■ Su plataforma Nexus presta ayuda a más de 10 millones de desarrolladores de software para reducir los riesgos de seguridad que supone usar código abierto. Para ello combina análisis, inteligencia y consejos para remediar cualquier fallo de seguridad detectado en DevOps.

www.sonatype.com

Snort

■ Su software puede utlizarse como un sistema de detección de intrusiones de una red (NIDS), así como realizar análisis de protocolos, búsqueda de contenido y monitorizar el proceso para prever ataques por vulnerabilidades o técnicas conocidas –como desbordamientos de búfer–.

www.snort.org

Sumo Logic

■ Cuenta con una plataforma de analítica de datos y ofrece inteligencia continua en tiempo real en todo el ciclo de vida de las aplicaciones. Así aplica su tecnología tanto a nivel de código como en el resto de los pasos hasta su despliegue.

www.sumologic.com

Synopsys

■ Su software está pensado para ayudar a los equipos de desarrollo a crear software seguro y de alta calidad, minimizando los riesgos y maximizando la velocidad y la productividad. Con una combinación de herramientas, servicios y experiencia, permite 'securizar' aplicaciones, proporciona análisis estáticos, análisis de composición de software y soluciones de análisis dinámico que permiten a los equipos encontrar y corregir rápidamente vulnerabilidades y defectos en código propietario, componentes de código abierto y comportamiento de aplicaciones.

www.synopsys.com

Qualys

■ Pensada para desarrollar soluciones en la nube, su tecnología da visibilidad, de forma rápida e intuitiva, de todos los activos de TI sin importar su ubicación. Ofrece integración nativa con AWS, Google Cloud, Azure y otras nubes, asi como análisis de vulnerabilidades, su corrección y protección de aplicaciones web, entre otras funciones.

www.qualys.com

Tripwire

■ Dispone de una plataforma que permite implementar normativas en las aplicaciones, implantar la protección por diseño mediante la automatización de procesos de seguridad en los flujos de trabajo pudiéndose integrar con SIEMs, IT-GRC y otros sistemas de gestión.

www.tripwire.com

Veracode

■ Ofrece una solución, basada en nube, que proporciona un entorno de seguridad durante todo el proceso de producción. Su automatización permite corregir con rapidez las vulnerabilidades conocidas en el código del software usado, sin importar si es comercial o de código abierto, entre otras funcionalidades.

www.veracode.com

XebiaLabs

■ Es unas de las referencias en software para DevOps y entrega continua y dispone de una plataforma en la que también tiene integradadas las herramientas de seguridad para desarrollar aplicaciones a gran escala pensadas para la nube. Ofrece un alto grado de configuración según las necesidades de DevOps. Entre otras capacidades propone el uso de las mejores prácticas de AWS, como las configuraciones predeterminadas recomendadas, el uso de roles IAM para una gestión de accesos potente y flexible y el uso de proxies cuando se conecta a AWS para garantizar una seguridad adicional.

xebialabs.com

7 Así cambiará SecDevOps en el futuro

"Desde un punto de vista técnico, nos sorprende la cantidad de problemas de seguridad que se descubren al comenzar a aplicar la filosofía SecDevOps, de los que ni siquiera éramos conscientes antes de hacerlo. Desde un punto de vista organizativo, nos asombra como el cambio de paradigma, metodología y mentalidad provoca un cambio positivo en prácticamente todo el mundo y mejora la colaboración y trabajo en equipo. Por eso creemos que, en poco más de una década, formará parte del día a día, y lo tendremos tan interiorizado que no le daremos importancia. Por otro lado, las herramientas y automatizaciones serán muy sofisticadas y harán uso de cantidades enormes de datos y modelos avanzados de inteligencia artificial para la toma inmediata de decisiones, de manera que simplificarán enormemente todos los procesos y permitirán, de manera sencilla, hacer cosas que hoy día ni siquiera imaginamos", resaltan desde **BBVA Next Technologies**.

"Con DevOps, los desarrolladores tienen y tendrán más influencia y control sobre las herramientas y la infraestructura que antes, por lo que los equipos de ciberseguridad deberán ser más proactivos para aprender lo que está sucediendo en su empresa", añade **John Walsh** de **CyberArk Conjur**.

"Quizá un aspecto importante de todo esto es que la ciberdelincuencia seguirá avanzando. Lo decisivo es que comenzamos a hacer lo correcto para hacer que sus ataques sean más difíciles. No podemos evitar todos los ataques, pero podemos aumentar la dificultad para los ciberdelincuentes. Esto reducirá la población de personas que pueden violar con éxito nuestras empresas e infraestructura. Hoy en día, no se necesita ser muy sofisticado para violar las aplicaciones de una empresa", concluye **Peter Chestna** de **CA Technologies**.

Dónde aprender más de SecDevOps

EVENTOS E INICIATIVAS

■ **Asociación Internacional SecDevOps.** Bajo el lema 'Software, seguro y rápido' se trata de la entidad, sin animo de lucro, que intenta aglutinar a los expertos en la materia. www.devsecops.org

■ **SecDevCon** es la referencia mundial en eventos sobre SecDevOps. Comenzó en 2015 y se celebra, cada año, en Boston, Singapur, Tel Aviv y Londres. En cada una participan los grandes expertos mundiales –tiene una parte de charlas y otra de formación–. En su última edición en Reino Unido, en octubre, un español, **Ernesto Bethencourte,** de BBVA Next Technologies, abrió el evento con su ponencia "Habilitando el cambio a la izquierda para desarrolladores de banca, desde cero... y sin romper el banco". www.devseccon.com

■ **Conferencia mundial SecDevOps. MediaOps** organiza encuentros con la participación de los referentes en este campo y compañías com IBM, CA Technologies, Red Hat, etc. Lo más curioso es que se puede asistir a ellas –la inscripción es gratis– a través de realidad virtual. devopsexperience.io

■ **DevSecOpsDays.** Eventos que aspiran a ser una serie global de conferencias –de uno y dos días– para educar, evolucionar y explorar conceptos relacionados con el desarrollo de la seguridad como código. Cada evento es organizado por voluntarios de la comunidad local y cuenta con expertos mundiales como DJ Schleen, Stefan Streichsbier o Swapnil Deshmukh, entre otros. Además, también está presente en grandes citas de la ciberseguridad como la RSA, en EEUU. www.devsecopsdays.com

PUBLICACIONES

■ **El proyecto Phoenix: DevOps y Agilidad para salvar un proyecto fracaso.** Publicado en 2013 por Gene Kim, Kevin Behr y George Spafford es la obra de referencia en DevOps. Explica qué supone en el cambio de culturas de las empresas de TI a través de la historia de un manager y su trabajo en una empresa ficticia, *PartsUnlimited*, dedicada a los automóviles y al que le dan 90 días para sacar adelante un proyecto que va con retraso y en el que se ha superado con creces el presupuesto inicial: el proyecto Phoenix. Ed. IT Revolution

■ **Guía de Seguridad en Aplicaciones para CISOs, de OWASP**. Excelente documento, completo y lleno de claves útiles, publicado por esta entidad sin ánimo de lucro para ayudar a los responsables de la seguridad TIC a gestionar los riesgos en aplicaciones, al considerar la exposición a amenazas emergentes y requisitos de cumplimiento. Eso sí, se centra en aplicaciones web, componentes de la arquitectura, seguridad de servidores web, servidores de aplicación y bases de datos y no incluye otros aspectos como la seguridad en la red o la infraestructura de red que soporta las aplicaciones. www.owasp.org

■ **Docker: SecDevOps. Rafael Troncoso**, **Fran Ramírez** y **Elías Grande**, explican técnicamente cómo utilizar el mundo de los contenedores –sobre Docker– para automatizar la seguridad en el desarrollo de aplicaciones. Ed. OxWord. *(Ver sección Bibliografía de esta edición de SIC, página 184)*

■ **DevOpsSec,** por **Jim Bird.** Publicado en 2016, su autor explica cómo implementar la seguridad, de forma automática, en el desarrollo de aplicaciones de forma ágil. Para ello ofrece una completa visión de las mejores herramientas y procesos poniendo como ejemplos a compañías como Netflix. "En otras palabras, comprenderá cómo usar DevOps para proteger DevOps", destaca Bird. Ed. O'Reilly Media, Inc.

■ **Securiting DevOps,** por **Julien Vehent**. Entrenida obra sobre cómo pasar del concepto DevOps a SecDevOps a través del protagonisa de la obra, Sam, un experto ficticio del mundo IT que entra a trabajar en una empresa de DevOps para hacer una plataforma web y móvil para administrar facturas médicas y facturación. O sea: una aplicación con datos críticos desarrollada por un pequeño equipo de gente –una *startup*–. Por ello, este libro tiene formato de "manual práctico, con una saludable dosis de conceptos, por lo que tendrá la oportunidad de poner en práctica la teoría de inmediato", explica su autor. Ed. Manning Publications