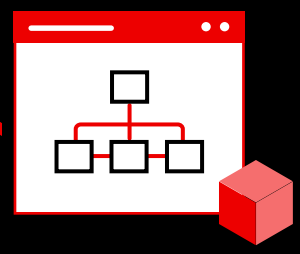
Red Hat
OpenShift
Platform Plus

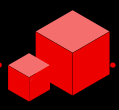
Diseñe una fábrica de software que respalde a DevSecOps

Una guía fundamentada para comenzar el proceso de adopción de DevSecOps

Contenido



Proteja su empresa de la mano de DevSecOps



Cada vez es mayor la cantidad de empresas que adoptan las tecnologías **de contenedores** y **de microservicios** y las **desarrolladas en la nube** para generar innovaciones y **transformarse digitalmente**. En este proceso de transformación, muchas empresas utilizan Kubernetes para organizar los contenedores y, así, respaldar las operaciones de la nube. Debido a que los **clústeres de Kubernetes** pueden incluir hosts en entornos de nube y en las instalaciones, Kubernetes es una plataforma ideal para alojar las aplicaciones que se desarrollan en la nube que requieren operaciones resistentes y de capacidad de ajuste rápido.

Sin embargo, se presentan desafíos nuevos, sobre todo en torno a la seguridad y la capacidad de gestión adecuadas. De hecho, el 50 % de los líderes sénior de TI en las empresas mencionan que la ciberseguridad es una de sus tres prioridades en lo que respecta a las iniciativas tecnológicas.[1]

Con los enfoques y las prácticas de DevSecOps, podrá incorporar la seguridad en las aplicaciones, los procesos y la plataforma y, de esa forma, mejorar la protección de la empresa.

En este ebook se analizan los aspectos fundamentales que deben considerarse para desarrollar una práctica exitosa de DevSecOps con Red Hat OpenShift Platform Plus y otras tecnologías de Red Hat y se proporcionan algunas pautas al respecto.

¿Qué son las aplicaciones desarrolladas en la nube?

Una **aplicación desarrollada en la nube** es un conjunto de servicios pequeños, independientes y sin conexión directa.

¿Qué es DevOps y DevSecOps?

DevOps es un modo de abordar la cultura, la automatización y el diseño de plataformas que se centra en aportar mayor valor empresarial y capacidad de respuesta mediante la prestación ágil y automatizada de servicios de alta calidad. **DevSecOps** amplía la cultura de colaboración de DevOps e incorpora la seguridad en todos los ciclos de vida de las aplicaciones. Incluye a las personas, los procesos y la tecnología para que la seguridad se siga extendiendo en los entornos distribuidos.

Con DevSecOps, las tareas en materia de seguridad son responsabilidad de todos los equipos, no de uno solo que debe encargarse de completarlas recién al final del proceso de desarrollo e implementación. Los integrantes de los equipos de seguridad, desarrollo y operaciones trabajan en conjunto y comparten los comentarios, el conocimiento adquirido y la información valiosa. Este enfoque permite incorporar la seguridad al comienzo del desarrollo de aplicaciones y de la implementación de infraestructuras, lo cual aumenta la protección y reduce los riesgos.

88%

de las empresas encuestadas utilizan Kubernetes para organizar los contenedores, y el 74 % lo utiliza en la etapa de producción.[2]

74%

de las empresas encuestadas cuenta con una iniciativa de DevSecOps.[2]

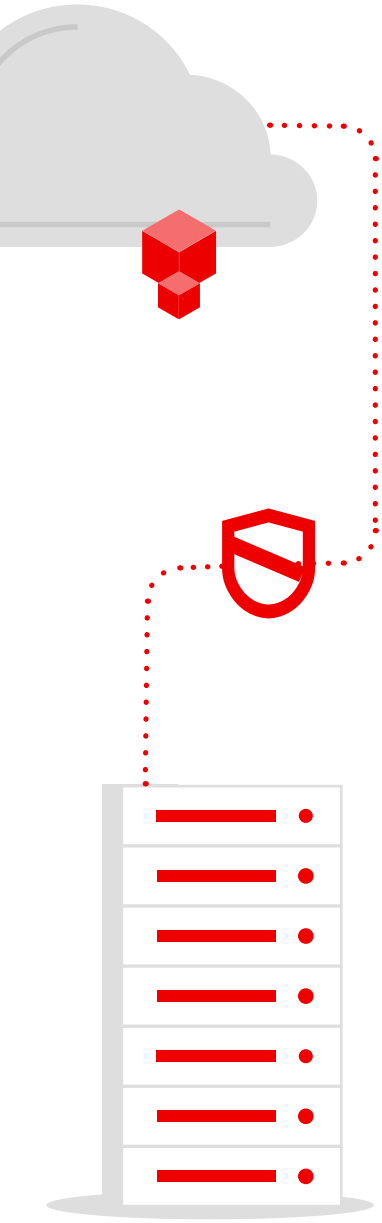
1 Flexera. "2021 Flexera State of Tech Spend Report", enero de 2021.

2 Red Hat, "Informe sobre la seguridad de Kubernetes", 2021.

Objetivos de DevSecOps

El objetivo de DevSecOps es distribuir e implementar con rapidez y según sea necesario las aplicaciones, los servicios y las funciones, que deben gozar de alta calidad y centrarse en la seguridad.

- Capacidad de ajuste
- Velocidad
- Seguridad
- Estabilidad



Desafíos para la implementación de DevSecOps

Procesos manuales

Cuando se requiere una intervención frecuente de las personas, las tareas de desarrollo, prueba y seguridad pueden llevar mucho tiempo y volverse tediosas, propensas a errores y difíciles de aplicar.

Colaboración limitada entre los equipos

En general, los equipos de desarrollo, seguridad y operaciones solo realizan tareas que pertenecen a sus campos de actividad, lo cual provoca que los procesos se fragmenten bastante, la información deba traspasarse de forma manual y el conocimiento y la comprensión de los desafíos y las necesidades de los otros equipos sean limitados.

Aplicación tardía de los procesos de seguridad

Con los enfoques tradicionales de desarrollo y lanzamiento de aplicaciones, las prácticas y las comprobaciones de seguridad se aplican recién al final del proceso, antes de que se implementen en la producción.

Complejidad del entorno de la aplicación

Puede ser un desafío comprender las conexiones y las implicaciones de seguridad de los diferentes elementos —contenedores, microservicios y servicios en la nube—, ya que forman parte de entornos complejos de desarrollo, prueba y producción de las aplicaciones a gran escala.

Dependencias externas

El desarrollo de aplicaciones en la nube casi siempre depende de una cierta cantidad de dependencias externas —como secciones de código open source, bibliotecas y servicios— que también deben protegerse.

Panorama de la seguridad en evolución

Las amenazas a la seguridad y las normas —incluidos los requisitos empresariales, técnicos y geográficos— cambian a un ritmo acelerado, lo cual dificulta que se mantenga actualizado y cumpla con las normativas.

Las personas, los procesos y la tecnología son fundamentales

DevSecOps no es un equipo ni un proceso único. Se trata de un enfoque integral que implica toda la empresa y que requiere cambios y adaptación en tres áreas: personas, procesos y tecnología.

Personas

Las personas son fundamentales para cualquier iniciativa que se lleve a cabo en toda una empresa, y DevSecOps no es la excepción. Todos los equipos —incluso los de las áreas de desarrollo, seguridad y operaciones— deben incorporarse, participar y tener confianza mutua para poder adoptar DevSecOps en toda la empresa.

Procesos

Los procesos permiten que los proyectos avancen por las distintas etapas, desde el inicio hasta la finalización. Por ello, a la hora de adoptar DevSecOps, es esencial que todos sean claros: tanto los de creación, implementación, gestión y adaptación de las aplicaciones y la infraestructura como los de incorporación de la seguridad a lo largo de sus ciclos de vida.

Tecnologías

La plataforma de aplicaciones proporciona las funciones necesarias para diseñar, implementar y ejecutar las aplicaciones y la infraestructura. Si utiliza una plataforma unificada que respalde a los equipos de desarrollo, seguridad y operaciones, tendrá una base para diseñar y adaptar la práctica de DevSecOps.

Prepare a su empresa para adoptar DevSecOps con éxito

Ninguna empresa puede implementar la práctica de DevSecOps por completo de la noche a la mañana, ni hacerlo en un solo paso. Se trata de un proceso de aprendizaje iterativo. Como tal, requiere una estrategia lógica y sostenible que lo guíe hacia el progreso y con la que aprenda con el tiempo.

Fomente la colaboración entre los equipos

Ofrezca incentivos y diseñe procesos que promuevan la colaboración en toda la empresa. Con la coordinación, los equipos pueden crear flujos de trabajo de DevSecOps completos que aportan mayor valor. El trabajo en equipo también ayuda a cultivar la responsabilidad compartida del desarrollo, la seguridad y las operaciones.

Documente su estado actual

Utilice marcos dinámicos como **GitOps** para documentar detalladamente los procesos actuales de desarrollo, gestión de cambios y control. De esa manera, comprenderá su situación actual y los desafíos que tiene que enfrentar, y podrá planificar el camino a seguir. A medida que adapte sus procesos, asegúrese de documentar los nuevos, así como el motivo de los cambios.

Evalúe sus procesos

Identifique los procesos que no sean compatibles con sus objetivos de DevSecOps y adáptelos. Entre ellos, se puede mencionar la infraestructura y las configuraciones de integración/implementación continuas (CI/CD) ineficaces o discrepantes, los procesos excesivamente centralizados y, además, aquellos que dependen de una intervención manual frecuente.

Defina el éxito y mídalo

Determine las expectativas de éxito en materia de DevSecOps en la empresa y establezca las métricas para medirlo o los indicadores clave de rendimiento (KPI) para realizar un seguimiento del progreso. Las métricas podrían calcular la duración del diseño y de la implementación de la aplicación, la tasa de errores y lanzamiento de cambios, el tiempo de resolución de problemas o la disponibilidad de la aplicación.

Comparta los conocimientos y las prácticas recomendadas

Conforme un equipo de los principales interesados; normalmente se lo conoce como comunidad de práctica (CoP) o centro de excelencia (CoE), y se dedica a compartir las prácticas recomendadas, las experiencias y los logros en torno a DevSecOps con toda la empresa. Este equipo también debería ayudar a otros que están listos para adoptar DevSecOps y comenzar a trabajar.

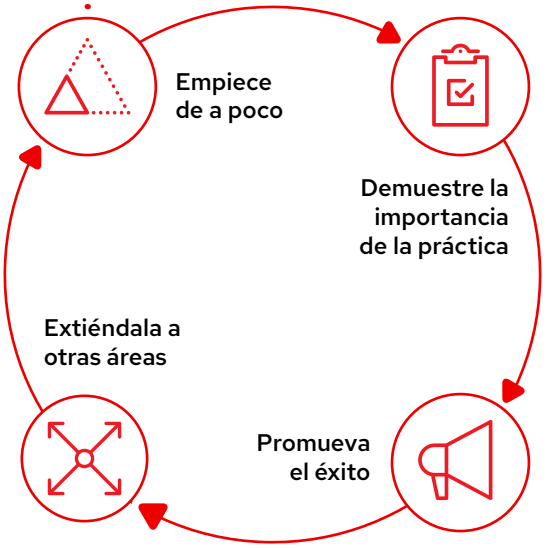
Comprométase con toda la empresa

Asegúrese de que todo el personal de la empresa se comprometa a adoptar DevSecOps. Explíqueles a los equipos los motivos de cada cambio y haga hincapié en el impacto positivo que pueden tener en sus funciones. Los equipos podrán progresar gracias al respaldo de los ejecutivos y los incentivos basados en métricas.

Inicie su práctica de DevSecOps

Una vez que haya definido la estrategia de DevSecOps, será el momento de comenzar. No todos los equipos de desarrollo estarán preparados para adoptar DevSecOps de inmediato. Comience con aquellos que hayan adoptado con éxito los nuevos procesos y las plataformas según las métricas. A menudo, los miembros de estos equipos son también buenos candidatos para formar parte de aquel de los principales interesados.

Empiece poco a poco, demuestre la importancia de la práctica de DevSecOps, extiéndala a otras áreas con cautela y repita los procesos. Trabaje para lograr éxitos progresivos en poco tiempo. Supervise el progreso con las métricas y aprenda de los proyectos o los procesos menos exitosos. Promueva el valor de DevSecOps con cada logro y comparta la experiencia del equipo con toda la empresa. Esto sienta las bases para que otros tomen su experiencia y ofrezcan aún más valor a partir de ella.



Adopte un enfoque basado en la fabricación de software para su distribución

La distribución de los sistemas de software modernos debe ser veloz, uniforme y de gran calidad. Si adopta un enfoque que se base en la fabricación de software, podrá habilitar, agilizar y aplicar los cambios de comportamiento y las conductas necesarios para que su empresa desarrolle una cultura que priorice la práctica DevSecOps. Asimismo, podrá desarrollar e implementar rápidamente aplicaciones de alta calidad utilizando una **cadena de suministro de software de confianza** y un conjunto uniforme de procesos ágiles, como el desarrollo basado en pruebas.

Beneficios de la fábrica de software

Un enfoque basado en la fabricación de software ofrece beneficios medibles:

Menor tiempo de espera para obtener cambios

Mayor frecuencia de implementación

Menor cantidad de tiempo para restaurar los servicios en los que se produjo el error

Baja tasa de errores en los cambios

Cifras de las métricas del rendimiento de la distribución de software[3]

Métrica del rendimiento de la distribución de software	Con una fábrica de software	Sin una fábrica de software
Tiempo de espera para obtener cambios	Menos de 1 hora	Entre 1 y 6 meses
Frecuencia de implementación	Según el uso (menos de 1 vez por día)	Una vez cada 1 o 6 meses
Tiempo necesario para restaurar los servicios	Menos de 1 hora	Entre 1 día y 1 semana
Tasa de errores en los cambios	Entre el 0 % y el 15 %	Entre el 16 % y el 30 %

*3 Google Cloud. "***Informe del estado de DevOps de Accelerate 2021***", septiembre de 2021.*

La fábrica de software

Una fábrica de software le permite transformar los procesos manuales que no son uniformes en operaciones automatizadas que sí lo son.

Sin una fábrica de software

Los procesos manuales y las aprobaciones ralentizan los procesos de desarrollo e implementación, crean expectativas confusas y dificultan la aplicación uniforme de la seguridad. Incluso los cambios pequeños pueden tomar días o semanas en implementarse, por lo que, a menudo, los equipos intentan realizar muchos en una sola implementación. Esto aumenta el riesgo de que se produzcan errores y compromete la seguridad.

La falta de transparencia en todo el proceso debilita la confianza entre los equipos. Las medidas de seguridad y cumplimiento se aplican de forma manual en una etapa avanzada del proceso, por lo que es posible que los errores no se detecten durante el desarrollo. Como resultado, es posible que las aplicaciones deban enviarse nuevamente a los desarrolladores para que corrijan los problemas de seguridad y cumplimiento que no se previeron. Estas sorpresas suelen provocar frustración y desconfianza entre los equipos en una fase que, de por sí, ya es estresante.

Con una fábrica de software

Los procesos definidos y automatizados aceleran el desarrollo y la implementación, refuerzan la seguridad de manera uniforme y establecen expectativas claras para todos los equipos involucrados. Como los cambios pequeños toman tan solo minutos, los equipos pueden implementar muchos a diario y con rapidez, lo que supone un menor riesgo en general.

La transparencia y la visibilidad son características clave en todas las fábricas de software, lo que promueve la confianza entre los equipos de desarrollo, operaciones y seguridad. Las medidas de seguridad y cumplimiento se aplican de forma automática durante la etapa de desarrollo, por lo que los problemas pueden detectarse y solucionarse con más anticipación durante el proceso. Al tener los procesos y las políticas documentados, los equipos entienden las expectativas y pueden prevenir sorpresas cuando implementan las aplicaciones en la etapa de producción.

Diseñe su propia fábrica de software

La **automatización** es el núcleo del enfoque basado en la fabricación de software. Es fundamental para trabajar en los entornos de la nube y adoptar las prácticas de DevSecOps. Lo ayuda a ajustar de forma controlada las operaciones de desarrollo, distribución, implementación e infraestructura. Asimismo, le permite preparar y eliminar de manera dinámica los recursos, los entornos y las aplicaciones. Por lo tanto, la empresa puede responder más rápido a los cambios.

Considere la posibilidad de automatizar todos los procesos del flujo de trabajo de DevSecOps: los de desarrollo, prueba, control de calidad del código, validación del cumplimiento, detección de puntos vulnerables y resolución de problemas. Puede utilizar los canales de CI/CD para automatizar tanto el desarrollo y la mejora de las aplicaciones como la implementación y la gestión de la infraestructura. Defina y documente las políticas de seguridad y riesgo y automatice la verificación del cumplimiento y la resolución de problemas de dichas políticas a lo largo de los ciclos de vida del software.

La automatización declarativa y basada en las intenciones facilitará y agilizará su capacidad de ajuste y adaptación.

La automatización declarativa le permite definir la configuración deseada para una aplicación o infraestructura, en lugar de un conjunto de instrucciones para configurar los recursos. Para ello, debe describir el objetivo final en lugar de los medios para alcanzarlo. A continuación, la plataforma de aplicaciones ajustará y configurará los recursos necesarios para alcanzar el estado deseado. También se autocorregirá para garantizar que los recursos permanezcan configurados de forma correcta a lo largo del tiempo. Este enfoque lo prepara para **GitOps**: un conjunto de prácticas para gestionar la configuración de las aplicaciones y la infraestructura mediante el sistema de control de versiones Git.

¿Qué debería automatizar y cuándo debería hacerlo?

Al igual que DevSecOps en su totalidad, la implementación de la automatización también es un proceso que requiere planificación. Siga estos pasos para comenzar con la automatización:

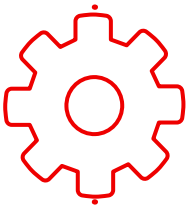
1. Documente el proceso en detalle.
2. Por cada paso que requiera alguna implementación manual, registre las decisiones y la forma en que se toman. Es posible que, para tomar decisiones, deba leer cierto material, considerar factores específicos, consultar a varios expertos, entre otras acciones.
3. Identifique todos los pasos manuales que puedan automatizarse con facilidad y evalúe el nivel del cambio que debería producirse. Por ejemplo, podría automatizar los cambios pequeños, pero solicitar la aprobación de ciertos equipos para los más grandes.
4. En el caso de los pasos manuales que no pueden automatizarse con facilidad, evalúe qué necesitaría para hacerlo y elabore un plan para implementarla.

Comience a automatizar los procesos ahora mismo: no espere hasta haber identificado todas las áreas que puedan necesitarla. La automatización iterativa de los procesos es, en sí misma, un proceso de DevOps. A medida que automatice, adapte y perfeccione sus procesos, obtendrá habilidades y experiencia valiosas para la práctica general de DevSecOps.

Céntrese en trabajo de interés

La automatización no busca sustituir a las personas; su objetivo es generar productividad, uniformidad y eficiencia. Es la paradoja de la automatización: cuando se pone en práctica, la intervención humana se vuelve más importante, pero menos frecuente.

Si bien algunas personas la perciben como una herramienta para eliminar puestos de trabajo, en realidad representan la posibilidad de que el personal más experimentado en TI se concentre en resolver los problemas de mayor importancia, en lugar de dedicarse a las tareas cotidianas y repetitivas.



Aprenda a automatizar los procesos en toda la empresa

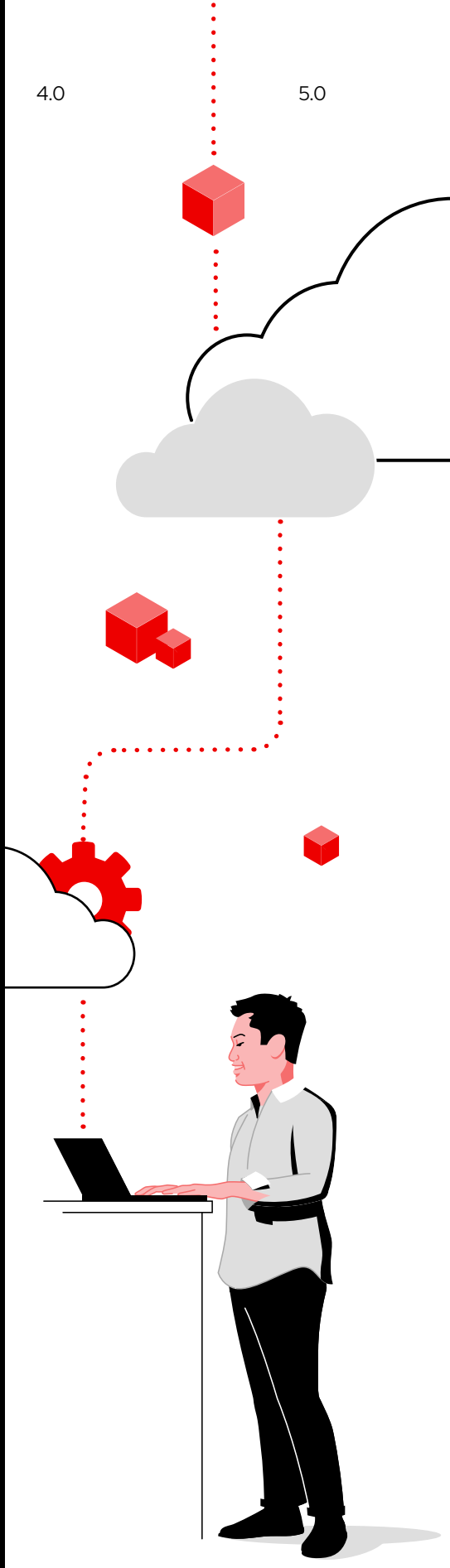
La automatización puede reunir a los recursos humanos, los procesos y las tecnologías para incrementar la agilidad, la innovación y el valor empresariales.

Para obtener más información acerca de la adopción de la automatización en toda la empresa, lea el **ebook sobre la empresa automatizada**.

Herramientas para la fábrica de software

Las herramientas constituyen una parte importante de la fábrica de software. Recomendamos que utilice (y automatice) estas categorías de herramientas. Si bien brindamos ejemplos para cada tipo de herramienta, también se pueden utilizar otras.

Categoría de la herramienta	Ejemplos
Gestión de proyectos	▸ Confluence con Jira ▸ Trello
Gestión del código fuente (SCM)	▸ Github ▸ GitLab
Entornos de desarrollo integrado (IDE)	▸ VS.code ▸ **Red Hat OpenShift Dev Spaces**
Repositorios de artefactos	▸ Nexus ▸ Artefactos
CI/CD	▸ **Red Hat OpenShift Pipelines** ▸ **Jenkins**
Tiempos de ejecución	▸ **Red Hat Runtimes** ▸ Golang
Diseño	▸ Maven ▸ Diseño de Dotnet
Pruebas de unidad	▸ JUnit ▸ NUnit
Análisis del código fuente	▸ SonarQube ▸ Fortify
Pruebas estáticas de la seguridad de las aplicaciones (SAST)	▸ Checkmarx ▸ **Red Hat Advanced Cluster Security for Kubernetes**
Pruebas de verificación de los usuarios	▸ Cucumber ▸ Cyprus
Pruebas dinámicas de la seguridad de las aplicaciones (DAST)	▸ Veracode ▸ Synopsys
Telemetría, métricas y registro	▸ **Prometheus** ▸ **Grafana** ▸ **Elasticsearch, Fluentd y Kibana (EFK)** ▸ Splunk
Malla de servicios	▸ Linkerd ▸ **Red Hat OpenShift Service Mesh**



Diseño, implementación y ejecución

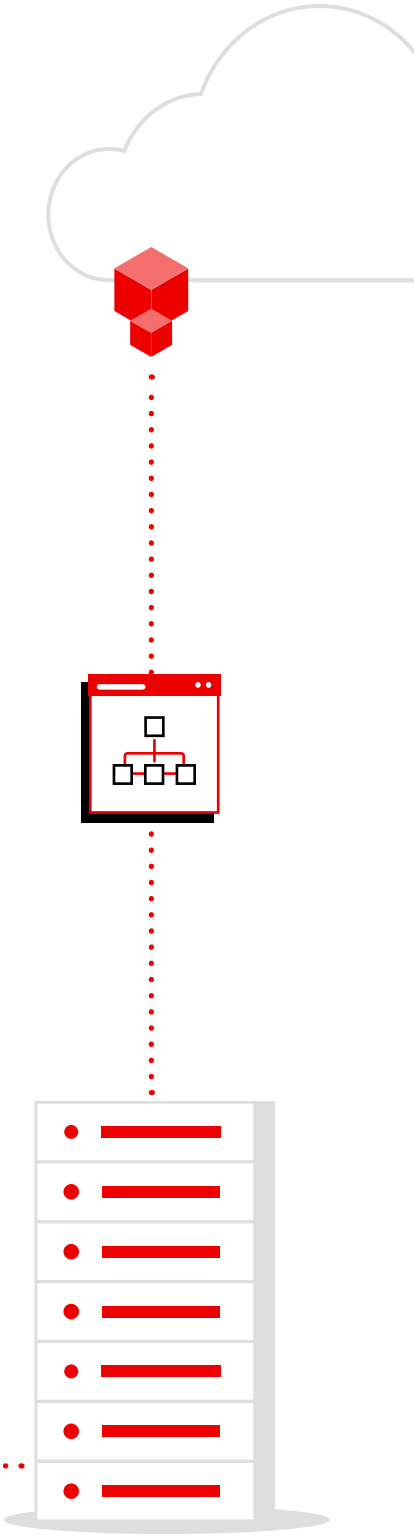
Los arquitectos de plataforma o los ingenieros de DevOps suelen configurar las fábricas de software en nombre de los desarrolladores. Cuando diseñe su fábrica de software, tenga en cuenta las prácticas recomendadas de seguridad en estas tres áreas: diseño, implementación y ejecución.

Diseño

Controle la seguridad de las aplicaciones y el cumplimiento normativo.

En el caso de las implementaciones en la nube, es fundamental que incorpore la seguridad a sus aplicaciones.

- Utilice fuentes confiables para el contenido de los contenedores y las aplicaciones externos, incluidos los tiempos de ejecución.
- Adopte un registro de contenedores privado y de confianza para gestionar las imágenes.
- Automatice sus canales de desarrollo e implementación.
- Implemente requisitos no funcionales en el código mediante prácticas ágiles como TDD.
- Incorpore la seguridad en los canales de la aplicación e incluya la calidad del código, los puntos vulnerables de las imágenes y el análisis de la implementación de Kubernetes.
- Automatice la implementación y la ubicación de las aplicaciones.



Implementación

Proteja su plataforma.

Es necesario que proteja la plataforma de Kubernetes y automatice las políticas de implementación para que la seguridad sea efectiva.

- Reduzca la superficie de ataque con un sistema operativo optimizado para contenedores.
- Automatice la gestión de la configuración y la aplicación de las políticas en todos los clústeres.
- Implemente el acceso con privilegios mínimos con controles de acceso basados en roles (RBAC) detallados.
- Cifre los datos de la plataforma y las aplicaciones en tránsito y en reposo.
- Utilice soluciones automatizadas de cumplimiento, evaluación de riesgos y resolución de problemas.
- Reduzca el riesgo de las implementaciones con las políticas de control de admisión de los pods Kubernetes.

Ejecución

Proteja los tiempos de ejecución de los contenedores.

Mantenga la seguridad de las aplicaciones dentro del tiempo de ejecución.

- Aísle las aplicaciones en ejecución con Security-Enhanced Linux® (SELinux), Security Context Constraints (SCC), espacios de nombres de Kubernetes, RBAC y políticas de red.
- Utilice los cupos para evitar conflictos con los recursos y problemas de rendimiento relacionados.
- Gestione el acceso a las aplicaciones y proteja sus datos mediante la gestión de usuarios de inicio de sesión único y la de la seguridad de entrada y salida, el tráfico cifrado entre pods y la gestión de la interfaz de programación de aplicaciones (API).
- Audite y supervise la actividad de la plataforma y la aplicación.
- Automatice la detección de amenazas y la respuesta frente a los pods con comportamientos inusuales, los eventos de aumento de privilegios y los procesos de riesgo como la criptominería.
- Utilice los controladores de admisión para prevenir la implementación de contenedores que no cumplan con las políticas de seguridad.
- Genere redes de confianza cero utilizando mallas de servicios y políticas de red.

Consejo sobre la seguridad

Lea el **Enfoque en capas para la seguridad de los contenedores y de Kubernetes** para obtener más información sobre la protección de las aplicaciones organizadas en contenedores que se gestionan con Kubernetes.

Diseño	Implementación	Ejecución
Ciclo de vida de las aplicaciones	**Gestión de la configuración de flotas**	**Determinación del estado de las flotas y alertas**
Análisis de los puntos vulnerables	Controlador de admisión de políticas	Análisis del comportamiento del tiempo de ejecución
Análisis de la configuración de las aplicaciones	Evaluación del cumplimiento	Recomendaciones de las políticas de redes
API para la integración de CI/CD	Creación de perfiles de riesgo	Detección de amenazas y medidas de respuesta
Contenido de confianza	Ciclo de vida de la plataforma de Kubernetes	Aislamiento del contenedor
Registro de contenedores	Gestión de identidades y de acceso	Aislamiento de las redes
Gestión de las compilaciones	Datos de la plataforma	Datos de la aplicación y acceso a ella
Canales de CI/CD	Políticas de implementación	Determinación del estado interno

DevSecOps

Implemente DevSecOps con ayuda de los especialistas

Red Hat cuenta con un ecosistema de partners certificados, una amplia experiencia y plataformas innovadoras para diseñar, proteger e implementar aplicaciones en entornos de nube híbrida. Desde hace años, respaldamos a las empresas y las ayudamos a superar sus retos tecnológicos y empresariales mediante las prácticas recomendadas del sector y las tecnologías de open source.

Las plataformas de Red Hat, por ejemplo, proporcionan una base ideal para las soluciones de DevSecOps gracias a una cadena de suministro de contenido de confianza, el respaldo de un equipo de seguridad exclusivo y backports clave de características de seguridad. También ofrecemos **cursos de capacitación y certificación**, **laboratorios interactivos**, **servicios de consultoría** y **soluciones gestionadas** para ayudarlo a desarrollar una práctica de DevSecOps exitosa con mayor rapidez.

Red Hat lo ayuda en cualquier etapa del proceso de adopción de DevSecOps en la que se encuentre.

Con las plataformas comprobadas de open source y los servicios de consultoría especializada que ofrecemos, puede implementar lo que necesite hoy, adaptarse a los cambios del futuro y aprender los métodos y los enfoques necesarios para adoptar DevSecOps de manera eficiente y eficaz.

Más información sobre la elección de Red Hat para DevSecOps.

Aproveche al máximo la inversión en DevSecOps

Red Hat Services puede ofrecerle los recursos que necesita para comenzar a desarrollar la práctica de DevSecOps, agilizarla y ampliarla.

- **Red Hat Open Innovation Labs**
  Un servicio de consultoría parecido a un programa en el que los clientes y los representantes de Red Hat colaboran para adoptar nuevas formas de trabajo —como DevSecOps— mientras generan beneficios empresariales.
- **Red Hat Services Solution: DevSecOps**
  Un servicio que lo ayuda a implementar una fábrica de software con un enfoque modular.
- **Red Hat Services Journey: adopción de los contenedores**
  Un servicio de consultoría que aborda la adopción de contenedores en flujos de trabajo clave.
- **Red Hat Services Journey: adopción de la automatización**
  Un servicio de consultoría que ofrece un marco para gestionar el proceso de adopción de la automatización en toda la empresa.

Implemente una plataforma para adoptar DevSecOps con éxito

Red Hat OpenShift Platform Plus proporciona una base tecnológica y un marco de trabajo bien pensado para DevSecOps. Se trata de una plataforma innovadora de aplicaciones que funciona en la infraestructura de nube y en las instalaciones y se ajusta a ellas de manera uniforme. Red Hat OpenShift Platform Plus es la combinación de una plataforma de Kubernetes empresarial de primer nivel con distintas funciones para diseñar, implementar, ejecutar, proteger y gestionar aplicaciones de manera uniforme en todo el entorno. Las herramientas de gestión de varios clústeres ofrecen una visibilidad completa de los clústeres de Kubernetes, así como control sobre ellos. Las funciones de DevSecOps y la seguridad propia de Kubernetes protegen la cadena de suministro de software, la infraestructura y las cargas de trabajo. Su entorno e información se encuentran protegidos gracias a los servicios de gestión de datos de los clústeres y a un registro con capacidad de expansión que está distribuido en todo el mundo.

Las interfaces de integración abierta y el **ecosistema de partners certificados** de Red Hat le permiten utilizar herramientas de desarrollo, pruebas, operaciones y seguridad, tanto actuales como nuevas, con Red Hat OpenShift Platform Plus. Muchos proveedores ofrecen **operadores certificados de Red Hat OpenShift** o **contenedores de software certificados** para simplificar la instalación y la gestión del software en las plataformas de Red Hat. También puede comprar e implementar muchos productos de software directamente desde **Red Hat Marketplace**. Por último, Red Hat trabaja junto a los principales partners proveedores de nube para ofrecer **servicios de nube de Red Hat OpenShift** completamente gestionados que le permitan no solo optimizar el proceso de implementación y las operaciones, sino también reducir los costos relacionados con la estructura interna.

Elementos de Red Hat OpenShift Platform Plus

Red Hat OpenShift

Red Hat OpenShift es una plataforma de aplicaciones de Kubernetes empresarial con operaciones automatizadas integrales, que permite gestionar las implementaciones de nube híbrida y edge computing. Incluye funciones adaptadas para los desarrolladores para aumentar la productividad y la velocidad.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes es una consola que ofrece visibilidad de todo el dominio de Kubernetes con funciones integradas de control y gestión del ciclo de vida de las aplicaciones.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes es una solución que ofrece funciones de seguridad propias de Kubernetes para mejorar la protección y la visibilidad de la infraestructura y las cargas de trabajo durante todo el ciclo de vida de las aplicaciones.

Red Hat Quay

Red Hat Quay es una plataforma open source de registro de las imágenes de los contenedores que proporciona almacenamiento y permite diseñar, distribuir e implementar los contenedores en los entornos de nube y centros de datos.

Red Hat OpenShift Data Foundation

Red Hat OpenShift Data Foundation es un sistema de servicios de datos y almacenamiento con capacidad de expansión que ofrece eficiencia de datos, resistencia y seguridad a los entornos de Red Hat OpenShift.

Red Hat OpenShift Platform Plus lo ayuda en todas las etapas del proceso de adopción de DevSecOps. Se adapta a su situación actual y le ofrece una base para avanzar a su propio ritmo.

Funciones de seguridad integradas

Utilice la recopilación y el análisis de datos del sistema, así como también más de 60 políticas de seguridad integradas que se pueden aplicar e implementar a todo el ciclo de vida de la aplicación, para supervisar las cargas de trabajo en ejecución y detectar problemas o amenazas de seguridad.

Operaciones uniformes

Aplique políticas operativas uniformes para la seguridad, la configuración, el cumplimiento y el control a los clústeres de Red Hat OpenShift en las infraestructuras de nube y en el centro de datos local.

Herramientas para desarrolladores

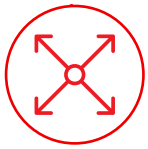
Cree, ejecute e implemente aplicaciones más rápido con una biblioteca incluida de herramientas de diseño, lenguajes, canales y marcos compatibles. El marco del operador ofrece integraciones para las últimas herramientas del desarrollador, que se probaron y verificaron para que puedan ejecutarse en Red Hat OpenShift.

Gestión completa

Gestione el entorno de Red Hat OpenShift con una interfaz uniforme tanto para administradores como para desarrolladores que funcione en entornos locales, de nube y del extremo de la red, incluidos aquellos que se basan en diferentes distribuciones de Kubernetes.

Soporte para DevSecOps

Integre la seguridad declarativa a las herramientas y los flujos de trabajo del desarrollador. Utilice los controles de Kubernetes para reducir las amenazas, aplicar las políticas de seguridad y disminuir el riesgo operativo.



Servicios de datos con capacidad de ajuste

Optimice la gestión de los datos en los clústeres. Red Hat OpenShift Data Foundation ofrece un almacenamiento permanente y resistente para las aplicaciones con estado y los servicios de clúster gracias a la compatibilidad con los protocolos de los datos de archivos, bloques y objetos.

Funciones de red de confianza cero

Implemente redes de confianza cero para lograr que la comunicación entre las aplicaciones y los servicios sea resistente y segura y pueda observarse. Red Hat OpenShift Service Mesh se incluye e integra en Red Hat OpenShift para ayudarlo a proteger las comunicaciones con mayor facilidad.

Red Hat OpenShift Platform Plus ofrece las tecnologías y las funciones necesarias para que adopte DevSecOps de forma efectiva. Lea la **guía de seguridad de Red Hat OpenShift** para entender su aplicación en toda la stack tecnológica.

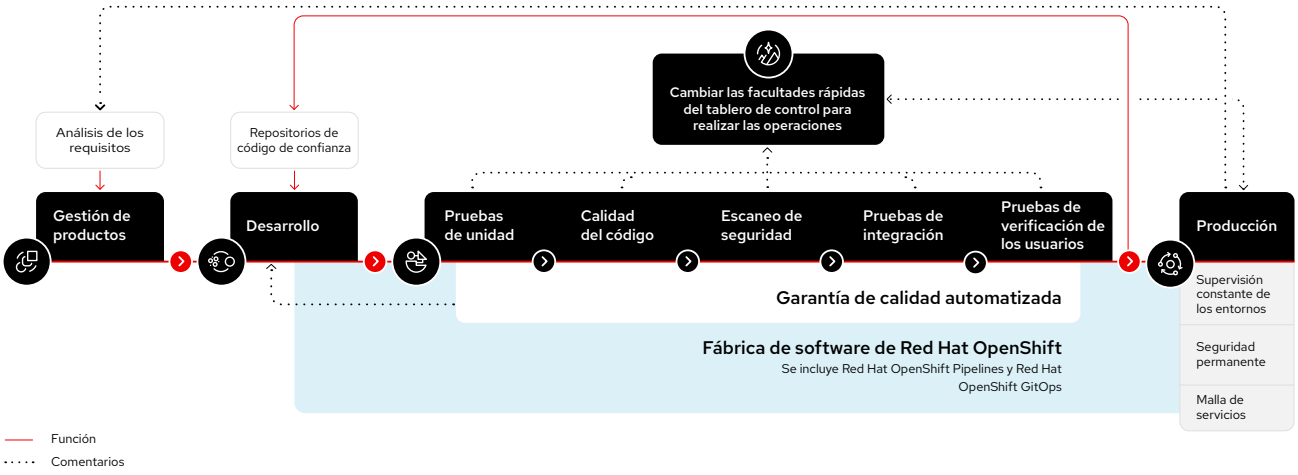
Dé los primeros pasos más rápido con la ayuda de los servicios de nube de Red Hat OpenShift.

Los servicios de nube de Red Hat OpenShift están disponibles en **AWS**, **Google Cloud**, **IBM Cloud** y **Microsoft Azure**, según lo que requiera su empresa. Cada opción ofrece entornos completos e integrales con todos los servicios que necesita, funciones sencillas de autoservicio y soporte permanente de los especialistas con acuerdos estrictos de nivel de servicio (SLA).

Acceda al resumen **Reduzca los costos y logre mayores resultados con los servicios gestionados de Red Hat OpenShift** para obtener más información.

Diseñe una base para la fábrica de software con Red Hat OpenShift Platform Plus

Red Hat OpenShift Platform Plus proporciona una base confiable y adaptable que se puede integrar con diferentes elementos para la fábrica de software. Le permite incorporar los controles de seguridad a sus canales de CI/CD para proporcionar a los desarrolladores recursos automatizados de protección en los flujos de trabajo actuales, proteger las cargas de trabajo y la infraestructura de Kubernetes de los errores de configuración y el incumplimiento normativo, e implementar la detección de las amenazas y las medidas de respuesta durante el tiempo de ejecución.



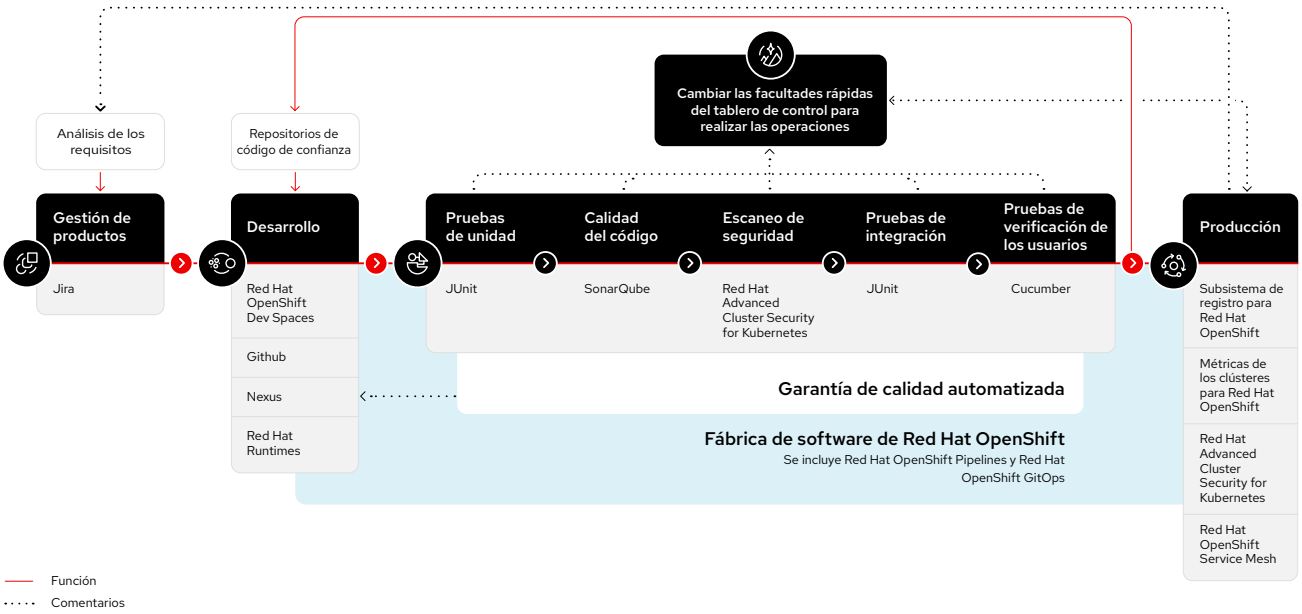
Diseñe fábricas de software completas con un ecosistema de herramientas de terceros

Para cada caso de uso, se requieren diferentes herramientas dentro de la fábrica de software. Si utiliza Red Hat OpenShift Platform Plus, puede diseñar cada etapa de la fábrica de software utilizando los productos y las tecnologías de terceros que prefiera, entre los que se incluyen los siguientes:

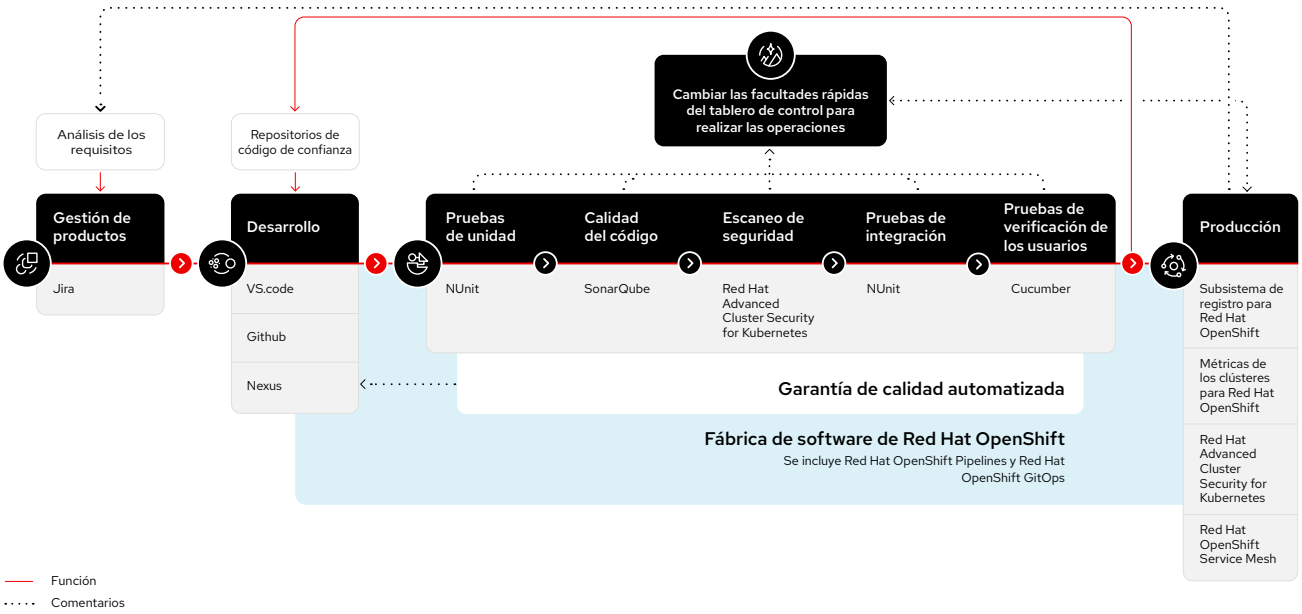
- Herramientas de gestión de acceso con privilegios
- Autoridades de certificación externas
- Soluciones de gestión de claves y almacenamientos externos
- Herramientas de gestión de puntos vulnerables y de análisis del contenido de los contenedores
- Herramientas de análisis del tiempo de ejecución de los contenedores
- Sistemas de gestión de la información y los eventos de seguridad (SIEM)
- Herramientas de gestión del control de versiones
- Repositorios de artefactos
- Herramientas de prueba del software

Por ejemplo, una fábrica de software para el desarrollo de aplicaciones de Spring Boot en la nube utilizaría herramientas de tiempo de ejecución, diseño y pruebas diferentes a las de una fábrica de software para aplicaciones de .NET Core. A continuación, se muestran posibles diseños para estas dos fábricas de software que ilustran la flexibilidad de la base de una fábrica de software de Red Hat.

Fábrica de software para el desarrollo en la nube de aplicaciones de Spring Boot basadas en microservicios



Fábrica de software para el desarrollo en la nube de aplicaciones .NET Core basadas en microservicios



Casos de éxito

Snam es una de las mayores redes de gas natural del mundo. Adoptó las tecnologías y los servicios de Red Hat, entre ellos, Red Hat OpenShift, Red Hat Quay y **Microsoft Azure Red Hat OpenShift**, para impulsar la transformación digital de la empresa. En la actualidad, puede implementar las aplicaciones de forma automatizada en tan solo 30 minutos y así aumentar en más de 10 veces la velocidad de la distribución de sus nuevos productos de software. Snam también puede ajustar las cargas de trabajo y las aplicaciones en cualquier nube pública o privada para cumplir con los requisitos empresariales futuros y reducir los riesgos potenciales relacionados con la dependencia de la nube.

> Red Hat OpenShift es un pilar en nuestro proyecto de transformación. Nos ha permitido crear una plataforma de TI confiable, eficiente y de alto rendimiento, lo que simplifica la gestión de las aplicaciones y los sistemas complejos.

Roberto Calandrini
Director de arquitectura, Servicios digitales y de IA, Snam

Más información

VodafoneZiggo, uno de los principales proveedores de servicios de comunicación y entretenimiento para consumidores y empresas en los Países Bajos, implementó una plataforma de nube híbrida con Red Hat OpenShift para unificar su infraestructura de aplicaciones. La empresa también contrató a Red Hat Consulting para que la orientara en la adopción de DevSecOps, así como en el paso a una cultura más abierta y colaborativa. VodafoneZiggo ahora podrá ampliarse horizontalmente de forma más rápida y eficiente a través de múltiples nubes y hasta el extremo de la red, a medida que las necesidades de la empresa y las demandas del mercado evolucionen.

> Creemos que Red Hat OpenShift es una capa uniforme para las aplicaciones y los servicios desarrollados en la nube y que nos permitirá impulsar la productividad y ofrecer innovación continua.

André Beijen
Director, Redes móviles, VodafoneZiggo

Más información

Comience a utilizar DevSecOps

La velocidad, la capacidad de ajuste y la seguridad son fundamentales para todo lo que se desarrolla en la nube.

Una fábrica de software basada en Red Hat OpenShift Platform Plus puede ayudarlo a establecer una práctica de DevSecOps exitosa que acelere el desarrollo, optimice las operaciones y proteja su empresa.

Pruebe Red Hat OpenShift sin costo:

cloud.redhat.com/try

Más información sobre Red Hat OpenShift Platform Plus:

red.ht/openshift-platform-plus

Copyright © 2022 Red Hat, Inc. Red Hat, el logotipo de Red Hat y OpenShift son marcas comerciales o marcas comerciales registradas de Red Hat, Inc. o sus subsidiarias en Estados Unidos y en otros países. Linux® es la marca comercial registrada de Linus Torvalds en Estados Unidos y en otros países.

F31657_0522_KVM

Red Hat