Parte 6: Integrando Gestión del Cambio, Seguridad de la Información y Cumplimiento

CertiProf®

Professional Knowledge

www.certiprof.com

6.0 Integrando DevOps con Otras Áreas

Puntos a cubrir

A lo largo de esta sección explicaremos cómo tomar los principios de DevOps y aplicarlos a la seguridad de la información, ayudándonos a alcanzar nuestros objetivos y asegurándonos de que la seguridad forma parte del trabajo de todos, todos los días. Una mejor seguridad garantiza que seamos defendibles y sensatos con nuestros datos, que podamos recuperarnos de los problemas de seguridad antes de que sean catastróficos y, lo más importante, que podamos hacer que la seguridad de nuestros sistemas y datos sea mejor que nunca.

En esta sección explicaremos:

1. Seguridad de la Información somos todos.
2. Integración con Gestión del Cambio, Seguridad y otros requisitos de Conformidad y Cumplimiento

Agenda

- 6.1 Seguridad de la Información somos todos
- 6.2 Integración con Gestión del Cambio, Seguridad y otros requisitos de Conformidad y Cumplimiento

6.1 Seguridad de la Información Somos Todos

La seguridad de la información como el trabajo de todos, todos los días

Cuando el área de Infosec se organiza como un silo fuera del Desarrollo y de Operaciones, muchos problemas surgen.

Infosec generalmente tiene menor número de colaboradores que las otras áreas, sin automatización e integración de los elementos de seguridad de la información en el trabajo diario de Dev y Ops, Infosec sólo puede realizar la verificación de conformidad, lo que es lo opuesto de la ingeniería de seguridad de la información.

DevOps puede ser una de las mejores maneras de integrar la seguridad de la información al trabajo diario de todos los involucrados en el flujo de valor de tecnología.

Prácticas para Seguridad de la Información

- Integrar la seguridad en las demostraciones de iteración del desarrollo
- Integrar la seguridad en el seguimiento de los defectos y en los análisis posteriores
- Integrar los controles de seguridad preventiva en los repositorios de código fuente y servicios compartidos
- Integrar la seguridad en nuestro proceso de despliegue
- Garantizar la seguridad de la aplicación
- Garantizar la seguridad de nuestra cadena de suministro de software
- Garantizar la seguridad del entorno
- Integrar la seguridad de la información en la telemetría de producción
- Crear telemetría de seguridad en nuestras aplicaciones
- Crear telemetría de seguridad en nuestro entorno
- Proteger nuestro pipeline de despliegue

Integrar Controles de Seguridad Preventivos

Agregar al repositorio de código fuente compartido:

- **Cualquier mecanismo o herramienta** que nos ayude a garantizar que nuestras aplicaciones y entornos estén seguros
- **Bibliotecas pre-aprobadas por la seguridad** para atender a objetivos específicos de Infosec, como bibliotecas y servicios de autenticación y encriptación

El control de versiones también sirve como un mecanismo de comunicación omnidireccional para mantener a todas las partes conscientes de los cambios que se están haciendo.

Integrar Controles de Seguridad Preventivos

El objetivo es proporcionar las bibliotecas o servicios de seguridad que cada aplicación o entorno moderno requiere, como la activación de la autenticación, autorización, administración de contraseñas, cifrado de datos y así sucesivamente.

Además, podemos proporcionar a Dev y Ops configuraciones de seguridad específicas para los componentes que utilizan en sus pilas de aplicaciones, como para el registro, la autenticación y el cifrado.

Podemos incluir elementos como:
- Bibliotecas de código y sus configuraciones recomendadas
- Administración secreta
- Paquetes de SO y compilaciones

Integrar Seguridad en el pipeline de despliegue

El objetivo:
- Proporcionar a Dev y Ops el feedback rápido sobre su trabajo
- Permitir que detecten y corrijan rápidamente problemas de seguridad como parte de su trabajo diario
- Impulsa el aprendizaje y evita errores futuros

Acciones:
- Automatizar el máximo posible de nuestras pruebas de seguridad
- Pruebas de seguridad automatizadas se ejecutarán en el pipeline de despliegue

Integrar Telemetría en la Seguridad

Para detectar un comportamiento problemático del usuario, que pueda ser un indicador o un facilitador de fraude y acceso no autorizado, debemos crear la telemetría relevante en nuestras aplicaciones.

Los ejemplos pueden incluir:

- Logins de usuario exitosos y fallidos
- La contraseña del usuario se restablece
- La dirección de correo electrónico del usuario se restablece
- Cambios en la tarjeta de crédito del usuario

Crear telemetría suficiente en nuestros entornos para detectar indicadores precoces de acceso no autorizado, especialmente en los componentes que se están ejecutando en la infraestructura que no controlamos (por ejemplo, entornos de hospedaje en la nube).

Ejemplos de alertas sobre ítems:
- Cambios en el sistema
- Cambios en el grupo de seguridad
- Cambios en la configuración
- Cambios en la infraestructura de la nube
- Intentos de XSS
- Intentos de SQLi
- Errores de servidor Web

Proteja el pipeline de despliegue

La infraestructura que soporta nuestros procesos de integración continua y el despliegue continuo también presenta una nueva área de superficie vulnerable a ataques, Por ejemplo, un invasor podría inyectar cambios maliciosos en nuestro repositorio de control de versiones y, por lo tanto, inyectar cambios maliciosos en nuestras aplicaciones y servicios.

Por ejemplo, un invasor podría inyectar cambios maliciosos en nuestro repositorio de control de versiones y, por lo tanto, inyectar cambios maliciosos en nuestras aplicaciones y servicios.

Por ejemplo, un invasor podría inyectar cambios maliciosos en nuestro repositorio de control de versiones y, por lo tanto, inyectar cambios maliciosos en nuestras aplicaciones y servicios.

Para proteger la construcción, integración o el despliegue continuo, las estrategias de mitigación pueden incluir:

- Proteger servidores de construcción e integración continuos
- Revisar todos los cambios introducidos en el control de versiones
- Detectar cuando el código de prueba contiene llamadas de API sospechosas
- Garantizar que todo proceso de IC se ejecute en su propio contenedor o VM aislada
- Garantizar de que las credenciales de control de versiones utilizadas por el sistema de CI sean de sólo lectura

6.2 Integrando con Otras Áreas

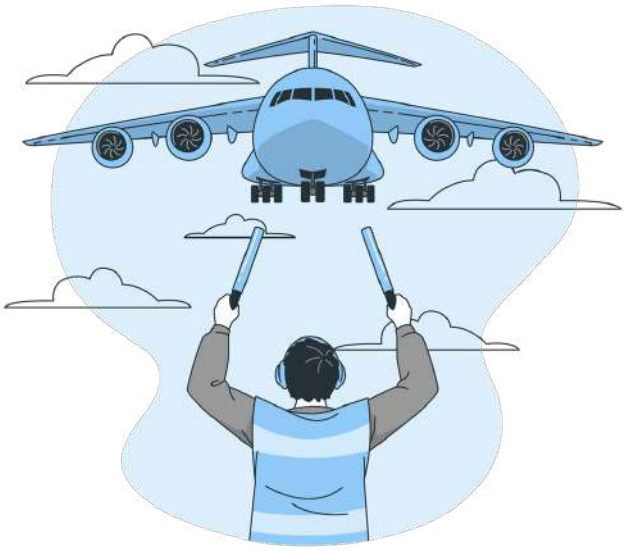
Integración con Gestión del Cambio, Seguridad y otros requisitos de Conformidad y Cumplimiento

En esta sección estudiaremos cómo proteger nuestra tubería de despliegue, así como la forma de lograr los objetivos de seguridad y cumplimiento en nuestros entornos de control, incluyendo la gestión de cambios y la separación de funciones. Algunas buenas prácticas incluyen:

- Integrar la seguridad y el cumplimiento en los procesos de aprobación de cambios
- Recategorizar la mayoría de nuestros cambios de menor riesgo como cambios estándar*
- Definir el tratamiento de los cambios normales*
- Reducir la dependencia en la separación de funciones
- Garantizar la documentación y las pruebas para los auditores y los responsables de cumplimiento

**en base a ITIL*

Seguridad en el Cambio



Casi toda organización de TI de cualquier tamaño significativo tendrá procesos de gestión de cambios existentes, que son los principales controles para reducir riesgos de operaciones y de seguridad.

El pipeline de despliegues ejecutando implementaciones de bajo riesgo:

- Mayoría de nuestros cambios no necesitará pasar por un proceso manual de aprobación de cambios
- Habremos confiado en controles como pruebas automatizadas y monitoreo de producción proactivo

Integrar la seguridad y el cumplimiento en procesos de aprobación de cambios

Los procesos de gestión de cambios buscan implementar controles para reducir los riesgos en las operaciones y de seguridad. Los directores de cumplimiento y de seguridad confían en los procesos de gestión de cambios para cumplir con los requisitos, y suelen exigir pruebas de que todos los cambios han sido debidamente autorizados.

Existen estos tipos de cambios:

- **Cambios estándar:** Son cambios de menor riesgo que siguen un proceso establecido y aprobado, pero que también pueden ser pre aprobados
- **Cambios normales:** Son cambios de mayor riesgo que requieren la revisión o aprobación de la autoridad de cambio acordada
- **Cambios urgentes:** Se trata de cambios de emergencia y, en consecuencia, de alto riesgo potencial, que deben ponerse en producción inmediatamente (por ejemplo, parche de seguridad urgente, restauración del servicio)

Nuestro pipeline de despliegue de estar configurado correctamente para que los despliegues sean de bajo riesgo, y la mayoría de nuestros cambios no necesitarán pasar por un proceso manual de aprobación de cambios, porque habremos confiado en controles como las pruebas automatizadas y la supervisión proactiva de la producción.

Recategorizar la mayoría de nuestros cambios de menor riesgo como cambios estándar*

Al contar con una cadena de despliegue fiable, ya nos hemos ganado una reputación de despliegue rápido, fiable y sin dramas. En este punto, deberíamos tratar de obtener el acuerdo de Operaciones de que nuestros despliegues son de bajo riesgo y pueden ser clasificados como cambios estándar, pre-aprobados por el CAB.

Lo ideal es que los despliegues sean realizados automáticamente por nuestras herramientas de gestión de la configuración y de canalización del despliegue (por ejemplo, Puppet, Chef, Jenkins) y que podamos vincular automáticamente estos registros de despliegues en PROD a elementos específicos en nuestras herramientas de planificación del trabajo (por ejemplo, JIRA, Rally, LeanKit, ThoughtWorks Mingle), lo que nos permite crear más contexto para nuestros cambios, como la vinculación a los defectos, los incidentes de producción o las historias de usuario.

Al hacer esto, podemos rastrear un despliegue de producción a los cambios en el control de versiones y, a partir de ahí, rastrearlos hasta los tickets de la herramienta de planificación.

Qué hacer cuando los cambios son clasificados como cambios normales

Para cambios normales que requerirán la aprobación de al menos un subconjunto de CAB nuestro objetivo es garantizar que podamos desplegar rápidamente, aunque no esté totalmente automatizado.

Por ejemplo, podríamos crear automáticamente un ticket de cambio de ServiceNow con un enlace a la con un enlace a la historia de usuario de JIRA, junto con los manifiestos de construcción y los resultados de las pruebas de nuestra y enlaces a los scripts de Puppet/Chef que se ejecutarán. Esto incluye identificar por qué estamos haciendo el cambio (por ejemplo, proporcionando un enlace a las características defectos o incidentes), a quién afecta el cambio y qué se va a cambiar.

Nuestro objetivo es compartir las pruebas y los artefactos que nos dan confianza en que el cambio funcionará en producción tal y como se ha diseñado, para que CAB puede aprobar más rápidamente.

Reducir la dependencia de la separación de funciones

A medida que aumenta la complejidad y la frecuencia de los despliegues, la realización de despliegues de producción requiere cada vez más que todos los miembros del flujo de valor vean rápidamente los resultados de sus acciones.

La separación de funciones a menudo puede impedir esto al ralentizar y reducir la información que reciben los ingenieros sobre su trabajo. Esto impide que los ingenieros asuman la calidad de su trabajo y reduce la capacidad de la empresa para crear aprendizaje organizativo.

En consecuencia, siempre que sea posible, debemos evitar utilizar la separación de funciones como control. En su lugar, deberíamos optar por controles como la programación por parejas la inspección continua de las comprobaciones del código y la revisión del mismo.

Estos controles nos pueden dar la seguridad necesaria sobre la calidad de nuestro trabajo.

Siempre que sea posible, debemos evitar el uso de la separación de tareas como control.

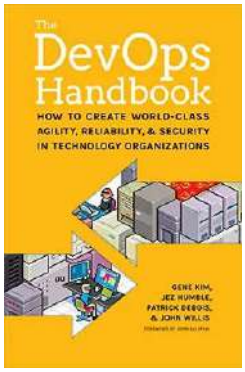
Garantizar la documentación y las pruebas necesarias para auditores y responsables de cumplimiento

A medida que las organizaciones tecnológicas adoptan cada vez más patrones DevOps, hay más tensión que nunca entre TI, auditoría y los responsables de cumplimiento. Para ayudar a cerrar esa brecha, hace que los equipos trabajen con los auditores en el proceso de diseño del control.

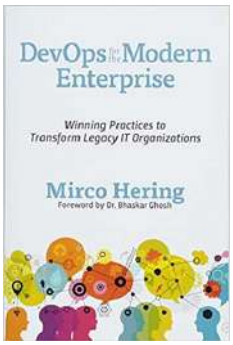
El DevOps Audit Defense Toolkit describe la narración de principio a fin del proceso de cumplimiento y auditoría para una organización ficticia (Parts Unlimited de "The Phoenix Project").
El documento describe cómo podrían diseñarse los controles en una cadena de despliegue para mitigar los riesgos declarados, y proporciona ejemplos de atestados de control y artefactos de control para demostrar la eficacia del control.

Se pretende que sea general para todos los objetivos de control, incluido el apoyo a la presentación de informes financieros precisos, el cumplimiento de la normativa (por ejemplo, SEC SOX-404, HIPAA, FedRAMP, contratos modelo de la UE y la propuesta de normativa Reg-SCI de la SEC), las obligaciones contractuales (por ejemplo, PCI DSS, DOD DISA) y las operaciones eficaces y eficientes.

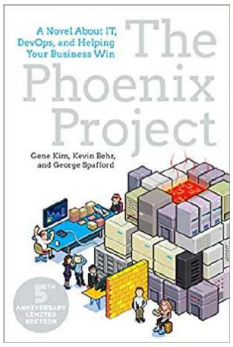
Fuente del Material



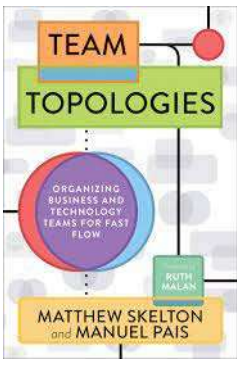
The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations Tapa blanda – Ilustrado, 6 Octubre 2016 de Gene Kim (Author), Patrick Debois (Author), John Willis (Author), Jez Humble (Author), John Allspaw (Foreword).



DevOps For The Modern Enterprise: Winning Practices to Transform Legacy IT Organizations Tapa blanda – 3 Abril 2018 de Mirco Hering (Author), Bhaskar Ghosh (Foreword).



The Phoenix Project (A Novel About IT, DevOps, and Helping Your Business Win) Tapa blanda – Ilustrado, 1 Febrero 2018 de Gene Kim (Author).



Team Topologies: Organizing Business and Technology Teams for Fast Flow Tapa blanda – Ilustrado, 17 Septiembre 2019 de Matthew Skelton (Author), Manuel Pais (Author), Ruth Malan (Foreword).

Material de Apoyo

- https://cloud.google.com/devops
- https://web.devopstopologies.com/
- https://itrevolution.com/the-three-ways-principles-underpinning-devops/
- https://techbeacon.com/devops/10-companies-killing-it-devops
- https://techbeacon.com/devops/10-companies-killing-it-devops-2020
- https://github.com/Netflix/SimianArmy
- https://netflixtechblog.com/the-netflix-simian-army-16e57fbab116

Ilustraciones:

- Storyset | Customize, animate and download illustration for free
- https://www.pinterest.es/pin/798192733957711009/?d=t&mt=login
- https://www.ithinkupc.com/es/blog/como-conseguir-la-eficiencia-en-un-entorno-bimodal-it
- https://compbcn.es/docker-en-pocas-palabras/
- https://jaxenter.com/devops-shifting-left-172792.html
- https://dev.to/mostlyjason/intro-to-deployment-strategies-blue-green-canary-and-more-3a3
- https://www.boldbi.com/integrations/azure-devops
- https://netflix.github.io/chaosmonkey/
- https://blog.aspiresys.pl/technology/chaos-monkey-how-netflix-deals-with-resilience/

DEVOPS ADVANCED PROFESSIONAL CERTIFICATE

DAPC™

CertiProf®

Professional Knowledge

@Certiprof @CertiProf CertiProf @Certiprof_llc CertiProf LLC

www.certiprof.com