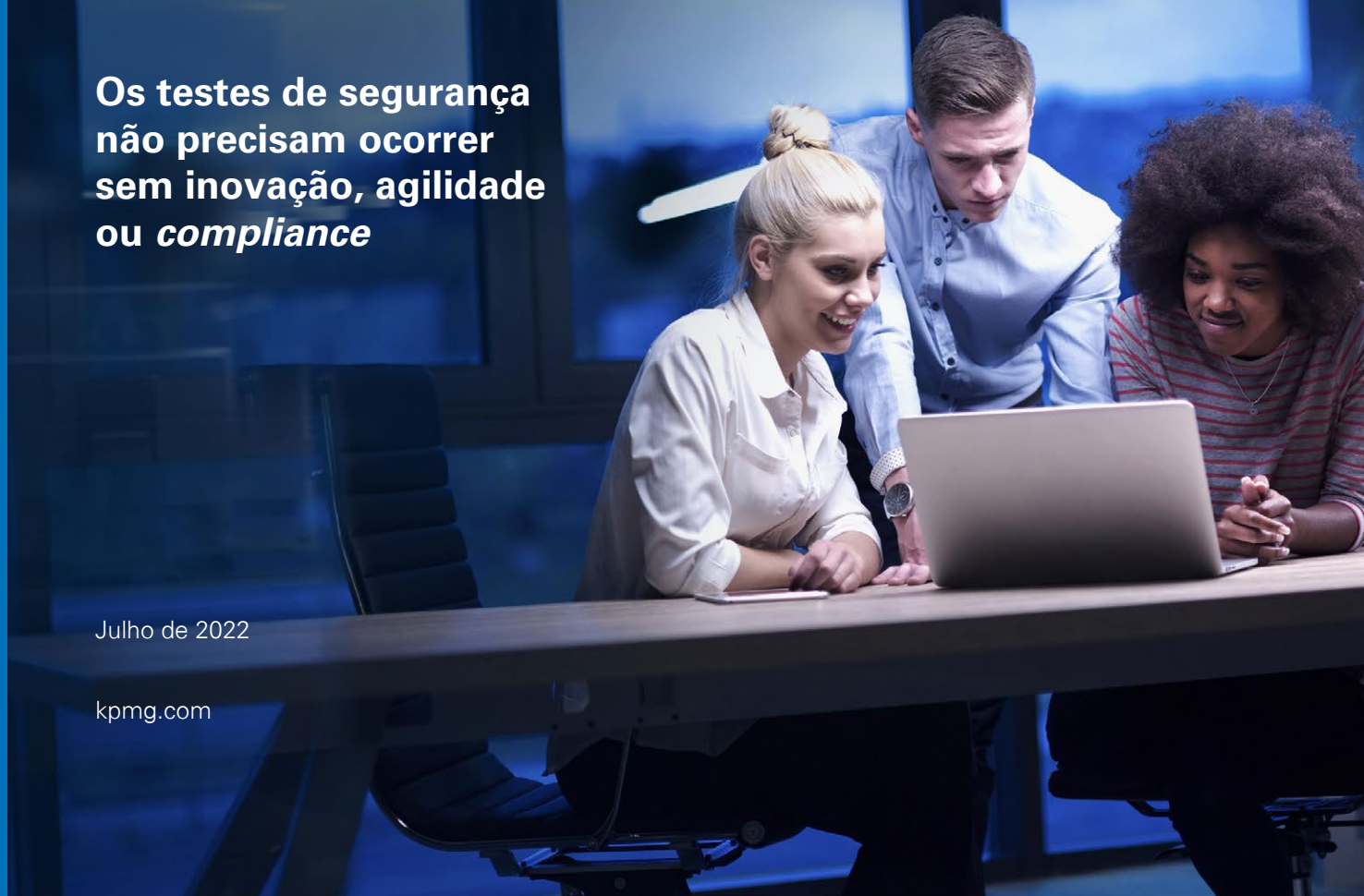
Redefinindo a Segurança por Design: Colaboração, Automatização e Verificação

Os testes de segurança não precisam ocorrer sem inovação, agilidade ou *compliance*



Julho de 2022

kpmg.com

Segurança e *compliance* não precisam passar por turbulências em seu desenvolvimento

Muitas empresas estão em meio a uma tarefa cada vez mais complexa, em que devem considerar a agilidade do desenvolvimento, a proteção contra ameaças à segurança e atenção aos requisitos de auditoria e *compliance*. Em última análise, esse é um exercício de criação e preservação de valor. Acreditamos que uma estrutura conectada, automatizada, com ferramentas integradas e colaboração multifuncional representa o modelo operacional do futuro.

Essa estrutura é a principal base da evolução do DevOps para o DevOps seguro e governado, em que a segurança é alocada no ponto mais inicial possível do processo de desenvolvimento (*shift left*), mas não às custas da governança ou, mais importante, da velocidade de entrega. O resultado é um fluxo de integração contínuo/entrega contínua (*continuous integration/continuous delivery* - CI/CD) muito eficiente, ao longo do qual um código de alta qualidade é construído, os testes são realizados e os aplicativos novos ou atualizados são implementados com segurança.

É fundamental esclarecer o público-alvo deste tipo de ação. Há três públicos envolvidos aqui: as organizações coletivas de entrega e suporte de tecnologia da informação (engenharia de TI), segurança da informação (InfoSec) e risco tecnológico (*Tech Risk*). Estamos focados em prevenir problemas como violações de dados, eventos cibernéticos, interrupções de aplicativos, divulgações não autorizadas, custos financeiros e de reputação resultantes e falhas de processo que levam a esses incidentes — sem inibir a inovação, segurança ou agilidade. A estratégia e a resposta em torno da prevenção de situações futuras estão sob a alçada coletiva desses grupos.

Para que esses grupos trabalhem juntos com eficiência, a base deve ser construída em ferramentas centralizadas que permitam automação e integração e uma estratégia de *shift left* orquestrada de análises operacionais, de segurança e auditoria.

Além disso, um modelo centrado no funcionário e focado no capital humano e os processos multifuncionais relevantes ajudarão a minimizar os gargalos de segurança, a complexidade da auditoria, os atrasos no desenvolvimento, as interrupções e outros problemas operacionais. Essa abordagem fornece uma maneira nova e duplicável de construir, proteger e entregar produtos e serviços às empresas de *software*.

O objetivo é que esses grupos reflitam profundamente se estão preparados para desenvolver, construir e implementar produtos e serviços com segurança, rapidez e escala. Para chegar lá, a dúvida para as equipes que participam do ciclo de vida do desenvolvimento de sistemas (*systems development lifecycle* - SDLC) não é saber se elas estão prontas, mas sim entender se elas conseguem trabalhar de maneira integrada.

Desafios de segurança e *compliance* de DevOps em toda a empresa

Engenharia de TI

- Falta de ferramentas adequadas e integração de ferramentas para auxiliar na análise de causa raiz, alertas automatizados, varreduras etc.
- A entrega geralmente é atrasada ao cumprir a natureza linear do gerenciamento tradicional de mudanças.
- A implementação na produção geralmente é atrasada por uma abordagem *big-bang* para a segurança.
- Os controles de *compliance* e segurança são isolados do SDLC.

Segurança da informação

- A validação da segurança é manual, restringindo a velocidade com que as mudanças são entregues.
- As iterações de produtos não oferecem análise ou modelagem de ameaças.
- Falta de controles, *compliance*, treinamento *secure-by-design* e colaboração multifuncional.
- As equipes não contam com indicadores-chave de riscos, de desempenho ou controles de monitoramento adequados.

Risco tecnológico

- A equipe não tem procedimentos e padrões adequados para assegurar um *compliance* consistente com os requisitos.
- Os controles não são documentados ou automatizados sempre que possível.
- Mudança de controles legados para controles ágeis.

Obter agilidade e *compliance* com segurança

Se as áreas de engenharia de TI, segurança da informação e riscos tecnológicos geralmente atuam separadas, seus processos, pessoas e tecnologias provavelmente também serão desconectados, o que leva a lacunas de agilidade, segurança e operações. Norteadas por uma estrutura de referência padronizada, as empresas podem construir um cenário completo sobre como essa mudança operacional pode beneficiar seus processos existentes. Para gerar valor rapidamente, garantir a segurança e realizar auditorias relevantes e significativas, as organizações são incentivadas a adotar um plano adequado impulsionado pela automação, ferramentas centralizadas e profissionais colaborativos e bem treinados.

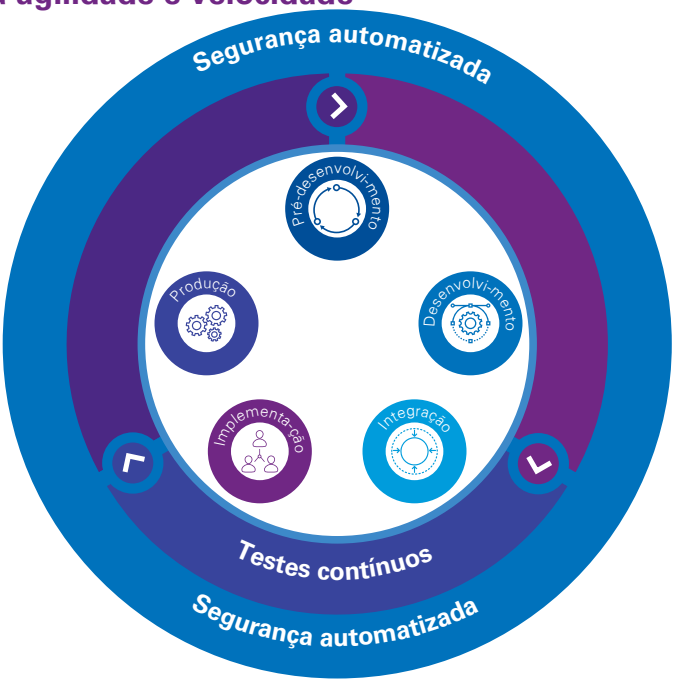
Do ponto de vista da engenharia de TI, a maioria das organizações atualmente conta com vários modelos operacionais em relação à maneira como as pessoas são organizadas, como os processos são projetados para disponibilizar o *software* e como a tecnologia é utilizada para suportar suas capacidades gerais de serviço.

Imagine uma empresa na qual equipes diversas agora atuam de maneira centralizada e orientada para o valor. Essa empresa oferece novos recursos, mudanças e correções rapidamente, sem comprometer a segurança e a governança. As ferramentas centralizadas e a estreita colaboração com as áreas de segurança da informação e de riscos tecnológicos permitem que a área de engenharia de TI reúna os requisitos para automatizar o fluxo de integração contínua/entrega contínua (CI/CD). De fato, a governança e a segurança automatizadas estão no centro operacional desse processo, garantindo que a organização não esteja despreparada para invasões ou seja freada por auditorias.

Nossa estratégia é projetada para mitigar riscos, aumentar a transparência de *compliance* e aumentar a agilidade e velocidade

Principais funções

- TI
- Segurança da informação
- Auditoria



Principais resultados

- Agilidade, velocidade e inovação de negócios
- Proteção contra ameaças à segurança de dados
- Redução de riscos e *compliance*

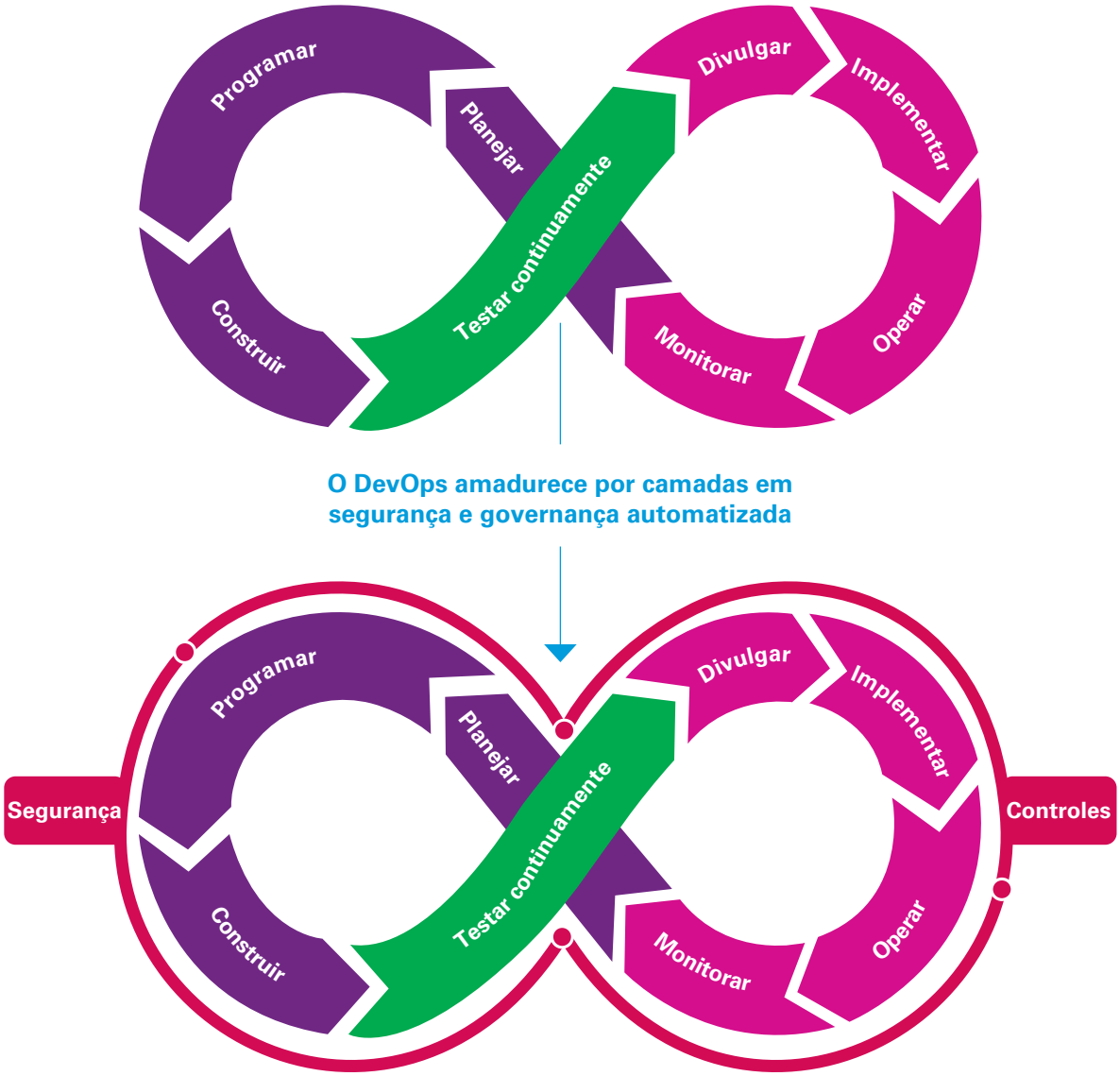
Ferramentas centralizadas

O objetivo final é reduzir ao máximo o risco operacional, de maneira rápida, sustentável e com o mínimo de atrito e de custos, para que a empresa possa concorrer efetivamente no mercado em rápida evolução atual. Colocar todas as equipes no lugar certo para atingir essa situação atualmente não é algo bem compreendido em muitas organizações. Consequentemente, a profundidade, amplitude e frequência de qualquer atividade de redução de risco que as organizações desejam estabelecer tende a ser subdesenvolvida no modelo tradicional de DevOps

De DevOps para o modelo DevOps seguro e governado

Em um nível alto, o DevOps é o alinhamento prático das equipes de desenvolvimento e operações de TI com o objetivo de agregar valor de negócios, por meio da entrega mais frequente de *software* novos e atualizados. Em resumo, o DevOps seguro e governado é a integração da segurança na equação do DevOps em cada etapa. Quando bem executada, essa abordagem acelera o desenvolvimento e a implementação, ao cumprir controles pré-definidos e testes automatizados em todo o SDLC.

O DevOps seguro e governado se baseia no modelo tradicional por camadas em controles automatizados de segurança e governança



O DevOps seguro e governado traz consigo uma arquitetura fundamentada pela segurança, regida por controles relevantes e focada em manter a velocidade de entrega. A varredura do código é incorporada ao fluxo de CI/CD para verificar as práticas de programação seguras antes da execução e implementação.

As principais facetas dessa abordagem incluem:

Mudar a segurança e o *compliance* "para a esquerda"

Garante que as normas de segurança e governança sejam abordadas desde o início do SDLC por meio da automação, não de processos manuais. Melhora a capacidade de implementar alterações na produção continuamente com mitigação de riscos.

Modelo de recursos de DevOps baseado em funcionários

Os dados sugerem que a terceirização das funções de DevOps leva a uma probabilidade significativamente maior de que a equipe apresente um baixo desempenho. Equipes centradas nos funcionários, formadas por *stakeholders* de negócios, são muito mais propensas a apresentar um alto desempenho.

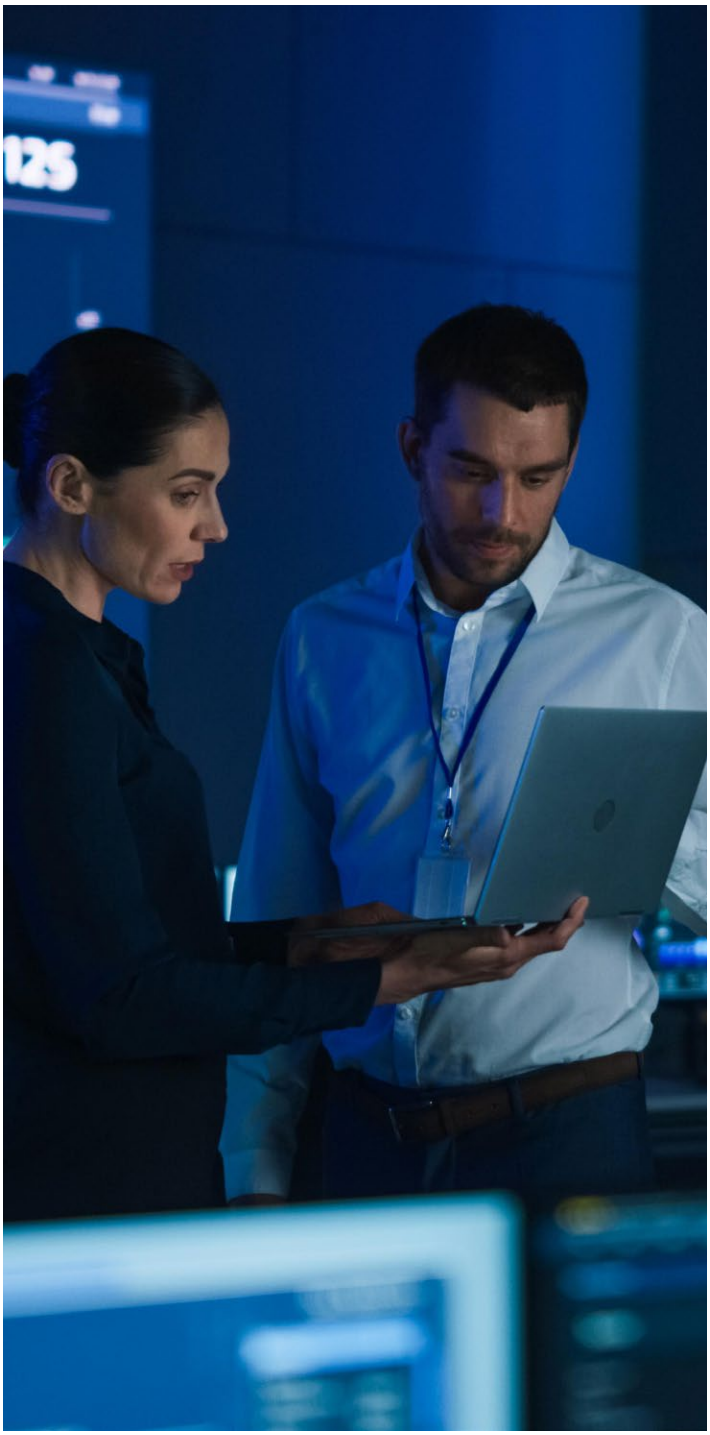
Segurança automatizada

Apresenta testes automatizados, como testes de segurança de aplicativos dinâmicos, interativos, estáticos e análise de composição de *software*, que avaliam se os requisitos de segurança foram abordados na construção.

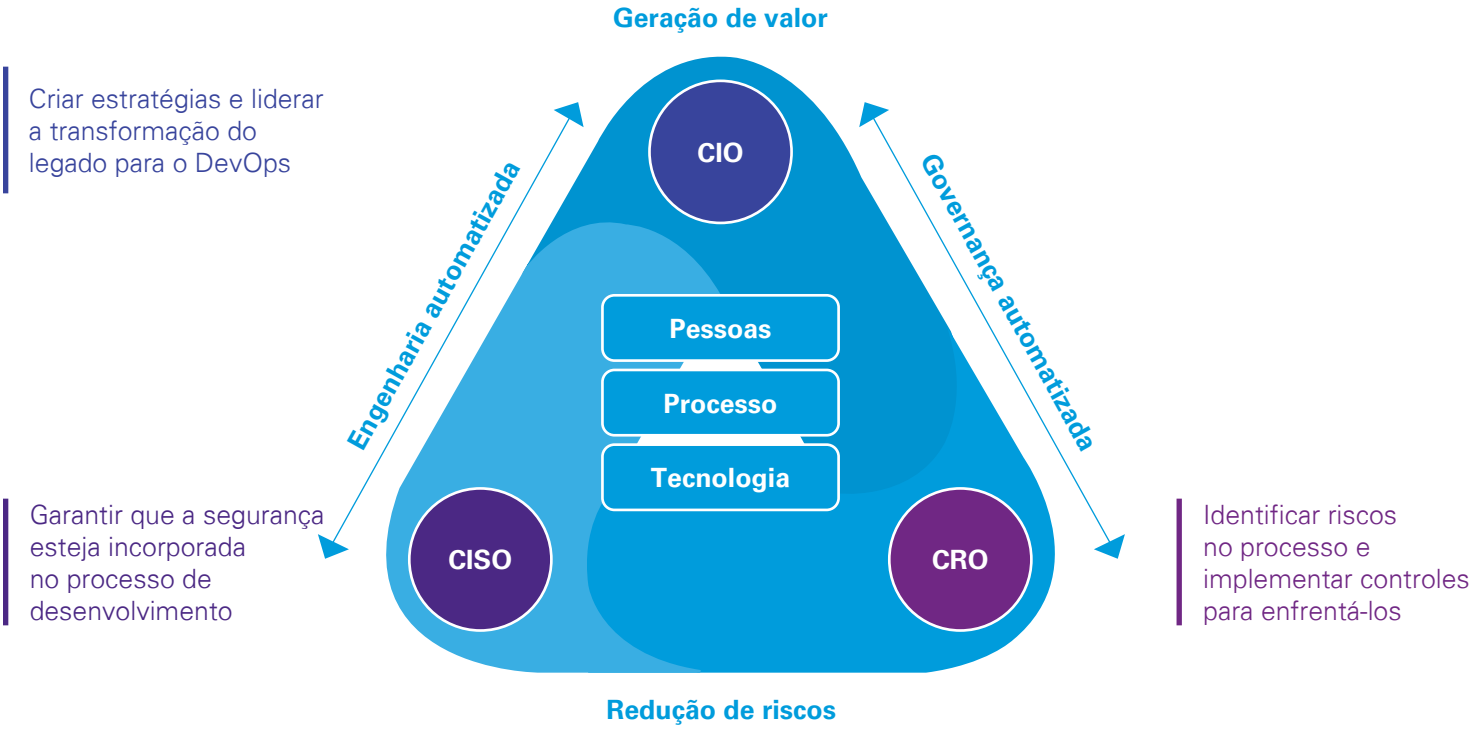
Os desafios de desenvolver um modelo de entrega seguro e governado levaram à criação de uma abordagem padrão para mitigar riscos e aumentar a transparência de *compliance*, ao mesmo tempo que atinge e mantém a agilidade e a velocidade de negócios. Construído sobre uma base de engenharia, governança e segurança automatizadas, o DevOps seguro permite uma colaboração interfuncional produtiva e contínua.

Uma estrutura transformadora

A abordagem da KPMG alinha os objetivos organizacionais automatizando a engenharia e a governança, sempre que possível e viável, possibilitando uma inovação mais rápida e menos riscos visíveis em um "único painel".



De DevOps para o modelo DevOps seguro e regulamentado (DevOps seguro e governado)

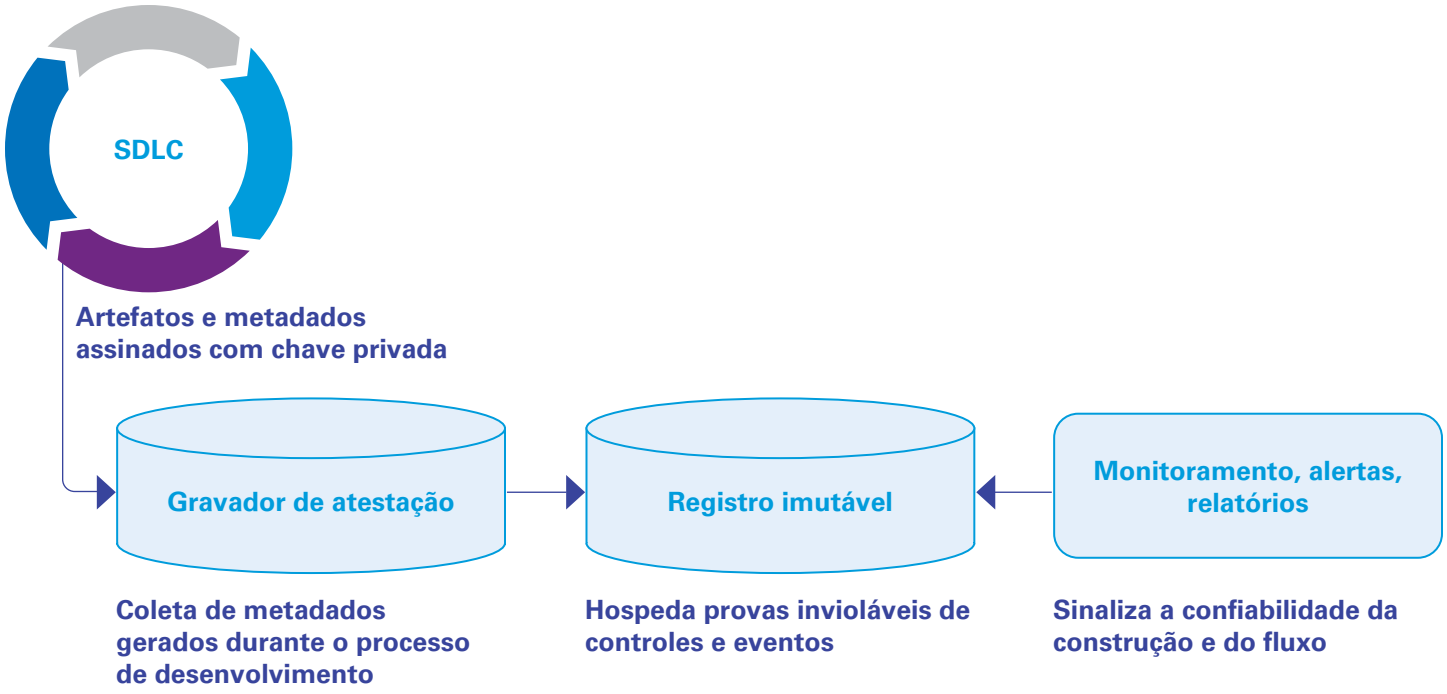


Estabelecer objetivos comuns e definir marcos operacionais cronológicos claros, com níveis progressivos de criticidade de negócios, alinha as áreas de engenharia de TI, segurança da informação e riscos tecnológicos e investe no sucesso de cada uma.

Ao adaptar a organização a um modelo de DevOps seguro e governado, a segurança e os controles se tornam um componente do conjunto de responsabilidades de toda a empresa.

Priorização da rastreabilidade

Um registro de mudança imutável representa um elemento fundamental de rastreabilidade que muitas empresas de desenvolvimento de software não têm nos seus fluxos de CI/CD.



Rastreabilidade: aqui está o desafio

No modelo de DevOps seguro e governado, um registro de alteração imutável (como um log de auditoria à prova de adulteração de todo o SDLC hospedado em um único local) é criado a partir de ferramentas e atividades de upstream. Esse registro então é alimentado pelas atividades de upstream do conjunto integrado de ferramentas.

Ele contribui para o desenvolvimento ou atualização do código (engenharia de TI), realizando testes de segurança proativos (segurança da informação) e garantindo que controles apropriados sejam acionados (riscos tecnológicos). É a maneira com a qual pode ser provado que o produto é preciso, seguro e compatível toda vez que o fluxo for executado.

Esse registro automatizado é criado no final do processo, como forma de agrupar o trabalho de cada grupo e verificar as várias etapas do SDLC. Quando for necessário lançar um novo produto ou atualização, o registro de mudança imutável permitirá rapidamente verificar se ele foi testado com sucesso e revisado por pares. A partir daí, é possível tomar a decisão de liberação rapidamente e com segurança ou, caso imprecisões, inconsistências ou vulnerabilidades sejam detectadas, pode-se pausar o processo, investigar e fazer reparos.

Uma transformação de DevOps segura do mundo real

Um cliente – uma empresa de software de gerenciamento de TI de destaque sediada nos EUA – havia sofrido um ataque na cadeia de suprimentos de *software* que afetou vários clientes, resultando em uma perda de confiança nas capacidades da empresa. Em última análise, a empresa queria transformar seu modelo de entrega sem comprometer os controles ou a agilidade.

Principais desafios

Em resumo, o sistema falhou porque o lançamento de atualizações de aplicativos não foi gerenciado de maneira eficaz. A segurança no qual o código foi construído e compilado em um formato executável não foi considerada, pois a empresa se concentrou em outras prioridades, principalmente na velocidade de lançamento no mercado. Consequentemente, as equipes de risco e segurança tinham uma visibilidade limitada do processo global em função da supervisão ineficaz da governança. Não havia uma abordagem consolidada de DevOps seguro no âmbito corporativo que englobasse engenharia de TI, segurança da informação e risco tecnológico.

Resposta da KPMG

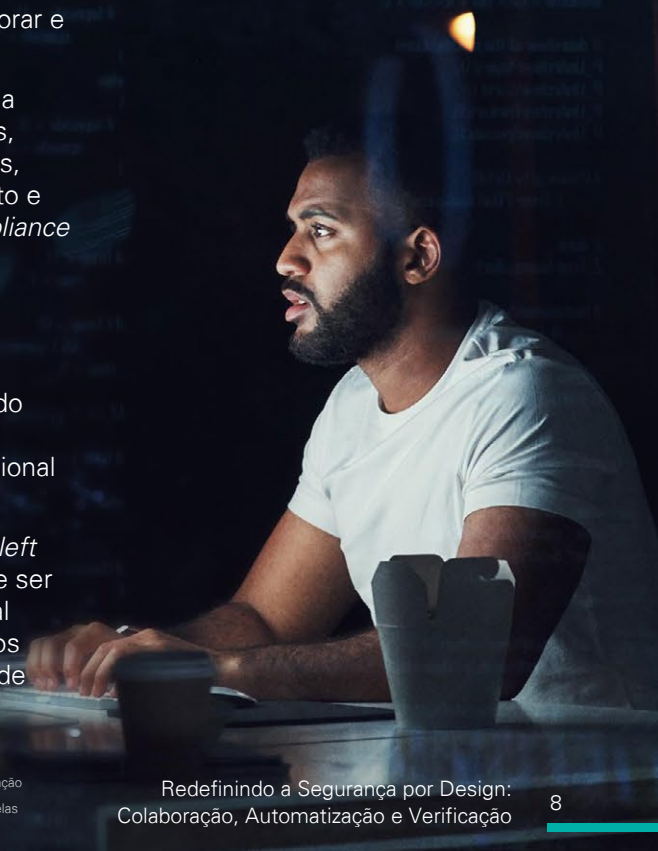
Após uma investigação e análise da causa raiz, foi possível realizar a engenharia reversa do código responsável pelo ataque. Isso forneceu informações sobre as vulnerabilidades existentes da empresa e como resolvê-las. A equipe envolvida no projeto revisou a documentação e coletou evidências baseadas nos dados em todos os aplicativos para desenvolver um roteiro detalhado e obter um alto nível de auditoria, conformidade e segurança de controles. Isso ajudou a empresa a criar um mecanismo de telemetria para coletar, registrar, monitorar e compartilhar dados do fluxo (*pipeline*).

A KPMG trabalhou em colaboração com as equipes do CIO, CRO e CISO da empresa para avaliar os amplos processos de gerenciamento de mudanças, fornecer visibilidade do status atual dos processos do fluxo interconectados, destacar riscos por meio de testes e incorporar controles de monitoramento e alertas para serem utilizados como base para incorporar segurança e *compliance* automatizadas no fluxo de CI/CD.

Resultado

Em resumo, esse projeto abordou a automação do SDLC e inspirou uma colaboração mais estreita entre as áreas de desenvolvimento de software, segurança e governança para garantir que a organização esteja fazendo todo o possível, em sincronia, para evitar ou mitigar futuras violações de dados. Poucas organizações estão fazendo isso, pois essa coordenação multifuncional simplesmente não está ocorrendo de maneira consistente.

Não se trata apenas de garantir a colaboração e realizar uma ação de *shift left* da segurança em resposta a uma instância isolada. O DevOps seguro deve ser um procedimento operacional padrão. Ele precisa ser a maneira com a qual as coisas são feitas em todos os fluxos de entrega e em todos os caminhos de produção. Ao final, ajudamos a empresa a criar um modelo de entrega de serviços rápido, seguro e compatível.



Como a KPMG pode ajudar

Os profissionais da KPMG trabalham com os clientes para contribuir com sua estratégia de TI. Nossos especialistas desenvolvem soluções tecnológicas inovadoras, projetadas para transformar seu modelo de entrega.

Muitas empresas de desenvolvimento de *software* estão começando a enxergar o valor da transição de um modelo tradicional de DevOps para uma abordagem que não se concentre apenas na segurança e nos controles, mas que também não comprometa a agilidade.

Nossos recursos de DevOps seguro incluem:

- Avaliação da capacidade de DevOps seguro e governado.
- Estratégia e transformação de DevOps seguro.
- Ferramentas avançadas e organização de engenharia.
- Serviços gerenciados e centrados na segurança.
- Governança, risco e *compliance*/auditoria interna.

Nós nos concentramos na colaboração entre nossas práticas de engenharia de TI, segurança da informação e auditoria de TI para gerar valor ao implementar nossos recursos, da mesma maneira abrangente que recomendamos aos clientes que abordam a transição de DevOps para o modelo DevOps seguro e governado.

Fale com o nosso time

Lavin Chainani
Diretor de risk management em tecnologia da KPMG nos EUA
lchainani@kpmg.com

Caleb Queern
Diretor de Cyber Security Services da KPMG nos EUA
cqueern@kpmg.com

James Williams
Diretor de Modern Delivery da KPMG nos EUA
jameswilliams@kpmg.com

Leandro Augusto
Sócio-líder de Cyber Security & Privacy da KPMG no Brasil e na América do Sul
lantonio@kpmg.com.br

Marcus Murph
Sócio de Advisory em tecnologia da informação da KPMG nos EUA
marcusmurph@kpmg.com

Cyndi Izzo
Sócia de risk management em tecnologia da KPMG nos EUA
cizzo@kpmg.com

Kyle Kappel
Sócio de Cyber Security Services da KPMG nos EUA
kylekappel@kpmg.com