ProMove
Business Innovation

Webinar - Startups e LGPD: Construindo um roadmap com base na ISO 27001 e MPS para Software e Serviços

Analia e Fabrício (Fafá)

Quem somos nós?

- Família
- Amigos

ProMove - https://www.promovesolucoes.com/

ProMove
Business Innovation

Quem sou eu?

- Propósito
- Colaboração

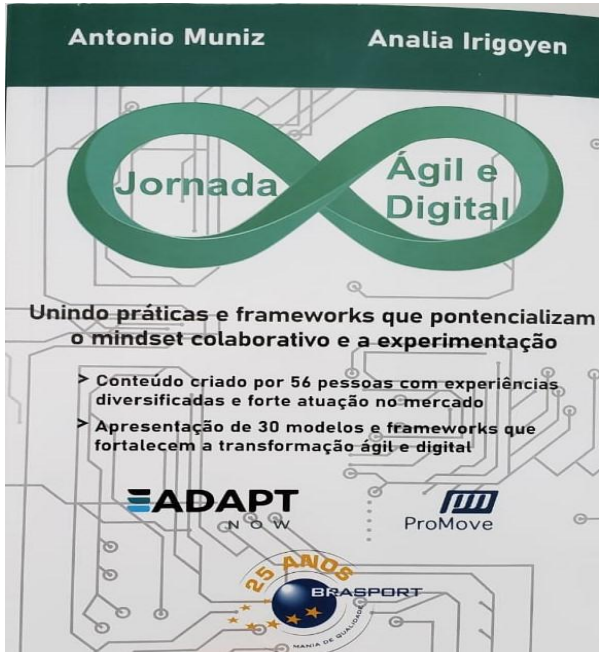
Jornada Colaborativa - https://www.jornadacolaborativa.com.br/

ProMove
Business Innovation

Quem sou eu?

- Aprendizado
- Pessoas

Fafá + Analia



ProMove
Business Innovation

Quais são os objetivos de segurança mesmo?

- Integridade
- Confidencialidade
- Disponibilidade

ProMove
Business Innovation

27k o que é isso? Controles para...

Organização SI - Responsabilidades

Aquisição, Desenvolvimento e manutenção de sistemas

Criptografia

Gerenciamento de incidentes de segurança da informação

Conformidade

Controle de Acesso

Relação com Fornecedores

Segurança Física e Ambiental

Segurança RH

Gerenciar Ativos

Políticas de SI

Continuidade de negócios

Segurança de Comunicações

Segurança de Operações

Dev Operação RH

Alta Direção Jurídica

LGPD o que é isso?

DPO (Data Protection Officer)

Dados Pessoais

Portabilidade

Direito das pessoas singulares

Consentimento

Direito Digital

Âmbito

Notificação

Privacidade

Dev Operação RH

Alta Direção Jurídica

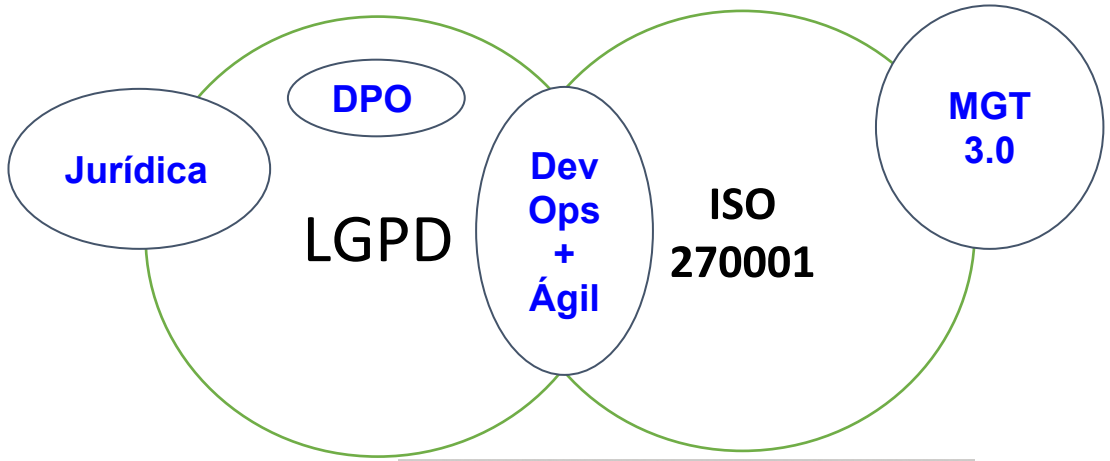
Qual a relação entre LGPD e 27 k?

- **Integridade** - Propriedade da exatidão e completeza da informação.
- **Confidencialidade** - a informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos autorizados.
- **Disponibilidade** - Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.

Segurança para a privacidade dos dados pessoais - **todo** o ciclo de vida dos dados pessoais, inclusive os processos de negócio - além da **SI.**

ProMove
Business Innovation

O que é MPS.SW e SV ? O que este modelo tem a ver com a 27k e a LGPD?



Eng. SW e SV

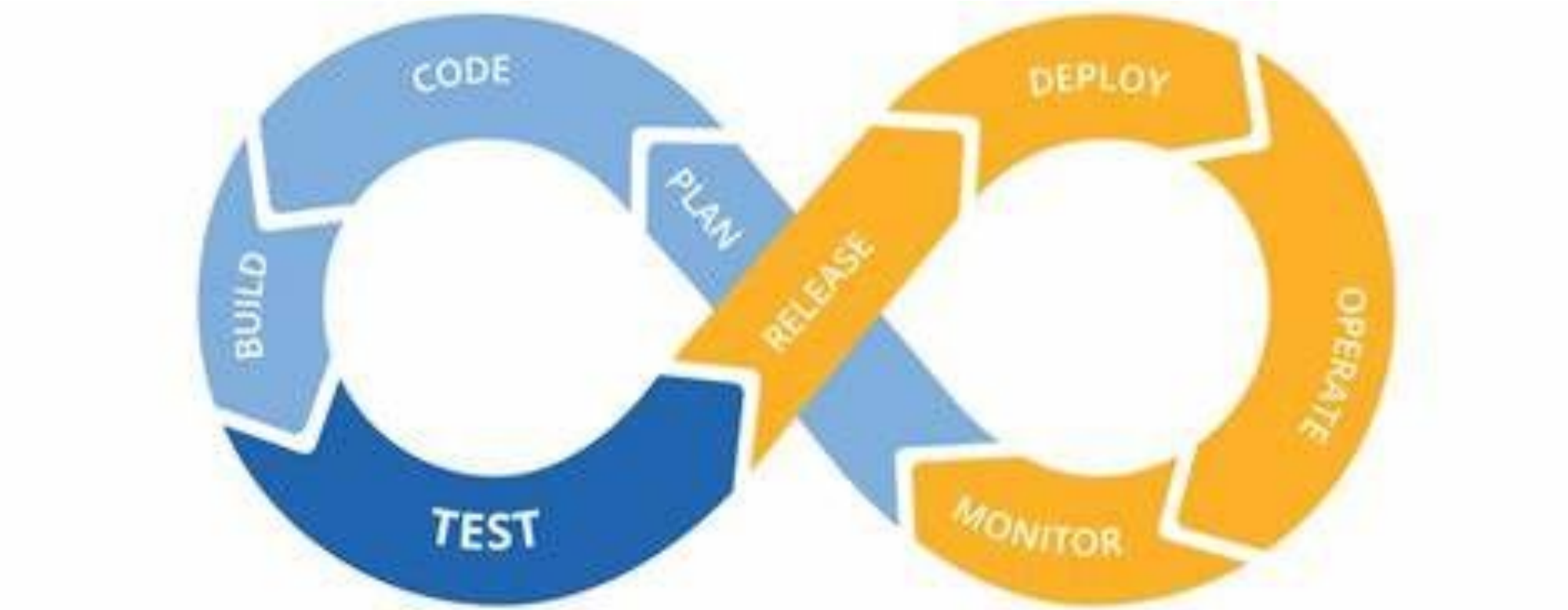
mps Br Melhoria de Processo do Software Brasileiro

"Existe **segurança sem privacidade de dados**, mas **não pode ter privacidade sem segurança.**"

MPS.SW e SV ajudam as empresas a entender o que fazer para definir governança em empresas que desenvolvem software ou serviços, disseminando a necessidade da padronização de processos e cultura.

ProMove Business Innovation

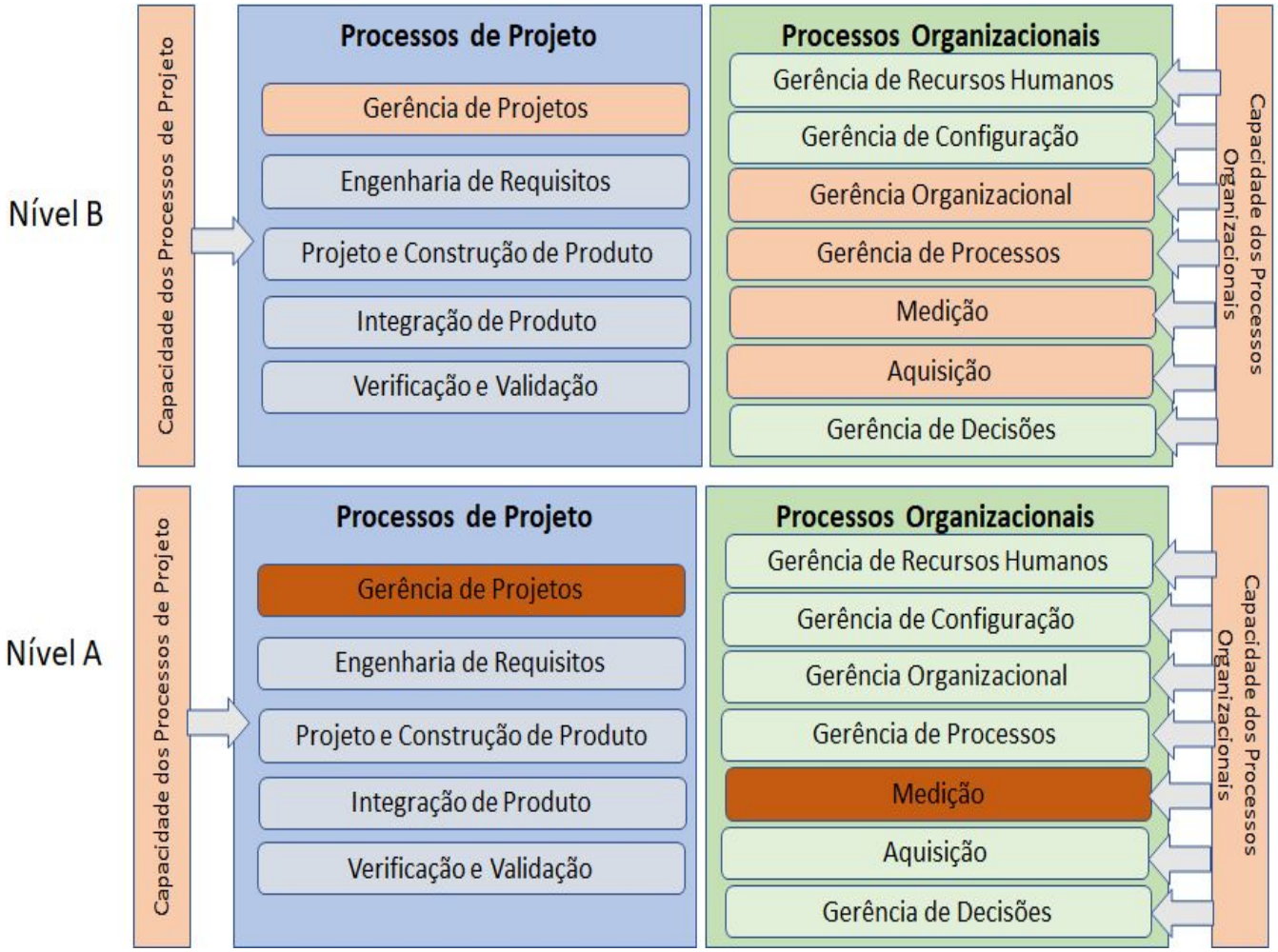
O que é MPS.SW e SV ? O que este modelo tem a ver com a 27k e a LGPD?



Potencializa a implantação de Processos DevOps apoiando na padronização, governança e escalamento do Ágil (webinar anterior)

ProMove
Business Innovation

O que é MPS.SW e SV ? O que este modelo tem a ver com a 27k e a LGPD?



ProMove
Business Innovation

Por que para startups e pequenas empresas é importante ser diferente? A solução pode ser efetiva, simples e engajada?

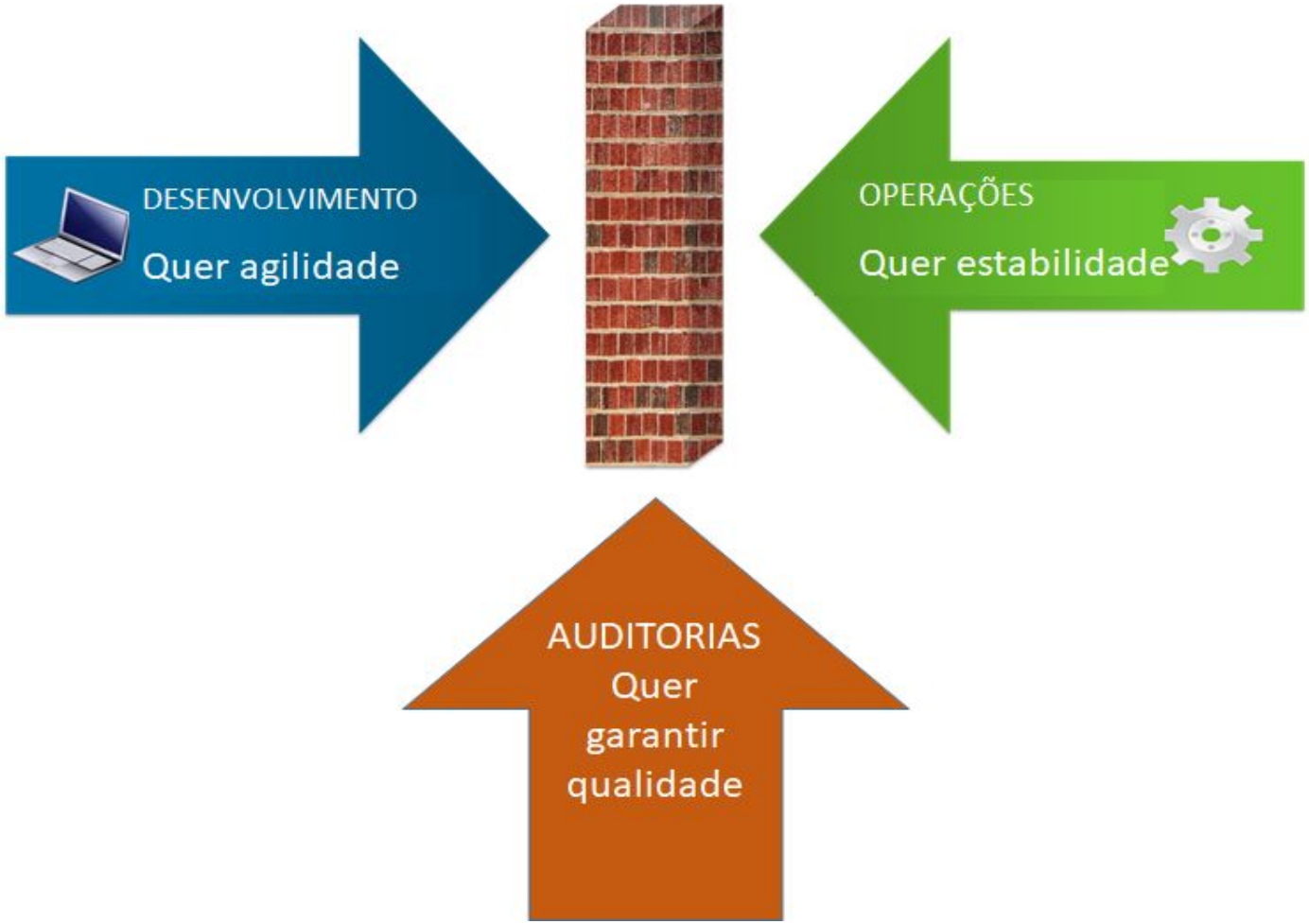
Livro Jornada DevOps: MUNIZ; SANTOS; IRIGOYEN; MOUTINHO (Brasport, 2019)

Sim é possível :-) :-)

SIM! Exemplos de algumas práticas de Governança :-)

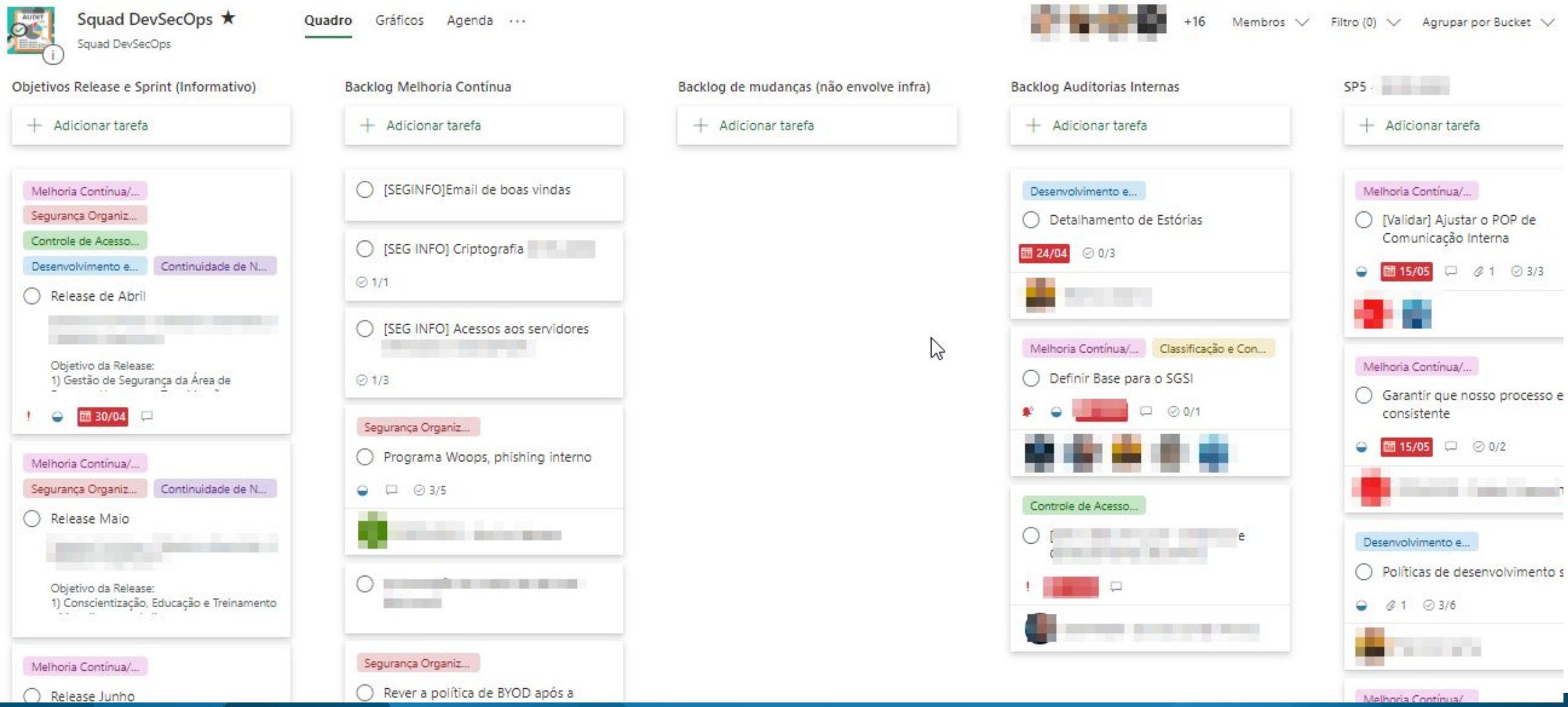
ProMove
Business Innovation

Por que não uma SQUAD DevSecOps com SCRUM?



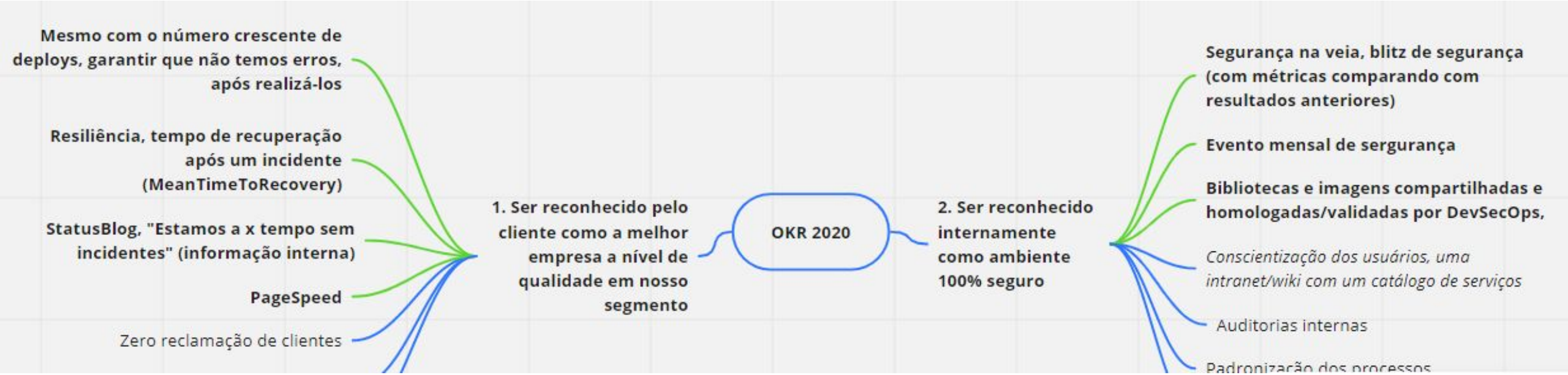
- DPO
- DBA
- Arquiteto
- TechLead
- PO
- Agile Master
- Infra, NOC,..
- TODOS :-)

Por que não uma SQUAD DevSecOps com SCRUM?



ProMove
Business Innovation

Exemplo OKR - Colaboração da Alta Direção - Indicadores SI



OBJECTIVES AND KEY RESULTS - 2020

Objetivo 1	Objetivo 2	Objetivo 3
Ser reconhecido pelo cliente como a melhor empresa a nível de qualidade em nosso segmento	Ser reconhecido internamente como ambiente 100% seguro.	Ter processos imperceptiveis viabilizados pela automação
KR1: Mesmo com o número crescente de deploys, garantir que não temos erros, após realizá-los	KR1: Segurança na veia, blitz de segurança (com métricas comparando com resultados anteriores)	KR1: DEVSECOPS: % de Automação, SONAR, Pipelines CI/CD, Infra Automatizada, Docker, etc
KR2: Resiliência, tempo de recuperação após um incidente (MeanTimeToRecovery)	KR2: Evento mensal de sergurança	KR2:
KR3: StatusBlog, "Estamos a x tempo sem incidentes" (informação interna)	KR3: Bibliotecas compartilhadas e homologadas/validadas por DevSecOps	KR3:
KR4: PageSpeed	KR4:	KR4:
KR5:	KR5:	KR5:

ProMove
Business Innovation

Exemplo Responsabilidades - Delegation Board (Delegation Poker) - MGT 3.0

genda ···

Membros Filtro (0) Agrupar

3. Consultar

+ Adicionar tarefa

- Consultar
- 3-Consultar.png
- 1

- Objetivos e Indicadores Estratégicos de SI (Manager: [redacted] | Squad: DevSecOps)

- [redacted]

4. Concordar

+ Adicionar tarefa

- Concordar
- 4-Concordar.png
- 1

- Indicadores de Desenvolvimento e Infra Operacionais de SI (Manager: [redacted] | Squad: DevSecOps+)

5. Aconselhar

+ Adicionar tarefa

- Aconselhar
- 5-Aconselhar.png
- 1

- Análise Vulnerabilidades Geral (Manager: [redacted] | Squad: DevSecOps+)

6. Perguntar

+ Adicionar tarefa

- Perguntar
- 6-Perguntar.png
- 1

- Tomada de decisões sobre o Mapa de conhecimento de segurança (Manager: [redacted] | Squad: DevSecOps+)

Exemplo Mapa/Matriz de Competência - MGT 3.0

Habilidade \ Pessoa	Pedro	Bruno	Lucas	Marcelo	Ana	Rafa	Gio	Rico	Sol	Vania
Security By Design	C	B	D	A	A	C	D	D	D	D
Security By Default	C	A	D	A	A	A	C	D	D	D
SONAR	C	B	C	D	B	B	D	C	C	C
Desenvolvimento Seguro	B	C	C	D	B	B	D	D	C	D
Segurança Física	B	B	C	A	A	B	B	C	C	C
Infra como código	C	A	C	C	C	C	A	C	C	C
Automação de Segurança (Dev)	B	B	C	C	B	C	C	D	D	D
Infra como serviço	C	A	C	B	B	C	A	C	C	C
Metodologia Ágil - SCRUM	A	B	A	C	A	A	C	A	A	B

Legenda	
A	Domino e consigo treinar outros
B	Domino mas sem total segurança
C	Iniciante no assunto, aprendendo atualmente
D	Não domino e gostaria de aprender
X	Não domino, mas pode esperar

C3PO	X	Não domino o assunto
Padawan		Iniciante no assunto
Princesa Leia		Já domino o assunto
Yoda		Domino e treino outros

Políticas de Dev Seguro + PR (Políticas de Pull Request) + SONAR (Análise de Vulnerabilidades + Ambiente Stage ("Staging") + Docker + Monitoramento de Vulnerabilidades

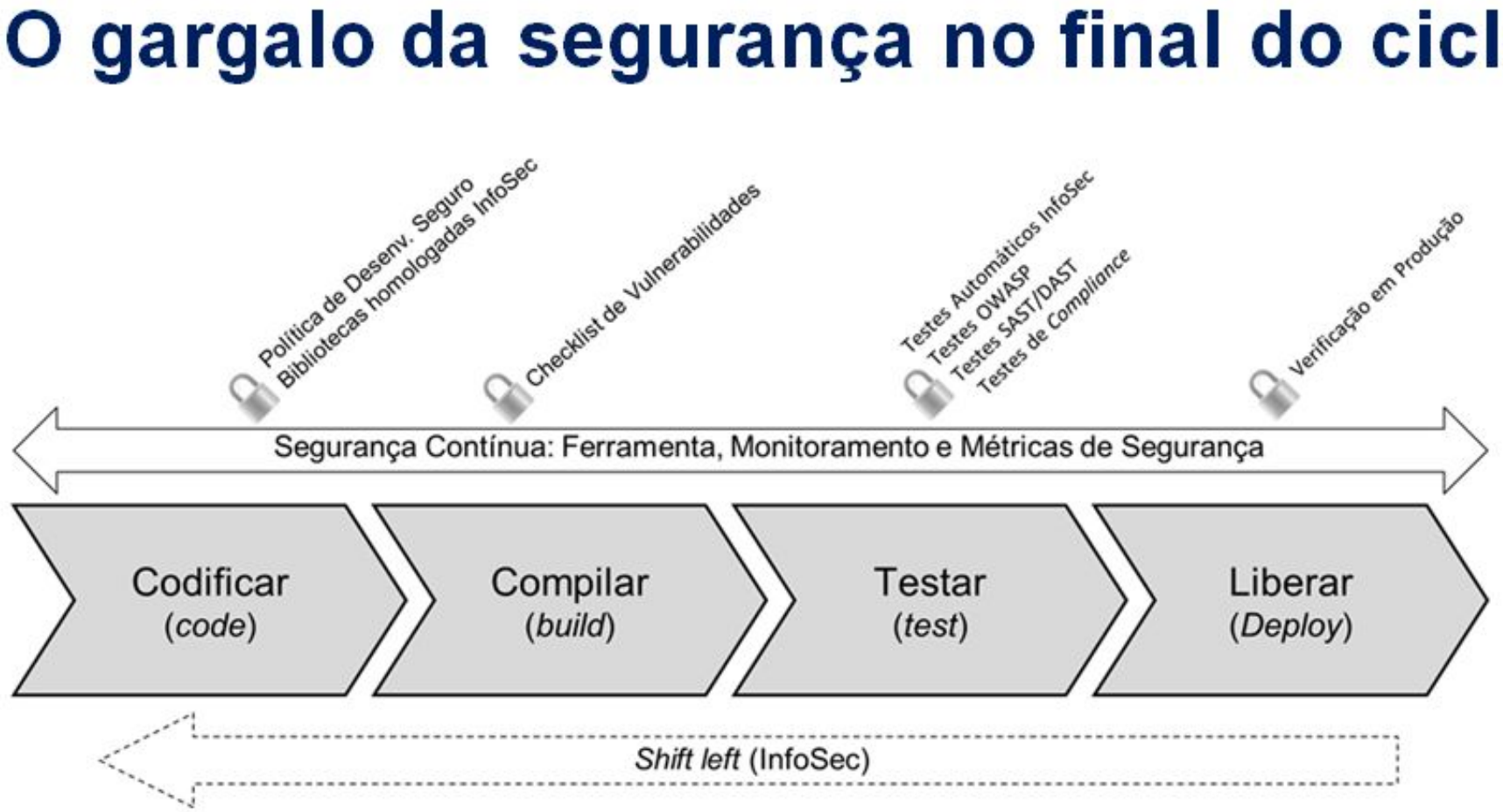


Imagem *Shift left* e a Segurança Contínua. Fonte: Rodrigo Santos, Palestra DevSecOps Infnet e AdaptNow, 2018.

Políticas de Dev Seguro + PR (Políticas de Pull Request) + SONAR (Análise de Vulnerabilidades + Ambiente Stage ("Staging") + Docker + Monitoramento de Vulnerabilidades

Desenvolvimento

1. Teste de código.
2. Revisão de código.
3. Teste de penetração – em casos em que o custo x benefício seja avaliado.
4. Servidores de IC como código.
5. Análise estática pode ser realizada considerando critérios específicos de segurança, garantindo a remoção dos erros antes mesmo da execução do build (SONAR, Veracode, Gauntlet e manual).

Evitar que usuários sem autorização acessem o ambiente:

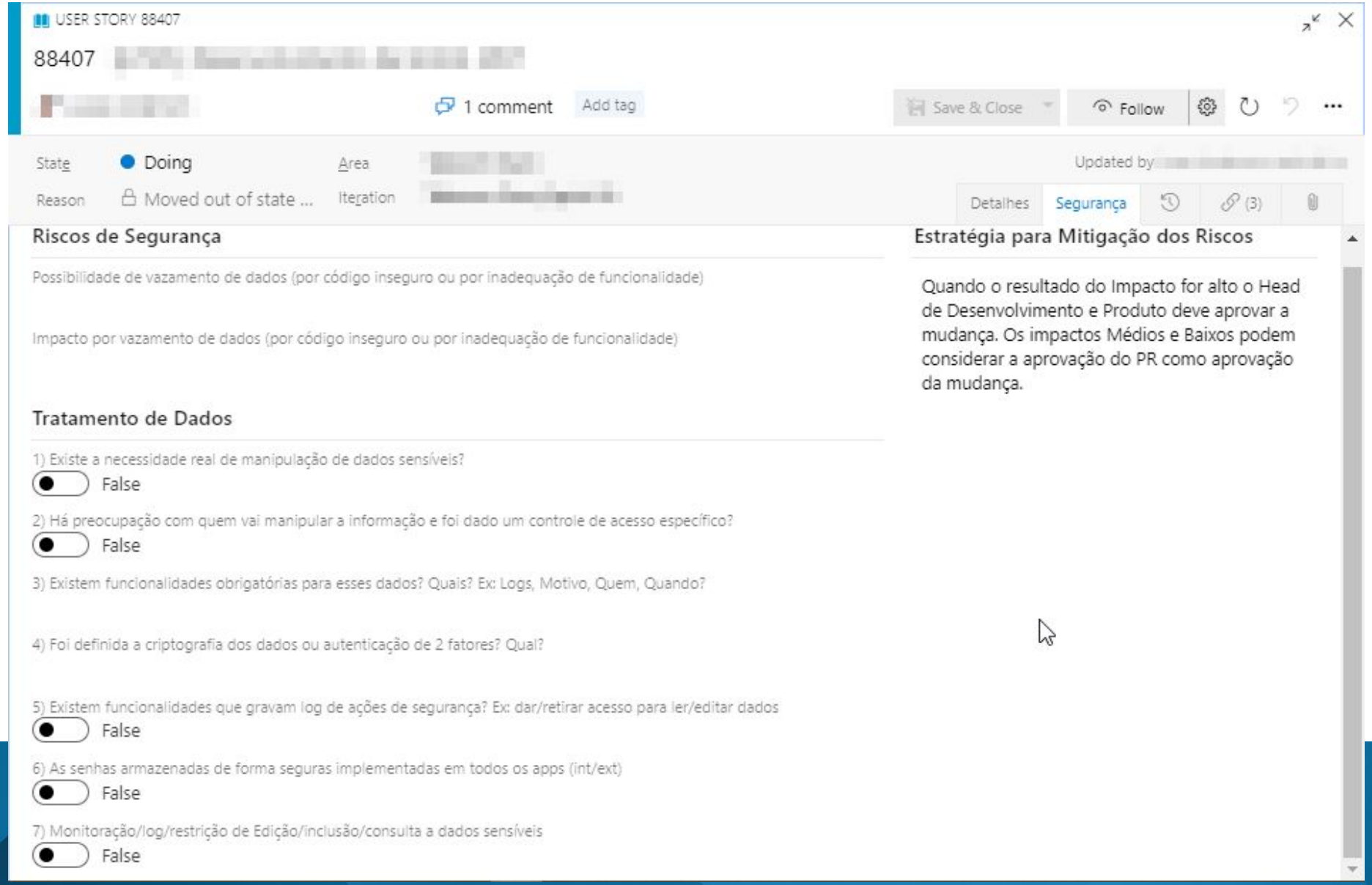
1. Controle das configurações de ambiente. (Docker + Ambiente de HMG e PRD)
2. Teste de ataques de injeção de SQL.
3. Use credenciais de IC somente leitura.
4. Use VM isoladas.
5. **Autenticação de dois fatores**

Ambiente:

1. Testes de vulnerabilidade
2. Testes automatizados Segurança de BD e senhas, por exemplo.

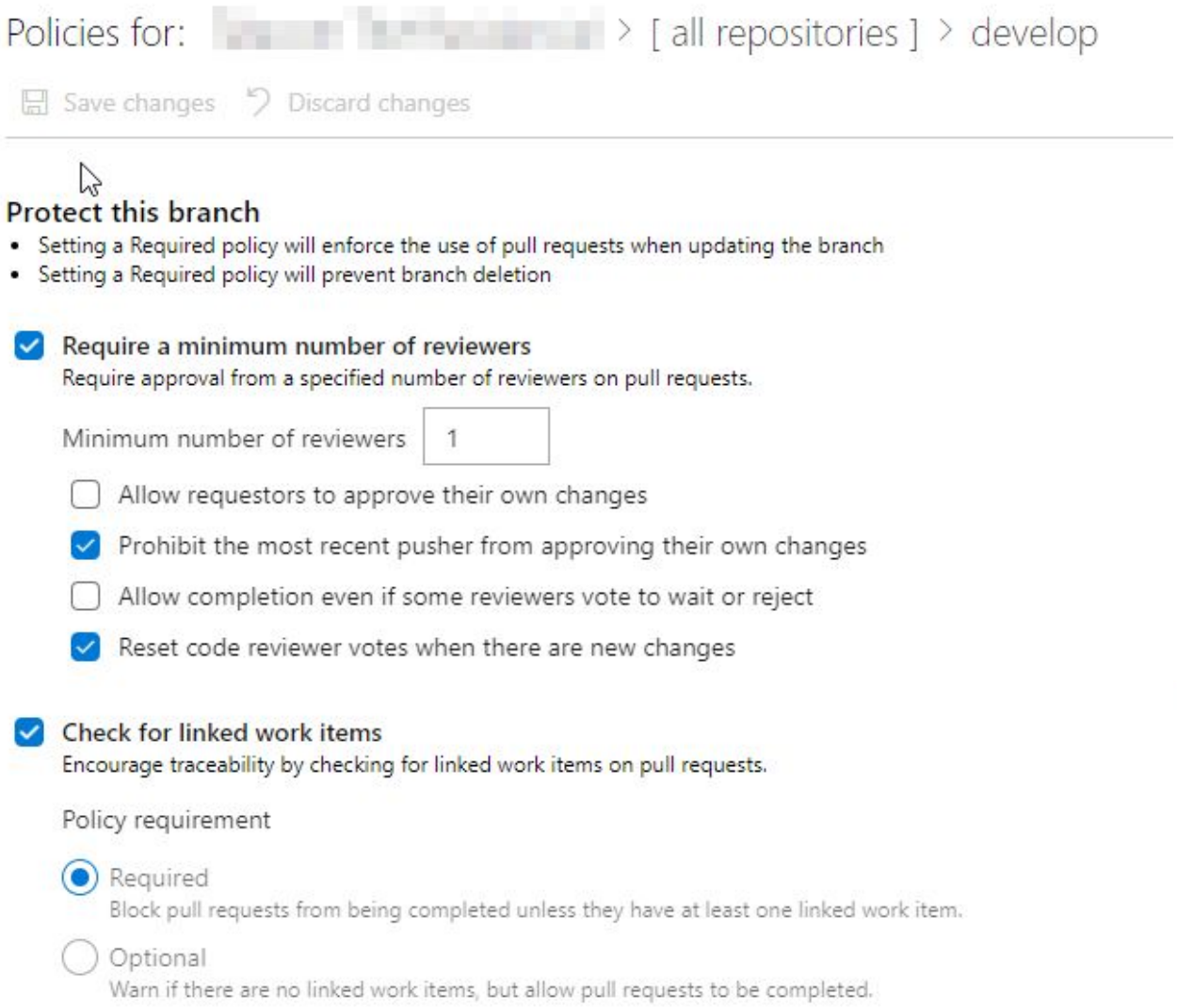
Livro Jornada DevOps: MUNIZ; SANTOS; IRIGOYEN; MOUTINHO (Brasport, 2019)

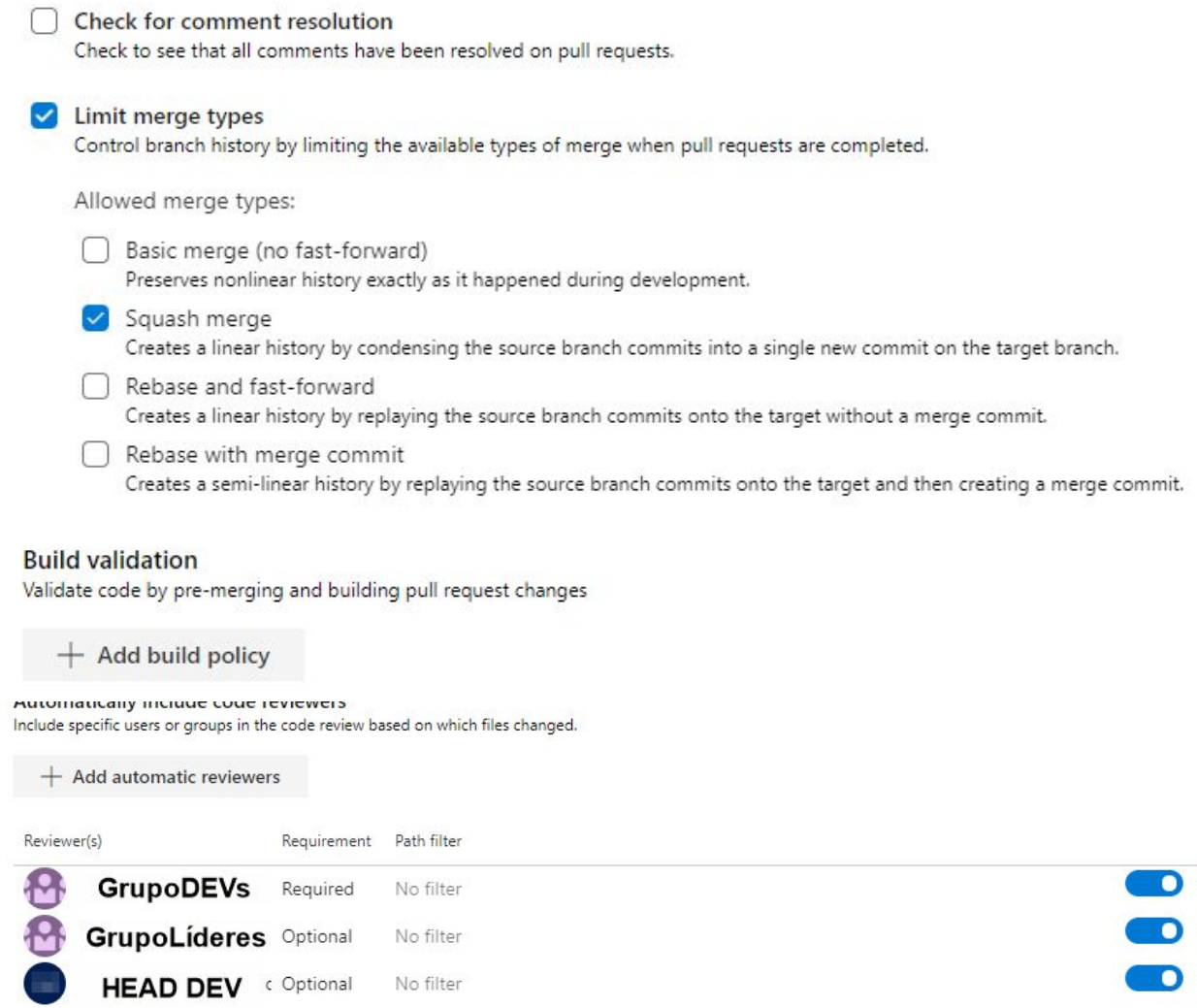
Políticas de Dev Seguro + PR (Políticas de Pull Request) + SONAR (Análise de Vulnerabilidades + Ambiente Stage (“Staging”) + Docker + Monitoramento de Vulnerabilidades



ProMove
Business Innovation

Políticas de Dev Seguro + PR (Políticas de Pull Request) + SONAR (Análise de Vulnerabilidades + Ambiente Stage (“Staging”) + Docker + Monitoramento de Vulnerabilidades





ProMove
Business Innovation

Algumas práticas do MPS que me ajudaram na Governança

GPC 1 (A partir do nível E) Uma estratégia é definida, mantida atualizada e utilizada para estabelecer a arquitetura de processos, criar e evoluir os ativos de processo e disponibilizá-los em uma biblioteca de ativos de processos.
GPC 2 (A partir do nível E) Uma estrutura de apoio para identificar e corrigir problemas nos processos, promover a melhoria contínua dos processos e a implementação, implantação e sustentação do uso das melhorias de processos é estabelecida
GPC 3 (A partir do nível F) Uma estratégia e um plano de garantia da qualidade para os projetos são desenvolvidos, executados e mantidos atualizados, com base nos dados históricos de qualidade.
GPC 4 (A partir do nível E) Oportunidades de melhoria dos processos derivadas dos objetivos de negócio, de avaliações da implementação dos processos e da exploração e avaliação de potenciais novos processos, técnicas, métodos e ferramentas são identificadas e mantidas atualizadas.
GPC 5 (A partir do nível E) Um plano de implementação de melhorias, com base na importância dos processos para o alcance dos objetivos de negócio da organização, é definido, executado e mantido atualizado.
GPC 6 (A partir do nível E) Os ambientes padrão de trabalho da organização são estabelecidos e mantidos atualizados. **As evidências apresentadas para este resultado permitem assegurar que a....**
GPC 7 (A partir do nível E) Um repositório organizacional de medidas e procedimentos para garantia da qualidade de medidas são definidos e mantidos atualizados. **As evidências apresentadas para este resultado permitem assegurar que a....**
GPC 8 (A partir do nível E) Processos padrão e ativos de processos organizacionais são implantados na organização. **As evidências apresentadas para este resultado permitem assegurar que a....**
GPC 9 (A partir do nível E) A efetividade das melhorias implantadas é avaliada com base nos objetivos de melhoria. **As evidências apresentadas para este resultado permitem assegurar que a....**

- Editais públicos pedem estas certificações
- Auxiliam na obtenção de certificado de compliance
- Auxiliam na obtenção de normas como: ISO 27 K, ISO 9001 e ISO 29110 – Capítulo Desenvolvimento
- Compatibilidade com o CMMi (certificação internacional)

CONTATO

ProMove - Business Innovation

promovesolucoes.com

contato@promovesolucoes.com

+55 21 3283 8340

/promovesolucoes @promovesolucoes

ProMove
Business Innovation

ProMove

Business Innovation