



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



Quem sou eu?

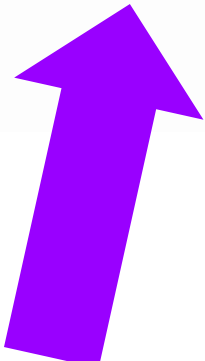
- Propósito
- Colaboração



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

Quem sou eu?

- Aprendizado
- Pessoas



Fafá + Analia



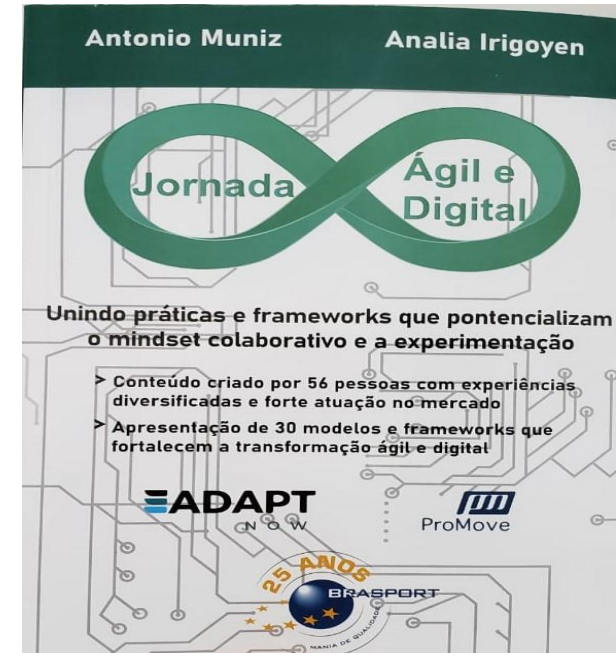
A Jornada Colaborativa é uma comunidade apoiadora, por pessoas e tecnologias que recebem livros usando experiências diversificadas dos coautores e coautores dos organizadores selecionados para manter o alto padrão de qualidade.

Os royalties dos livros, além de recursos dos coautores, são usados para ajudar na compra dos exemplares que usamos no Summit Jornada Colaborativa e a receita é doada para instituições caritativas (doamos R\$ 20 mil para 4 instituições com o Summit em 2019).

Parabenizamos a dedicação dos organizadores e coautores para concretizar essa obra e agradeceremos à organização que apoiou a Summit Jornada Colaborativa para transferir material cada vez mais suas vidas.

Antonio Muniz
Fundador da Jornada Colaborativa e fundador do

Analia Irigoyen
Líder de time organizador e curadora



Quais são os objetivos de segurança mesmo?



- Integridade
- Confidencialidade
- Disponibilidade



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

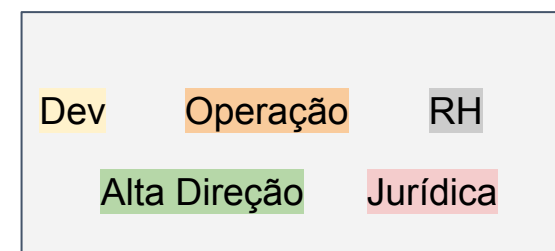
Consentimento

Direito Digital

Âmbito

Notificação

Privacidade



Qual a relação entre LGPD e 27 k?

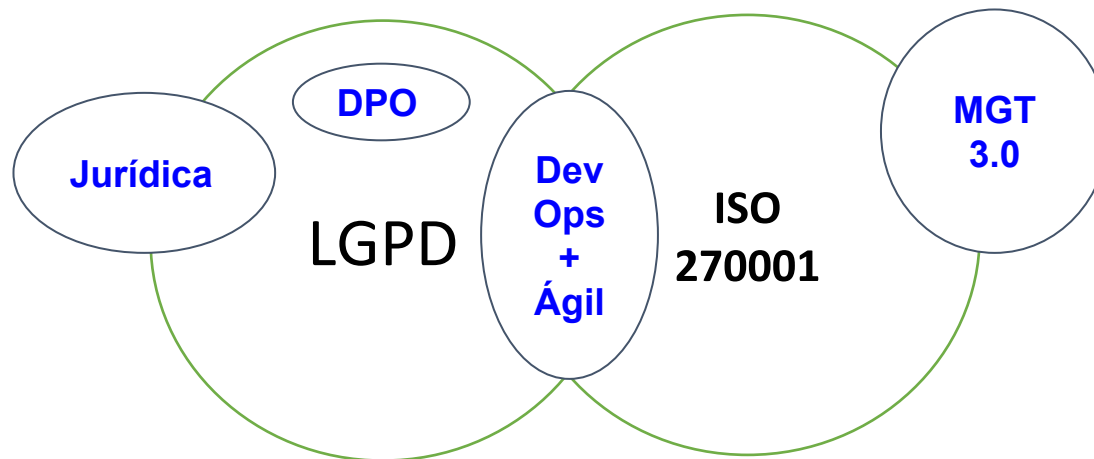
- **Integridade** - Propriedade da exatidão e completeza da informação.
- **Confidencialidade** - a informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos autorizados.
- **Disponibilidade** - Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.



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



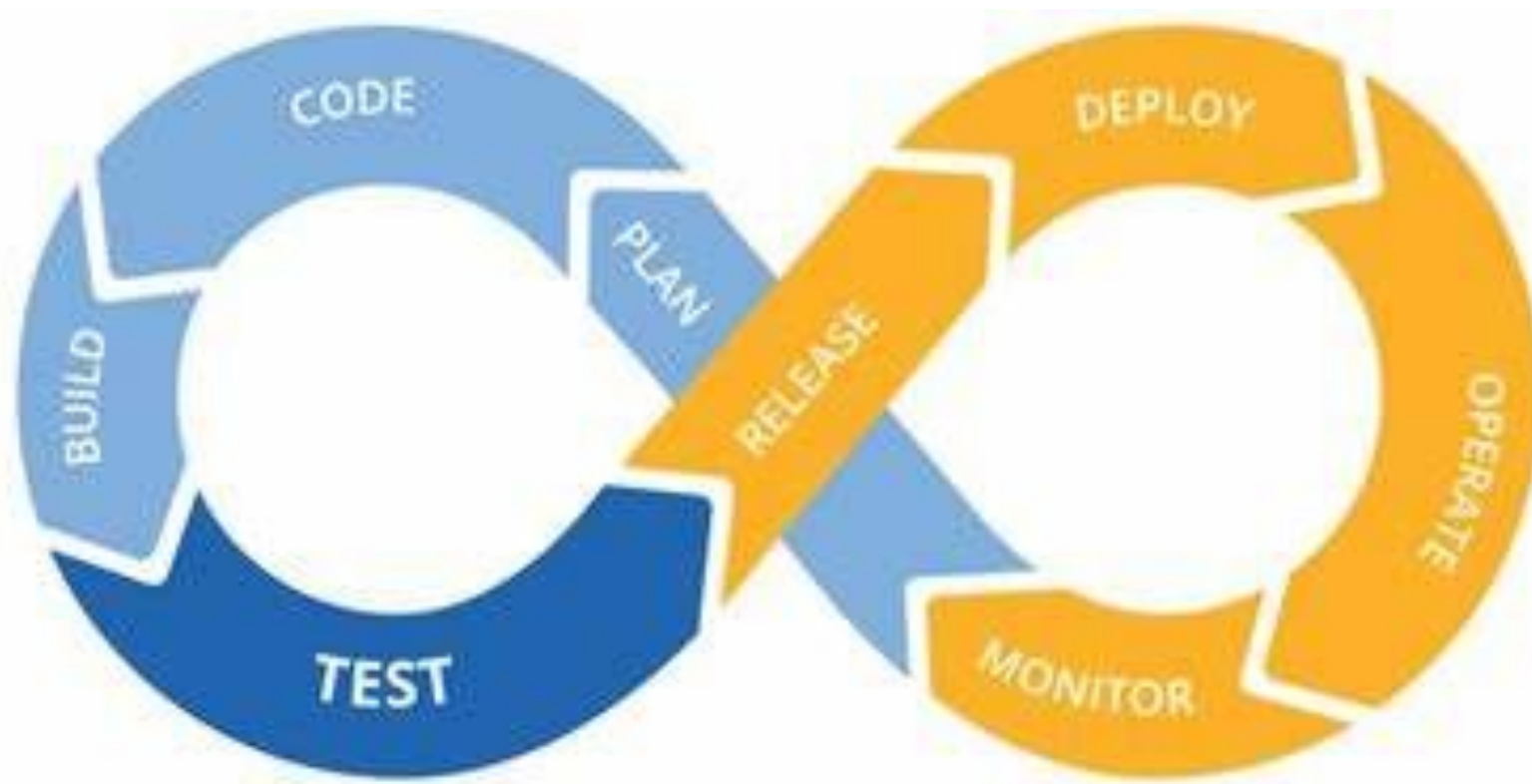
O que é MPS.SW e SV ? O que este modelo tem a ver com a 27k e a LGPD?



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

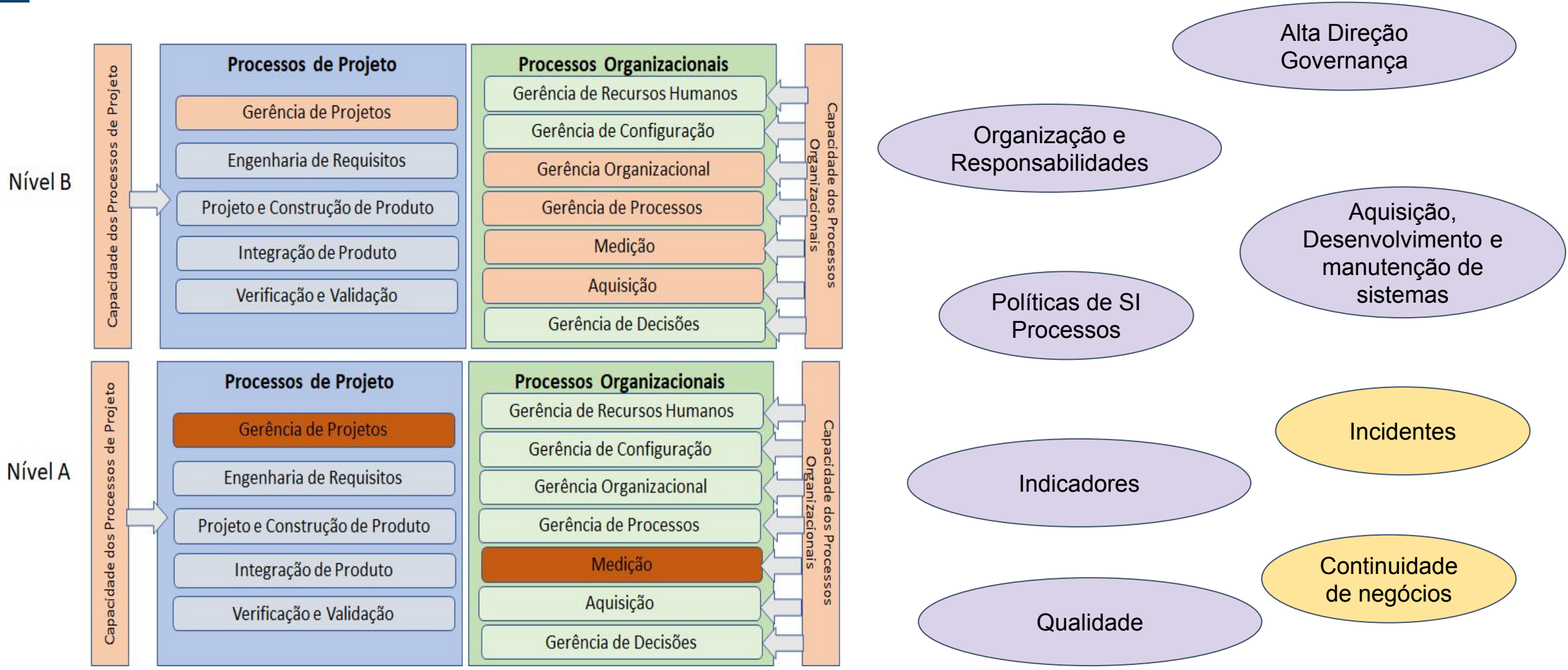
MPS.SW e SV ajudam as empresas a entender **o que fazer** para definir **governança** em empresas que desenvolvem **software ou serviços**, disseminando a necessidade da **padronização de processos e cultura**.

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)

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



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 :-) :-)



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?

Squad DevSecOps ★
Squad DevSecOps

Quadro Gráficos Agenda ...

+16 Membros Filtro (0) Agrupar por Bucket

Objetivos Release e Sprint (Informativo)

- + Adicionar tarefa
- Melhoria Contínua/...
Segurança Organiz...
Controle de Acesso...
Desenvolvimento e... Continuidade de N...
 Release de Abril
Objetivo da Release:
1) Gestão de Segurança da Área de...
30/04
- Melhoria Contínua/...
Segurança Organiz... Continuidade de N...
 Release Maio
Objetivo da Release:
1) Conscientização, Educação e Treinamento
- Melhoria Contínua/...
 Release Junho

Backlog Melhoria Contínua

- + Adicionar tarefa
- [SEGINFO]Email de boas vindas
1/1
- [SEG INFO] Criptografia
1/3
- [SEG INFO] Acessos aos servidores
- Segurança Organiz...
 Programa Woops, phishing interno
3/5
- [Redacted]
- Segurança Organiz...
 Rever a política de BYOD após a

Backlog de mudanças (não envolve infra)

- + Adicionar tarefa

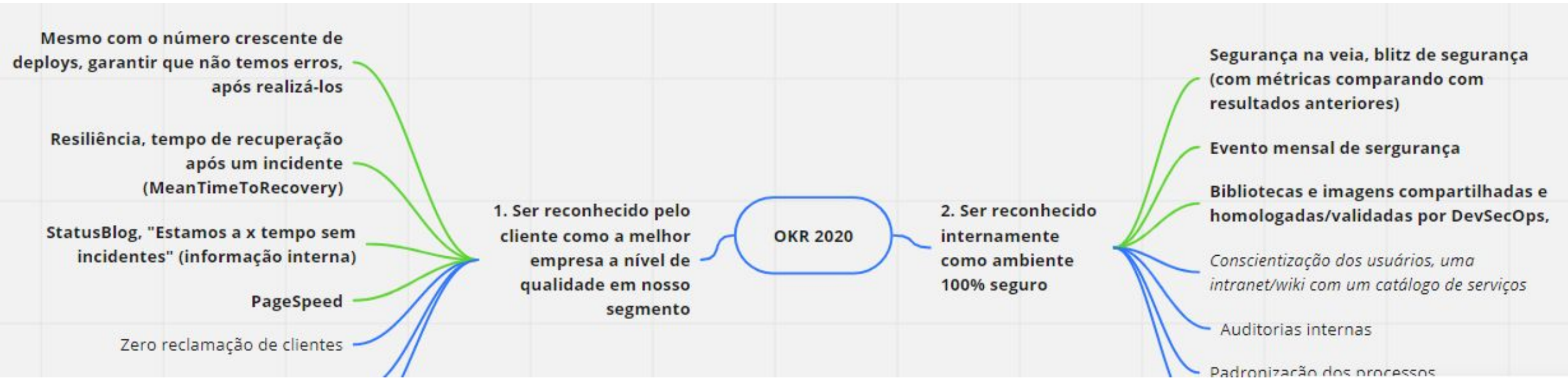
Backlog Auditorias Internas

- + Adicionar tarefa
- Desenvolvimento e...
 Detalhamento de Estórias
24/04 0/3
[Redacted]
- Melhoria Contínua/... Classificação e Con...
 Definir Base para o SGSI
0/1
[Redacted]
- Controle de Acesso...
 [Redacted]
- [Redacted]

SP5

- + Adicionar tarefa
- Melhoria Contínua/...
 [Validar] Ajustar o POP de Comunicação Interna
15/05 1 3/3
[Redacted]
- Melhoria Contínua/...
 Garantir que nosso processo e consistente
15/05 0/2
[Redacted]
- Desenvolvimento e...
 Políticas de desenvolvimento s
1 3/6
[Redacted]
- Melhoria Contínua/...

Exemplo OKR - Colaboração da Alta Direção - Indicadores SI



OBJECTIVES AND KEY RESULTS - 2020

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

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

Agenda ...

Membros ▾ Filtro (0) ▾ Agrupar ▾

3. Consultar

+ Adicionar tarefa



Consultar

Eu consultarei

- Consultar
- 3-Consultar.png
- @ 1

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



4. Concordar

+ Adicionar tarefa



Concordar

Nós

- Concordar
- 4-Concordar.png
- @ 1

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

5. Aconselhar

+ Adicionar tarefa



Aconselhar

Eu aconselharei

- Aconselhar
- 5-Aconselhar.png
- @ 1

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

6. Perguntar

+ Adicionar tarefa



Perguntar

Eu perguntarei

- 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

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

O gargalo da segurança no final do ciclo

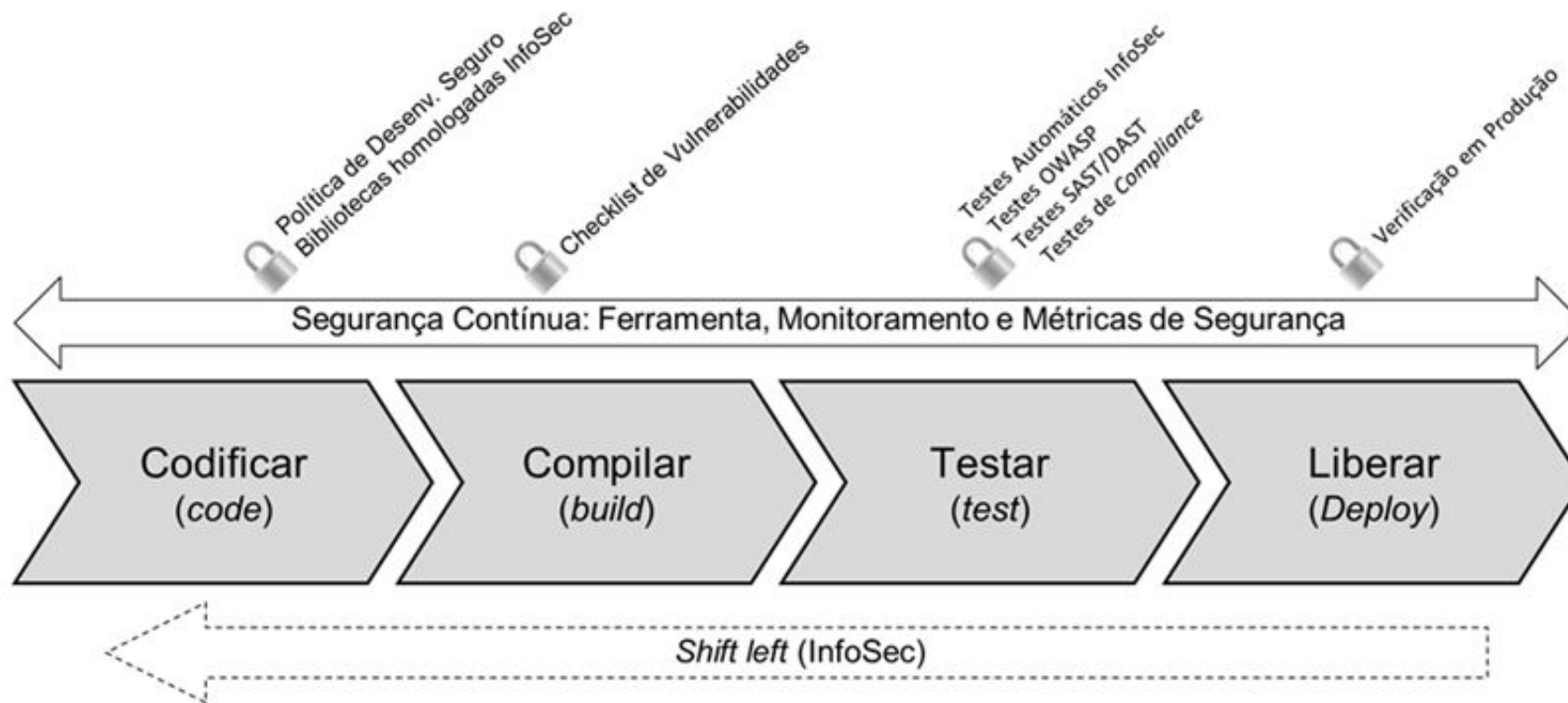


Imagem *Shift left* e a Segurança Contínua. Fonte: Rodrigo Santos, Palestra DevSecOps Infnet e AdaptNow, 2018.

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.

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

USER STORY 88407

88407

1 comment Add tag

Save & Close Follow

State **Doing** Area Updated by

Reason Moved out of state ... Iteration

Detalhes **Segurança** (3)

Riscos de Segurança

Possibilidade de vazamento de dados (por código inseguro ou por inadequação de funcionalidade)

Impacto por vazamento de dados (por código inseguro ou por inadequação de funcionalidade)

Tratamento de Dados

- 1) Existe a necessidade real de manipulação de dados sensíveis?
 False
- 2) Há preocupação com quem vai manipular a informação e foi dado um controle de acesso específico?
 False
- 3) Existem funcionalidades obrigatórias para esses dados? Quais? Ex: Logs, Motivo, Quem, Quando?
- 4) Foi definida a criptografia dos dados ou autenticação de 2 fatores? Qual?
- 5) Existem funcionalidades que gravam log de ações de segurança? Ex: dar/retirar acesso para ler/editar dados
 False
- 6) As senhas armazenadas de forma seguras implementadas em todos os apps (int/ext)
 False
- 7) Monitoração/log/restrrição de Edição/inclusão/consulta a dados sensíveis
 False

Estratégia para Mitigação dos Riscos

Quando o resultado do Impacto for alto o Head de Desenvolvimento e Produto deve aprovar a mudança. Os impactos Médios e Baixos podem considerar a aprovação do PR como aprovação da mudança.

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

Policies for: [redacted] > [all repositories] > develop

 Save changes  Discard changes

Protect this branch

- Setting a Required policy will enforce the use of pull requests when updating the branch
- Setting a Required policy will prevent branch deletion

Require a minimum number of reviewers

Require approval from a specified number of reviewers on pull requests.

Minimum number of reviewers

- Allow requestors to approve their own changes
- Prohibit the most recent pusher from approving their own changes
- Allow completion even if some reviewers vote to wait or reject
- Reset code reviewer votes when there are new changes

Check for linked work items

Encourage traceability by checking for linked work items on pull requests.

Policy requirement

- Required
Block pull requests from being completed unless they have at least one linked work item.
- Optional
Warn if there are no linked work items, but allow pull requests to be completed.

Check for comment resolution
Check to see that all comments have been resolved on pull requests.

Limit merge types
Control branch history by limiting the available types of merge when pull requests are completed.

Allowed merge types:

- Basic merge (no fast-forward)
Preserves nonlinear history exactly as it happened during development.
- Squash merge
Creates a linear history by condensing the source branch commits into a single new commit on the target branch.
- Rebase and fast-forward
Creates a linear history by replaying the source branch commits onto the target without a merge commit.
- Rebase with merge commit
Creates a semi-linear history by replaying the source branch commits onto the target and then creating a merge commit.

Build validation

Validate code by pre-merging and building pull request changes

[+ Add build policy](#)

Automatically include code reviewers

Include specific users or groups in the code review based on which files changed.

[+ Add automatic reviewers](#)

Reviewer(s)	Requirement	Path filter
 GrupoDEVs	Required	No filter
 GrupoLíderes	Optional	No filter
 HEAD DEV	Optional	No filter

En
 En
 En

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)

ProMove - Business Innovation

promovesolucoes.com

contato@promovesolucoes.com

+55 21 3283 8340

 /promovesolucoes

 @promovesolucoes



ProMove
Business Innovation