



Security by Design

HACKERS TO HACKERS

C O N F E R E N C E

Alessandra Monteiro Martins



Head GPS | DPO D1

Alessandra Monteiro Martins

Formada em Licenciatura em Informática pela Universidade do Estado do Amazonas, Especialista em Governança de TI pela Universidade Católica de Brasília, Certificações ISO 27002, ITIL v3, COBIT5, Scrum Master, KMP I, CTFL, PDPFe outras.

Atuando no Mercado de Tecnologia da Informação desde 2004, trabalhando há mais de 5 anos, voltada para Qualidade de Software, Projetos, DevSecOPs, Segurança da Informação, Governança de TI, SI e Corporativa.



Roteiro



- Contexto – LGPD e GDPR
 - Conceitos
- Princípios: US, Data Protection, Privacy by Design e Default, Security by Design
 - Problemas
 - Pessoas | Processos | Ferramentas
 - Automação
 - Boas Práticas: Segurança
 - Governanças
 - Conformidade



Contexto: GDPR Overview





Contexto: LGPD Resumo

1

Objetos: Dados Pessoais e Pessoais Sensíveis Tratados e/ou coletados em Território Nacional

2

Papéis: Pessoa Natura: Órgão de Pesquisa; Agentes de Tratamento: Controlador, Operador, Encarregado de Dados; Autoridade Nacional de Proteção de Dados (ANPD 13.853/2019)

3

Operações de Tratamento: Classificação, Coleta, Recepção, Armazenamento, Acesso, Extração, Utilização, Processamento, Avaliação ou Controle da Informação, Modificação, Transmissão, Produção, Comunicação, Transferência, Reprodução, Distribuição, Eliminação

4

Uso Compartilhado: Transferência Internacional, Difusão, Comunicação

5

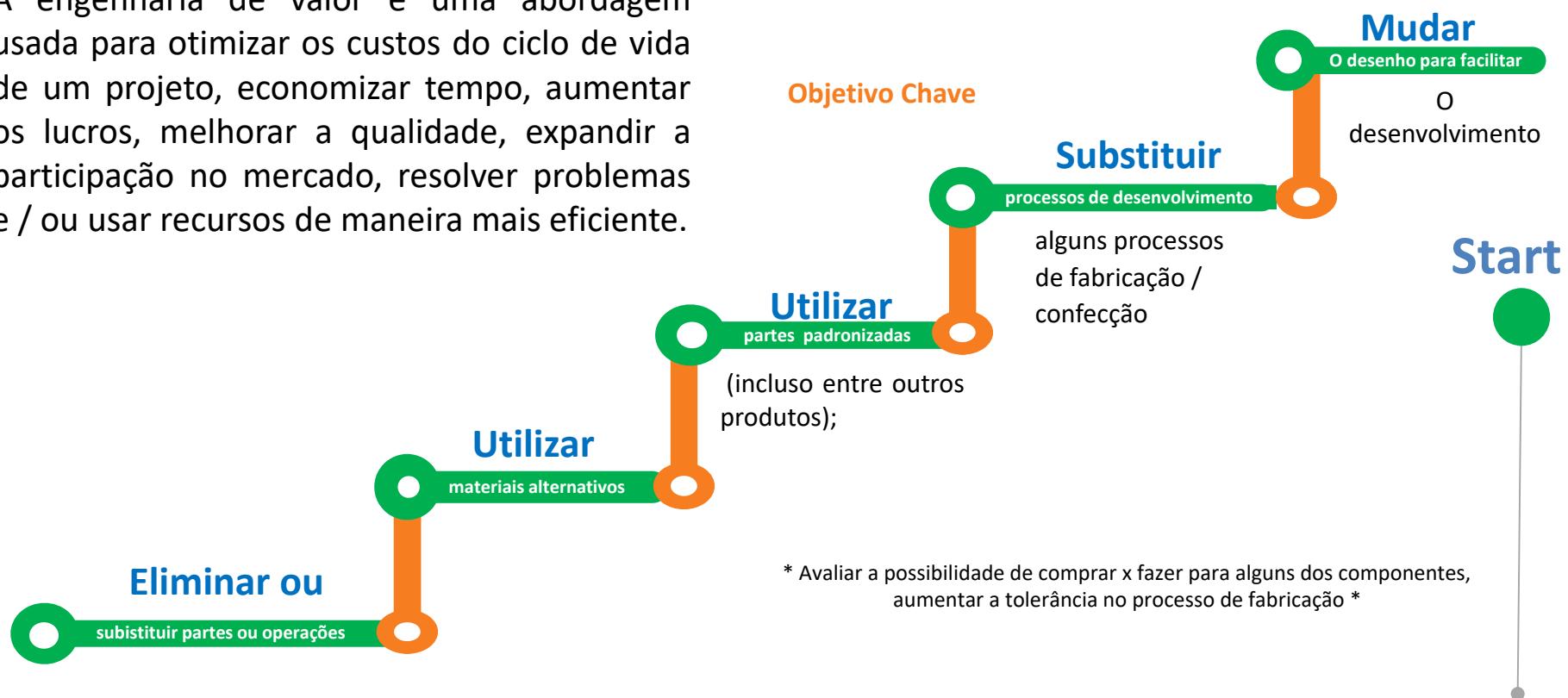
Direitos do Titular: Bloqueio, Eliminação, Anonimização, Revogação, Petição, Revisão das Decisões Automatizadas, Acesso, Explicação, Retificação, Oposição, Cancelamento, Portabilidade, Confirmação

6

Deveres dos Agentes de Tratamento: Nomear o Encarregado (DPO), Relatório de Análise de Impacto de Atividade (DPIA), Registro das Atividades, Privacy by Design, Security by Design, Centro de Tratamento e Resposta a Incidentes “Notificação”, Governança de Dados, Governança de Riscos e Compliance, Segurança da Informação, Padronização de formatos de Arquivos para acesso e compartilhamento

Conceitos: Engenharia de Valor

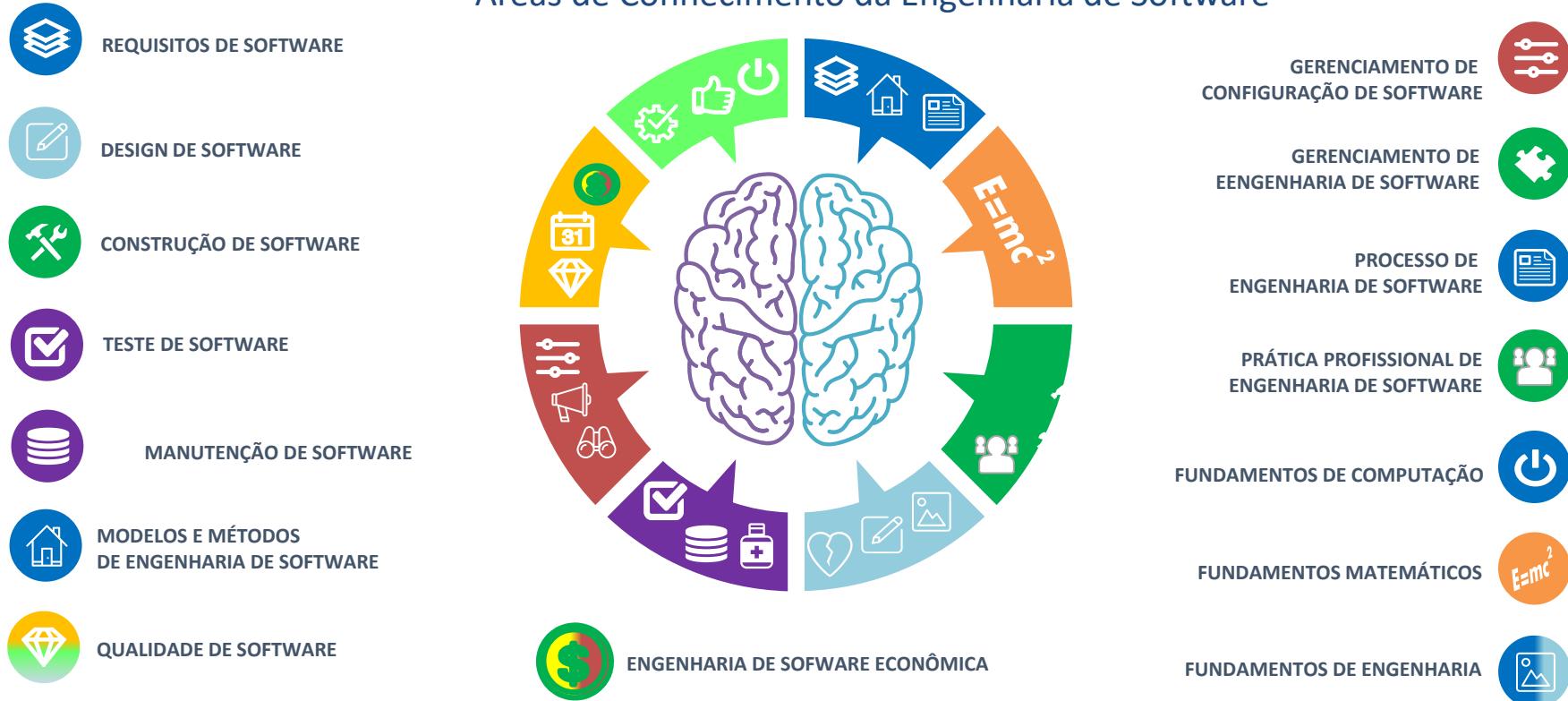
A engenharia de valor é uma abordagem usada para otimizar os custos do ciclo de vida de um projeto, economizar tempo, aumentar os lucros, melhorar a qualidade, expandir a participação no mercado, resolver problemas e / ou usar recursos de maneira mais eficiente.



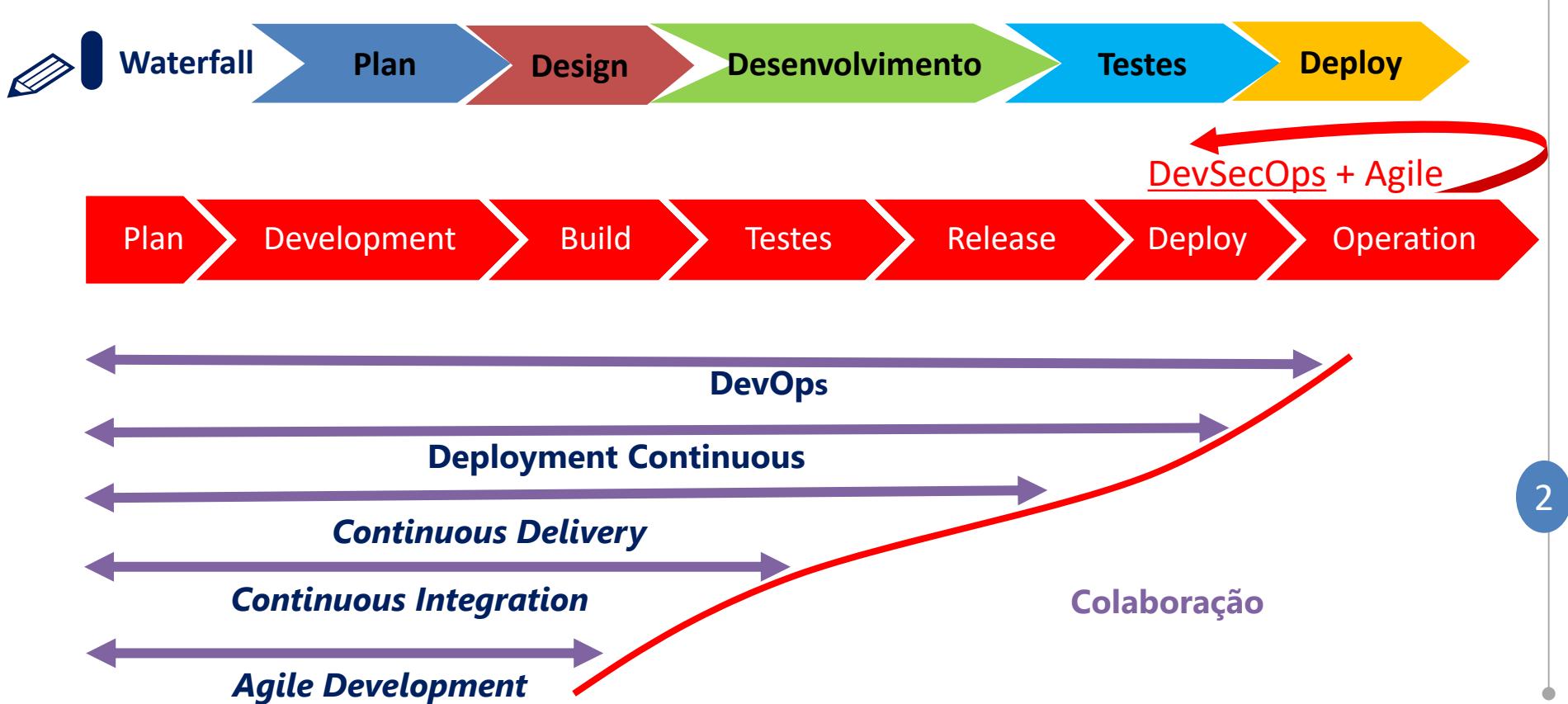
Conceitos: Engenharia de Software

Knowledge Area (KA) SWEBOK

Áreas de Conhecimento da Engenharia de Software



Conceitos: Metodologias

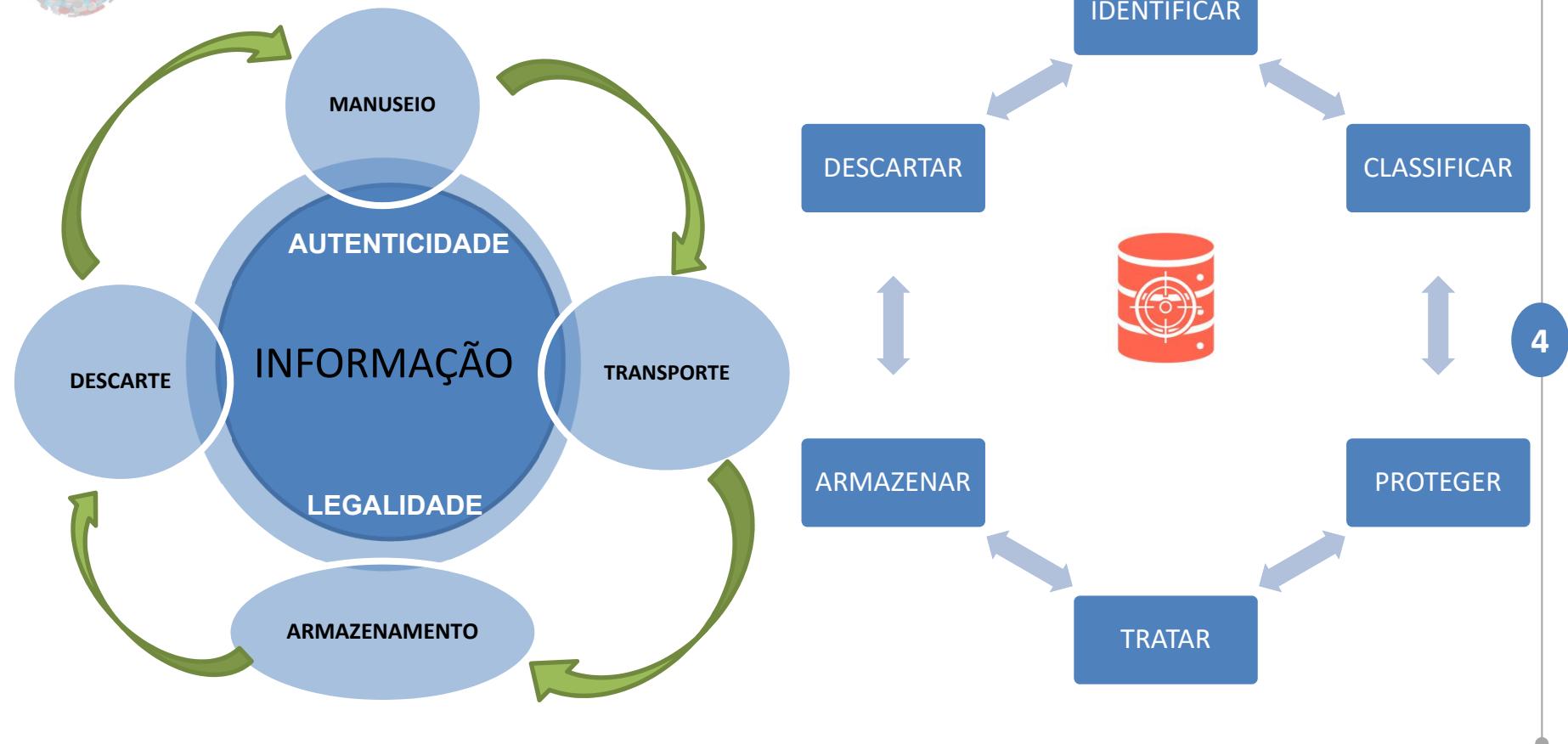


Conceitos: Ciclos de Vida





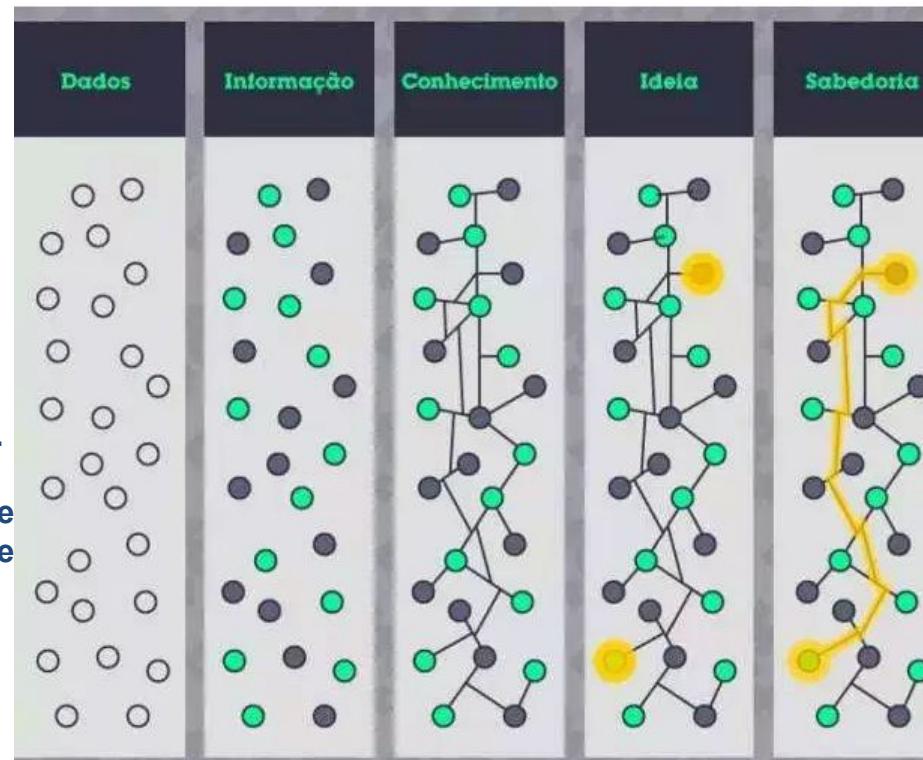
Conceitos: Ciclos de Vida



Conceitos: Dados e Informações

DADO:

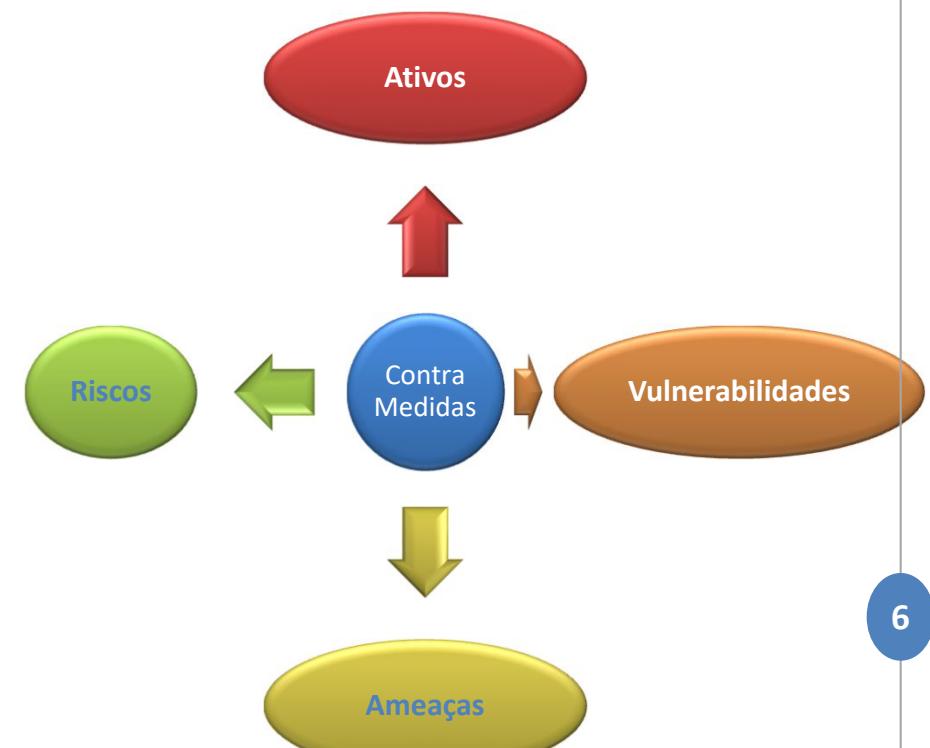
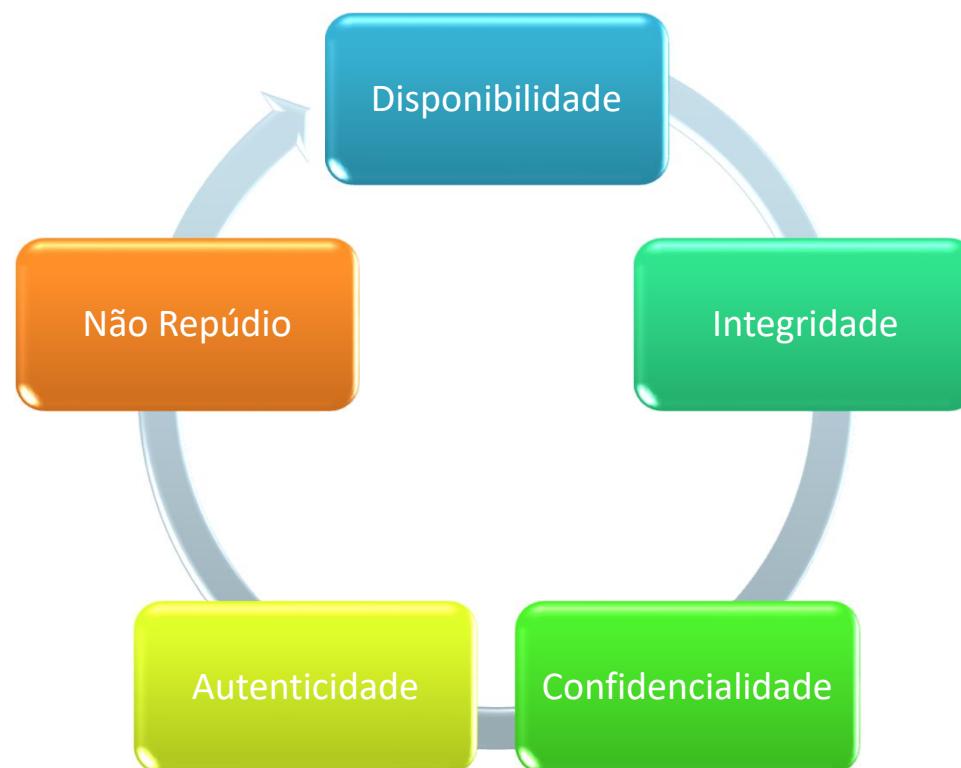
Qualquer elemento quantitativo ou qualitativo, em sua forma bruta referentes ao mundo real. Por si só não leva a compreensão de determinado fato ou situação. Facilmente estruturado e transferível, frequentemente quantificado, facilmente obtido por máquinas.



INFORMAÇÃO:

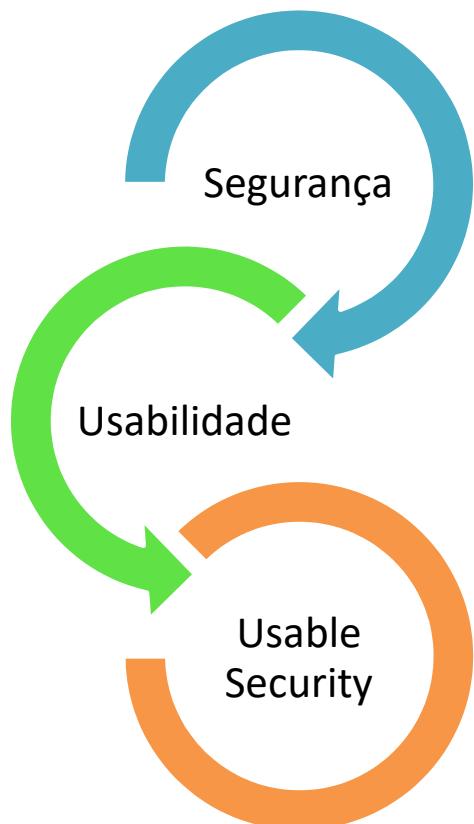
É o produto dos dados obtidos, devidamente registrados, classificados, organizados, relacionados e interpretados dentro de um contexto para gerar conhecimento conduzindo a melhor compreensão dos fatos.
Dados dotados de relevância e propósito.
Exige consenso em relação ao significado, exige necessariamente a mediação humana.

Conceitos: Segurança da Informação



Conceitos: Desenvolvimento Seguro





Conceitos: Usable Security

8

Segurança não é dificultar todas as operações, é sobre restringir o acesso a operações com efeitos indesejáveis.

Usabilidade não é fazer tudo por meio de operações fáceis, também, trata-se de melhorar o acesso a operações com efeitos desejáveis.

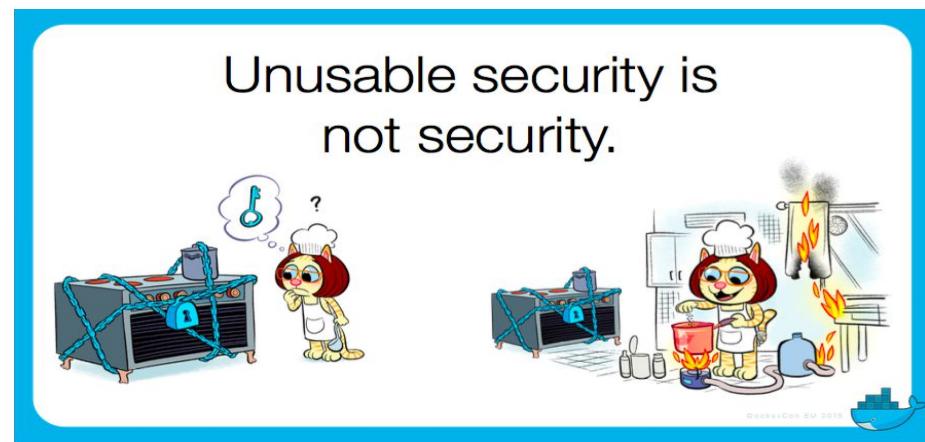
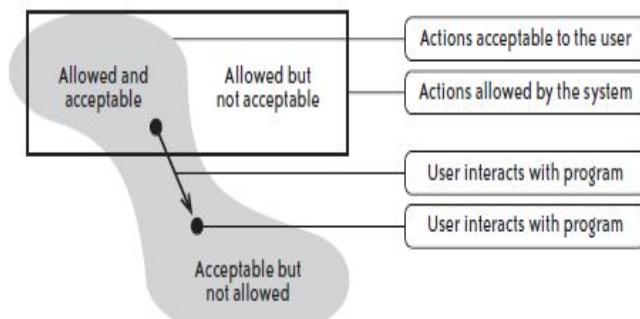
A tensão entre os dois surge na medida em que um sistema é incapaz de determinar se um determinado resultado é ou não desejável.

Segurança e usabilidade entram em harmonia quando um sistema interpreta corretamente os desejos do usuário de forma aceitável.

Conceitos: Usable Security

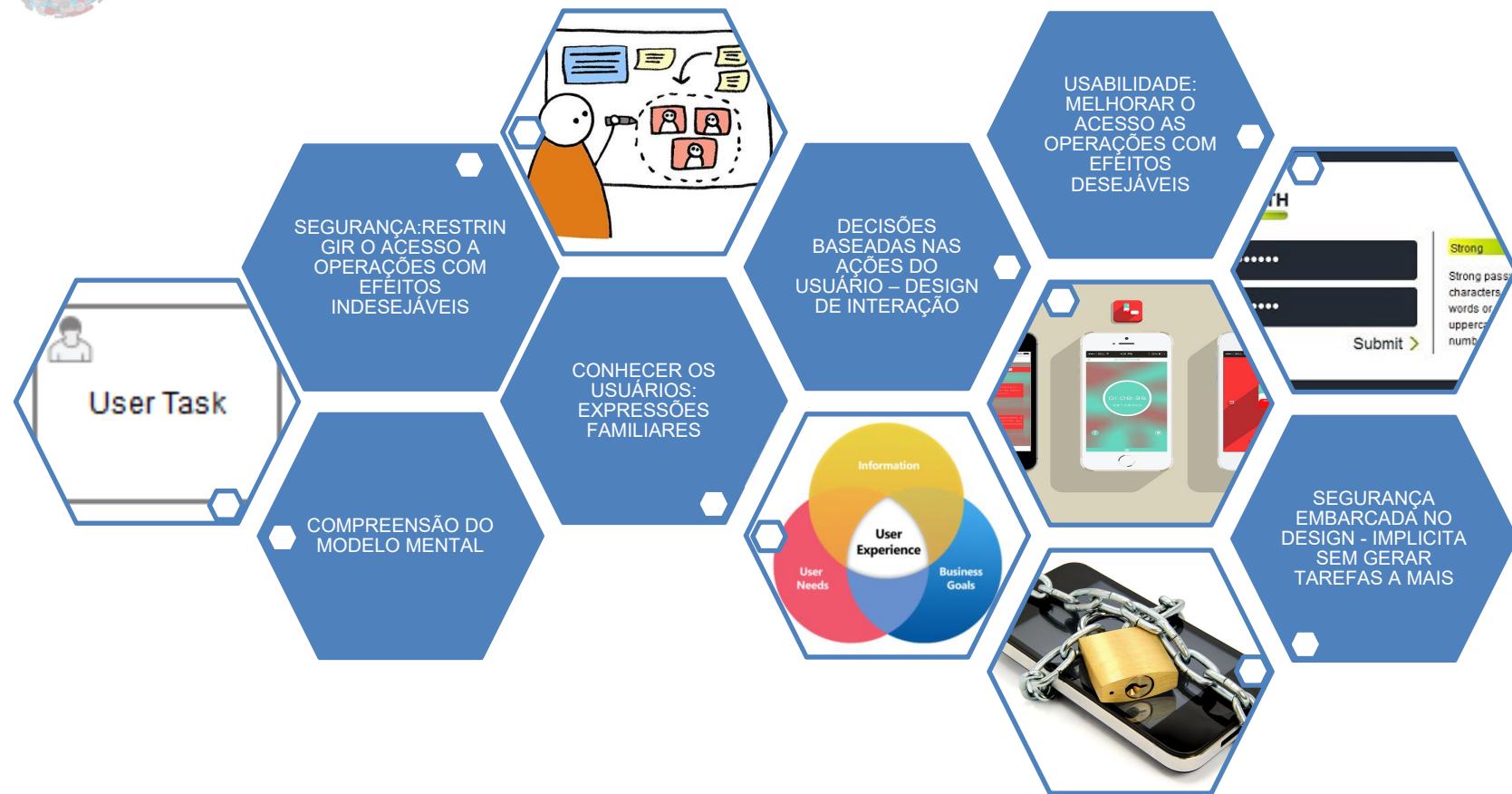
Sistemas seguros com boa usabilidade devem impor decisões de segurança com base nas informações do usuário, as ações devem permitir que essas ações sejam expressas de maneira familiar, e não baseadas em um conhecimento prévio e mais profundo de segurança e seus termos.

Em resumo a Segurança deve ser de fácil uso e compreensão dentro do nível de entendimento do usuário que a utiliza.





Princípios: Usable Security



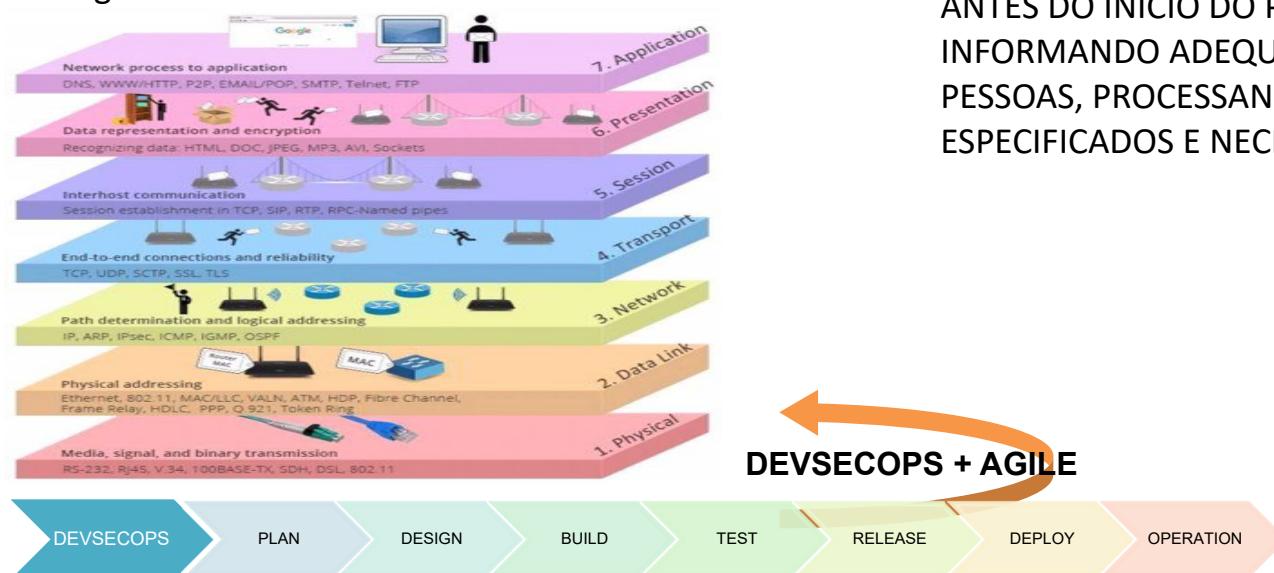
10

Princípios: Data Protection by Design e by Default

BY DESIGN:

“ UMA ABORDAGEM QUE GARANTE QUE SEJAM ABORDADAS AS QUESTÕES DE PRIVACIDADE E PROTEÇÃO DE DADOS NA FASE DE DESIGN DE QUALQUER SISTEMA, SERVIÇO, PRODUTO OU PROCESSO E DEPOIS DURANTE TODO O CICLO DE VIDA.”

ico.org.uk



BY DEFAULT:

“ UMA ABORDAGEM QUE EXIGE QUE SEJAM PROCESSADOS APENAS OS DADOS NECESSÁRIOS PARA ATINGIR O OBJETIVO ESPECÍFICO PELO QUAL OS DADOS FORAM COLETADOS. É PRECISO ESPECIFICAR QUAIS DADOS SERÃO COLETADOS E TRATADOS ANTES DO INÍCIO DO PROCESSAMENTO, INFORMANDO ADEQUADAMENTE AS PESSOAS, PROCESSANDO APENAS OS DADOS ESPECIFICADOS E NECESSÁRIOS” [.ico.org.uk](http://ico.org.uk)

Princípios: Privacy By Design



1 - Proatividade e não reatividade - Prevenir não remediar



2 - Embarcada no Design – Design visando a Privacidade



3- Segurança fim a fim - Proteção durante o ciclo de vida completo



4 - Respeito pela privacidade do Usuário - Mantenha centrado no usuário



5 - Privacidade como Configuração Padrão



6 - Funcionalidade Completa - Soma positiva não soma zero



7 - Visibilidade e Transparência - Mantenha aberto

Privacidade por Default significa que, uma vez que um produto ou serviço tenha sido liberado para o público, as configurações de privacidade mais rígidas devem ser aplicadas por padrão, sem nenhuma entrada manual do usuário final. Além disso, quaisquer dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto devem ser mantidos apenas durante o tempo necessário para fornecer o produto ou serviço. Se mais informações do que o necessário para fornecer o serviço forem divulgadas, a "privacidade por padrão" foi violada.

Princípios: Security By Design

1 - Minimizar a superfície de área de ataque



Através da utilização de patterns de desenvolvimento de código e boas práticas de desenvolvimento seguro.

2 - Estabelecimento de Padrões



Através da utilização de senhas fortes, ciclo de vida de senhas, autenticação multifator e tokens.

3 - Princípio do Menor Privilégio



Através da criação de contas com a menor quantidade de privilégios necessários para executar seus processos de negócios. Isso engloba direitos de usuário, permissões de recursos, como limites de CPU, memória, rede e permissões do sistema de arquivos.

4 – Princípio da Defesa em Profundidade



Utilizando um controle que seria razoável, mais controles que abordam riscos de diferentes maneiras são melhores. Os controles, quando usados em profundidade, podem tornar vulnerabilidades extremamente difíceis de explorar e, portanto, improváveis de ocorrer.

5 – Falhar com Segurança



Os aplicativos geralmente não processam transações por vários motivos. A forma como eles falham podem determinar se um aplicativo é seguro ou não, por exemplo se expõe, endpoints, paths, strings de conexão etc.

Princípios: Security By Design

6 - Não Confie nos Serviços

Todos os sistemas externos com parceiros, integradores, brokers, devem ser tratados de maneira semelhante, os dados devem ser sempre verificados para garantir a segurança de exibição ou compartilhamento com o usuário final.

7 - Separação de deveres

Através da determinação de papéis que têm diferentes níveis de confiança do que usuários normais. Em particular, os administradores são diferentes dos usuários normais, utilizando RBAC para atribuição de permissionamento.

8 - Evitar a segurança por obscuridade

A segurança de um aplicativo não deve depender do conhecimento do código-fonte mantido em segredo. A segurança deve se basear em muitos outros fatores, incluindo políticas razoáveis de senha, defesa em profundidade, limites de transação de negócios, arquitetura de rede sólida e controles de fraude e auditoria.

9 - Mantenha a Segurança simples

Onde os desenvolvedores devem evitar o uso de negativos duplos e arquiteturas complexas quando uma abordagem mais simples seria mais rápida e simples.

10 - Correção de Problemas de Segurança da maneira correta

Quando um problema de segurança for identificado, é importante desenvolver um teste para ele e entender a causa raiz do problema. Quando padrões de design são usados, é provável que o problema de segurança seja difundido entre todas as bases de código, portanto é essencial desenvolver a correção correta sem introduzir regressões.

Pessoas: Uma visão geral de Times



THE
DEVELOPER'S
CONFERENCE

PSBD 2,6 ,7

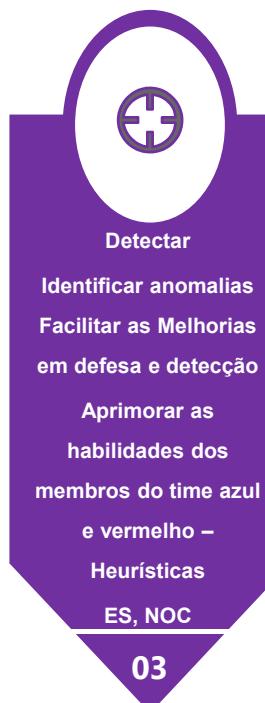
Blue Team



Orange Team



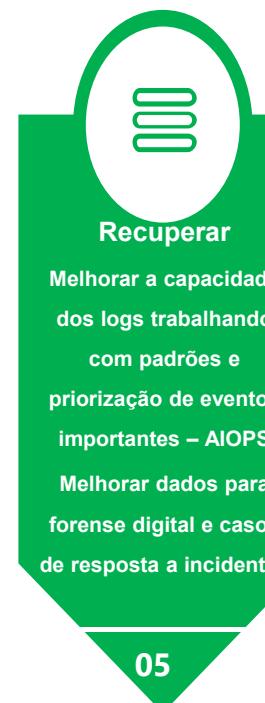
Purple Team



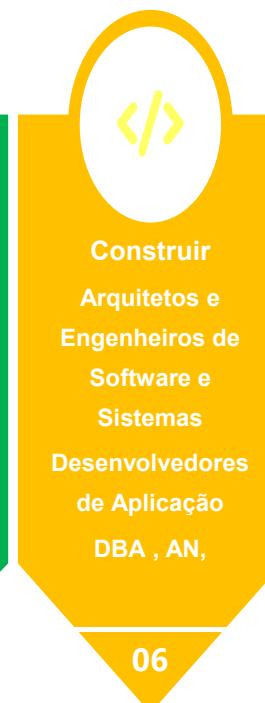
Red Team



Green Team



Yellow Team



15

Pessoas: Sugestão de Papéis

PSBD 2,6 ,7

Papéis:



1. Process Master (Scrum Master)
2. Service Master (Product Owner)
3. DevOps Engineer



4. Gatekeeper – Release Coordinator
5. Reliability Engineer (opcional)



6. Time Desenvolvimento (Dev,
QA,DBA)
7. Time de Operação

Arquiteto de Soluções
Arquiteto Corporativo

Arquiteto de Infraestrutura
Engenheiro de Software

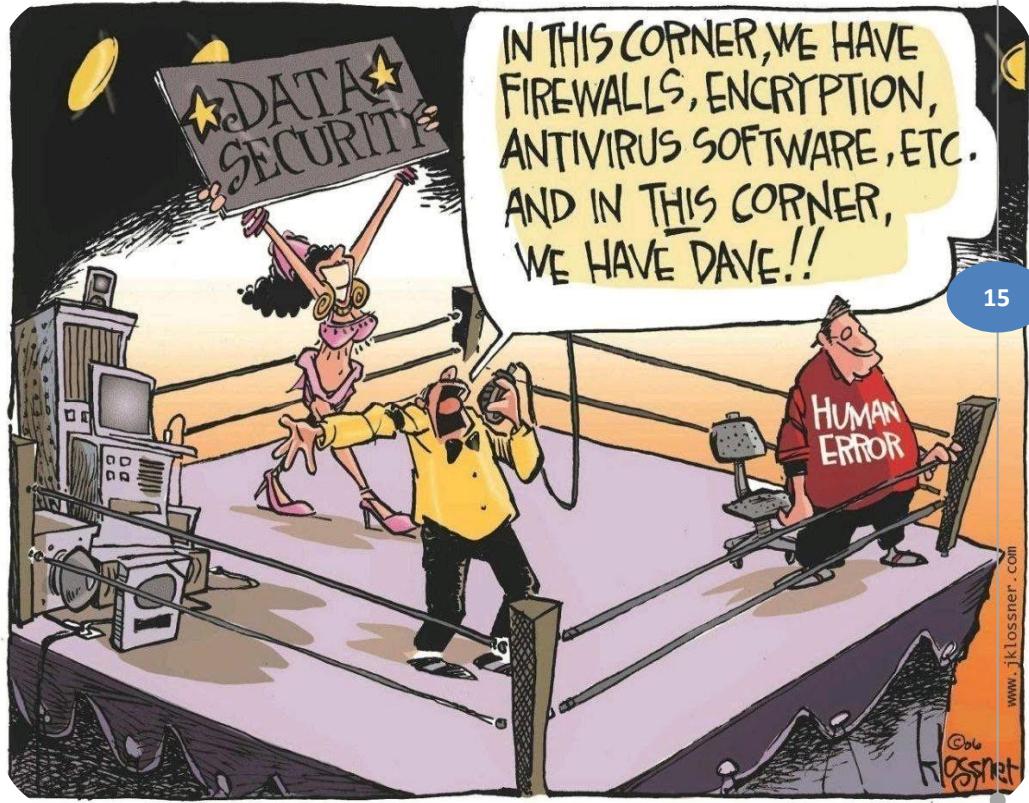
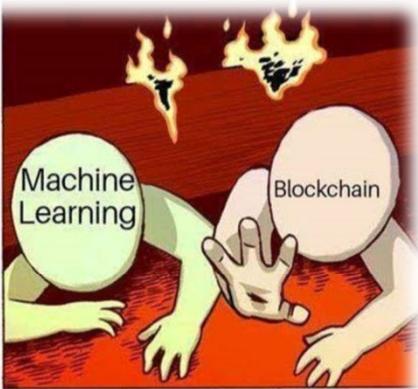
Engenheiro/ Arquiteto de Software

Arquiteto de Dados, Analista de Negócios,
Desenvolvedores, Analista de Testes,
Designers, Analista de Segurança

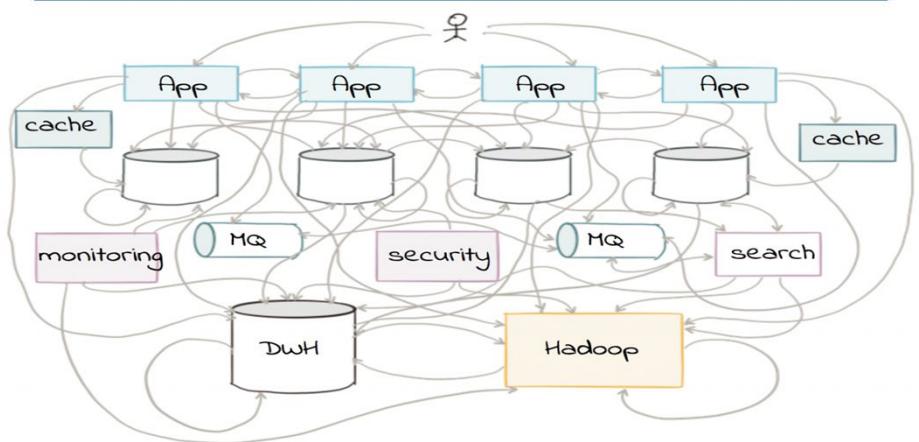
DBA, Analista de Segurança, Analista de
Monitoramento, Analista de Infraestrutura e
Suporte, Arquiteto / Enghenheiro de Segurança

16

Problemas:



Problemas:



Problemas:

Privacy Warnings Issued Over Russian-Owned FaceApp

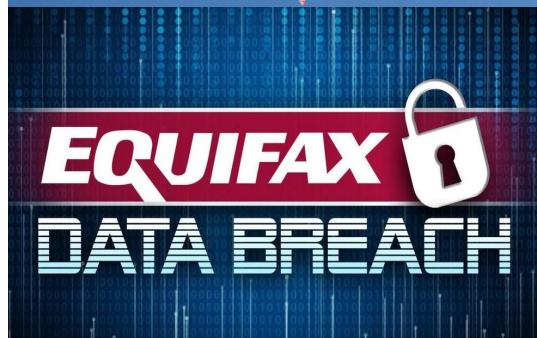
By John Shumway | July 17, 2019 at 3:40 pm | Filed Under: FaceApp, John Shumway, Pittsburgh News, Privacy



Security fears over Russian aging app 'FaceApp' as experts warn it can access ALL of your pictures even if you say not to

- FaceApp puts a filter over your face to augment it to look like an old person
- It uses artificial intelligence to edit a picture in your gallery and transforms it
- Experts are concerned that it can access and store images from your camera roll
- But people are giving FaceApp access to use, modify, adapt and publish any images of you that you offer up in exchange for its AI, the terms of service says

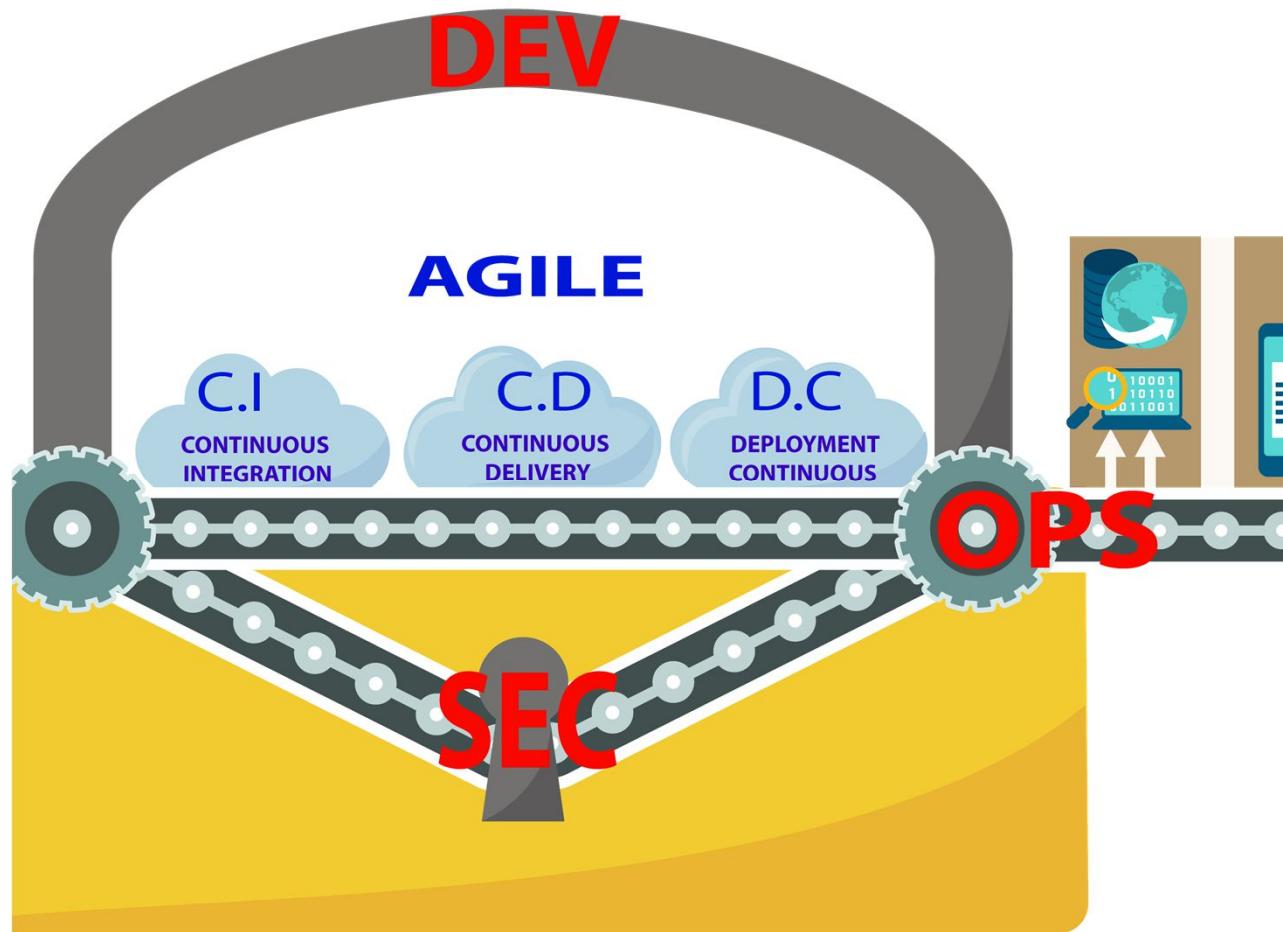
By VICTORIA BELL FOR MAILONLINE





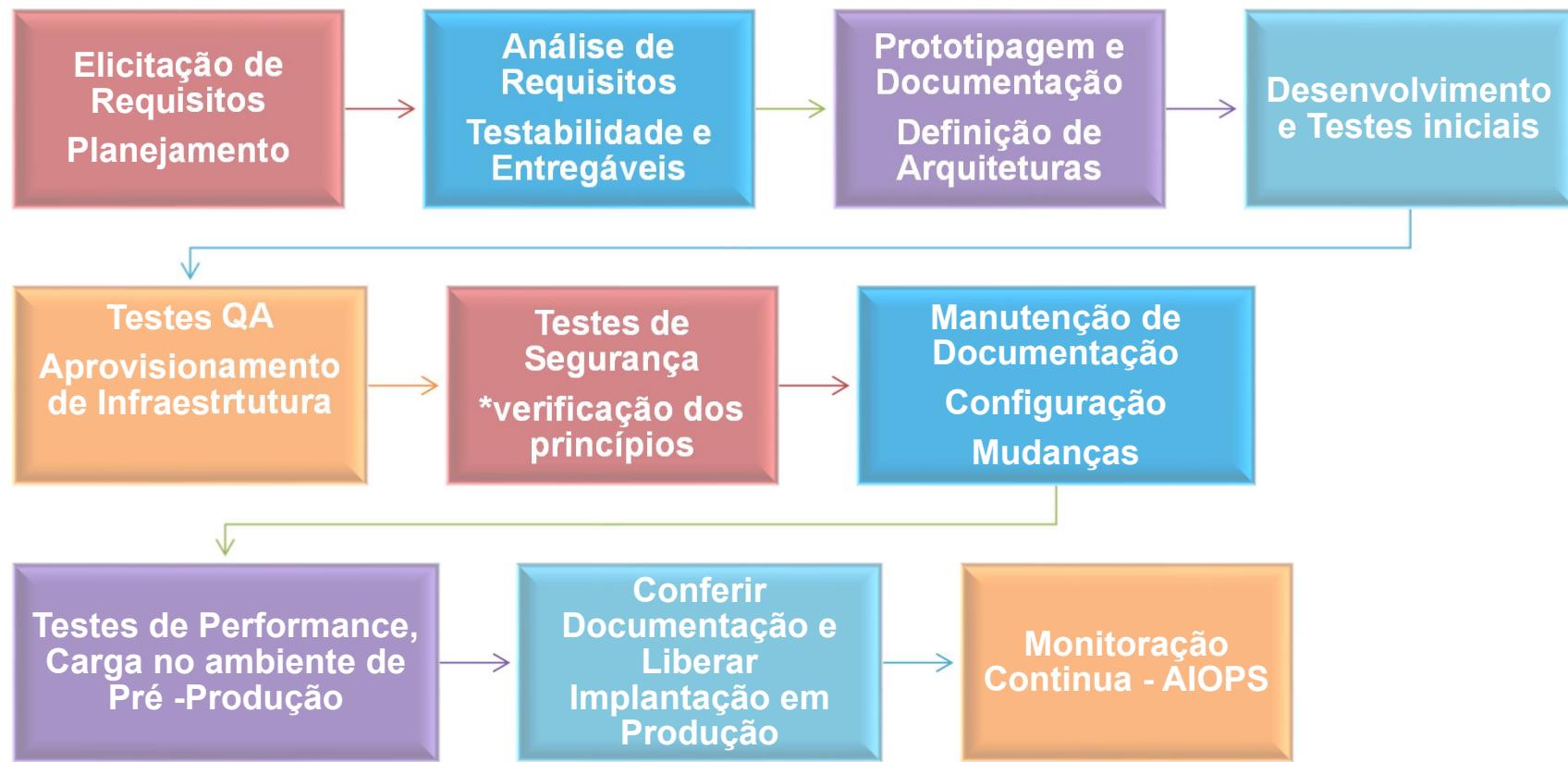
OK, Cleanup our mess





Processos:

PSBD 2,3,6 ,7





Processos:

PSBD 1, 2, 3, 5,



Ferramentas:

PSBD 1, 4, 5, 7 PBD 2, 3, 5

PERIODIC TABLE OF DEVOPS TOOLS (V3)																		2	En	
1	Os																	2	En	
	Gl GitLab																	Sp Splunk		
3	Fm	4	En																	
	Gh GitHub		Dt Datcal																	
11	Os	12	En																	
	Sv Subversion		Db DBMaestro																	
19	En	20	En	21	Os	22	Fm	23	Os	24	Fr	25	Fr	26	Fm	27	En	28	Fr	
	Cw ISPW		Dp Delphix		Jn Jenkins		Cs Codeship		Fn FitNesse		Ju JUnit		Ka Karma		Su SoapUI		Ch Chef		Tf Terraform	
37	Pd	38	Fm	39	Pd	40	Fm	41	Fr	42	Fr	43	Os	44	Pd	45	En	46	Os	
	At Artifactory		Rg Redgate		Ba Bamboo		Vs VSTS		Se Selenium		Jm JMeter		Ja Jasmine		Sl Sauce Labs		An Ansible		Ru Rudder	
55	Pd	56	Os	57	Os	58	Fm	59	Os	60	Fr	61	Fm	62	Pd	63	En	64	Os	
	Nx Nexus		Fw Flyway		Tr Travis CI		Tc TeamCity		Ga Gatling		Tn TestNG		Tt Tricentis Tosca		Pe Perfecto		Pu Puppet		Pa Packer	
73	Fm	74	En	75	Fm	76	Pd	77	Fr	78	Os	79	Os	80	En	81	Os	82	Os	
	Bb BitBucket		Pf Perforce		Cr Circle CI		Cb AWS CodeBuild		Cu Cucumber		Mc Mocha		Lo Locust.io		Mf Micro Focus UFT		Sa Salt		Ce CFEngine	
																		Eb ElasticBox		
																		Ca CA Automic		
																		De Docker Enterprise		
																		Ae AWS ECS		
																		Cf Codefresh		
																		Hm Helm		
																		Aw Apache OpenWhisk		
																		Ls Logstash		



Follow @xebialabs

91	En	92	Os	93	Fm	94	En	95	En	96	Fm	97	Os	98	Os	99	Os	100	En	
	XLi XebiaLabs XL Impact		Ki Kibana		Nr New Relic		Dt Dynatrace		Dd Datadog		Ad AppDynamics		Ei ElasticSearch		Ni Nagios		Zb Zabbix		Zn Zenoss	
106	En	107	Pd	108	Fm	109	Fm	110	Fm	111	En	112	En	113	En	114	Pd	115	Pd	
	Sw ServiceNow		Jr Jira		Tl Trello		Sk Slack		St Stride		Cn CollabNet VersionOne		Ry Remedy		Ac Agile Central		Og OpsGenie		Pd Pagerduty	
																		Sn Snort		
																		Tw Tripwire		
																		Ck CyberArk		
																		Vc Veracode		
																		Ff Fortify SCA		

Ferramentas:

PSBD 1, 4, 5, 7 PBD 2, 3, 5



The Periodic Table of Security

The elements that make up the remit of a security professional

- | | |
|--|--|
|  Access Control & Biometrics |  Intruder Alarms |
|  Facilities |  IT & Cyber Security |
|  Fire Alarms/Detection/Protection |  Peripheral Services & Components/Tools |

- Physical Security
 - Safe Cities
 - Safety & Health
 - Security Guarding and Support Services
 - Video Surveillance (CCTV)

Keep on top of every element of security

Running alongside FIREX, Safety & Health Expo and Facilities Show, IFSEC International 2019 will bring you access to the latest, leading solutions in security and beyond.

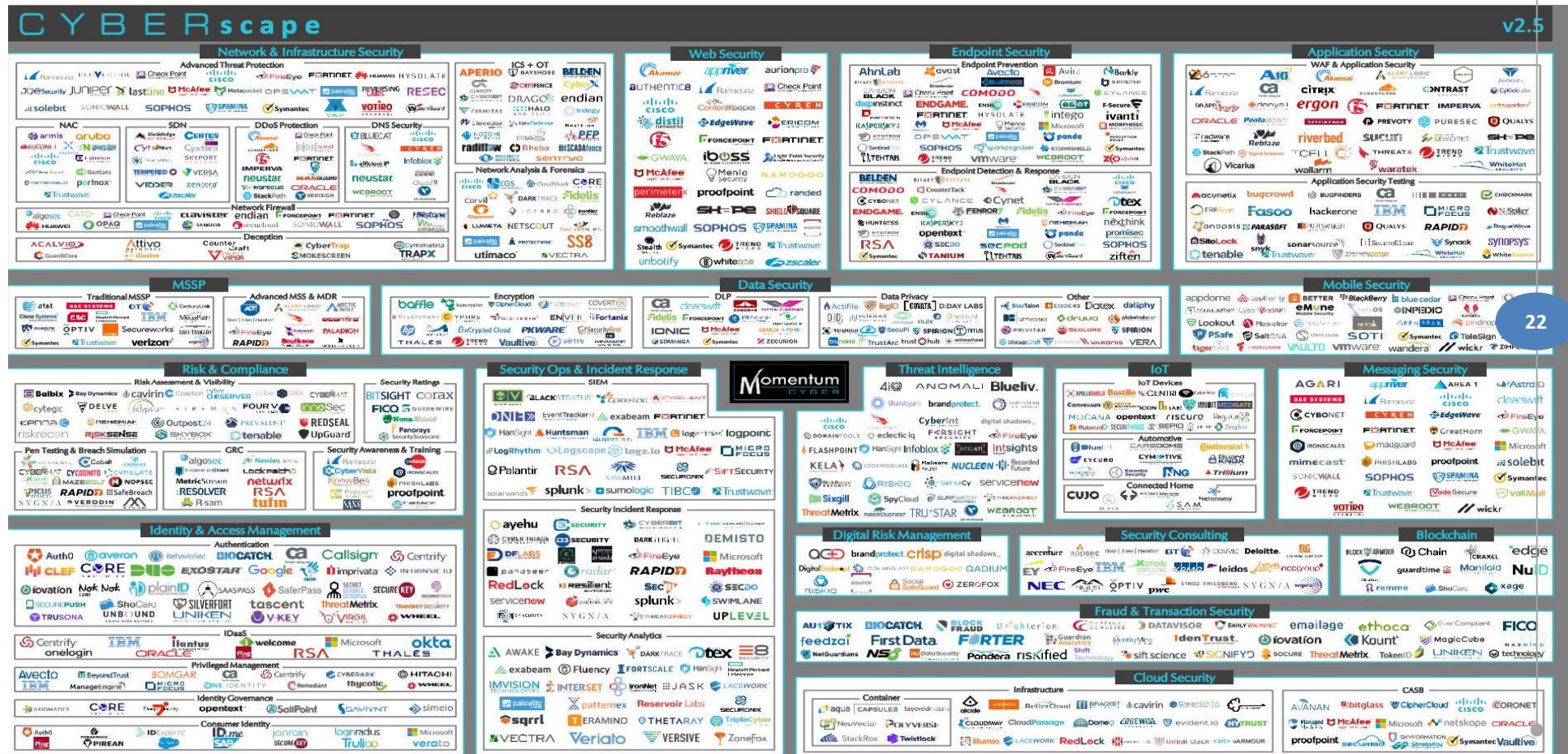
[LEARN MORE](#)

Bi	Fc	Rf	Ha	In	Cn	Ca	Cc	Ci	Tr	Cv	P	Tc	IP	Rs	Ti				
Biometrics	Facial Recognition	NFC	Home Automation	Integration	Connectivity	Cloud Safety Containers	Command and Control	CC	Intelligent Transport	Cash & Valuables in Transit	Personnel	CCTV Points, Towers & Columns	IP-Cameras	Emergency Surveillance	Thermal Imaging				
Cr	Card Readers	Fg	Firewalls	St	Smartboards	Ia	Smoke Alarms	IoT	Internet of Things	Eq	Equipment Installation Test	Gs	Gates & Shutters	Sm	Scanners & Monitors	Cs	Corporate Security		
De	Door Entry	Fn	Fingerprints	Ta	Time and Attendance	Wa	Wireless Alarms	Ln	LAN/WAN Switches	Ps	Power Supplies	Kc	Keys & Cabinets	Tf	Technical Furniture	Cm	Cross Management		
Ha	Home Automation	Vi	Vision Identification	An	Analogue Converters	Nk	Network Security	S	Switches	Pt	Power Tools and Radio Charging	Fi	Fence Intrusion Detection	Ci	Critical Infrastructure	Ra	Risk Analysis & Assessment		
Ic	IP Access Control	Vp	VDP	Ds	Data Storage Solutions	Va	Video Analytics	Au	Armories	Sl	Sales / Locks	Ir	Infrared Parameter Monitoring	Cy	Cyber Resilience	Gt	Guard Tour Services/ Systems		
Id	ID Cards	Aw	Alarm Warning	Em	Enterprise Management	Bt	Batteries/ Chargers/ Power Supply	Ag	Asset Tagging/ Tracking Services	Se	Security Enclosures	Pp	Perimeter Protection Systems	Dr	Disaster Recovery/ Business Continuity	Us	Urban Security		
Lk	Locking	Fl	False Alarm Prevention	Fo	Fibre Optics	Cw	Callouts/ Detection/ Protection	Bb	Banners & Bolards	Ss	Security Seals	Bd	Big Data / Data Analytics	Er	Emergency Response	Ap	Aviation/ Port Security		
Fa	Fire Alarms	Dt	Fire Directors	Rc	Alarm Receiving Centres	Gh	Gas Heat Detectors	Fe	Fire Extinguishers	Do	For Doors	Sg	Fire Signalling	Sd	Smoke Detectors	Ppe	Personal Protective Equipment	Dm	Decommissioning
																Gd	Gas Detection		
																Sc	Spill Containment		
																W	Working At Height		
																Am	Air Monitoring		
																Es	Emergency Response		
																Sf	Site Safety		
																Osh	Occupational Health and Safety		
																Sch	Screening		

21

PSBD 1, 4, 5, 7 PBD 2, 3, 5

Ferramentas:



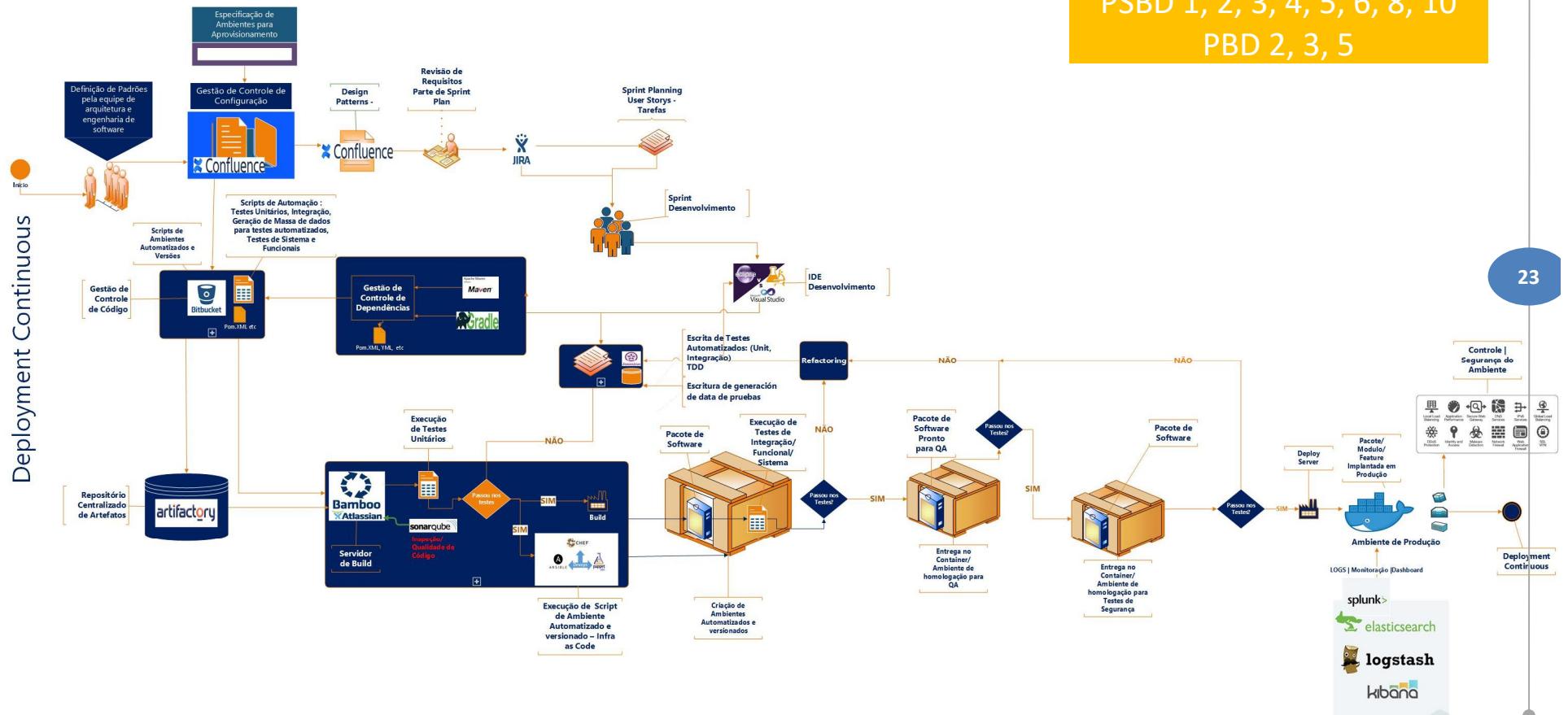


Checklist Deployment Continuous:

- Controle de defeitos documentados (gestión de problemas e incidentes)
- Controle de código de infraestrutura (ambientes)
- Testes de aceitação automatizados
- Geração de Massa de testesautomatizada
- Fluxo de verificação automática de defeitos corrigidos
- Ambiente de testes apartado e versionado
- Servidor de Deployment
- Crição de ambientes automatizado e versionado conteinerização de ambientes produtivos)
- Processo automatizado de solicitações de mudanças
- Criação de registros
- Supervisão da Implementação automatizada ferramentas

Automação: abordagem DevSecOps

PSBD 1, 2, 3, 4, 5, 6, 8, 10
PBD 2, 3, 5

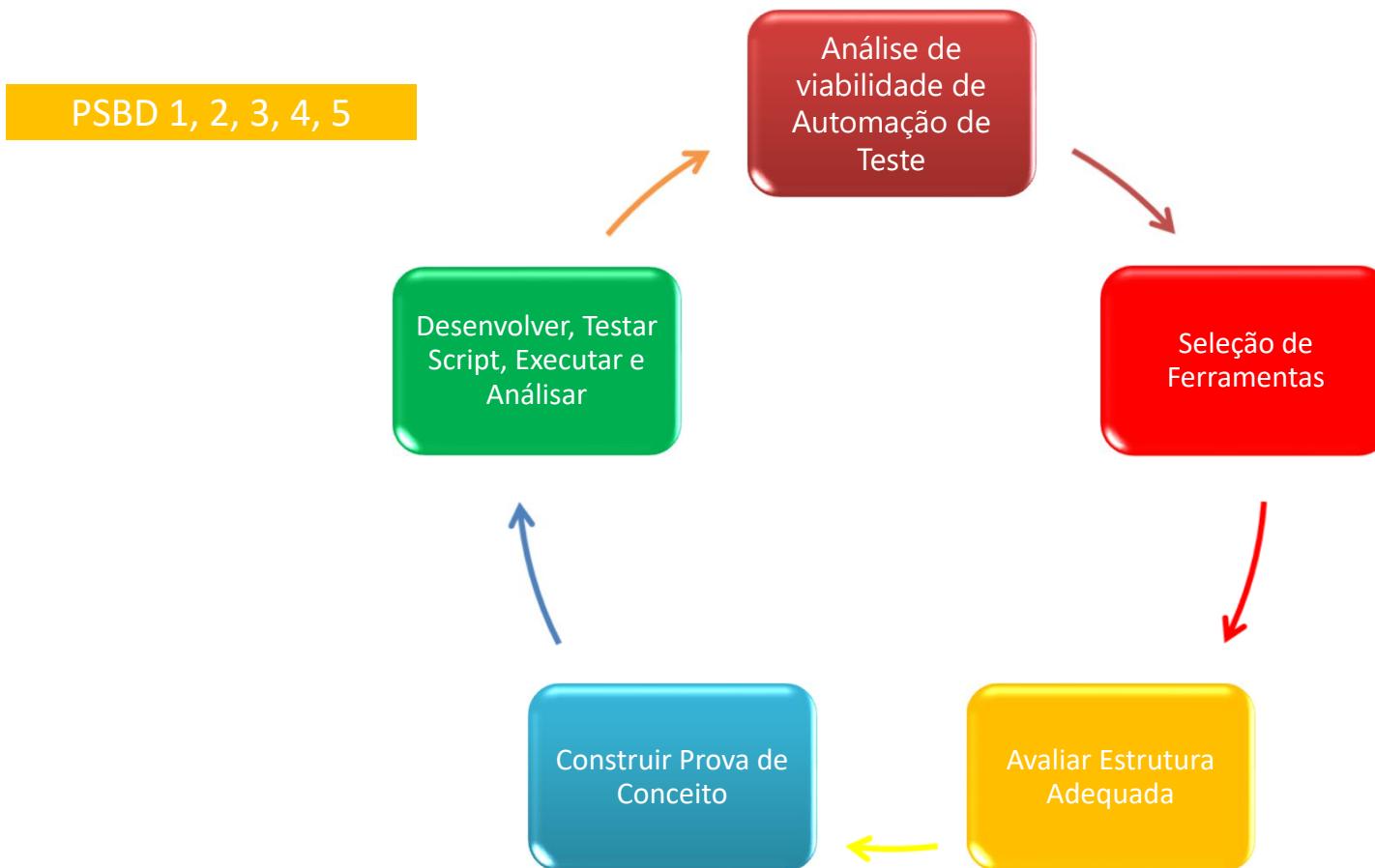


23

Automação: abordagem de Testes



24



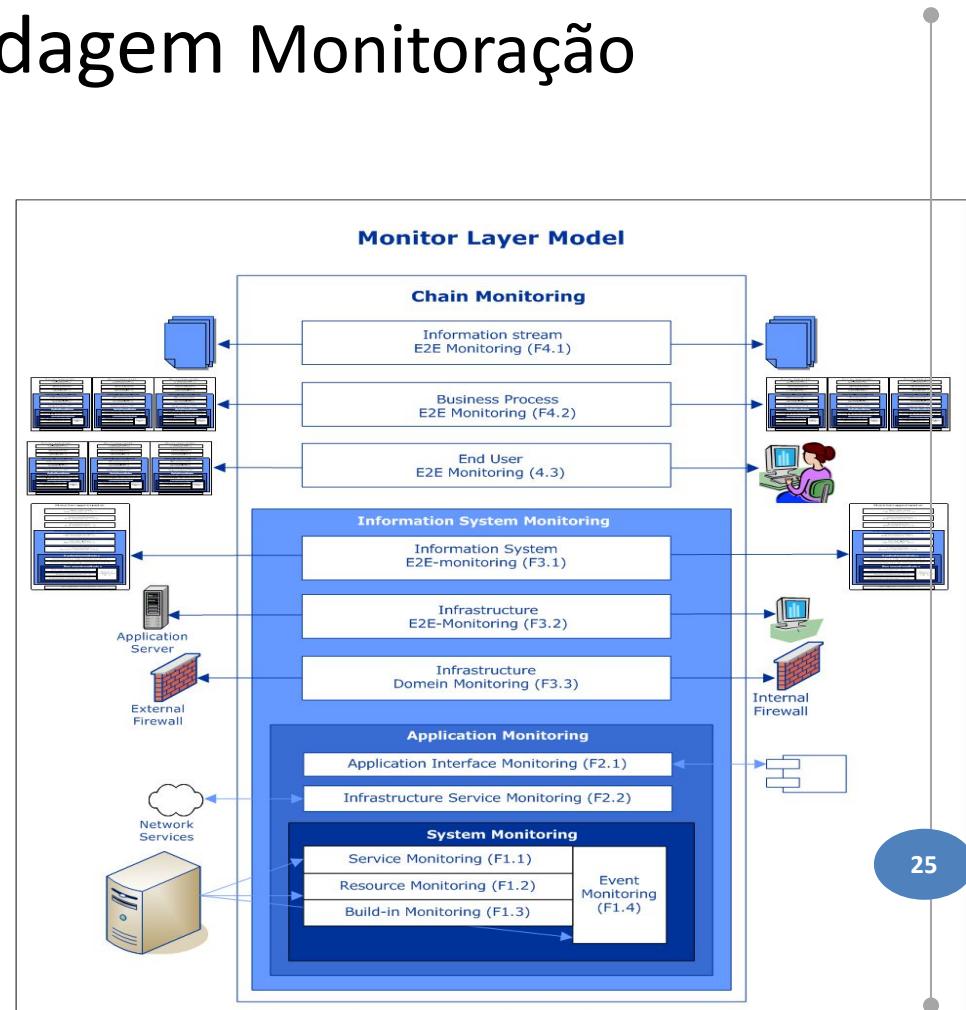
Automação: abordagem Monitoração

PSBD 1, 2, 3, 4, 5, 6, 10

Os seguintes padrões de melhores práticas se aplicam a um dispositivo de monitoramento DevOps limpo durante a programação:

- S1. Cada evento tem um número único
- S2. Cada evento refere-se ao item de configuração do software que fez a exceção.
- S3. Cada evento possui um código de gravidade atribuído.
- S4. Cada evento também define a ação de recuperação.
- S5. Cada novo evento será registrado no backlog do produto da equipe OPS.

Durante a fase de compilação, deve-se saber quais funções de monitor são aplicáveis. A equipe de atendimento e operações são partes interessadas importantes para serem envolvidas.



PSBD 1 ao 10

Segurança: Pilares



26



CiberSegurança

Política de CiberSegurança
Política de Classificação e Fluxo da Informação
Política de Desenvolvimento Seguro
Política de Senhas
Normas de Criptografia
Gestão de Identidade e Controle de Acesso



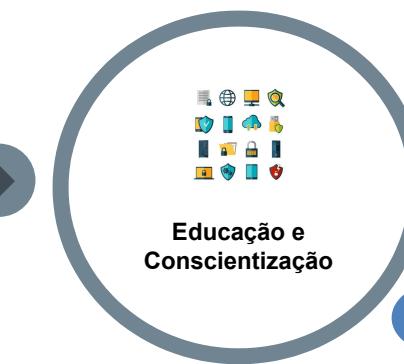
Resposta a Incidentes

Política Corporativa de Segurança da Informação
Política de Gestão de Incidentes
Plano de Gestão de Comunicação e Crises
Análise de Impacto do Negócio - BIA
CIRT
Base de Conhecimento



Continuidade de Negócios

Programa de Gestão da Continuidade
Política de Continuidade do Negócio
Plano de Recuperação de Desastres
Plano de Contingência
Plano de Continuidade Operacional
Política de Gestão de Ativo
Gestão de Defeitos



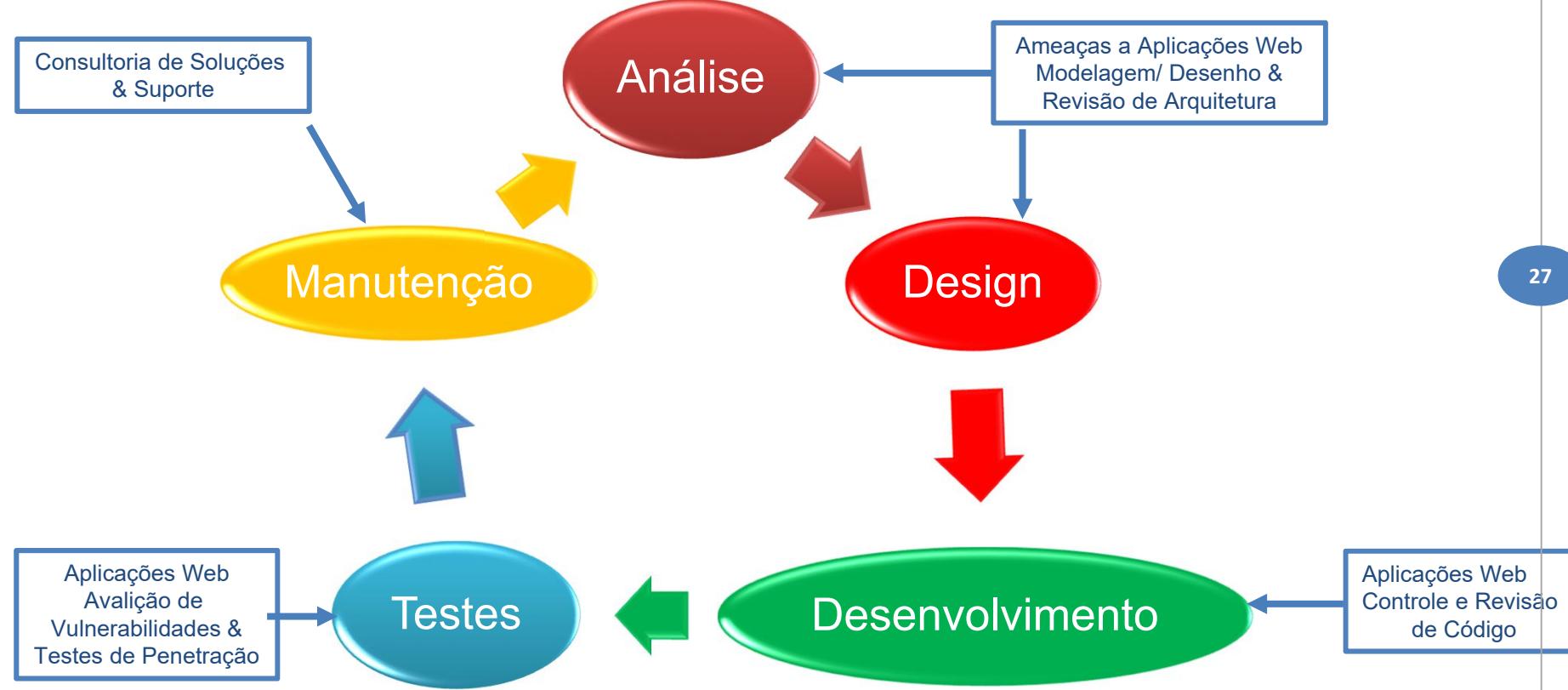
Educação e Conscientização

Plano de Segurança Física e do Ambiente
Política de Segurança Patrimonial e Recursos Humanos
Cronograma de Ações e Eventos de Conscientização sobre Segurança da Informação e Pessoal
Cronograma de Educação e Capacitação

Segurança: automação de testes



PSBD 1, 2, 4, 5, 6, 8



Governanças: Boas Práticas

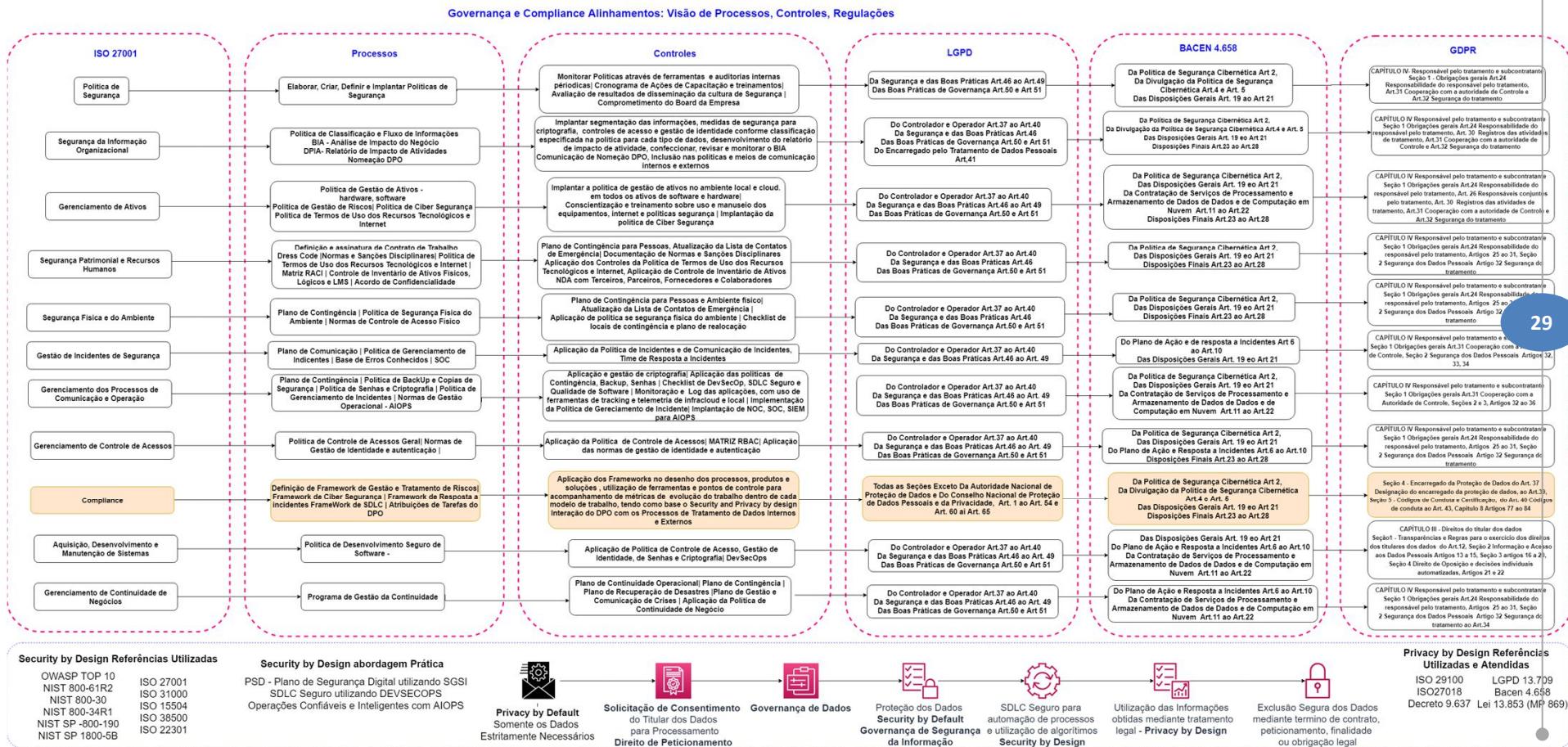


PSBD 2, 5, 7



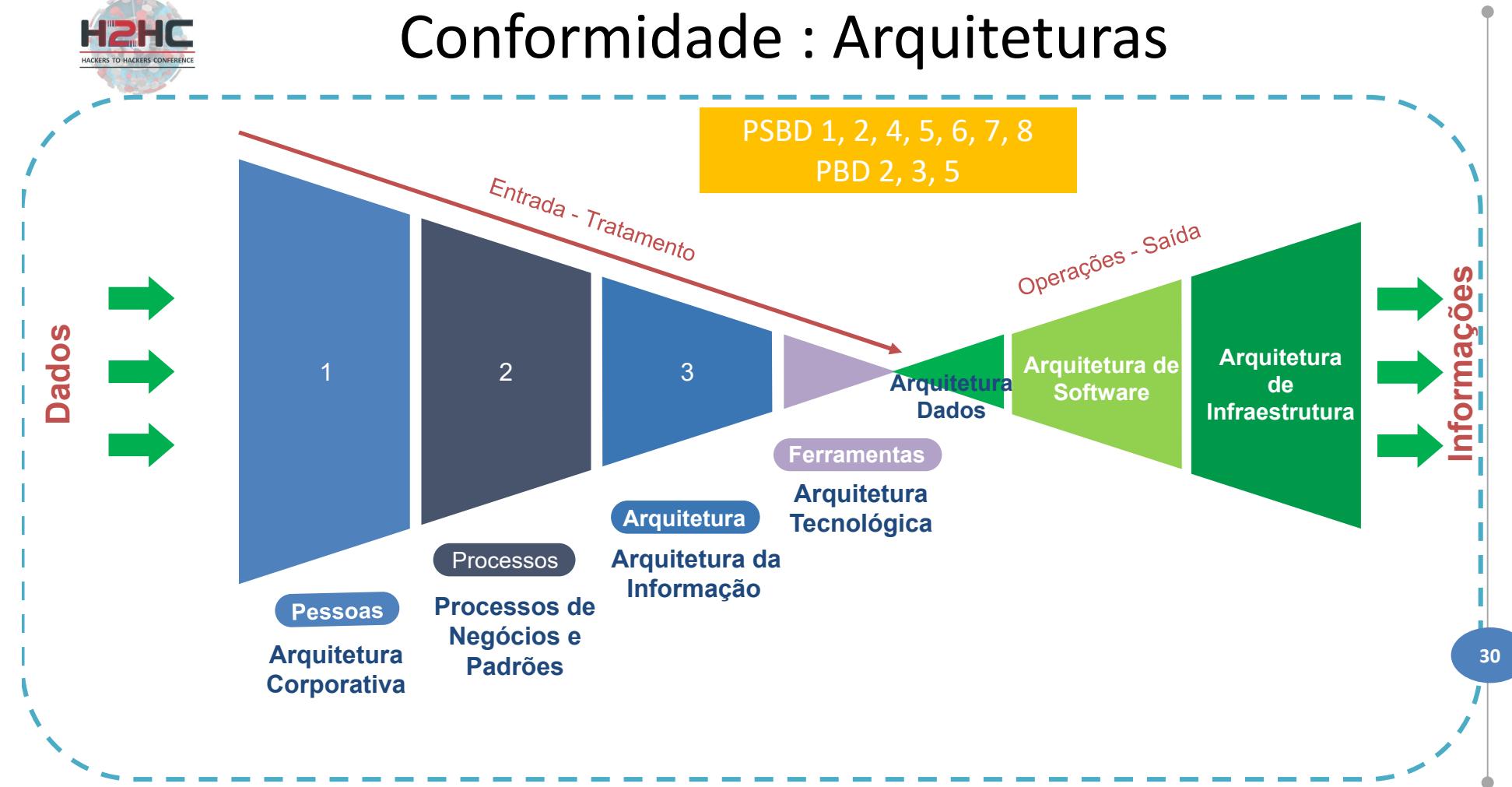
PSBD 2, 5, 7

Conformidade : Alinhamentos



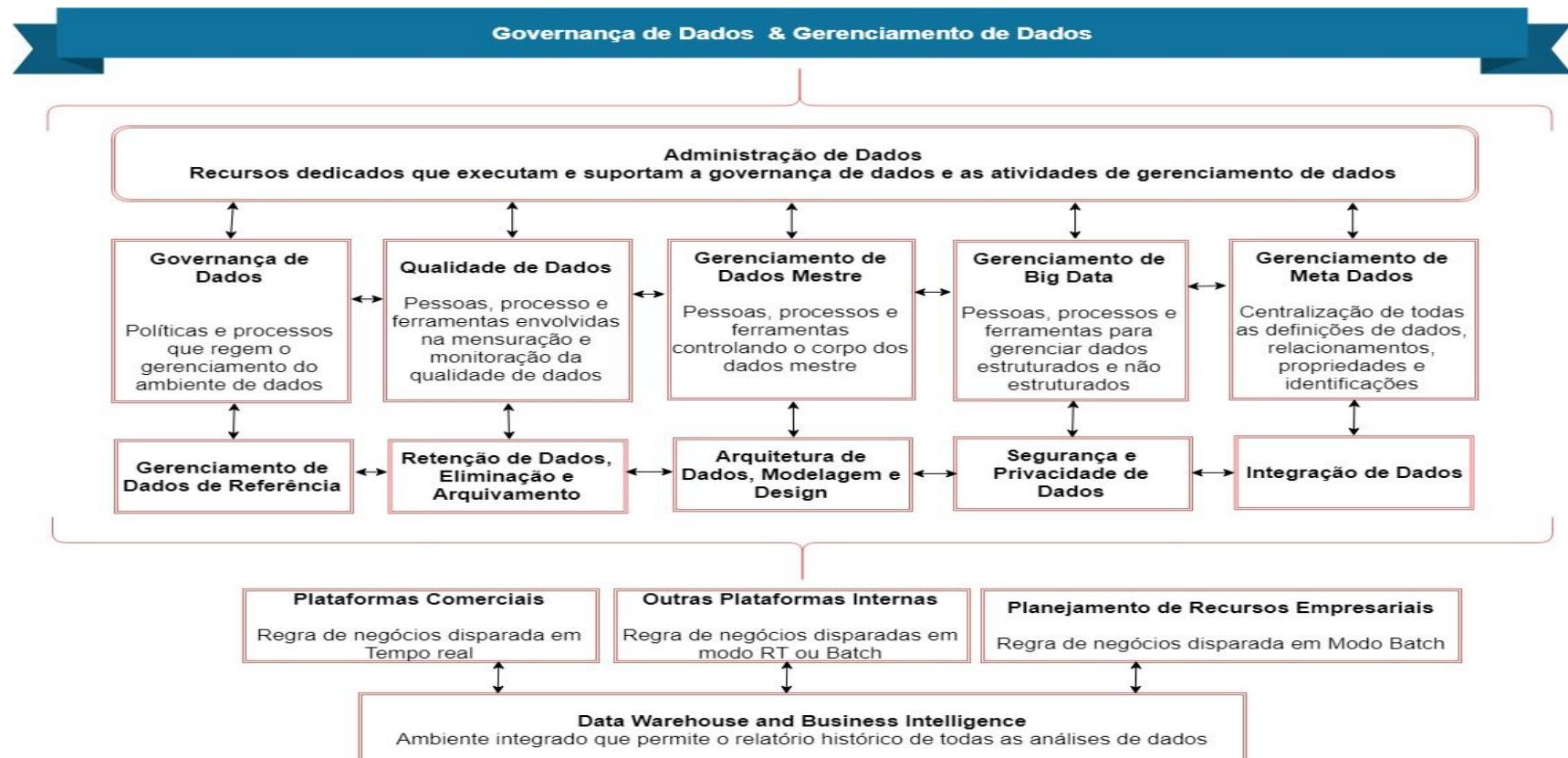


Conformidade : Arquiteturas



Conformidade : Dados

PSBD 1, 2, 4, 5, 6, 7, 8 PBD 2, 3, 5



Conformidade: Desenvolvimento Seguro

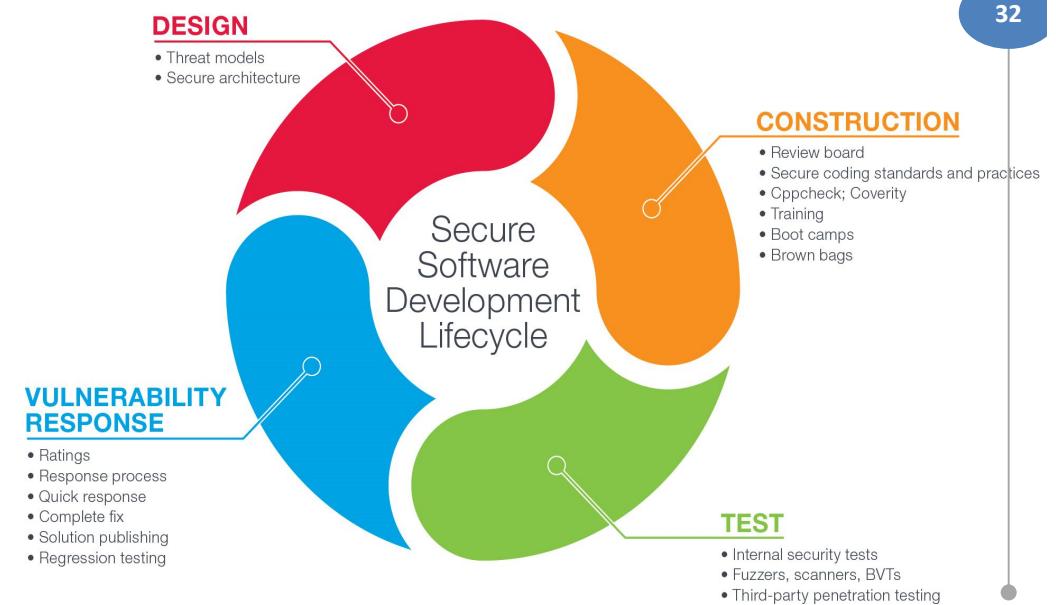
PSBD 1, 2, 3, 4, 5

Modelos de Maturidade:

- Capability Maturity Model Integration 2 (CMMI);
- Team Software Process (TSP),
- 3 FAA-iCMM, o Trusted CMM / Trusted Software Metodologia (T-CMM / TSM),
- Modelo de maturidade de capacidade de engenharia de segurança de sistemas (SSE-CMM)

SDLC Frameworks:

- Ciclo de Vida de Desenvolvimento de Software de Computação Confiável da Microsoft;
- Processo de Software de Equipe para Desenvolvimento Seguro de Software (TSPSM-Secure);
- Corrigibilidade por Construção;
- Métodos Ágeis;
- Common Criteria;
- SAMM (Software Assurance Maturity Model);
- SSF (Software Security Framework);



32



Conformidade: Desenvolvimento Seguro

Checklist Desenvolvimento Seguro de Software

PSBD 1, 2, 4, 5

1. Validação de entrada - 16
2. Codificação de saída - 6
3. Autenticação e Gerenciamento de Senhas - 34
4. Gerenciamento de Sessão - 18
5. Controle de Acesso - 23
6. Práticas Criptográficas - 6
7. Tratamento de erros e registro - 35
8. Segurança de Comunicação - 8
9. Configuração do Sistema - 15
10. Segurança do banco de dados - 13
11. Gerenciamento de arquivos - 14
12. Gerenciamento de Memória - 9
13. Práticas Gerais de Codificação -12

Total 214



Dev+OPS

X

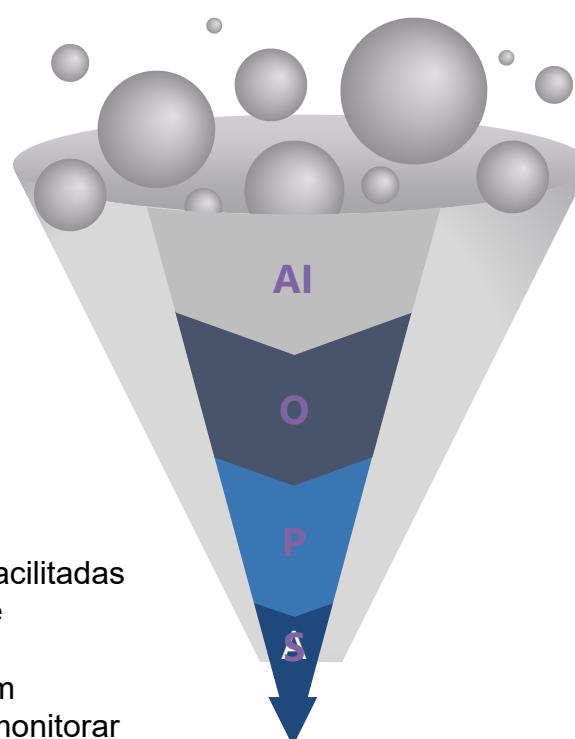
AI+OPS

Combinação de

- Filosofia Cultural, Práticas e Ferramentas
- Entrega de aplicações em serviços em alta velocidade
- Nada de silos, feedback rápido
- DevOps inclui pensamento de sistemas holísticos
- Automação de trabalho “penoso”, repetitivo

Habilidades:

- Metodologias de Desenvolvimento Ágil facilitadas por ciclos de liberação e implantação
- Operações colabora com Desenvolvimento para monitorar Operações de auto serviço



Promovendo

- Plataformas de Tecnologias multi camadas que automatizam e melhoram as Operações de TI
- Eliminação de erros humanos e economia de tempo
- Componentes chave incluindo big data e machine learning

Acções:

- Detecta automaticamente e reage a problemas em tempo real e de forma inteligente automatizando devops e cloudops
- incluiu a utilização de insumos de ferramentas de monitoramento existentes, aplicação de técnicas de algoritmos, análise e produção de uma saída que é um item de ação com insight para a equipe de operação

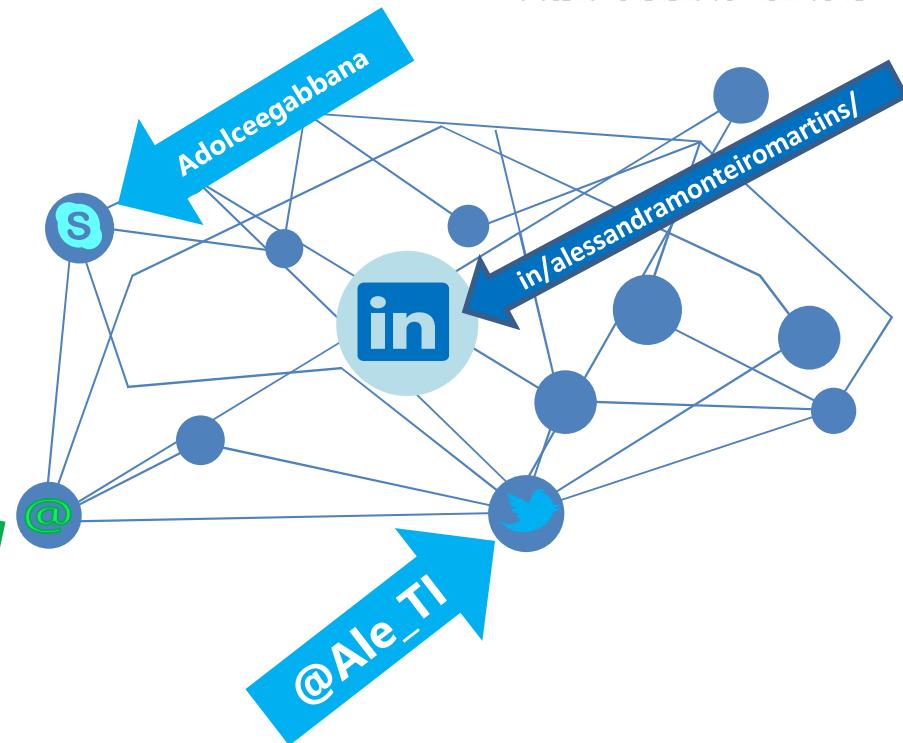
Referências:

- FILHO, Wilson de Pádua – “Engenharia de Software: Fundamentos Métodos e Padrões – LTC -3º Edição , 2009, Rio de Janeiro
- COSTA, I; NETO, M; COSTA NETO, P; JUNIOR, J. et al. Qualidade em Tecnologia da Informação. São Paulo: Editora Atlas, 2013.
- CORREIA, M. Segurança no Software. Lisboa: Editora, 2010.
- LYRA, M. et al. Segurança e Auditoria em Sistemas de Informação. Rio de Janeiro: Editora Ciência Moderna, 2008.
- MIGUEL, A. Gestão de Projectos de Software. Lisboa: Editora QFCA, 2010.rios, E;
- MOREIRA, T. et al. Teste de Software. Rio de Janeiro: Alta Books, 2013. C. 2010.
- SOLOMON, M.G; KIM, D. et at. Fundamentos de Segurança de Sistemas de Informação. Rio de Janeiro: Editora LTC, 2014.
- MORAIS, Gleicon - “CAIXA DE FERRAMENTAS DEVOPS – Casa do Código, 2017 São Paulo, SP.
- AGNER, Luiz. **Ergodesign e arquitetura de informação: trabalhando com o usuário.** Rio de Janeiro: Editora Quartet, 2º Edição, 2010
- Data Management Body of Knowledge (DAMA DMBoK®) – LLC Editora, 1º Edição, 2012. Data & Information – DAMA Brasil, 1º Edição, 2015.
- Guidelines and Strategies for Secure Interaction Design – Capítulo 13, KA-PING YEE
- OWASP – Code Review versão 2.0
- http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- <https://www.checkmarx.com/glossary/a-secure-sdlc-with-static-source-code-analysis-tools/>
- https://www.hack2secure.com/images/Pdf/Hack2Secure_Secure_SDLC_Services.pdf
- <https://www.eccouncil.org/programs/certified-application-security-engineer-case/>
- <https://www.us-cert.gov/bsi/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes>
- <https://br.pinterest.com/pin/797207571509409038/visual-search/?x=6&y=8&w=530&h=298>
- <https://twitter.com/dockercon/status/666188361>
- <https://slideplayer.com/slide/15950081/456091136>
- <https://mikecardus.com/leaders-responsibility/>
- <https://www.eenewsembedded.com/news/static-analysis-secure-software-development-lifecycle>
- https://www.owasp.org/index.php/OWASP_Testing_Guide_Appendix_C:_Fuzz_Vectors
- <https://www.owasp.org/images/1/19/OTGv4.pdf>
- <https://docs.zephyrproject.org/latest/security/security-overview.html>
- Exin White Paper





Cyber Security Girls





HACKERS TO HACKERS

C O N F E R E N C E