

IDEIAS DIFERENTES. CONEXÕES DE IMPACTO.

DIAS 05, 06, 07 E 08 / SETEMBRO

SANTA RITA DO SAPUCAÍ



HACK
TOWN 2019

SANTA RITA DO SAPUCAÍ - MG

https://docs.google.com/forms/d/e/1FAIpQLSeywqNZHYyQEblMcYSJ4_UWc5XOW1oUjxzH6e2M1OiTItD9Bw/viewform?usp=pp_url

<http://twixar.me/W6B1>

- PALESTRANTE

PAULA PAPIS

Mais de 20 anos de experiência na área de tecnologia, atuando em cargos de liderança na gestão de serviços em empresas no Brasil e exterior. Atualmente, Consultora autônoma de Segurança da Informação. Graduada em Comunicação pela PUC-SP, Mestrado em Ciências Política na PUC-SP e MBA em Gestão Estratégica de TI pelo IPT-USP. Fundadora da Comunidade CyberSecurityGirls BR, com o objetivo de trazer mais mulheres para a área de Segurança da Informação.

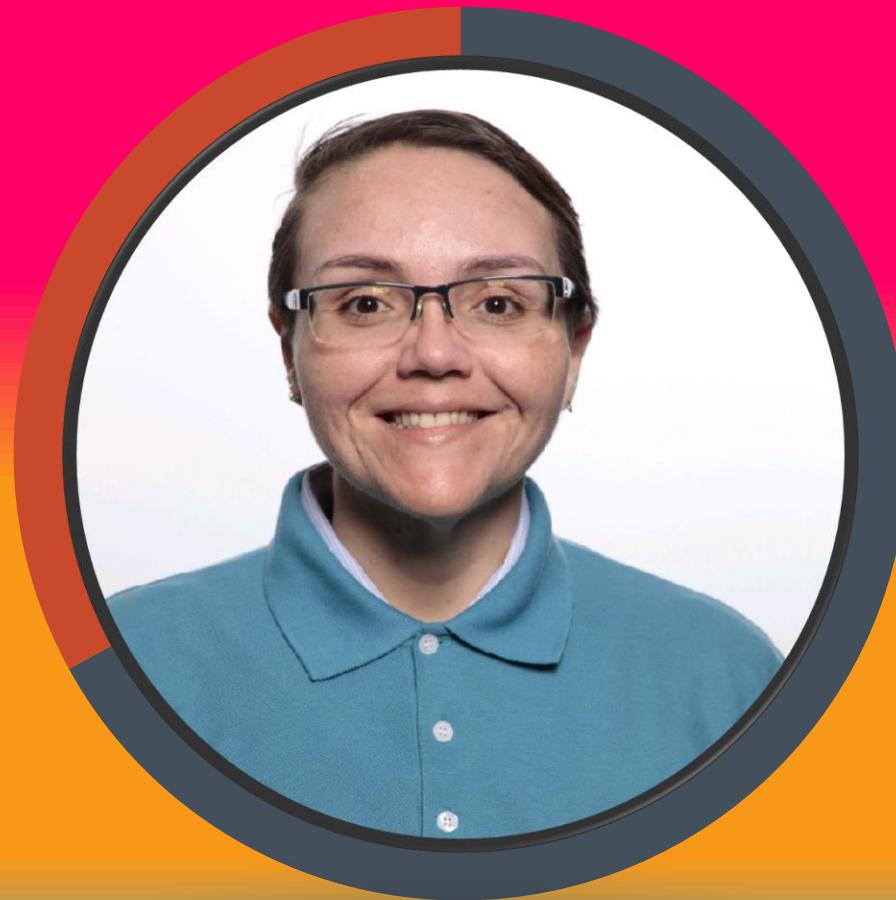


- PALESTRANTE

ALESSANDRA 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, e outras.

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

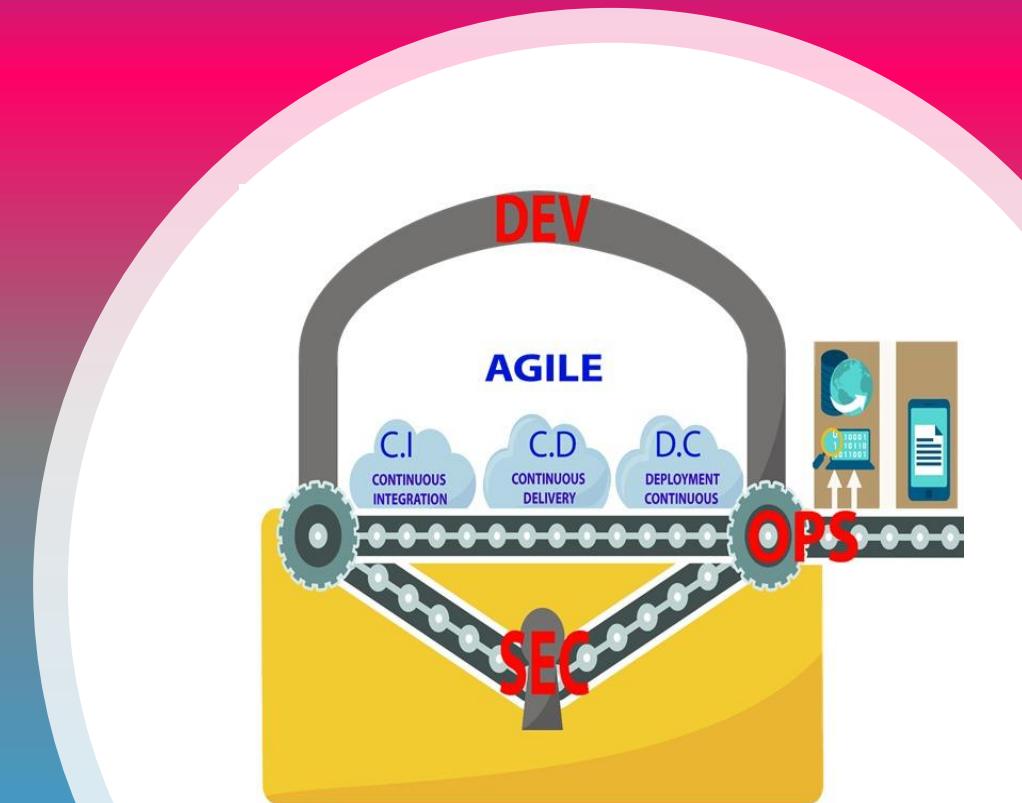




Cyber
Security
Girls

Jornada Security by Design

O QUE NÃO TE CONTARAM E VOCÊ PRECISA SABER
PARA ENTREGAR APLICAÇÕES COM INTEGRIDADE,
ALTA DISPONIBILIDADE E CONFIABILIDADE PARA SEUS
CLIENTES E USUÁRIOS



Roteiro

A Jornada



MITOS



CONCEITOS & PRINCÍPIOS



CONTEXTO



PAPÉIS & RESPONSABILIDADES



PROCESSOS



FERRAMENTAS

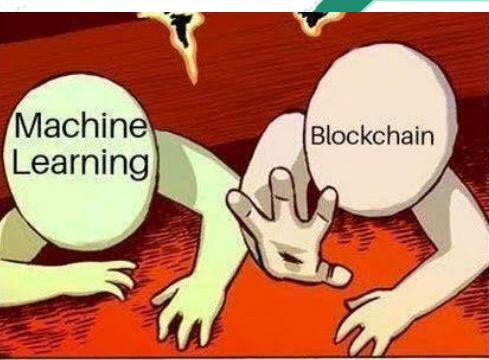


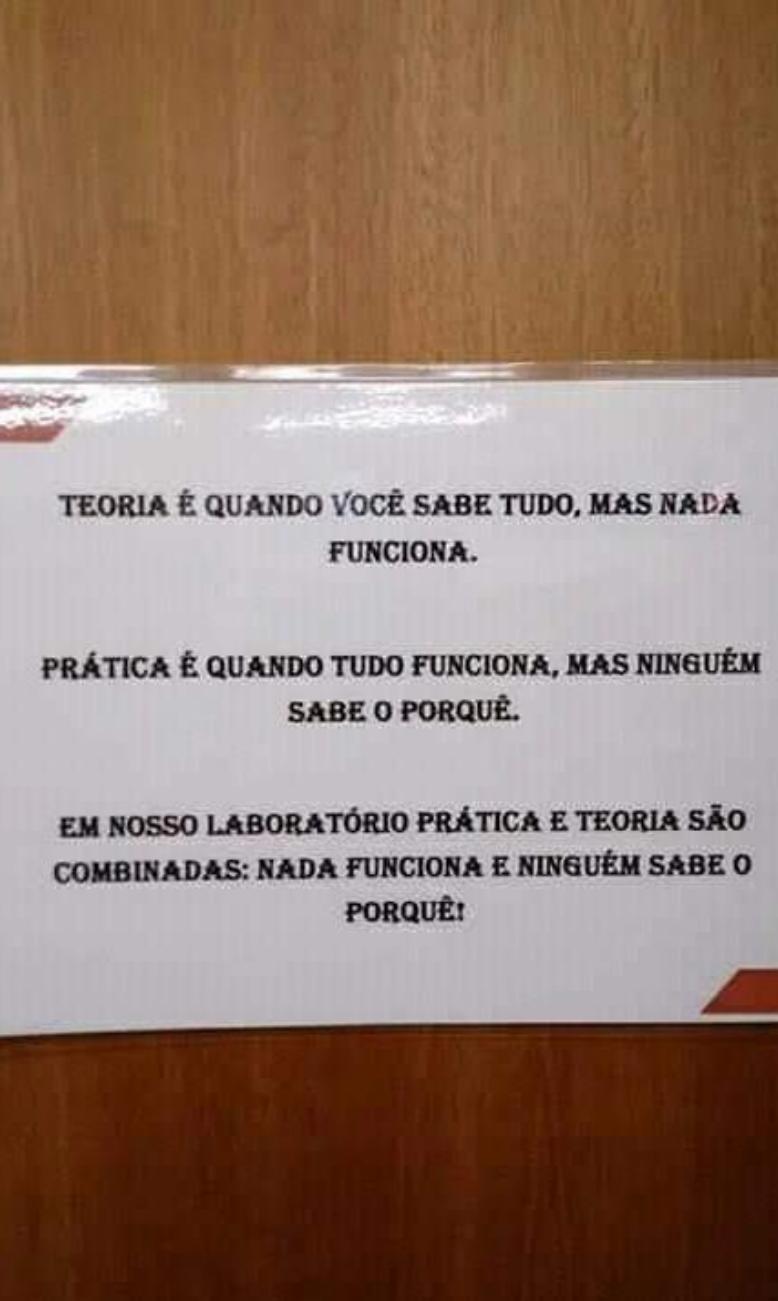
BOAS PRÁTICAS

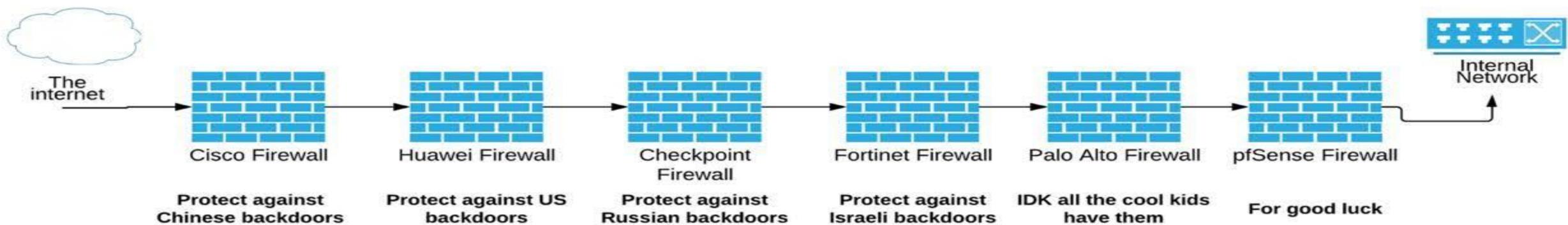
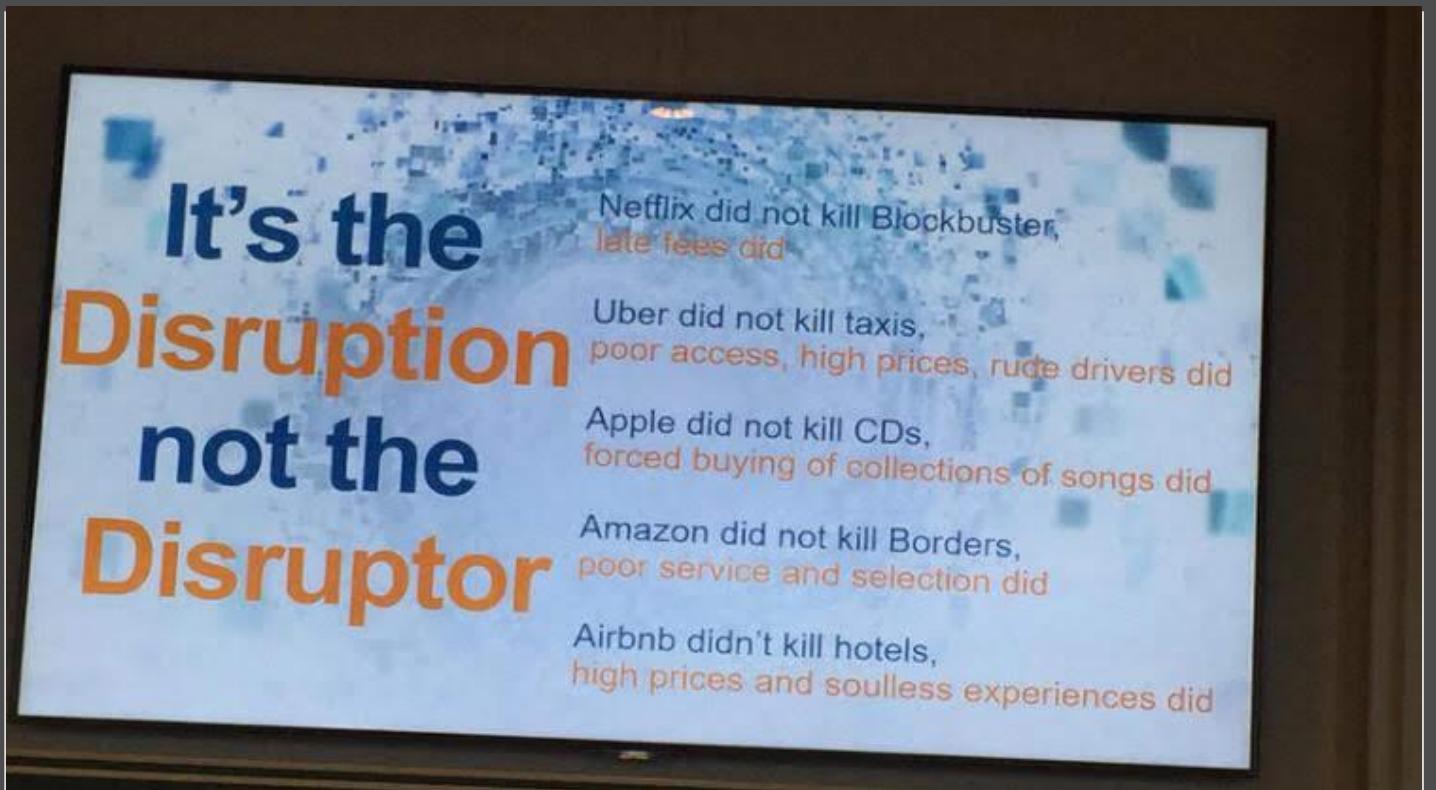


CILADAS

MITOS







CONCEITOS

ENVOLVIDOS

CLOUD

Cloud é um modelo computacional que permite acesso a recursos compartilhados e configuráveis de infraestrutura, plataforma e soluções de tecnologia (servidores, armazenamento, bancos de dados, rede, software, analytics, etc.) de forma flexível, on demand e escalável.

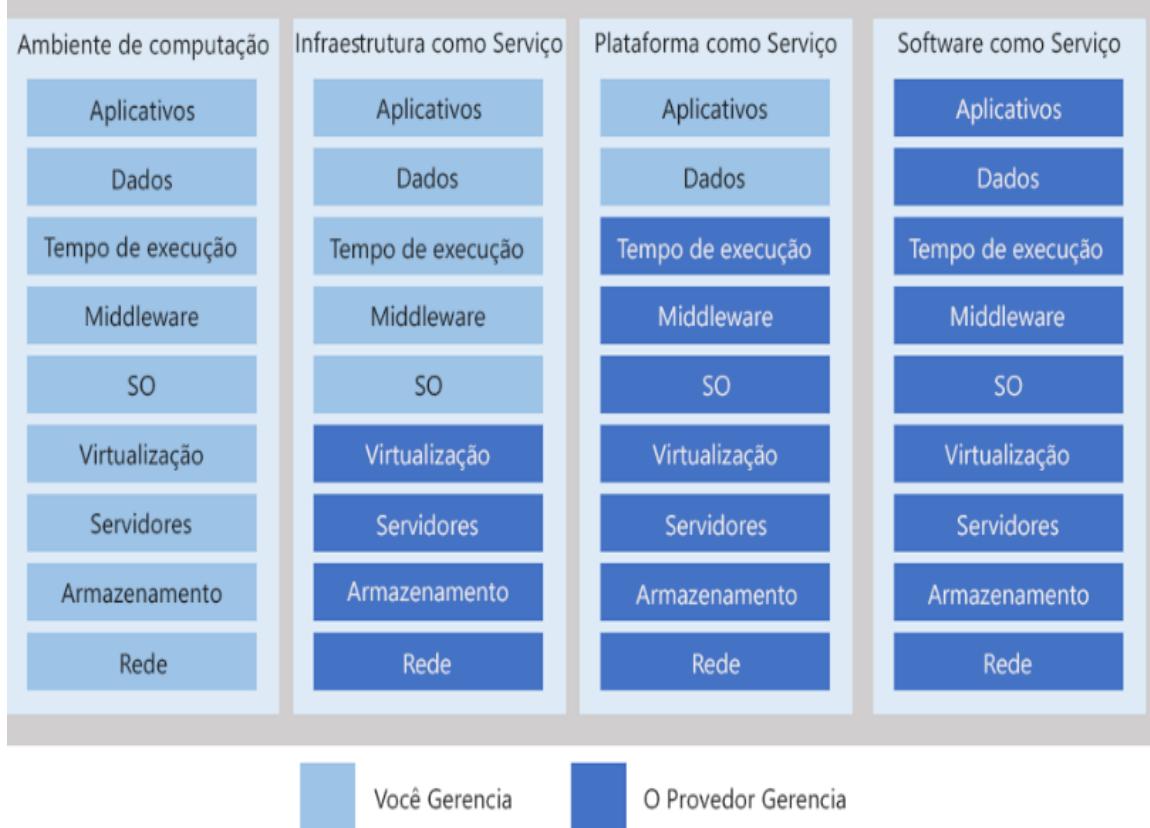


DEVSECOPS

DevSecOps é um termo criado para descrever um conjunto de práticas para integração entre os times de Desenvolvimento de Software, Segurança e Operações e a adoção de processos automatizados para produção rápida e segura de aplicações e serviços.

IaaS

INFRAESTRUTURA COMO SERVIÇO



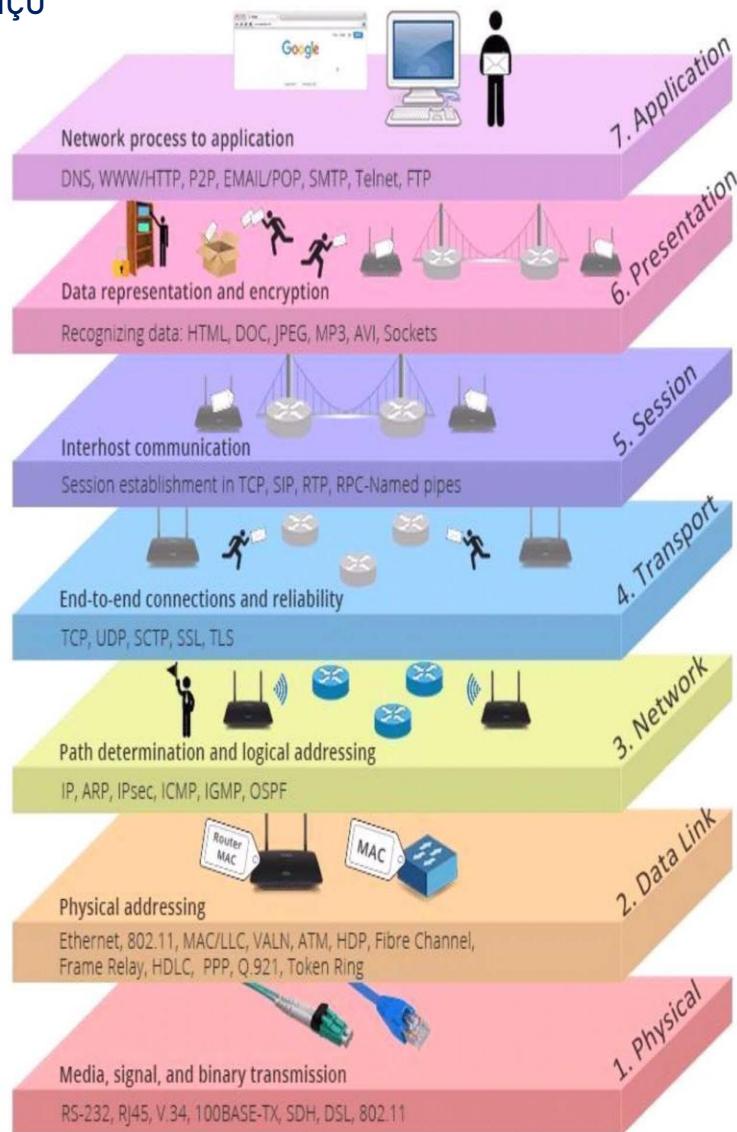
PaaS

PLATAFORMA COMO SERVIÇO



SaaS

SOFTWARE COMO SERVIÇO



ARQUITETURAS



NEGÓCIOS

Estrutura e comportamento de um sistema de negócios (não necessariamente relacionado a computadores). Abrange objetivos de negócios, funções ou recursos de negócios, funções e processos de negócios, etc. As funções de negócios e os processos de negócios geralmente são mapeados para os aplicativos e dados de que precisam.

As estruturas de dados usadas por uma empresa e / ou seus aplicativos. Descrições de dados no armazenamento e dados em movimento. Descrições de armazenamentos de dados, grupos de dados e itens de dados. Mapeamentos desses artefatos de dados para qualidades de dados, aplicativos, locais etc.

DADOS



Estrutura e comportamento de aplicativos usados em um negócio, focados em como eles interagem entre si e com os usuários. Focado nos dados consumidos e produzidos por aplicativos e não em sua estrutura interna. No gerenciamento de portfólio de aplicativos, os aplicativos geralmente são mapeados para funções de negócios e para tecnologias de plataforma de aplicativos.

TECNOLÓGICA

Estrutura e comportamento da infraestrutura de TI. Abrange os nós de cliente e servidor da configuração de hardware, os aplicativos de infraestrutura que são executados neles, os serviços de infraestrutura que eles oferecem aos aplicativos, os protocolos e as redes que conectam aplicativos e nós.

APLICAÇÕES



Arquitetura x Engenharia:

SOFTWARE

PREOCUPA-SE

COM A DEFINIÇÃO DOS COMPONENTES DE SOFTWARE, SUAS PROPRIEDADES EXTERNAS, E SEUS RELACIONAMENTOS COM OUTROS SOFTWARES. SE REFERE TAMBÉM À DOCUMENTAÇÃO DA ARQUITETURA DE SOFTWARE DO SISTEMA, QUE FACILITA: A COMUNICAÇÃO ENTRE OS STAKEHOLDERS, REGISTRA AS DECISÕES INICIAIS ACERCA DO PROJETO DE ALTO NÍVEL, E PERMITE O REUSO DO PROJETO DOS COMPONENTES E PADRÕES ENTRE PROJETOS.

ENVOLVE-SE

COM AS TECNOLOGIAS E A MODELAGEM DO SOFTWARE. O ARQUITETO AJUDAR A EVITAR O DÉBITO TÉCNICO, AS QUEDAS DE PERFORMANCE, FALTA DE ESCALABILIDADE, QUE PODE SER CAUSADO PELOS DESENVOLVEDORES. ARQUITETOS TEM UM BOM CONHECIMENTO DE SOLUÇÕES EM ALTO NÍVEL, CONHECEM DESIGN PATTERNS, CONCEITOS COMO SOLID, DRY, YAGNI E TENTAM APLICÁ-LOS ONDE FOR CABÍVEL E POSSÍVEL.

PREOCUPA-SE

COM A ESPECIFICAÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE SOFTWARE, COM APLICAÇÃO DE TECNOLOGIAS E PRÁTICAS DE GERÊNCIA DE PROJETOS E OUTRAS DISCIPLINAS, VISANDO ORGANIZAÇÃO, PRODUTIVIDADE E QUALIDADE

ENVOLVE-SE

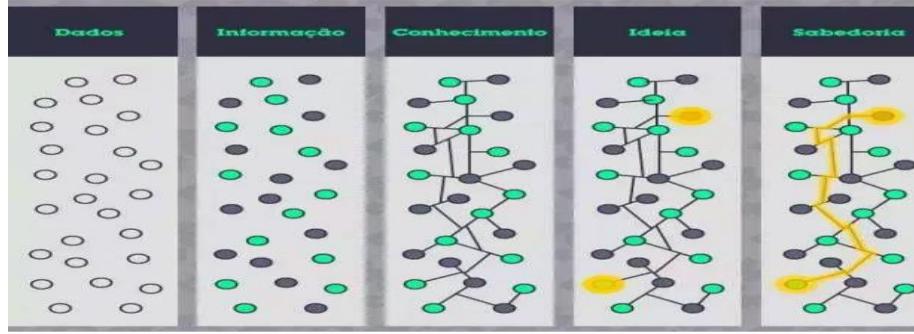
COM AS TÉCNICAS DE DESENVOLVIMENTO ÁGIL, LIDERANÇA DE EQUIPES. A FUNÇÃO DE UM ENGENHEIRO DE SOFTWARE É MANTER A EQUIPE, COM SEU MELHOR ÍNDICE DE PRODUÇÃO POSSÍVEL, SANANDO PROBLEMAS DO PROCESSO DE DESENVOLVIMENTO DE SOFTWARE.



ARQUITETURAS

ARQUITETURA DEVOPS ENGLOBA GANHOS DE PRODUTIVIDADE ATRAVÉS DO APRIMORAMENTO E AUTOMAÇÃO DE FLUXOS (WORKFLOWS) DE TRABALHO, POR MEIO DE TÉCNICAS PRÁTICAS COMO CONTINUOUS INTEGRATION E CONTINUOUS DELIVERY, O MONITORAMENTO SE TORNA UM FATOR MUITO MAIS IMPORTANTE DO QUE ARQUITETURA E DESIGN.



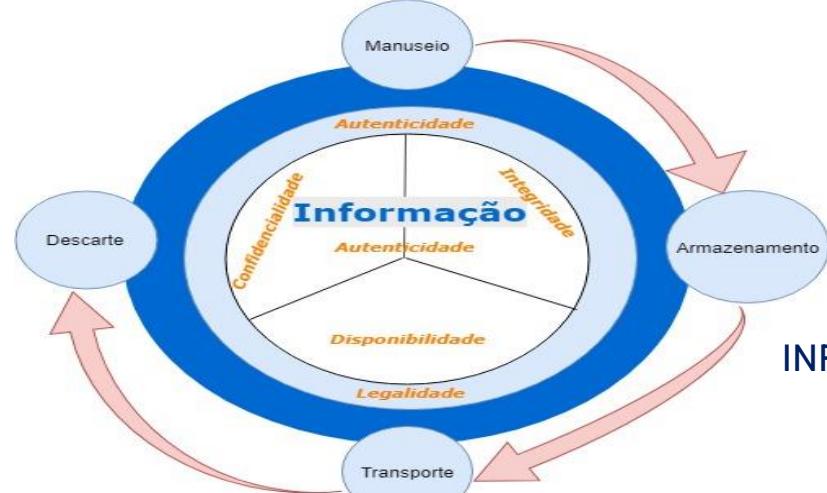


DADO



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.

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. SÃO DADOS DOTADOS DE RELEVÂNCIA E PROPÓSITO. EXIGE CONSENSO EM RELAÇÃO AO SIGNIFICADO, EXIGE NECESSARIAMENTE A MEDIAÇÃO HUMANA.



INFORMAÇÃO

DADO



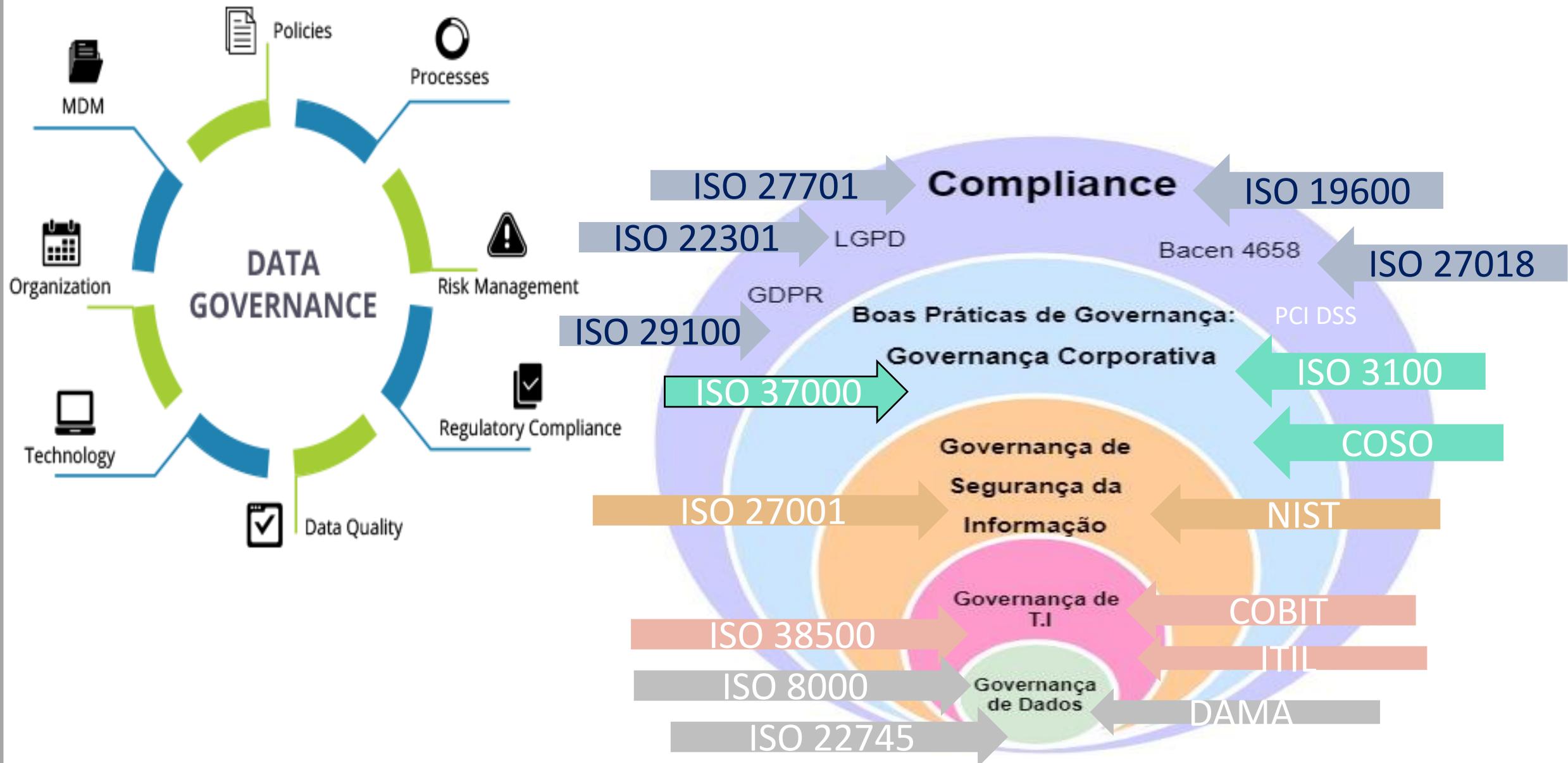
CICLOS DE VIDA



Ciclo de Vida do Dado



Governanças: Corporativa, SI, TI e Dados





Princípios: LGPD & GDPR

Finalidade da Coleta e Tratamento das Informações

Adequação

Necessidade

Livre Acesso

Qualidade dos Dados

Transparência

Segurança

Prevenção

Não Discriminação

Responsabilização

Prestação de Contas

1 Data Protection by Design

2 Privacy by Design

3 Data Protection by Default

4 Privacy First

5 Privacy Awareness

6 Security Obligations



PRINCÍPIOS PRIVACY BY DESIGN & DEFAULT

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.



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.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.



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.

Contexto: A Lei 13.709

Art.3

Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- I A operação de tratamento seja realizada no território nacional;
- II A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Medida Provisória nº 869, de 2018)
- III Os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

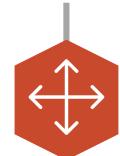


§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

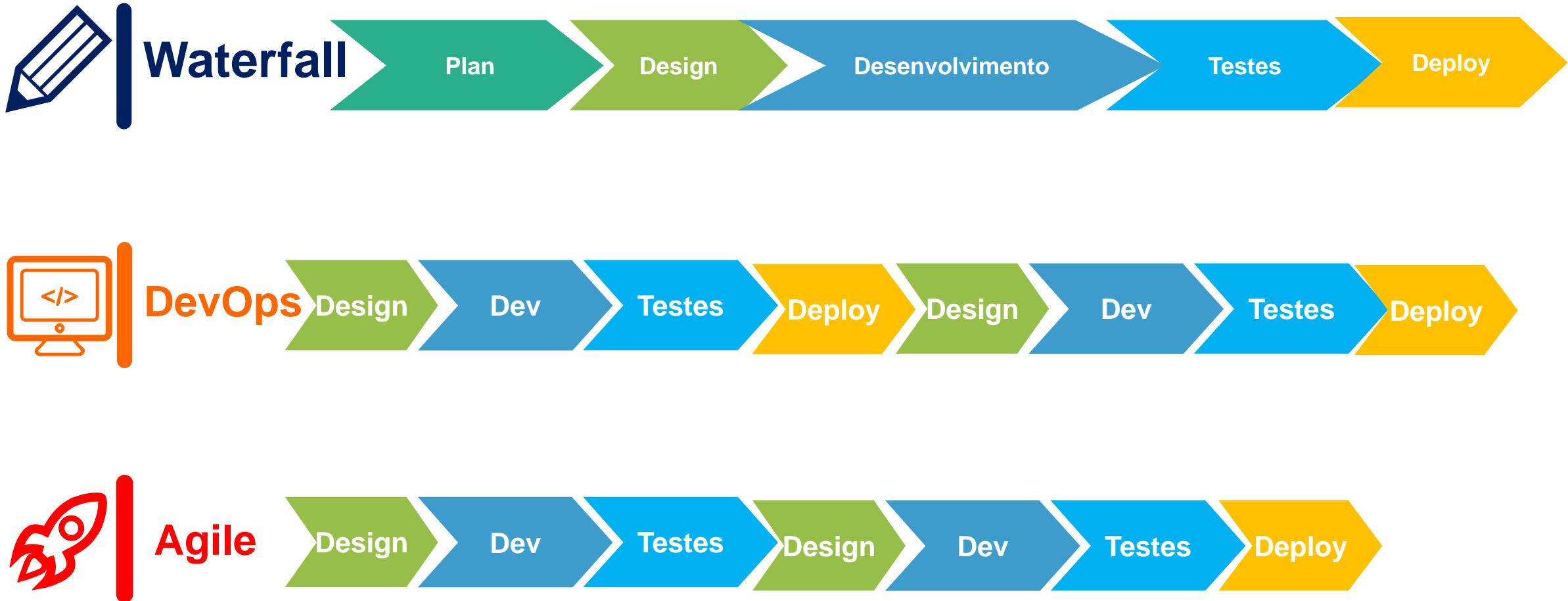
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

CONTEXTO OBJETOS E ESCOPO LGPD

Dados Pessoais	Dados Pessoais Sensíveis	Dados Anonimizados	Decisões Automatizadas
<ul style="list-style-type: none">• CPF• RG• IP• Cookies• Geolocalização• Nome• Endereço	<ul style="list-style-type: none">• Biometria• Saúde• Dados referente a orientação ou vida Sexual• Filiação Partidária, Filosófica, Sociológica	<ul style="list-style-type: none">• Não identificável• Pseudonimizados• Reversível• Tecnologia e Meios Técnicos Razoáveis	<ul style="list-style-type: none">• Profiling• Análise Consequencialista

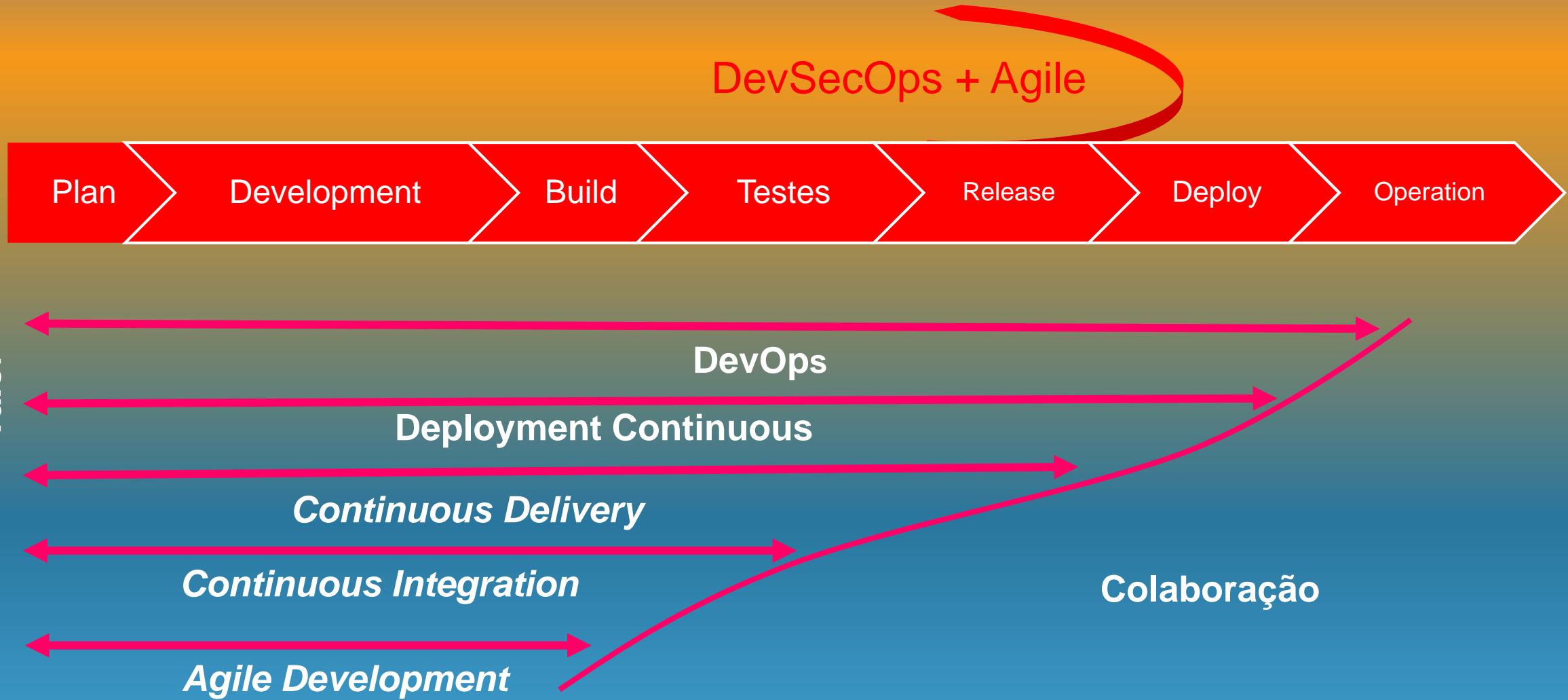


Contexto: DevOps Versus Outros Modelos





Contexto: Diferença Entre DevOps X CI X CD X DC



Papéis e Responsabilidades pela Lei



- Pessoa Natural - Titular dos Dados, pessoa física particular, pessoa natural;



- Órgão de pesquisa - órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;



- Agentes de Tratamento - refere-se ao conjunto do Controlador e Operador juntos;



- Autoridade Nacional de Proteção de Dados (ANPD) - órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei;



- Controlador - Responsável pelas operações de tratamento dos dados pessoais, pessoa física ou jurídica de caráter público ou privado;



- Encarregado - Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

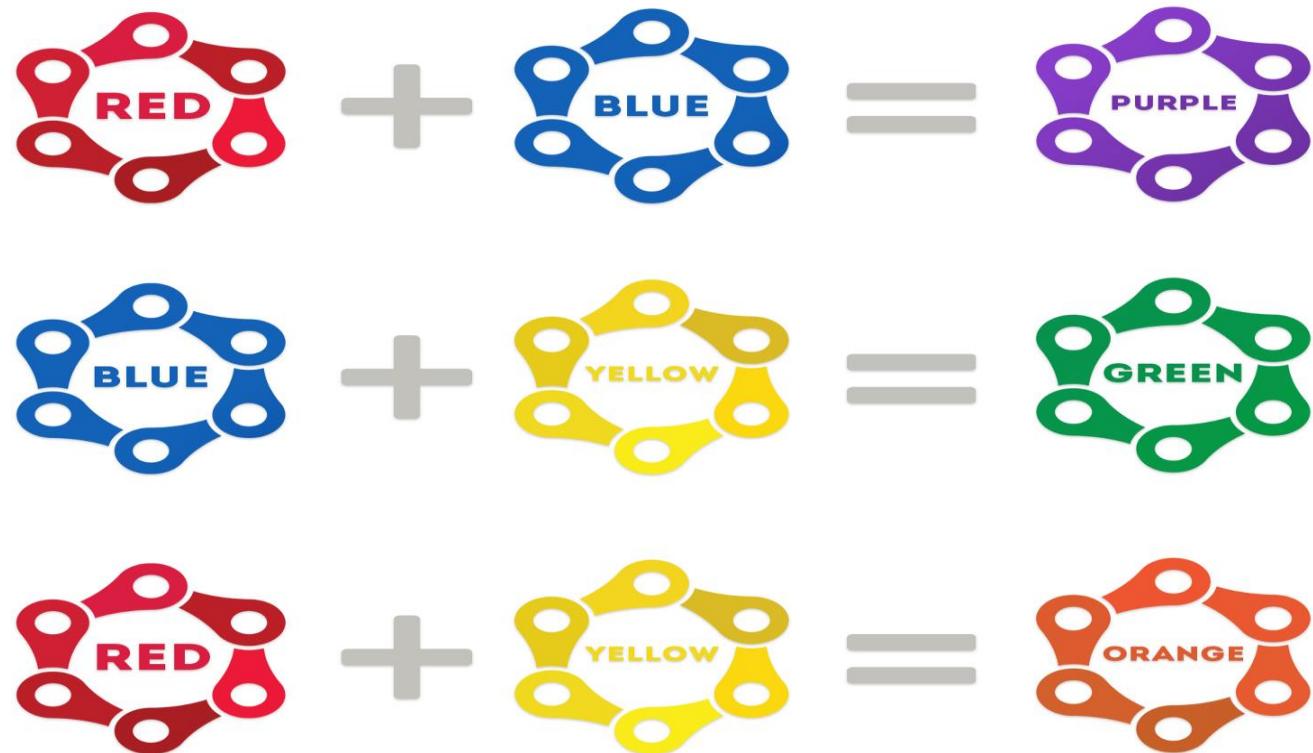


- Operador - Quem executa o tratamento em nome do Controlador, pessoa física ou jurídica de caráter público ou privado;

Papéis: Responsabilidades dos Agentes de Tratamento



Papéis: uma visão de Pessoas + Habilidades + Processos

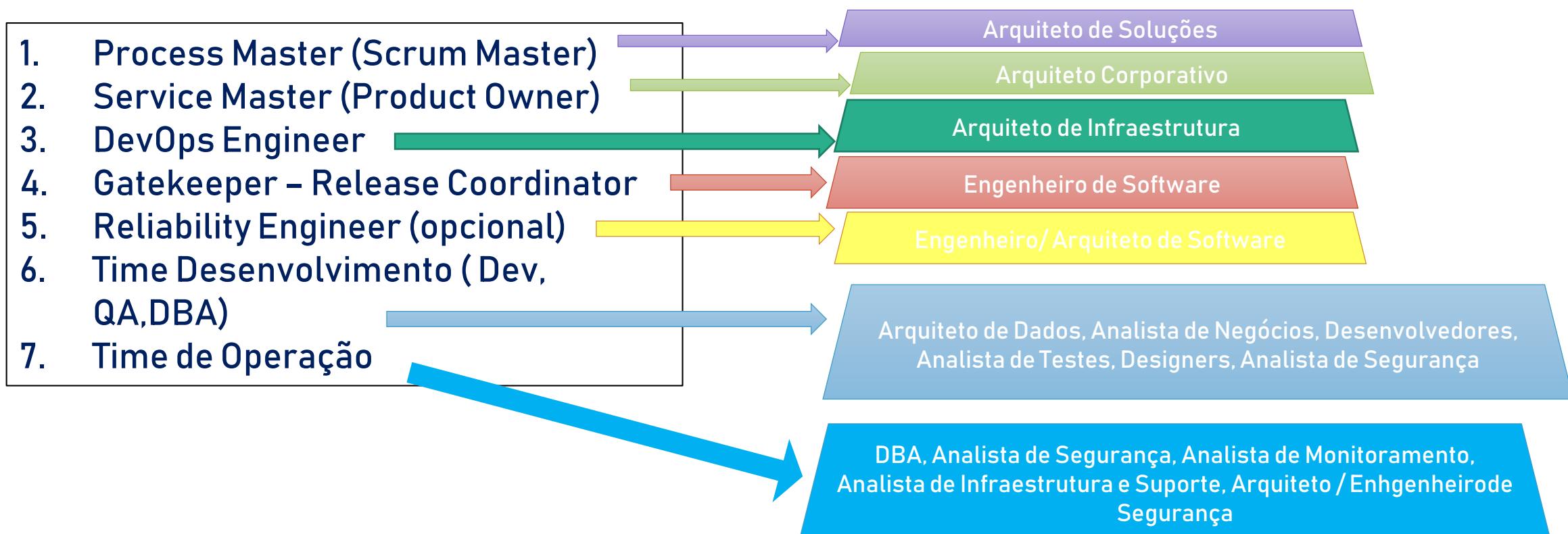


Papéis e Responsabilidades: uma visão de Times



Papéis e Responsabilidades: Sugestão de Composição de Papéis para Implantação DevSecOps

Papéis:



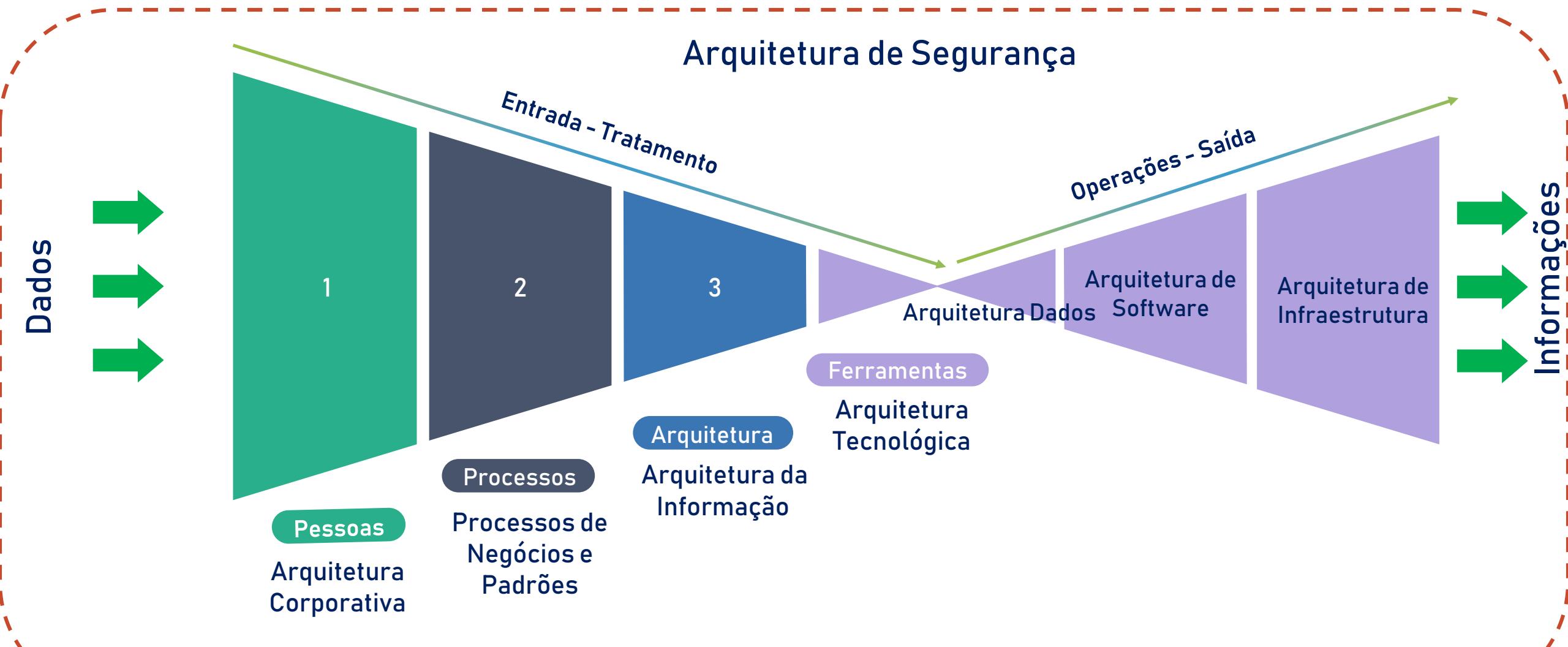
Papéis e Responsabilidades: Importância da Adoção de uma Cultura Segurança e Privacidade

Pontos Chaves para uma Implantação de Sucesso

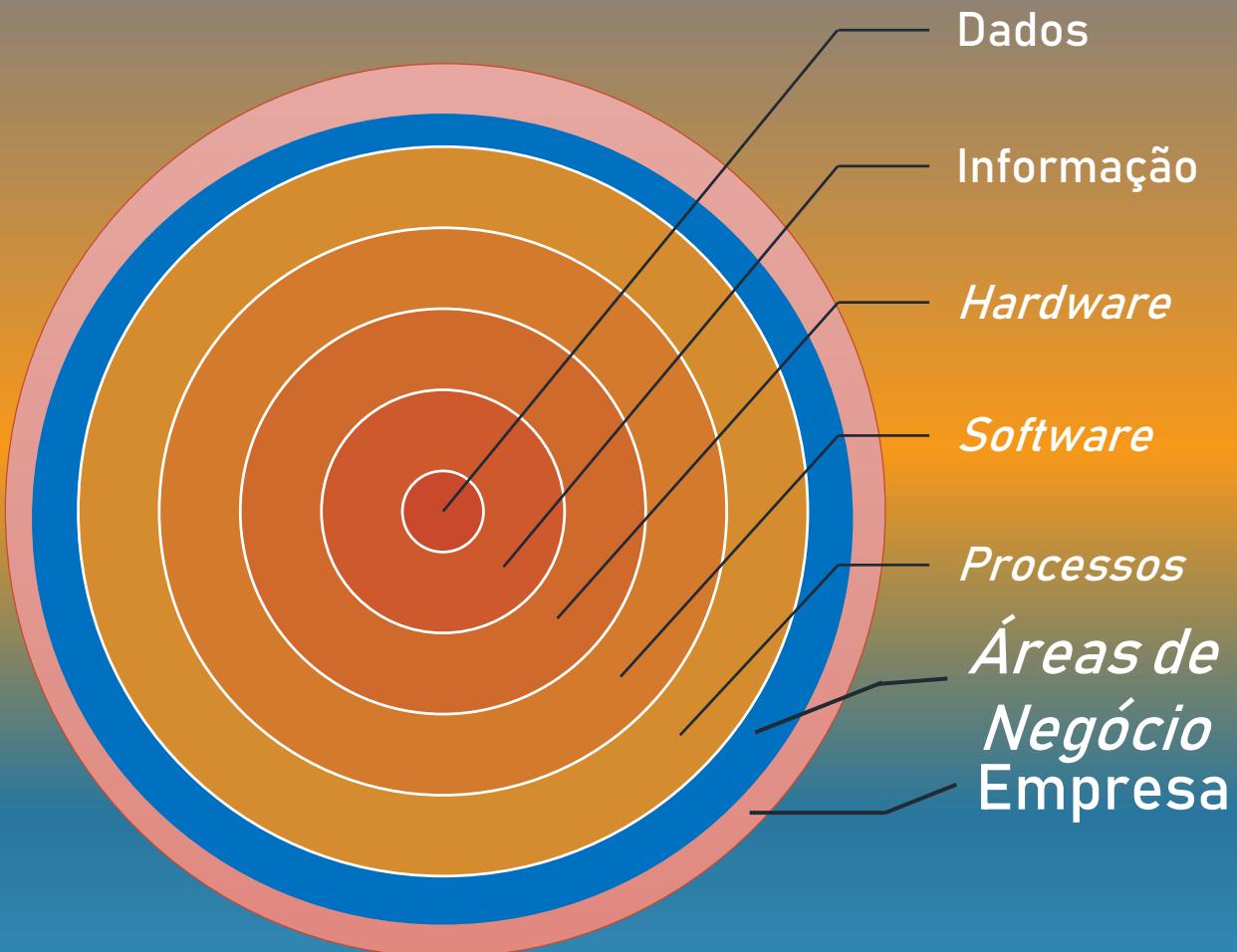
- 1 | Mentalidade e Valores**
- 2 | Princípios e Padrões**
- 3 | Processos e Práticas**
- 4 | Ferramentas**



Processos : Security by Design – Data Protection by Design

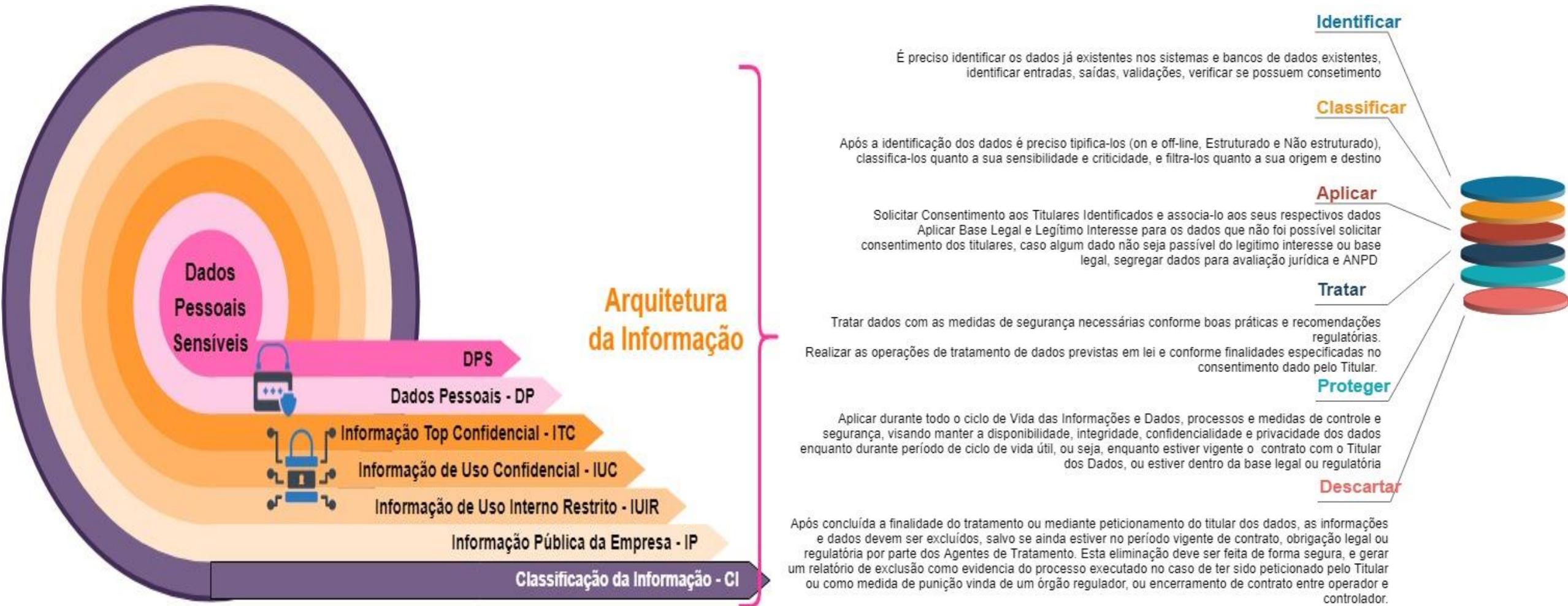


Processos: Por onde começar a organizar



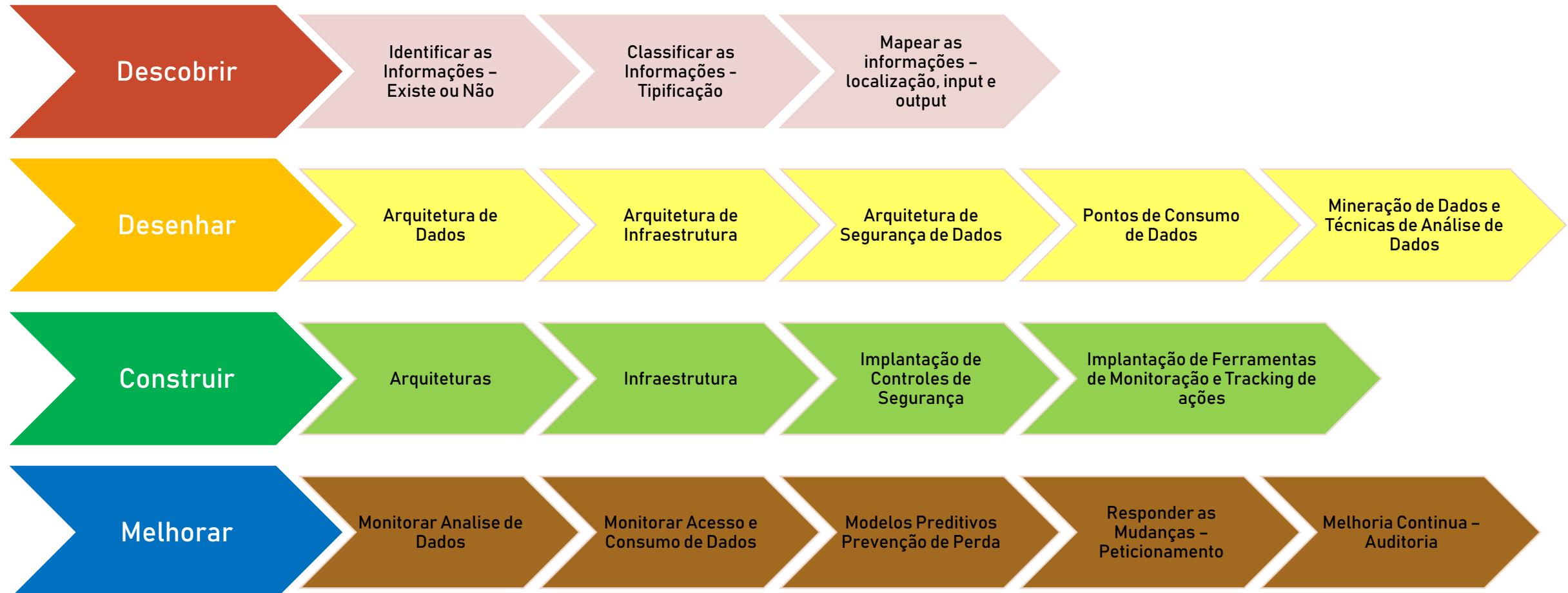
1 – Data Protection by Design

Processos: começando pela Arquitetura



Data Protection by Default

Processos: definição de fases para adequação



Privacy by Design

Processo: Etapas End to End



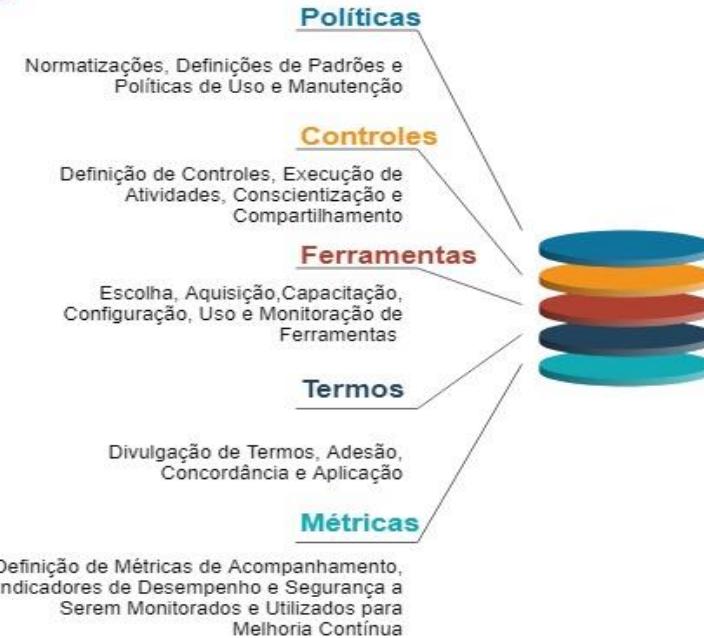
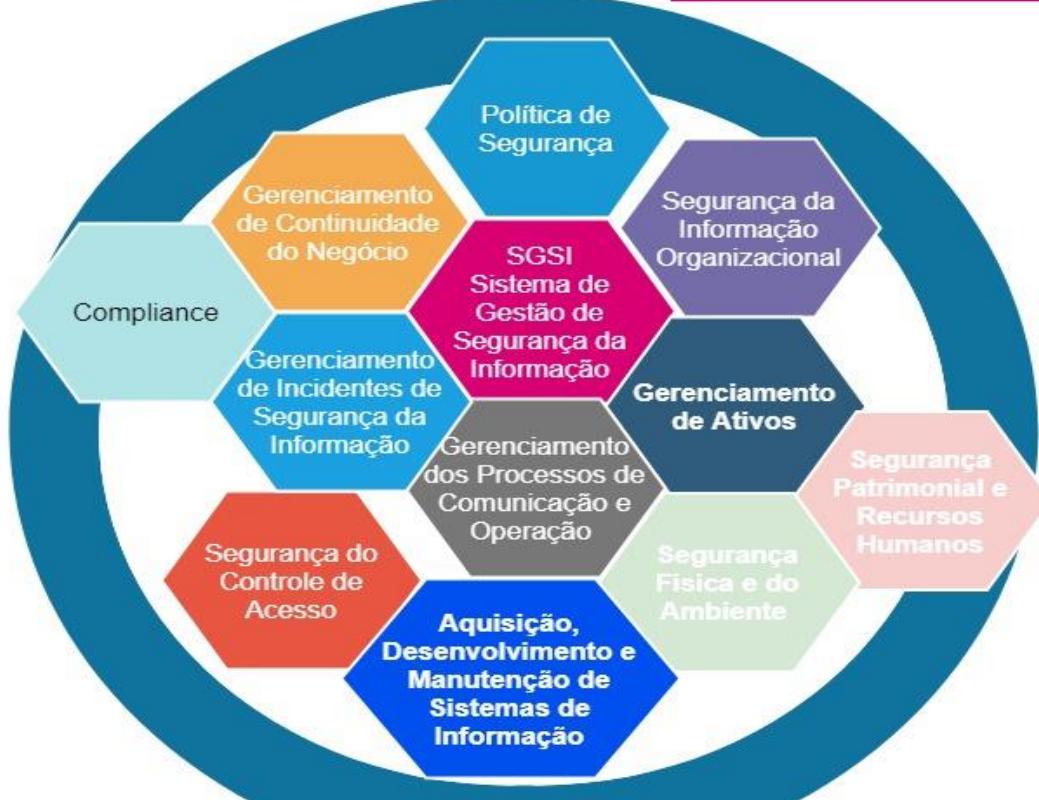
Processos: sugestão de métricas para dados

COMPLETUEDE	Existe algum valor de dado faltando ou em um estado inutilizável?
CONFORMIDADE	Todas as expectativas de volume de dados estão conforme as especificações? Todos os valores estão no formato especificado?
CONSISTÊNCIA	Existem instâncias de dados provendo informações conflitantes sobre o mesmo objeto de dado? Existe valor consistente de dados através dos ativos?
ACURACIDADE	Os dados representam com precisão valores do mundo real conforme o modelo especificado?
DUPLICAÇÃO	Existem múltiplas representações desnecessárias do mesmo dado em diferentes ativos de dados?
INTEGRAÇÃO	Falta alguma relação ou conexão entre dados importantes?

PRIVACY FIRST

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Processos



PRIVACY AWARENESS

Processos: Overview Macro



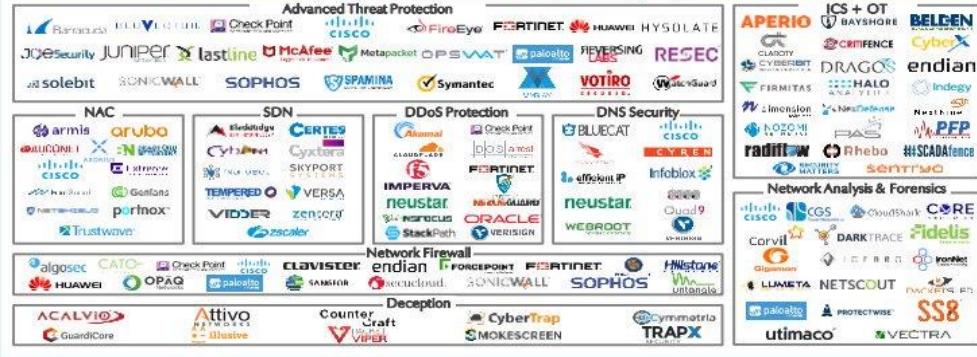
SECURITY OBLIGATIONS- SECURITY BY DEFAULT

Ferramentas:

C Y B E R *scape*

v2.5

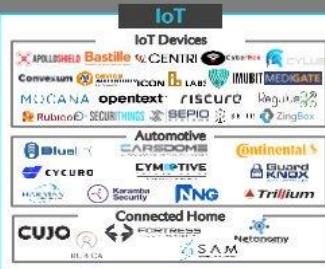
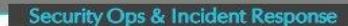
Network & Infrastructure Security



MSSP



Risk & Compliance



Identity & Access Management



IaaS
Iantus  welcome



Ferramentas:

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 Biometrics	Fc Facial Recognition	Rf RFID	Ha Home Automation	In Integration	Cn Connectors	Ca Cases/Safety Containers	Cc Command and Control	Ci CI	Tr Intelligent Transport	Cv Cash & Valuables in Transit	P Personnel	Tc OOLTV Poles, Towers & Columns	IP IP Cameras	Rs Remote Surveillance	Ti Thermal Imaging		
Cr Card Readers	Fg Fencing / Turnstiles	St Smartcards	Ia Intruder Alarms	IoT Internet of Things	Eq Equipment-Installation/Test	Gs Grills & Shutters	Sm Screens & Monitors	Cs Company Security	It IT Management/Cloud Services	Ct Court Surveillance	Pv Public Space Surveillance	Cd Codecs	Ls Lenses	Sv Servers	Ts Transmission		
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 Crisis Management	Ns National Security	Es Event Security	Cg Uniform/Clothing/Equipment	Cp Control Panels	Sn Monitors & Screens	Su Surveillance	Va Video Analytics		
Ha Home Automation	Vi Visitor 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	Gt Guard Tour Services/Systems	Vh Vehicle Immobilisers/Tracking	Dg Digital Recording Transmission	Ml Multiplexers					
Ic IP Access Control	Vp VOIP	Ds Data Storage Solutions	Va Video Analytics	Au Armouries	Sl Sales / Locks	Ir Intra-Red Perimeter Protection	Cy Cyber Resilience	Sm Social Media Intelligence	Kh Key Holder Management & Services	Ar ANPR	Dv Digital Video Storage	Nvr NVRs					
Id ID Cards	Aw Alarm Warnings	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	Lw Lone Worker Protection	Ch Camera Housings	Dc Dome Cameras	Ptz PTZ Cameras					
Lk Locking	Fl False Alarm Prevention	Fo Fibre Optics	Cw Cablewise Detection/Protection	Bb Barriers & Bollards	Ss Security Seals	Bd Big Data and Analytics	Er Emergency Response	Ap Aviation/Port Security	M Monitoring	C Cameras	Dvr DVRs						
Fa Fire Alarms	Dt Fire Detectors	Rc Alarm Receiving Centres	Gh Gas/Hear Detectors	Fe Fire Extinguishers	Do Fire Doors	Sg Fire Signalling	Sd Smoke Detectors	Ppe Personal Protective Equipment	Dm Decontamination	Gd Gas Detection	Sc Spill Containment	W Working At Height	Am Air Monitoring	Es Emergency Rescue	Sf Site Safety	Osh Occupational Health and Safety	Sch Scheduling

Ferramentas:

The Periodic Table Of Cybersecurity

An overview of key companies and investors in cybersecurity (as of 3/23/2017)

Id IDQuantique	Ph PhishMe
Po Post-Quantum	Kn KnowBe4
Qu QuintessenceLabs	Ad Agari Data
Wi Wickr	Vo Votiro
Vi Virtru	Gr GreatHorn
Em EmailAge	Wst Wombat Security Technologies
Is Ionic Security	Gi GigaTrust

Symbol --> **Ta**
Name --> **Tanium**

Secure Communications	Autonomous Systems	Cyber Insurance	Anti-Fraud Security
Predictive Intelligence	IoT/ IIoT Security	Identity & Access Mgmt.	Most Active VC Investors
Deception Security	Mobile Security	Network & Endpoint Security	Top Exits Since 2012
Set SentinelOne	Da Darktrace	Cye CyActive	Br Bromium
Cyr Cymmetria	Ex Exabeam	Seb SecBI	Bi BIOWATCH
Nn Nozomi Networks	Tril Trillium	Pe Pwnie Express	Sc Silent Circle
Pap Payfone	App AppDome	Atk AttackIQ	SS Security Scorecard
4I 4IQ	Cle Cylance	Pa PatternEx	Tr TrapX
Ts TopSpin Security	Pr Protectwise	Jn Javelin Networks	Ri Rubicon Labs
Ind Indegy	Mo Mocana	Lo Lookout	Zi Zimperium
Mo Mocana	Trs Trustlook	Sl Sirin Labs	Ce Cydence
Trs Trustlook	Bd Bay Dynamics	Ce Cydence	Bd Bay Dynamics
An Anomali	Ar ArmorWay	Al AlienVault	In illusive networks
Cyb Cyberfog	Sif Sift Science	Ssx Skybox Security	Au Auth0
Acs Argus Cyber Security	Bn Bastille Networks	Op OpenPeak	Hy Hypori
Bn Bastille Networks	As Avast Software	Rn RedSeal Networks	Bt BitSight Technologies
Op OpenPeak	Hy Hypori	Rn RedSeal Networks	Ks Kenna Security
En Endgame	Pht Phantom	Si Sixgill	CyX CyberX
Ks Karamba Security	Bnk Bayshore Networks	Ap Appthority	Apk Appknox
Bnk Bayshore Networks	Mm Mobi Magic	Mm Mobi Magic	Sa SafeBreach
Ap Appthority	Pn Prevalent Networks	Pn Prevalent Networks	Co Corax
En Endgame	Sk Skycure	Cybr Cyberreason	At Acclvio Technologies
Pht Phantom	Si Sixgill	CyX CyberX	At Acclvio Technologies
Ks Karamba Security	Bn Barracuda Networks	Bn Barracuda Networks	Trst Trusteer
Bn Barracuda Networks	Trst Trusteer	Atg AVG Technologies	Kd Krux Digital
Trst Trusteer	Atg AVG Technologies	Kd Krux Digital	Moi MobileIron
Atg AVG Technologies	Ops OpenDNS	Moi MobileIron	Ops OpenDNS

On OneLogin	Tse Thycotic Software	Ta Tanium	Bii Bitdefender	Zs Zscaler	Sty Shift Technology
Cy Centrify	Nnl Nok Nok Labs	Lor LogRhythm	Cs Code42 Software	Th ThreatMetrix	Ga Guardian Analytics
Be BeyondTrust	Tra Trusona	Cr CrowdStrike	Sn SnoopWall	Dn Distil Networks	Fot Forter
Seu SecureAuth	Iw iWelcome	Dg Digital Guardian	St StackPath	Ko Kount	Ze ZeroFOX
So Socure	Ve Veridu	Av Avecto	Loo LogicMonitor	Ju Jumio	Ri Rippleshot
Trll Trulioo	Moq MoQom	Coa CounterTack	Cl Cloudflare	Fe Feedzai	Ra Ravelin
Tn Tempered Networks	Sy Simplified	Cb Carbon Black	Il Illumio	Wo White Ops	Sii Simility

Nea New Enterprise Associates	Bvp Bessemer Venture Partners	Ic Intel Capital	Apa Accel Partners	Ah Andreessen Horowitz	Lvp Lightspeed Venture Partners	Kpc Kleiner Perkins Caufield & Byers	Nvp Norwest Venture Partners	Gv Google Ventures	Sca Sequoia Capital
Pan Palo Alto Networks	Fi FireEye	Ai AirWatch	Ma MANDIANT	Bn Barracuda Networks	Trst Trusteer	Atg AVG Technologies	Kd Krux Digital	Moi MobileIron	Ops OpenDNS

 CB INSIGHTS

Ferramentas:

The Periodic Table of Data Privacy

An overview of the key elements of data privacy

1 E Ethics		Fundamental principles of data protection												Core legislation		Independent bodies												Traits and skills of the most reliable privacy advisors												Legislation and practices whose powers and requirements can conflict with data privacy		2 EDPB European Data Protection Board																													
3 Ac Access	4 Co Contract	5 Ri Right to be Informed		6 Lo Legal obligation		7 Rf Right to be forgotten		8 Vi Vital interests		9 Pb Public Interest		10 Rp Restriction of processing		11 Wt Withdraw consent		12 Ob Objection		13 DSe Data sharing (external)		14 DSi Data Sharing (internal)		15 Eu End users		16 Em Employees		17 Cu Customers		18 Su Suppliers		19 Mb Marketing databases		20 Pa Partners		21 Hc Hardcopies		22 Ct Controller		23 Pro Processor		24 Go Governance		25 Tr Training		26 Is Information security		27 Ps Physical security		28 TOMs technical and organizational measures		29 Pg Processing records		30 Bn Breach notifications		31 DPA Data Protection Act (UK)		32 ClIs data protection laws (Ireland & Germany)		33 FDPA Federal data protection act (USA)		34 Re Relevance		35 Ty Transparency		36 ISO International organization for standardization		37 EDPB European Data Protection Board		38 Local legislators		39 Local regulators	
11 Ri Right to be informed	12 Lo Legal obligation	13 ePD ePrivacy Directive (EU)	14 NIL Law from EU/EEA member states (joining/leaving)	15 C Confidentiality	16 I Integrity	17 A Availability	18 Lr Local regulators	19 GDPR General Data Protection Regulation (EU)	20 L Lawfulness	21 Fa Fairness	22 N Necessary	23 Ay Accuracy	24 LI Local legislators	25 D Duration	26 ISAE International Standard on Auditing Engagements	27 D Duration	28 IP Information Privacy	29 GDPL General data protection law (Germany)	30 PDPL Personal data protection law (Singapore)	31 PPL Protection of privacy law (Israel)	32 PDPA Personal data protection act (Singapore)	33 D Duration	34 ISAE International Standard on Auditing Engagements	35 D Duration	36 IP Information Privacy	37 GDPL General data protection law (Germany)	38 PDPL Personal data protection law (Singapore)	39 ISAE International Standard on Auditing Engagements	40 In Independent	41 Au Authoritative	42 Ct Consultative	43 Re Reliable	44 H Honest	45 Cs Consistent	46 Su Supportive	47 Lk Legal Knowledge	48 Tk Technical knowledge	49 Cm Change Management	50 Pm Project management	51 UtD Up-to-date	52 Ex Experienced	53 Nk Network	54 As Auditing skills	55 Sc SonicWall Charter (China)	56 Pa Patriot Act (US)	57 FISA Foreign Intelligence Surveillance Act (US)	58 CLOUD Clarifying useful cross-border use of data act (US)	59 IA Intelligence Act (France)	60 G G-10 (Germany)	61 YL Yarosheva Law (Russia)	62 MiFID II Markets in financial instruments directive (EU)	63 OFAC Office of Foreign Assets Control (US)	64 FINTRAC Financial transaction and reporting analysis Centre (Canada)	65 C17 Cross Circular Echo (Luxembourg)	66 MLO Money Laundering Reporting Order	67 Bc Background checking	68 KYC Know your customer	69 Em Employee online monitoring													
70 Sc SonicWall Charter (China)	71 Pa Patriot Act (US)	72 FISA Foreign Intelligence Surveillance Act (US)	73 CLOUD Clarifying useful cross-border use of data act (US)	74 IA Intelligence Act (France)	75 G G-10 (Germany)	76 YL Yarosheva Law (Russia)	77 MiFID II Markets in financial instruments directive (EU)	78 OFAC Office of Foreign Assets Control (US)	79 FINTRAC Financial transaction and reporting analysis Centre (Canada)	80 C17 Cross Circular Echo (Luxembourg)	81 MLO Money Laundering Reporting Order	82 Bc Background checking	83 KYC Know your customer	84 Em Employee online monitoring	85 Sc SonicWall Charter (China)	86 Pa Patriot Act (US)	87 FISA Foreign Intelligence Surveillance Act (US)	88 CLOUD Clarifying useful cross-border use of data act (US)	89 IA Intelligence Act (France)	90 G G-10 (Germany)	91 YL Yarosheva Law (Russia)	92 MiFID II Markets in financial instruments directive (EU)	93 OFAC Office of Foreign Assets Control (US)	94 FINTRAC Financial transaction and reporting analysis Centre (Canada)	95 C17 Cross Circular Echo (Luxembourg)	96 MLO Money Laundering Reporting Order	97 Bc Background checking	98 KYC Know your customer	99 Em Employee online monitoring																																										
100 Sc SonicWall Charter (China)	101 Pa Patriot Act (US)	102 FISA Foreign Intelligence Surveillance Act (US)	103 CLOUD Clarifying useful cross-border use of data act (US)	104 IA Intelligence Act (France)	105 G G-10 (Germany)	106 YL Yarosheva Law (Russia)	107 MiFID II Markets in financial instruments directive (EU)	108 OFAC Office of Foreign Assets Control (US)	109 FINTRAC Financial transaction and reporting analysis Centre (Canada)	110 C17 Cross Circular Echo (Luxembourg)	111 MLO Money Laundering Reporting Order	112 Bc Background checking	113 KYC Know your customer	114 Em Employee online monitoring	115 Sc SonicWall Charter (China)	116 Pa Patriot Act (US)	117 FISA Foreign Intelligence Surveillance Act (US)	118 CLOUD Clarifying useful cross-border use of data act (US)	119 IA Intelligence Act (France)	120 G G-10 (Germany)	121 YL Yarosheva Law (Russia)	122 MiFID II Markets in financial instruments directive (EU)	123 OFAC Office of Foreign Assets Control (US)	124 FINTRAC Financial transaction and reporting analysis Centre (Canada)	125 C17 Cross Circular Echo (Luxembourg)	126 MLO Money Laundering Reporting Order	127 Bc Background checking	128 KYC Know your customer	129 Em Employee online monitoring																																										



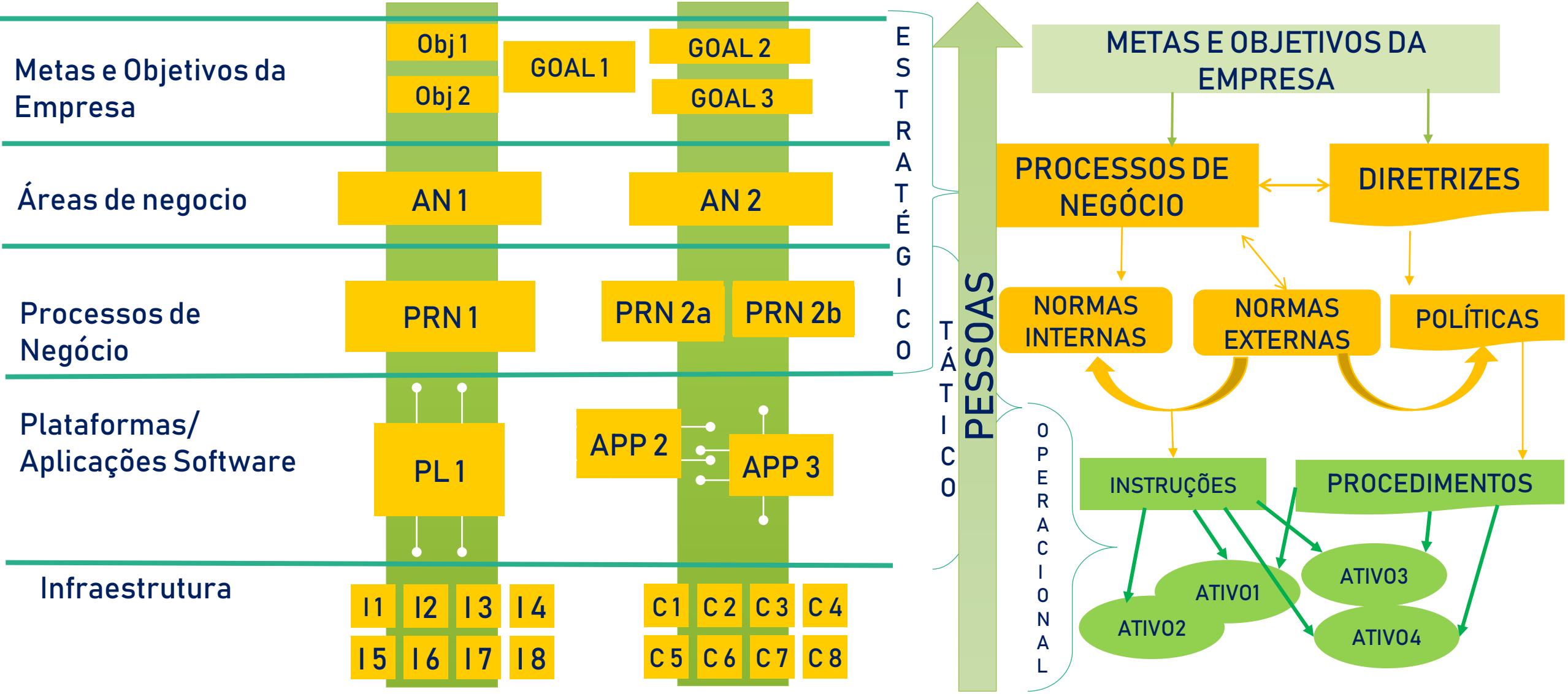
Ferramentas:

1	Os	PERIODIC TABLE OF DEVOPS TOOLS (V3)												2	En																								
GI GitLab		Os Open Source		Fr Free		Fm Freemium		Pd Paid		En Enterprise		ScM Source Control Mgmt.		DA Database Automation		CI Continuous Integration		T Testing		Co Configuration		D Deployment		C Containers		RO Release Orchestration		Cloud		AOps AIOps		A Analytics		M Monitoring		S Security		Co Collaboration	
	3	Fm	4	En	Gh	Dt	Dtical																																
	11	Os	12	En	Sv	Db	DBMaestro																																
	19	En	20	En	Cw	Dp	Delphix	Jn	Jenkins	Cs	Codeship	Fn	FitNesse	Ju	JUnit	Ka	Karma	Su	SoapUI	Ch	Chef	Tf	Terraform	XLd	XebiaLabs XL Deploy	Ud	UrbanCode Deploy	Ku	Kubernetes	Cc	CA CD Director	Pr	Plutora Release	Ai	Alibaba Cloud	Os	OpenStack	Ps	Prometheus
	37	Pd	38	Fm	39	Pd	40	Fm	41	Fr	42	Fr	43	Os	44	Pd	45	En	46	Os	47	En	48	Os	49	Os	50	Pd	51	Fm	52	Pd	53	Pd	54	En			
	At	Artifactory	Rg	Redgate	Ba	Bamboo	Vs	VSTS	Se	Selenium	Jm	JMeter	Ja	Jasmine	Sl	Sauce Labs	An	Ansible	Ru	Rudder	Oc	Octopus Deploy	Go	GoCD	Ms	Mesos	Gke	GKE	Om	OpenMake	Cp	AWS CodePipeline	Cy	Cloud Foundry	It	ITRS			
	Nx	Nexus	Fw	Flyway	Tr	Travis CI	Tc	TeamCity	Ga	Gatling	Tn	TestNG	Pe	Perfecto	Pu	Puppet	Pa	Packer	Cd	AWS CodeDeploy	Ec	ElectricCloud	Ra	Rancher	Aks	AKS	Rk	Rkt	Sp	Spinnaker	Ir	Iron.io	Mg	Moogsoft					
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				
XL XebiaLabs Enterprise DevOps																																							
91	En	92	Os	93	Fm	94	En	95	En	96	Fm	97	Os	98	Os	99	Os	100	En	101	En	102	En	103	En	104	Os	105	Os										
XLi	XebiaLabs XL Impact	Ki	Kibana	Nr	New Relic	Dt	Dynatrace	Dd	Datadog	Ad	AppDynamics	EI	ElasticSearch	Ni	Nagios	Zb	Zabbix	Zn	Zenoss	Cm	Checkmarx SAST	Wp	Signal Sciences Wpp	Bd	BlackDuck	Sr	SonarQube	Hv	HashiCorp Vault										
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										



Follow @xebialabs

Boas Práticas: Arquitetura Corporativa



Boas Práticas:

DEVSECOPS

NEGÓCIOS QUE PERMITEM RECEPΤIVIDADE

REDUZIR O TEMPO DE ESPERA PARA MUDANÇAS

MONITORAMENTO CONTÍNUO

CONTINUOUS DELIVERY

INFRAESTRUTURA AUTOMATIZADA

INTEGRAÇÃO CONTÍNUA

TESTES AUTOMATIZADOS

CONTROLE DE VERSÕES

Práticas



ALTA CONFIANÇA

INOVAÇÃO

ORIENTAÇÃO A DESEMPENHO

EMPODERAMENTO DE TIMES

REDUÇÃO DE VARIAÇÃO

ALTA COOPERAÇÃO

Cultura

FLUXO CONTÍNUO & VISIBILIDADE

PRINCÍPIOS LEAN & AGILE

FOCO EM PRODUTOS

FLUXO DO SISTEMA

AMPLIAR FLUXO DE FEEDBACK

EXPERIMENTAÇÃO CONTÍNUA

Boas Práticas: Níveis de Maturidade DevSecOps

1- Regressivo

- Processos que não podem ser repetidos, pouco controlados e reativos.

2 – Repetível

- Processos Documentados e parcialmente automatizados.

3 – Consistente

- Processos automatizados aplicados ao longo de todo ciclo de vida da aplicação.

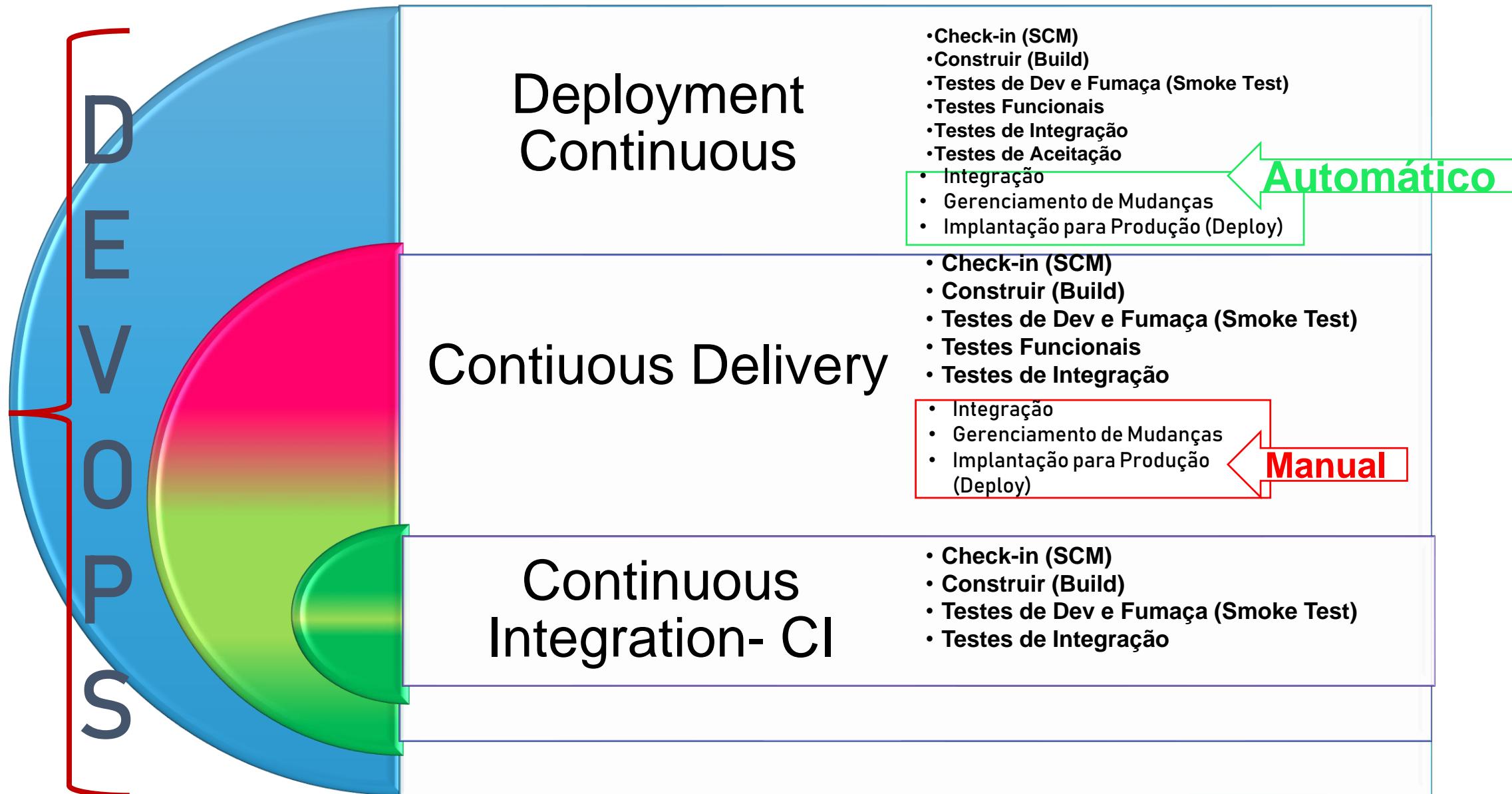
4 – Gerido Quantitativamente

- Processos medidos e Controlados.

5 – Otimizado

- Foco em melhorias de processos.

Boas Práticas: Diferença Entre DevOps X CI & CD

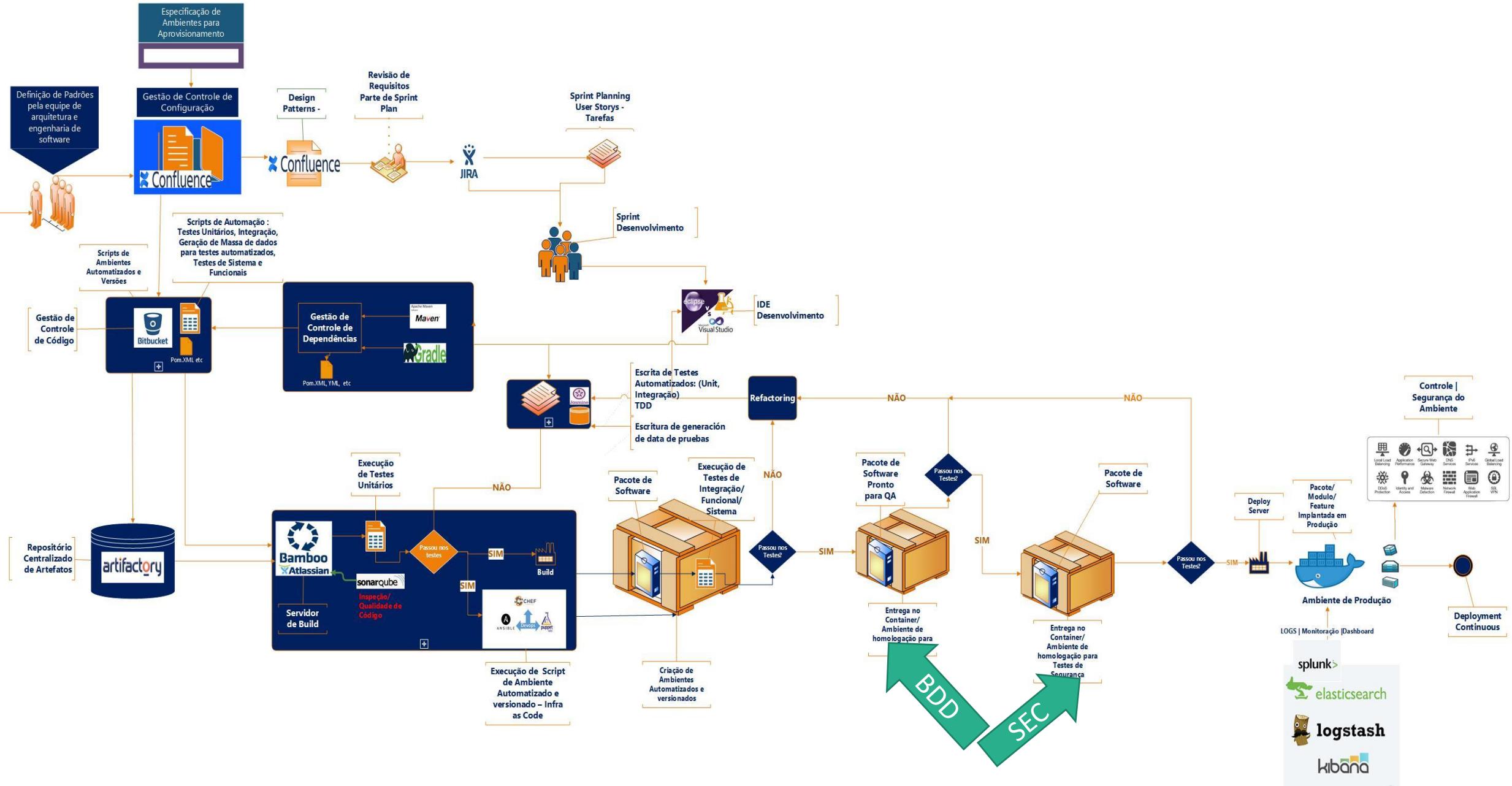


Boas Práticas Checklist Deployment Continuous:

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

Boas Práticas: Secure Deployment Continuous

Deployment Continuous

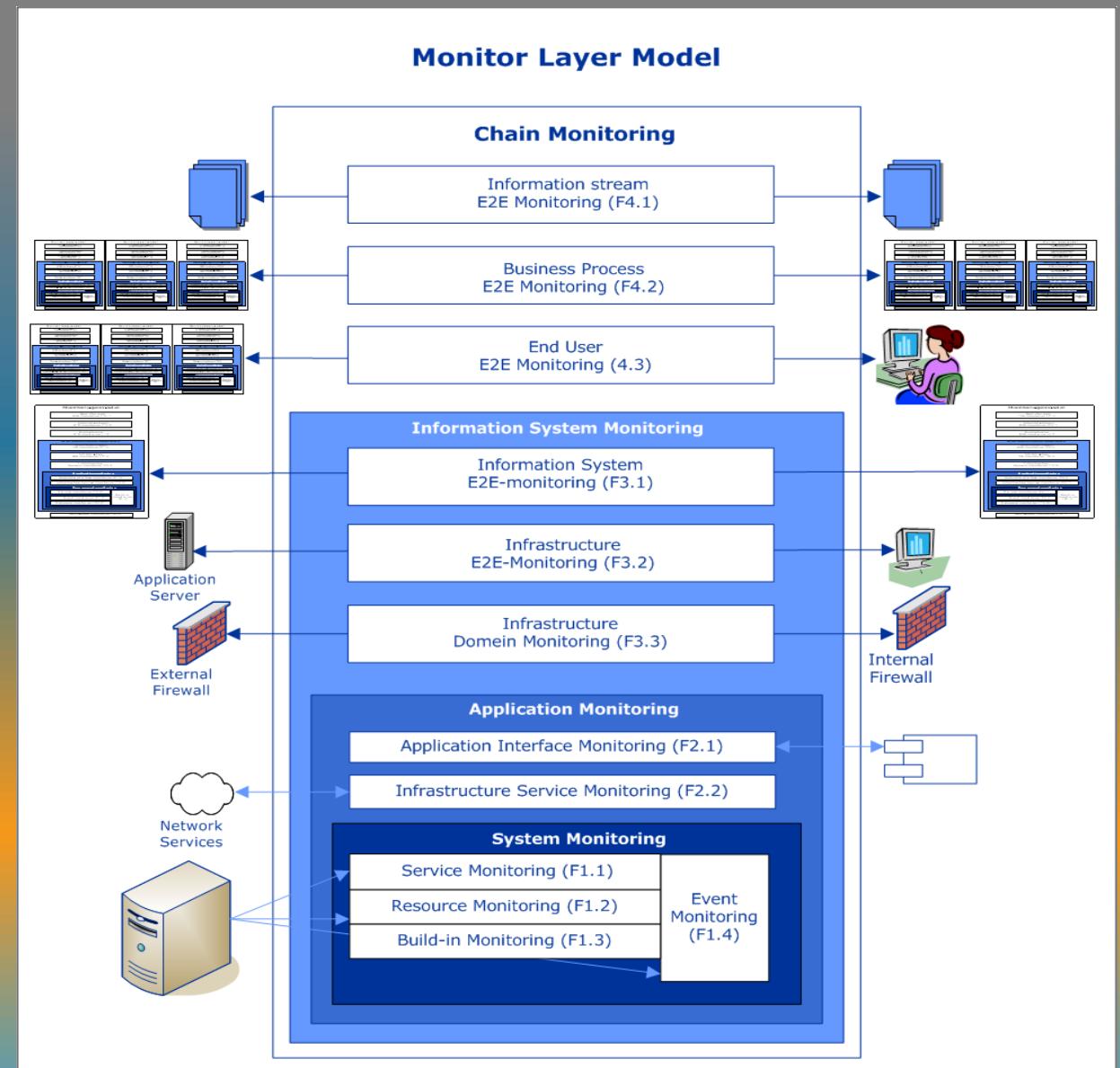


Boas Práticas: Monitoração Contínua

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.



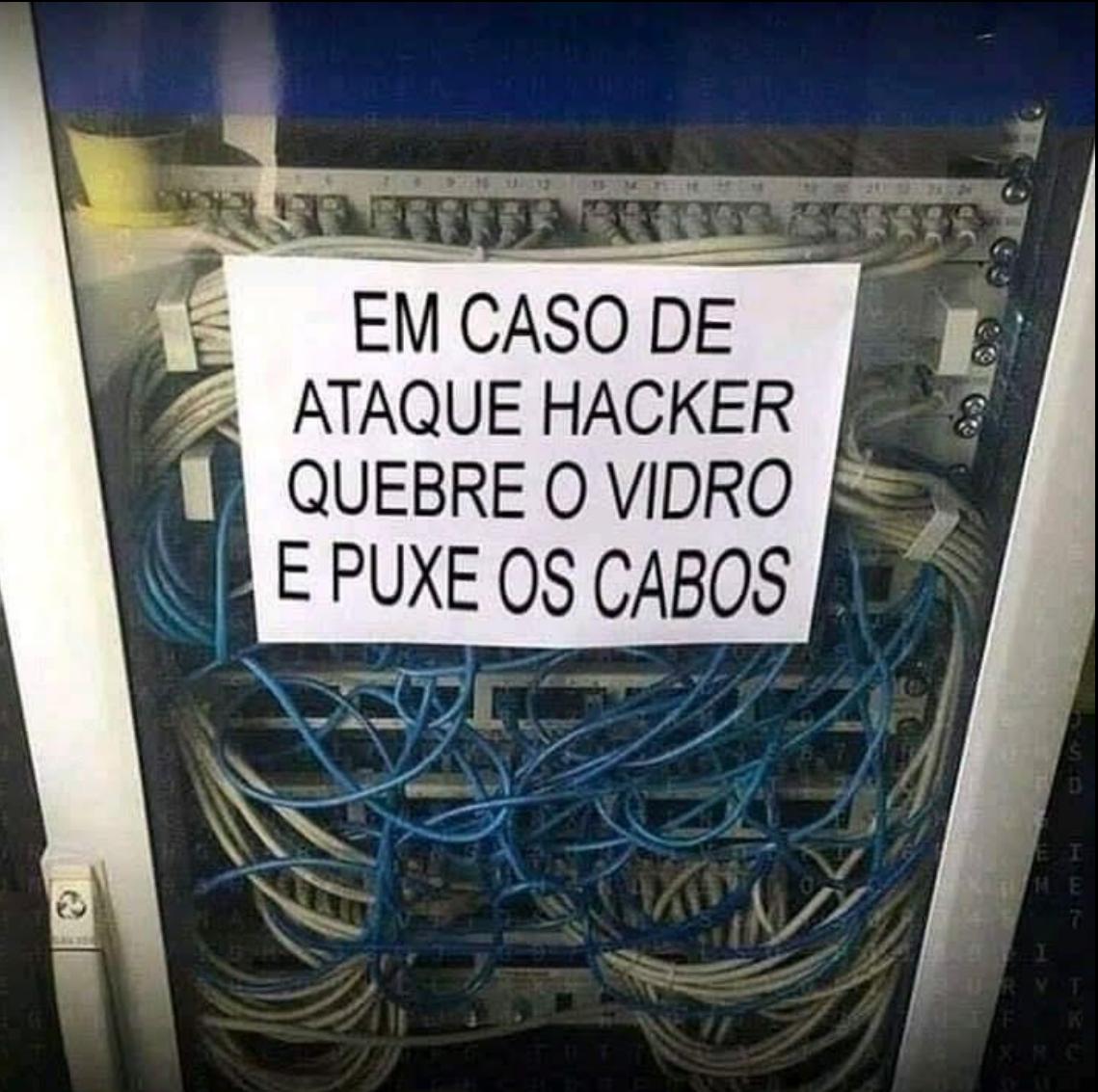
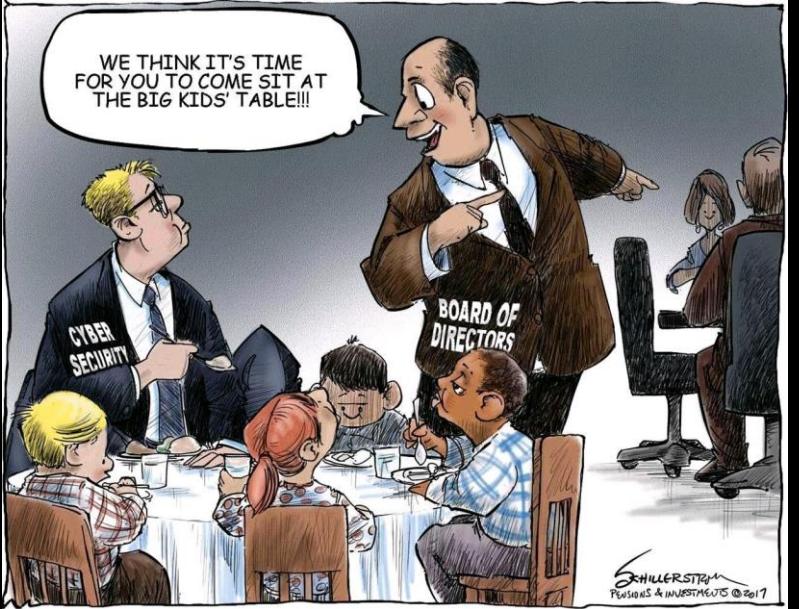
CILADAS

SPEED COMPARISON

Just how fast EXTREME GO HORSE really is:

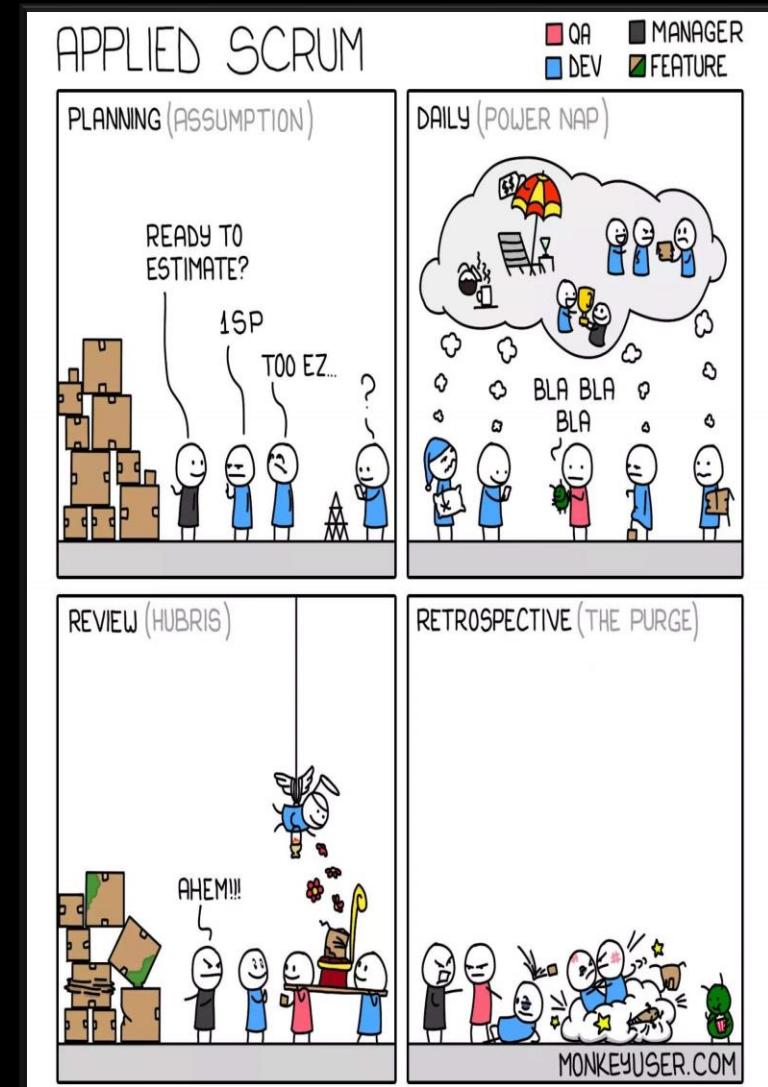
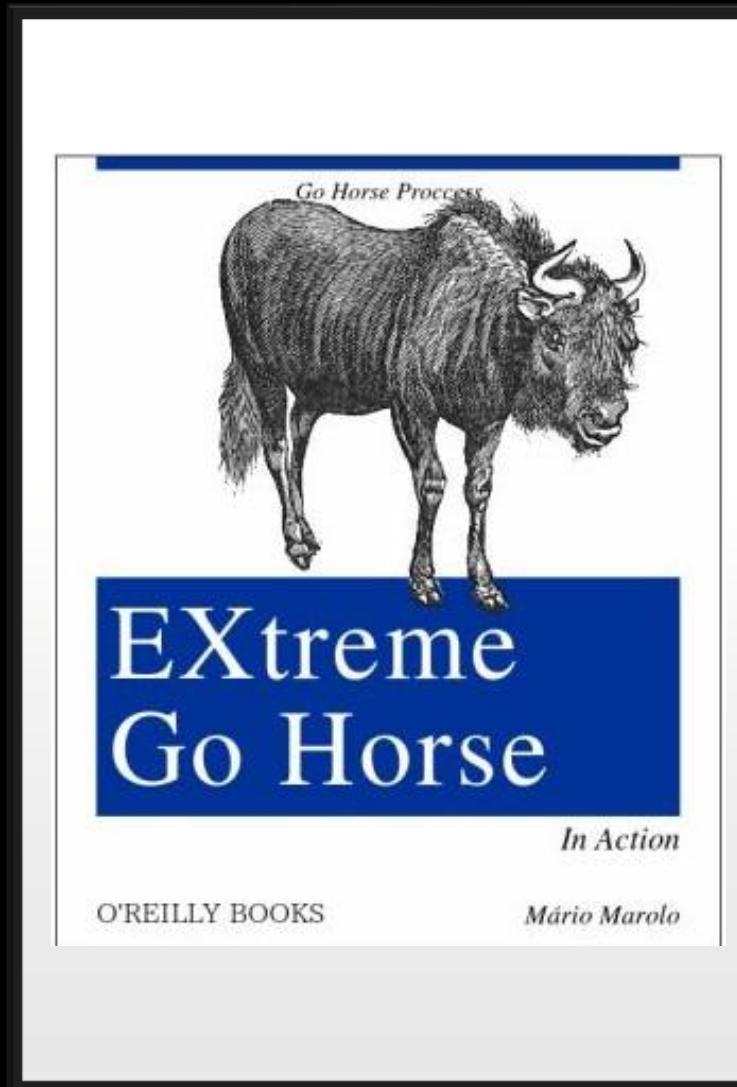
F
I
N
I
S
H

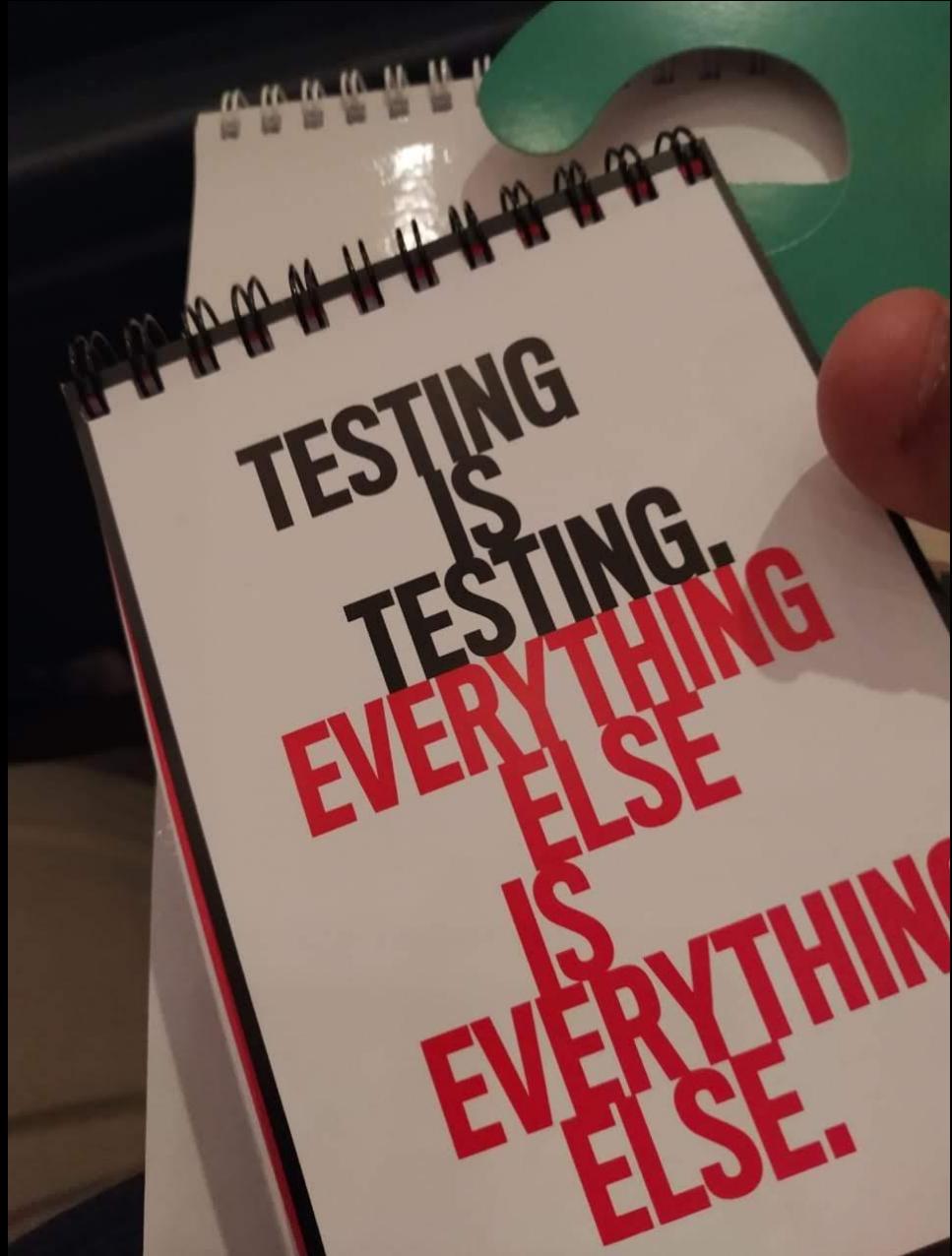
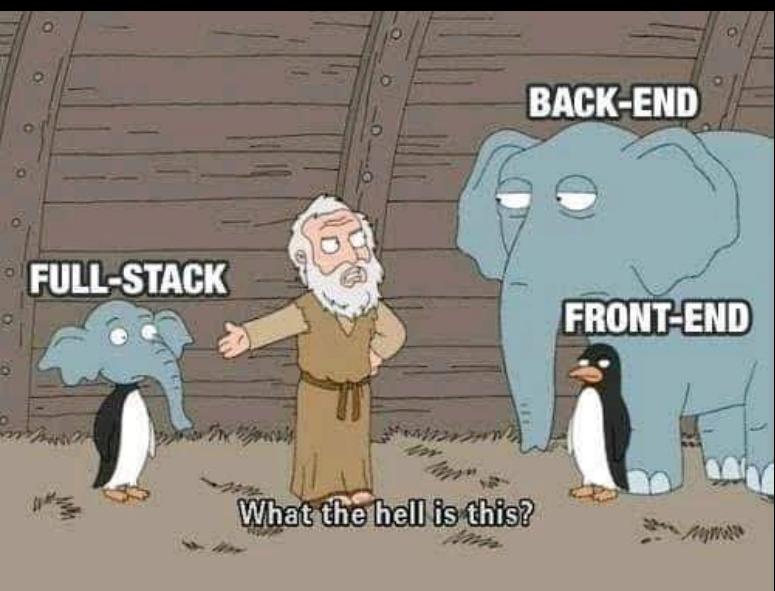
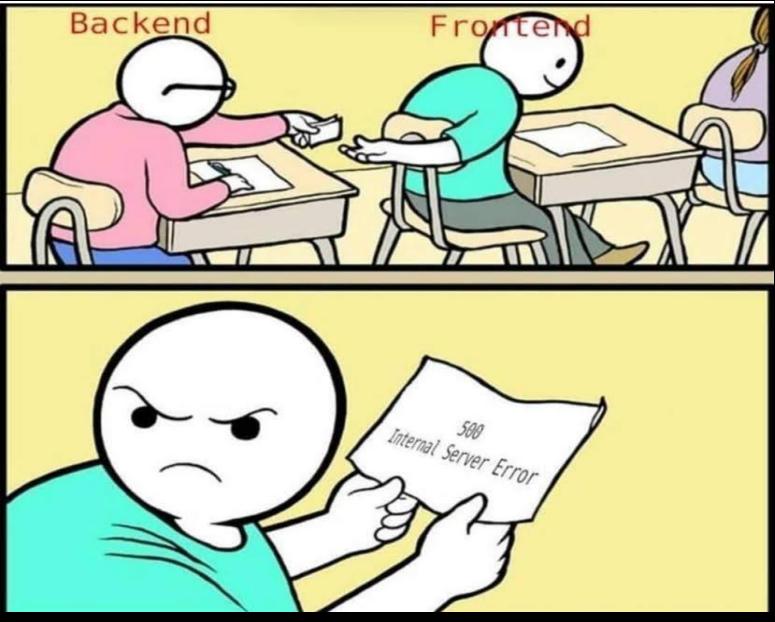


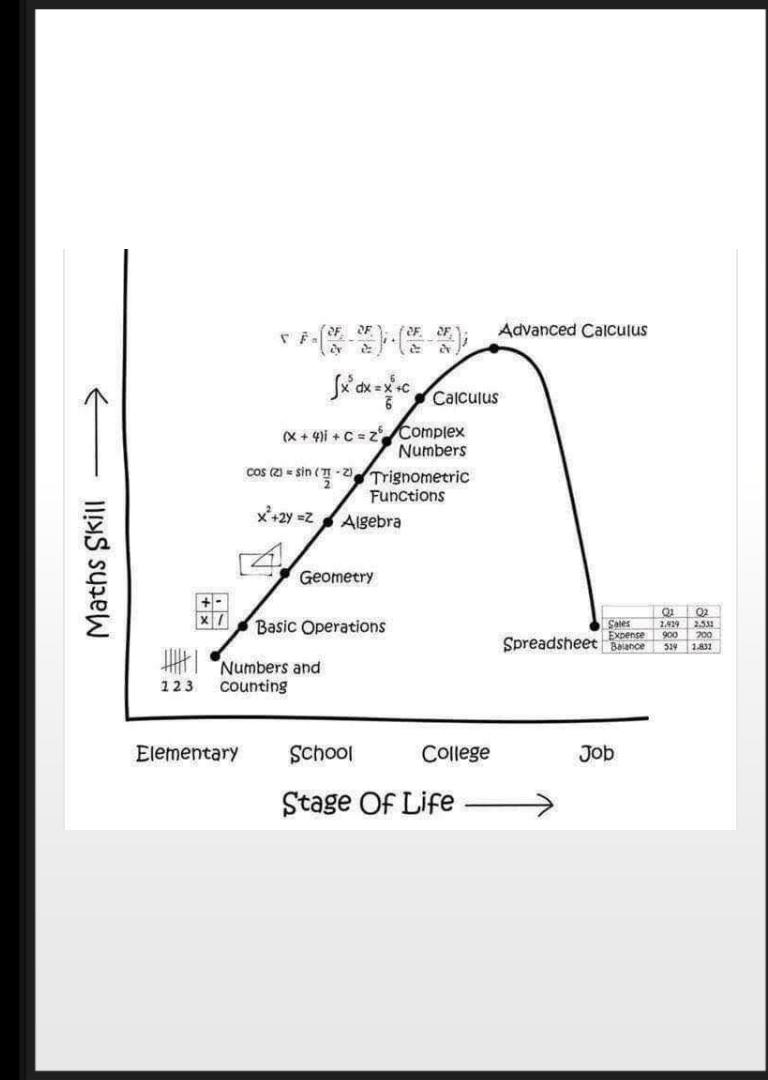
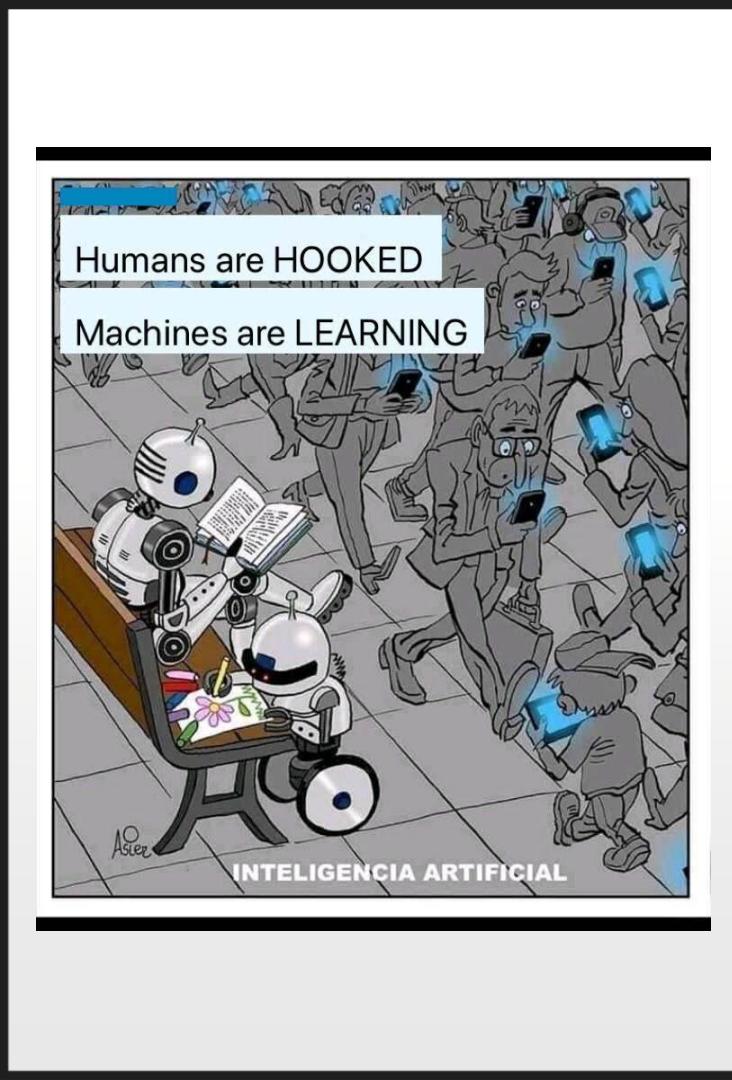
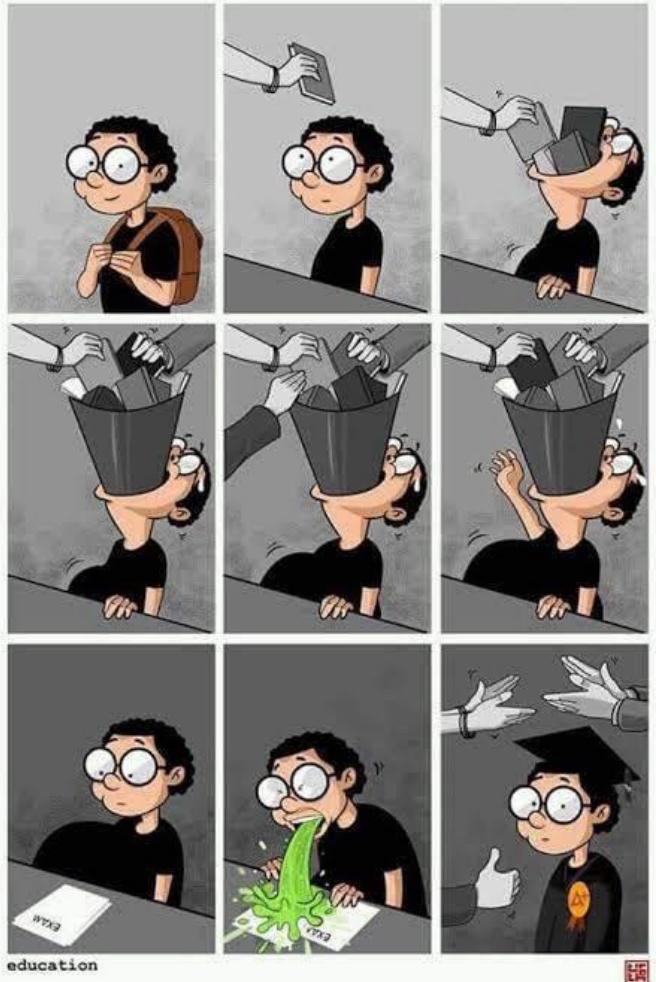


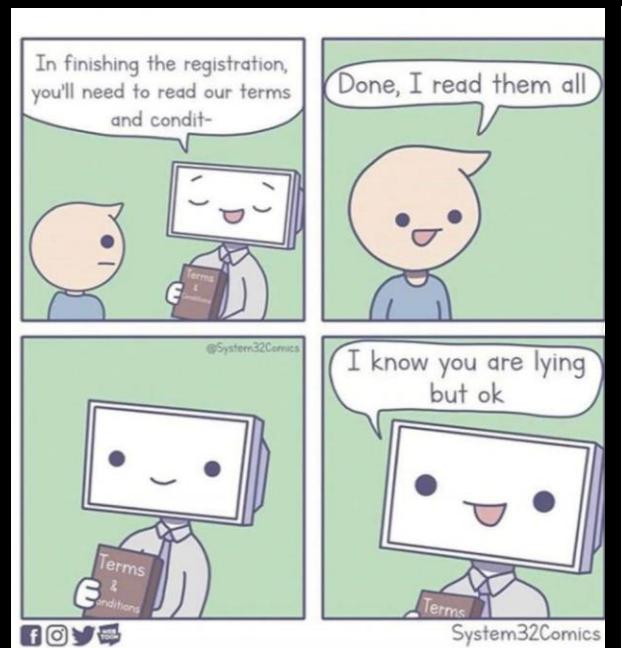
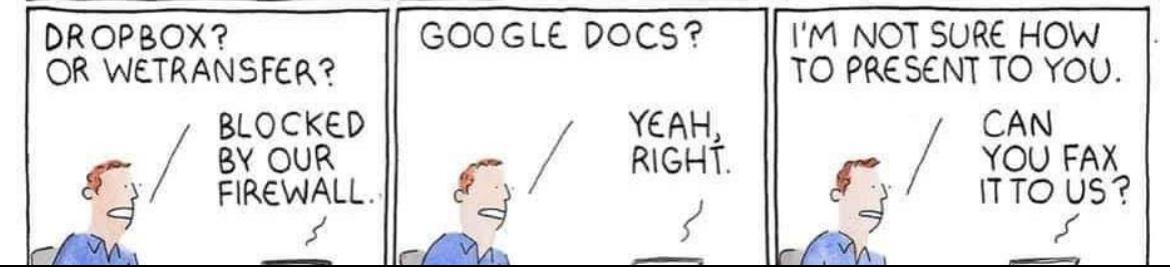
Sleeping Positions



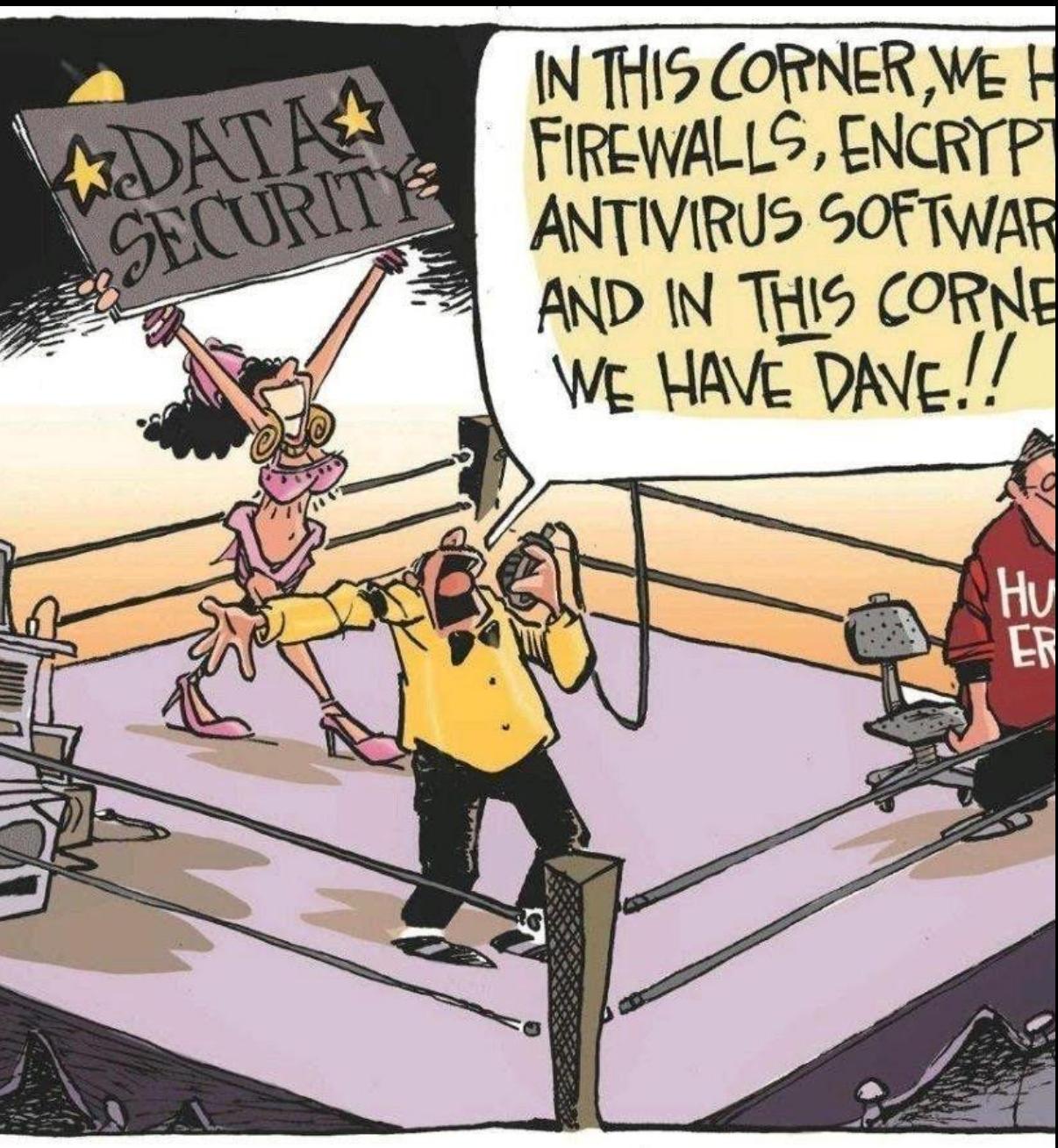
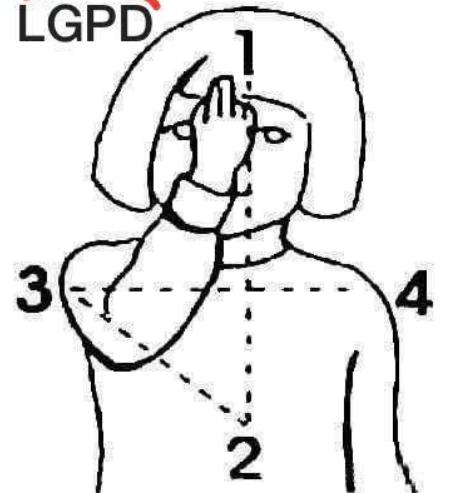








4 EASY STEPS FOR ~~GDPR~~ COMPLIANCE LGPD



REFERÊNCIAS:

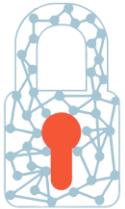
BIBLIOGRAFIA & SITES:



<https://biocienciaforadehora.wordpress.com/2016/09/07/informacao-x-conhecimento-2/>
<https://www.diogovidal.com.br/inicio/dados-x-informa%C3%A7%C3%A3o-qual-a-diferen%C3%A7a>
<http://eleganthack.com/towards-a-new-information-architecture/>
<https://genehughson.wordpress.com/2011/12/07/so-what-exactly-does-an-architect-do/>
https://en.wikipedia.org/wiki/Architecture_domain
<http://www.blrdata.com.br/arquitetura-de-dados-consultoria>
<https://www.bdo.com/blogs/nonprofit-standard/may-2018/the-integration-of-data-privacy>
<https://www.protiviti.com/SA-en/data-management-advanced-analytics/sap-solutions/data-governance>
<https://blog.gojekengineering.com/data-infrastructure-at-go-jek-cd4dc8cbd929>
<https://www.slideshare.net/ccgmag/turning-information-chaos-into-reliable-data-tools-and-techniques-to-interpret-organize-and-increase-reliable-business-results>
<https://www.ics.ie/news/what-is-privacy-by-design-a-default>
<https://www.iso.org/committee/45086/x/catalogue/>
<http://sites.computer.org/ccse/SE2004Volume.pdf>
<https://slideplayer.com/slide/3458452/>
http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm
<https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700>
<https://twitter.com/brysonbort/status/1071481534060920835>
<https://www.cbinsights.com/research/periodic-table-cybersecurity-startups/>
<https://ifsecglobal.com/wp-content/uploads/2018/12/8793-IFSEC-Global-Periodic-Table-1.pdf>
<https://thisismyclassnotes.blogspot.com/2019/02/periodic-table-of-data-privacy.html>

AGNER, Luiz. Ergodesign e arquitetura de informação: trabalhando com o usuário. Rio de Janeiro: Editora Quartet, 2º Edição, 20109

Data Management Body of Knowledge (DAMA DMBoK®) – LLC Editora, 1º Edição, 2012.
Data & Information – DAMA Brasil, 1º Edição, 2015.



Cyber
Security
Girls



monteiromartins@bol.com.br

