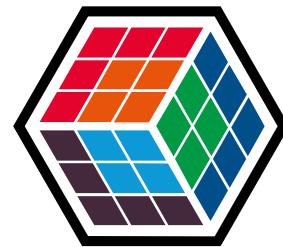




**Cyber
Security
Girls**



THE DEVELOPER'S CONFERENCE

Trilha Arquitetura de Dados

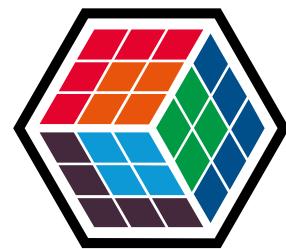
Alessandra Monteiro Martins

Especialista em Governança de TI pela Universidade Católica de Brasília,
Licenciada em Informática pela Universidade do Estado do Amazonas,
Certificações ITIL, COBIT, ISO27002, CTFL, KMPI, Scrum Master, CLF, PDPF





Cyber
Security
Girls



THE DEVELOPER'S CONFERENCE

**Arquitetando seus dados na
Prática para LGPD**





THE
DEVELOPER'S
CONFERENCE

Agenda

- Contexto da LGPD: Objetos, Princípios, Direitos e Deveres
 - Conceitos: Arquiteturas, Governanças, Dados e Informações
 - Papéis
 - Problemas
 - Como a Arquitetura pode Influenciar



Como alinhar Arquitetura e Conformidade Legal

- Contribuições da Governança de Dados para Compliance
- Referências

Contexto da LGPD

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.





THE
DEVELOPER'S
CONFERENCE

Contexto da LGPD

OBJETOS E ESCOPO

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 da LGPD

OPERAÇÕES



Contexto da LGPD

PAPÉIS



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 em todo o território nacional



THE
DEVELOPER'S
CONFERENCE



Controlador - Responsável pela 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;

Contexto da LGPD

DIREITOS & DEVERES



THE
DEVELOPER'S
CONFERENCE



Contexto da LGPD

Sanções



THE
DEVELOPER'S
CONFERENCE

Sanções	Multa	Regras	Parâmetros	Outras Penalidades
Advertência, com indicação de prazo para adoção de medidas corretivas;	Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração	No cálculo do valor da multa de que trata o inciso II, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.	As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:	LEI N° 12.965, DE 23 DE ABRIL DE 2014 (Marco Civil)
Publicização da infração após devidamente apurada e confirmada a sua ocorrência	Multa diária, observado o limite total a que se refere o inciso II	A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.	I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.	Sem prejuízo das demais sanções civis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11. Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.
Bloqueio dos dados pessoais a que se refere a infração até a sua regularização	O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.	O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.		
Eliminação dos dados pessoais a que se refere a infração;				

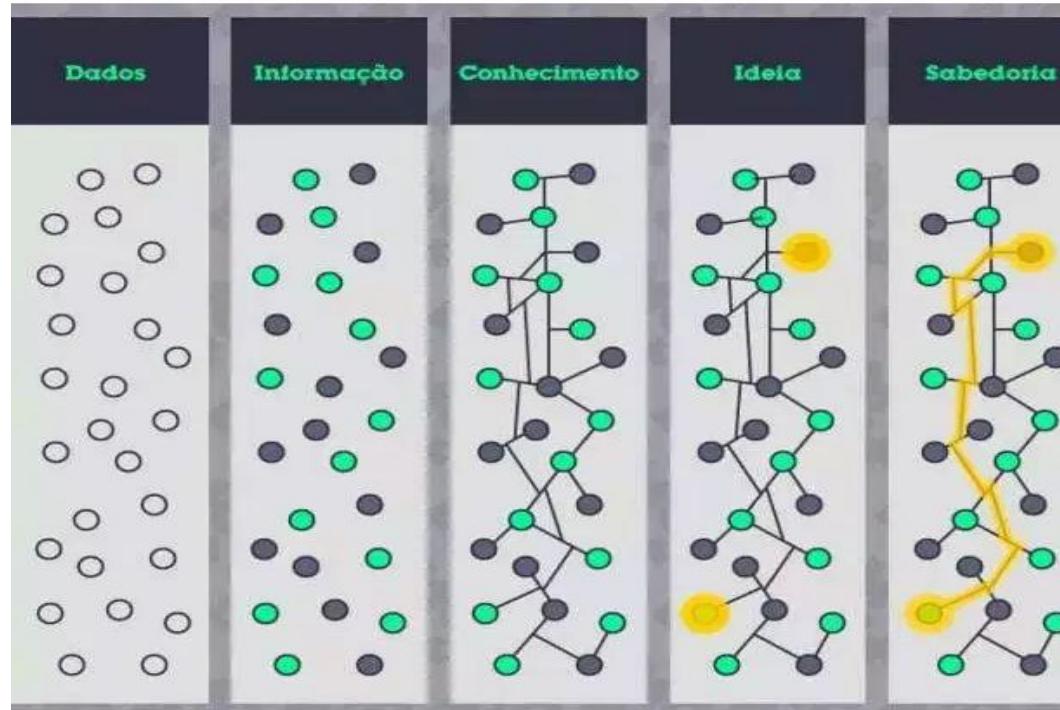


THE
DEVELOPER'S
CONFERENCE

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: 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.



Dados



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.



Aplicações



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

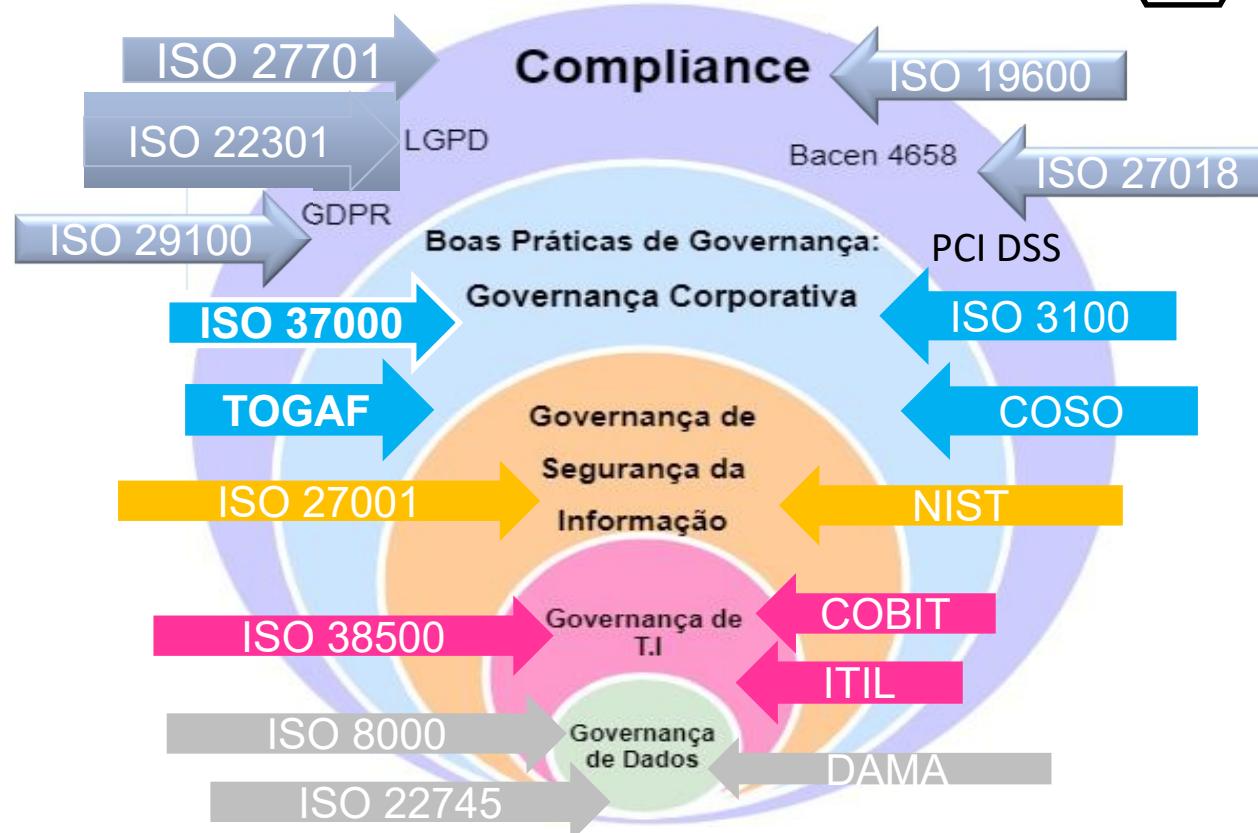


Estrutura e comportamento da infraestrutura de TI. Abrange os nós de cliente e servidor da configuração de hardware, os aplicativos de infraestrutura que são executados neles, os serviços de infraestrutura que eles oferecem aos aplicativos, os protocolos e as redes que conectam aplicativos e nós.



THE
DEVELOPER'S
CONFERENCE

Conceitos: Governanças



Papéis:





Papéis:



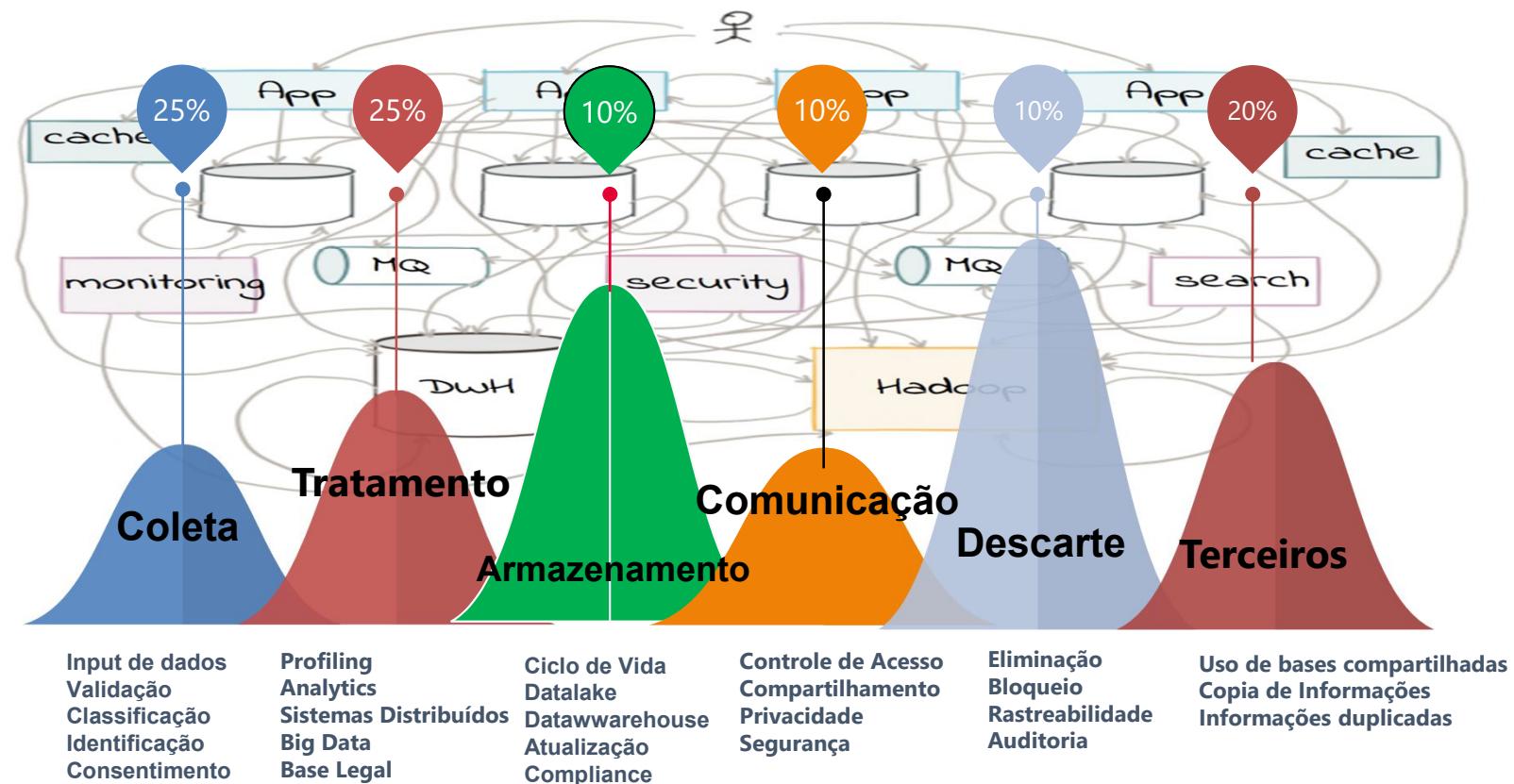
THE
DEVELOPER'S
CONFERENCE





THE
DEVELOPER'S
CONFERENCE

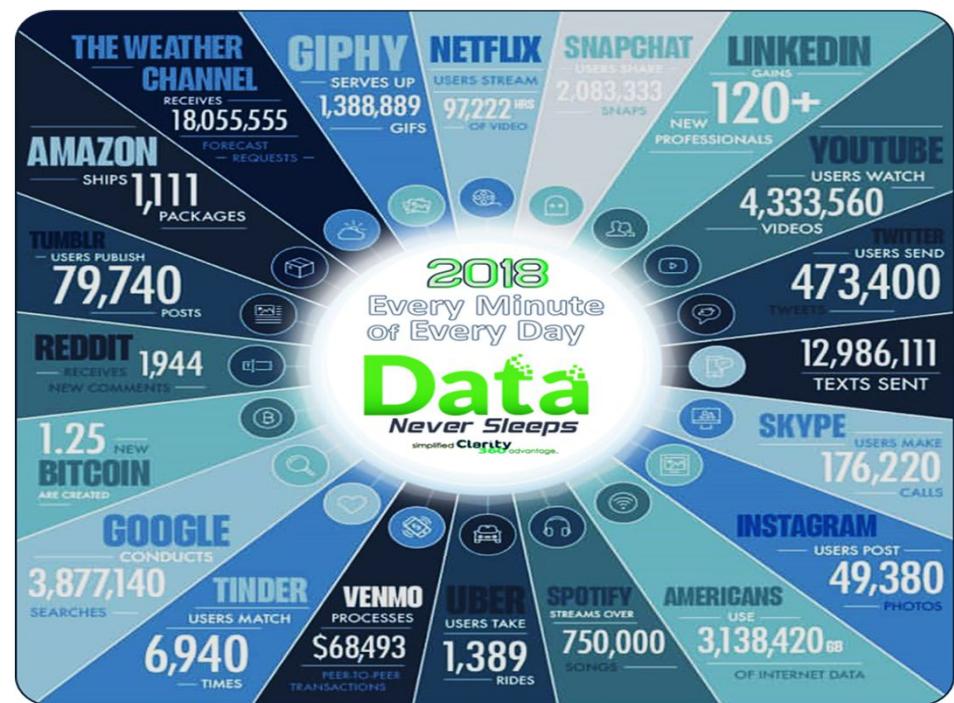
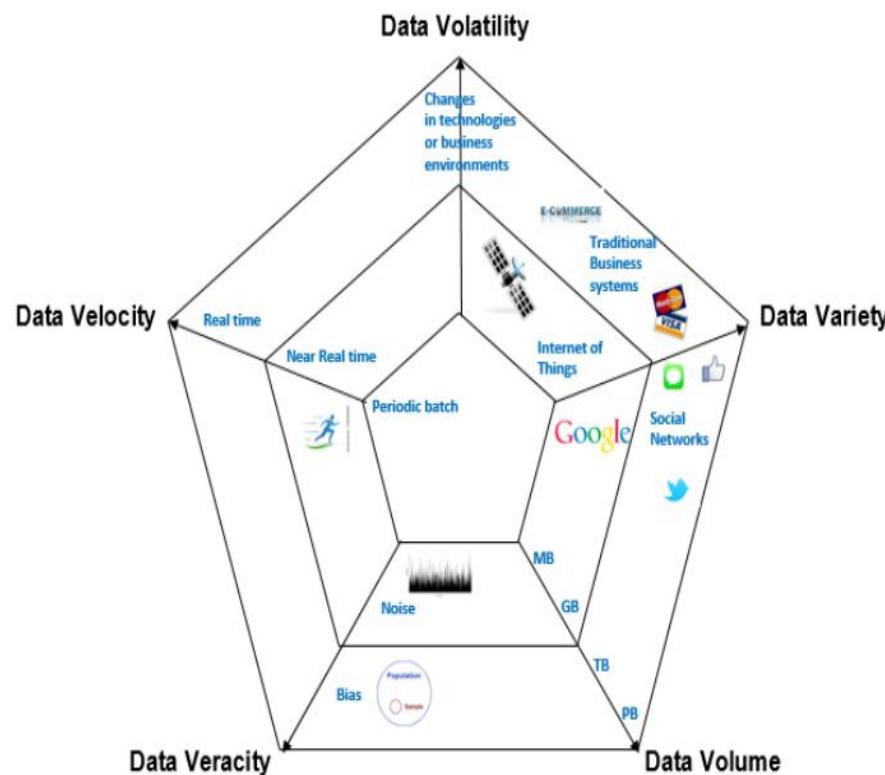
Problemas:



Problemas: Desafios



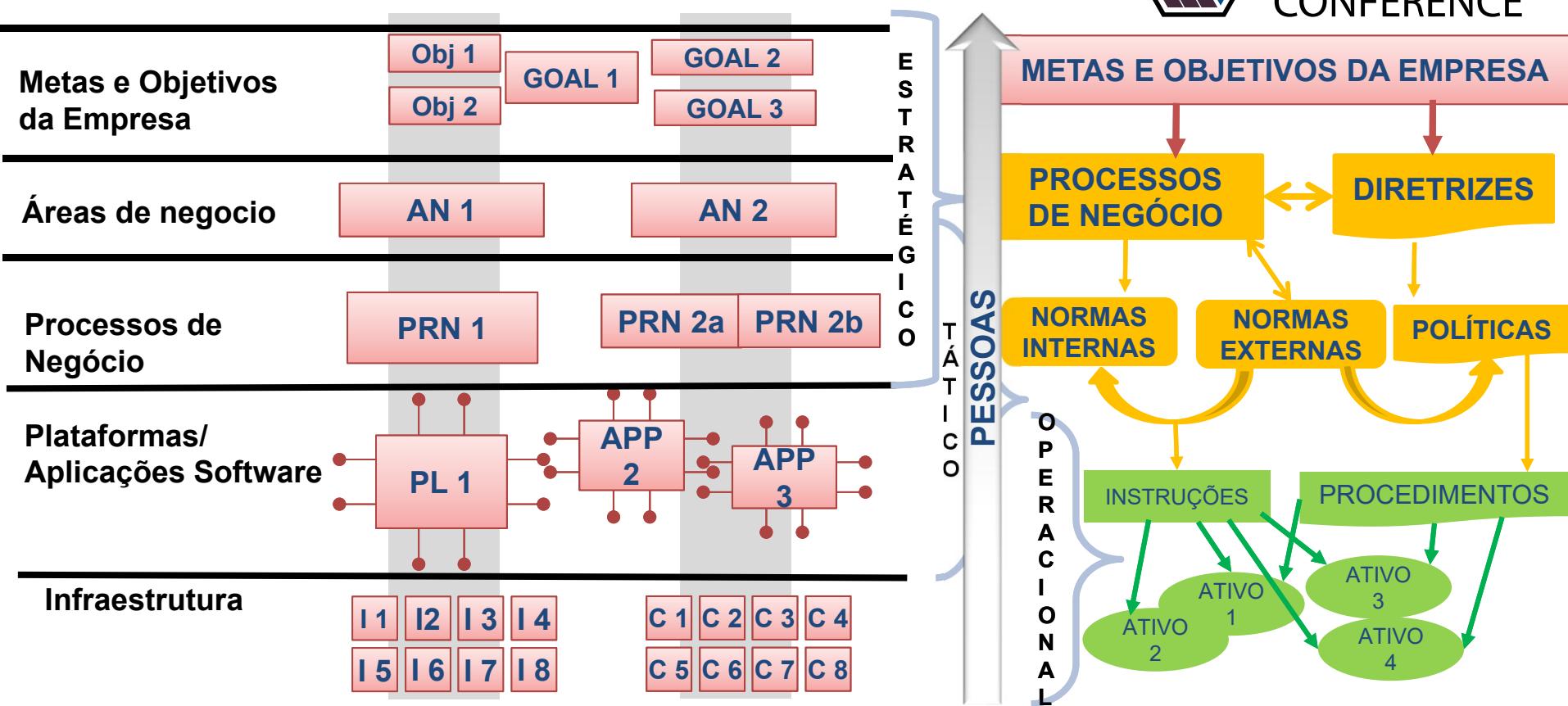
THE
DEVELOPER'S
CONFERENCE





THE
DEVELOPER'S
CONFERENCE

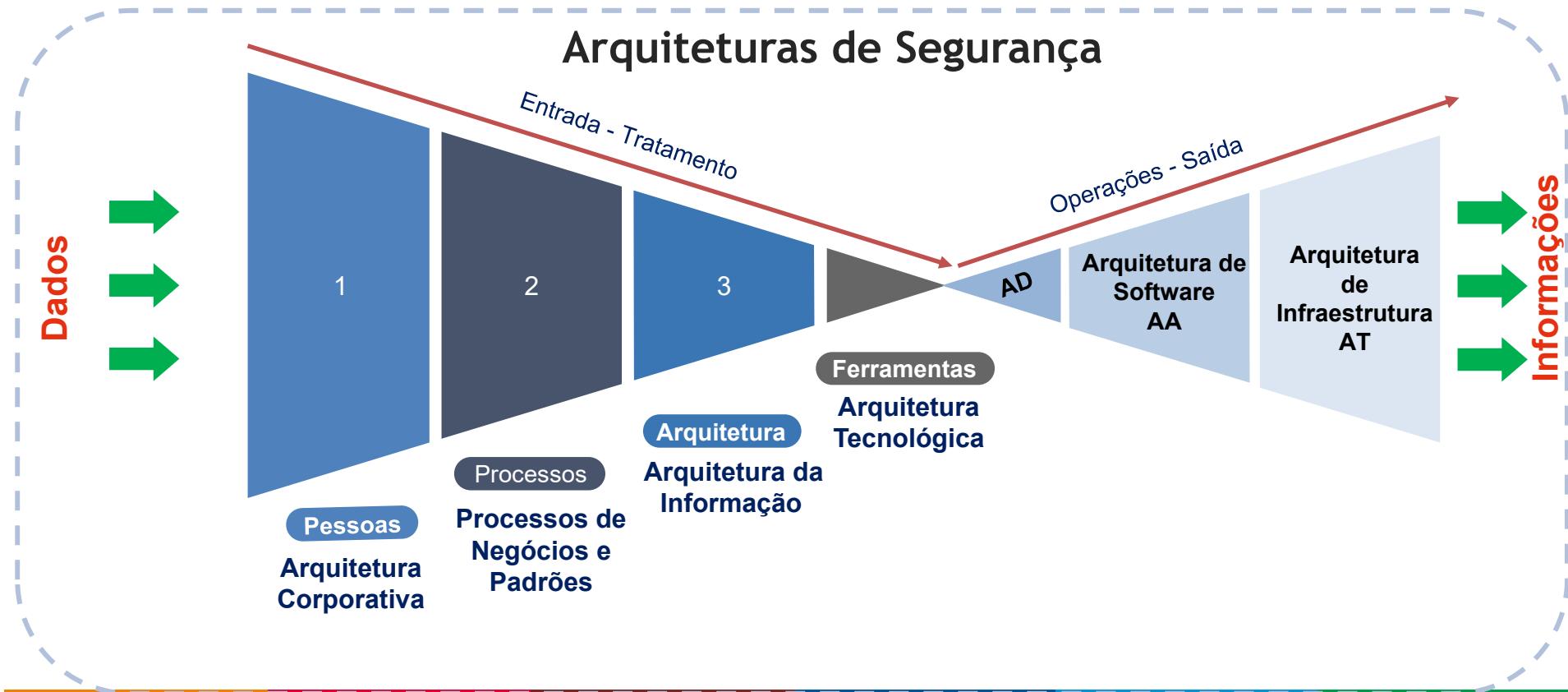
Como a Arquitetura pode Influenciar



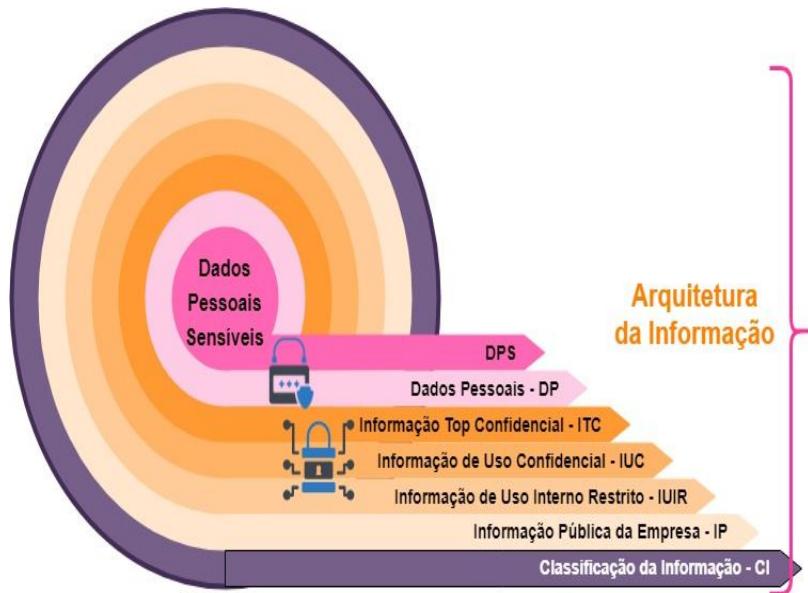
Como alinhar Arquitetura e Conformidade Legal



THE
DEVELOPER'S
CONFERENCE



Contribuições da Governança de Dados para Compliance

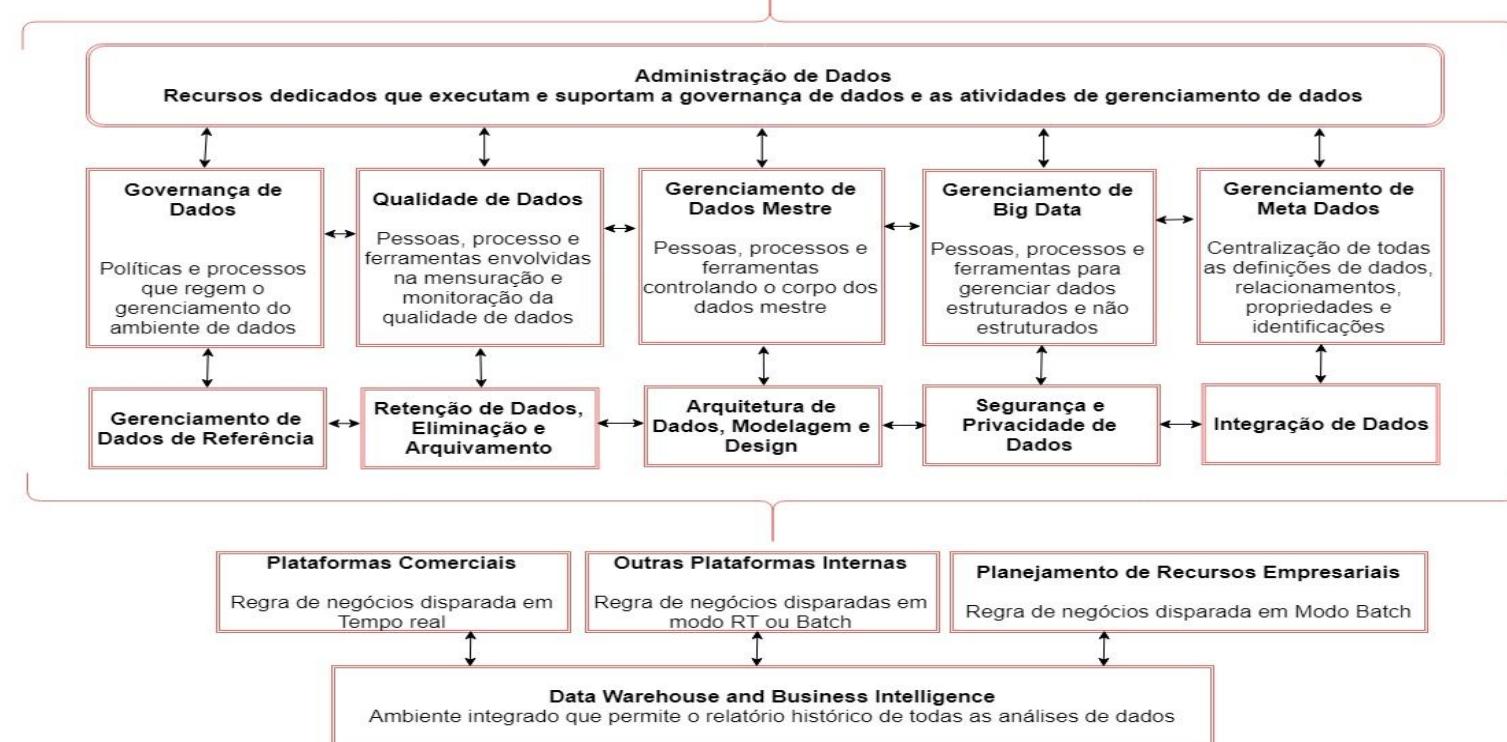


Contribuições da Governança de Dados para Compliance



THE
DEVELOPER'S
CONFERENCE

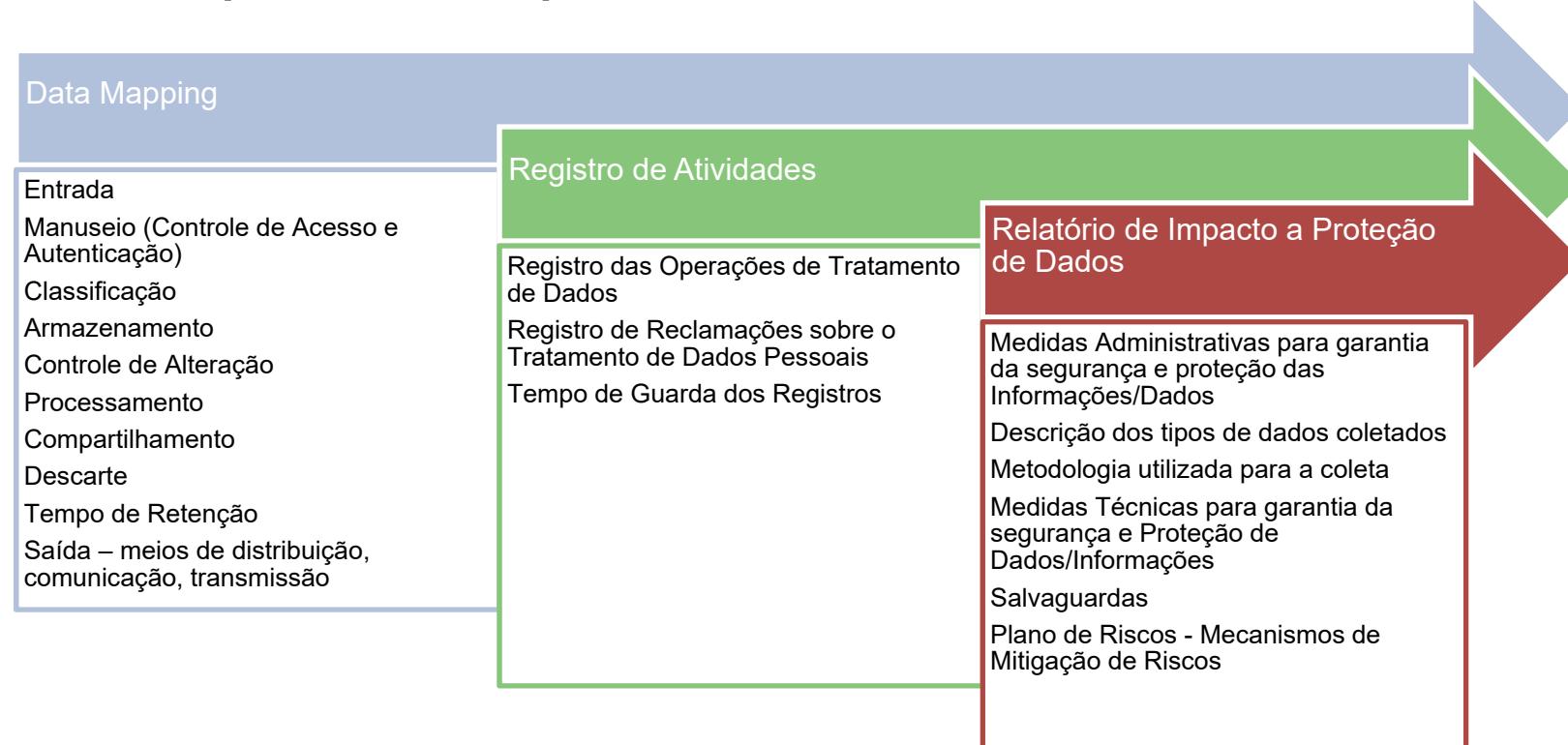
Governança de Dados & Gerenciamento de Dados





THE
DEVELOPER'S
CONFERENCE

Contribuições da Governança de Dados para Compliance



Métricas de Qualidade de Dados, por onde começar “fechar a torneira”...



THE
DEVELOPER'S
CONFERENCE

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?

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.



THE
DEVELOPER'S
CONFERENCE

Referências:

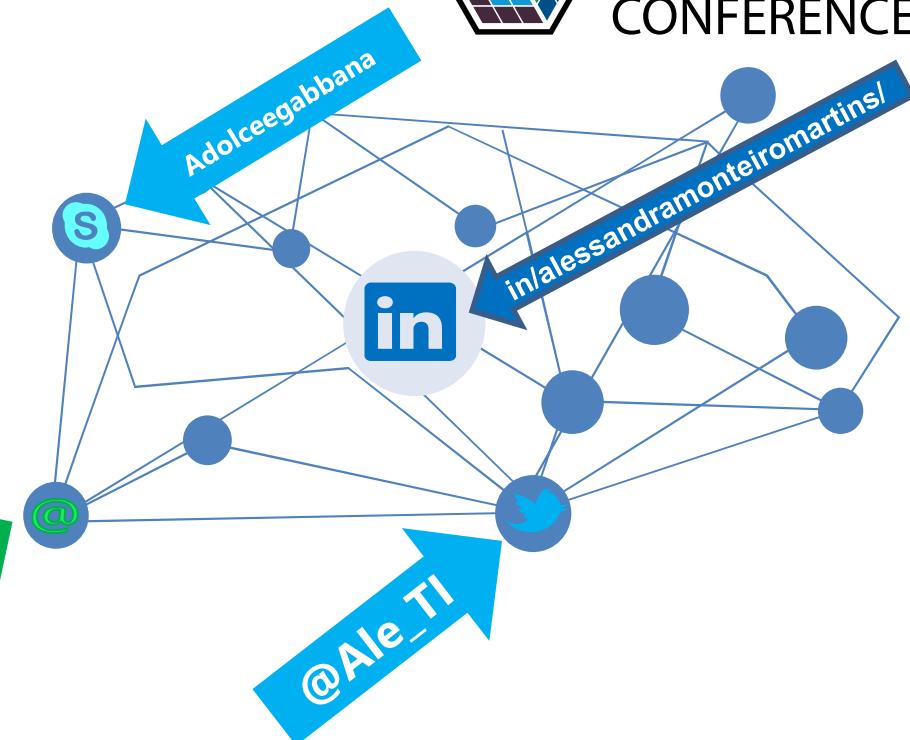
- FILHO, Wilson de Pádua – “Engenharia de Software: Fundamentos Métodos e Padrões – LTC -3º Edição , 2009, Rio de Janeiro
- AGNER, Luiz. **Ergodesign e arquitetura de informação: trabalhando com o usuário.** Rio de Janeiro: Editora Quartet, 2º Edição, 20109
- Data Management Body of Knowledge (DAMA DMBoK®) – LLC Editora, 1º Edição,2012. Data & Information – DAMA Brasil, 1º Edição, 2015.
- http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- https://pt.wikipedia.org/wiki/Arquitetura_de_dados
- <https://www.opengroup.org/togaf>
- https://pt.wikipedia.org/wiki/Arquiteto_de_software
- <https://profissoesemti.wordpress.com/2009/11/21/entrevista-arquiteto-de-dados/>
- <https://www.fiap.com.br/mba/mba-em-arquitetura-de-solucoes/>
- https://pt.wikipedia.org/wiki/Arquitetura_empresarial
- <https://pt.itpedia.nl/2018/02/03/een-nieuw-beroep-informatiebeveiligingsarchitect/>
- <http://www.sgi.cefetmg.br/wp-content/uploads/sites/83/2017/03/PDTI-2018-2020.pdf>
- <https://www.linkedin.com/pulse/afinal-o-que-%C3%A9-arquitetura-de-solu%C3%A7%C3%A3o-%C3%A9-qual-nas/>
- <https://www.slideshare.net/ulfmattsson/cloud-data-governance-risk-management-and-compliance-ny-metro-joint-cyber-security-conference-2014>
- <https://vitoralbertoklein.wordpress.com/2011/09/16/o-que-e-arquitetura-empresarial/>
- <https://www.linkedin.com/pulse/20140613155546-11856035-togaf-the-open-group-architecture-framework/>
- https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf
- <https://www.ico.org.uk>
- <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>



THE
DEVELOPER'S
CONFERENCE

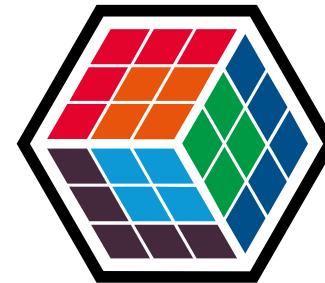


monteiromartins@bol.com.br





Cyber
Security
Girls



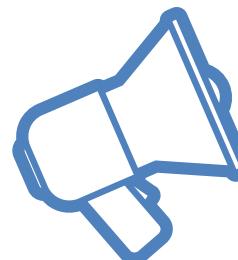
FemmeIT
O JEITO FEMININO DE FALAR DE TI

govprivacysec@yahoo.com
@

@Ale_TI



THE DEVELOPER'S CONFERENCE



OBRIGADA