



**Cyber
Security
Girls**



THE DEVELOPER'S CONFERENCE

Trilha – Transformação Digital & Inovação

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



Cyber
Security
Girls



THE DEVELOPER'S CONFERENCE

Transformação Digital & Compliance, Como não travar a Inovação?



THE
DEVELOPER'S
CONFERENCE



Cyber
Security
Girls



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.

Agenda



THE
DEVELOPER'S
CONFERENCE

➤ **Conceitos: Dados e Informações**

- *Inovação , Disrupção*
- *Transformação Digital*
- *UX+ Jobs To be Done*
- *Usable Security*

➤ **Contexto da LGPD**

- *Objetos e Operações*
- *Papéis, Direitos e Deveres*

➤ **Arquiteturas– Conceito e Contextos**

- *Papéis*

➤ **Como Não Travar a Inovação?**

- *Princípios*

- *Boas Práticas by Design e By Default*
- *Contribuições das Governanças para Inovação e Compliance*

➤ **Referências**

Conceitos: Dados e Informações

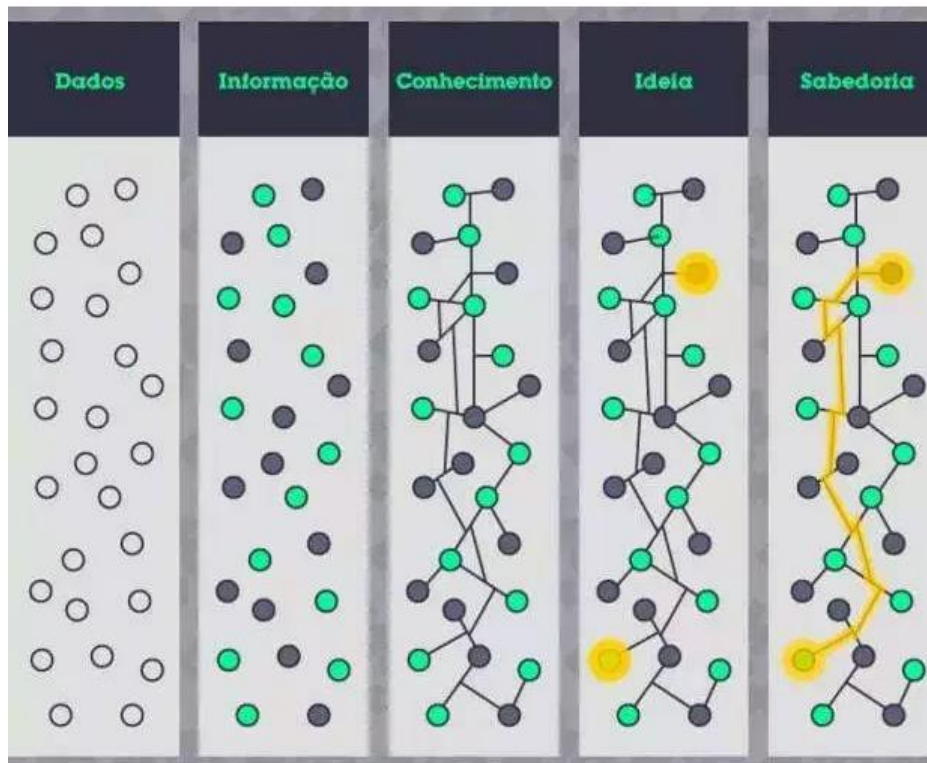


THE
DEVELOPER'S
CONFERENCE

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:

A 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. São dados dotados de relevância e propósito. Exige consenso em relação ao significado, exige necessariamente a mediação humana.

Conceitos: Inovação



“é um *substantivo feminino*, ação ou efeito de inovar. Por extensão, aquilo que é novo, coisa nova, novidade.” Google

“Inovação é um Estado de Espírito”

Conceitos: Inovação



Many Types of Innovation



Selling Motion



Tools



Market



Technology
and Product



Solutions



Business
Model



Process

”A palavra é derivada do termo latino *innovatio*, e se refere a uma ideia, método ou objeto que é criado e que pouco se parece com padrões anteriores.” Wiki

Conceitos: Disrupção



“é um *substantivo feminino*,
e as definições são:
“interrupção do curso
normal de um processo.

Eletricidade,
restabelecimento brusco de
corrente elétrica, causando
faíscas e intenso gasto da
energia acumulada.“Google

Conceitos: Transformação Digital



THE
DEVELOPER'S
CONFERENCE



” pode ser definida como um fenômeno que incorpora o uso da tecnologia digital às soluções de problemas tradicionais. Assim, abrange mudanças procedurais em diversos âmbitos de uma sociedade, isto é, essa transformação modifica o paradigma da utilização da tecnologia, por exemplo, das seguintes áreas: governo, economia, mercado de trabalho, educação, medicina, artes, ciência, comunicação global, entre outros.” Wiki

Conceitos: UX – User Experience



THE
DEVELOPER'S
CONFERENCE

“é o conjunto de elementos e fatores relativos à interação do usuário com um determinado produto, sistema ou serviço cujo resultado gera uma percepção positiva ou negativa. O termo foi utilizado pela primeira vez por Donald Norman na década de 1990. Segundo Norman, UX envolve não somente aspectos relacionados ao design (hardware, software, interface, usabilidade, facilidade de busca etc), mas também destaca os aspectos afetivos e experienciais, significativos e valiosos de interação humano-computador e propriedade do produto.

A experiência do usuário é de natureza subjetiva, pois é sobre a percepção e pensamento individual no que diz respeito ao sistema. Ela é também dinâmica, pois é constantemente modificada ao longo do tempo, devido à evolução das circunstâncias e inovações.” WIKI

Conceitos: Jobs to Be Done



A teoria do trabalho a ser realizado é melhor definida como um grupo de princípios que explicam como tornar o marketing mais eficaz e a inovação mais previsível, concentrando-se no trabalho a realizar do cliente. **A teoria é baseada na noção de que as pessoas compram produtos e serviços para fazer um "trabalho".** j-t-b-d.com

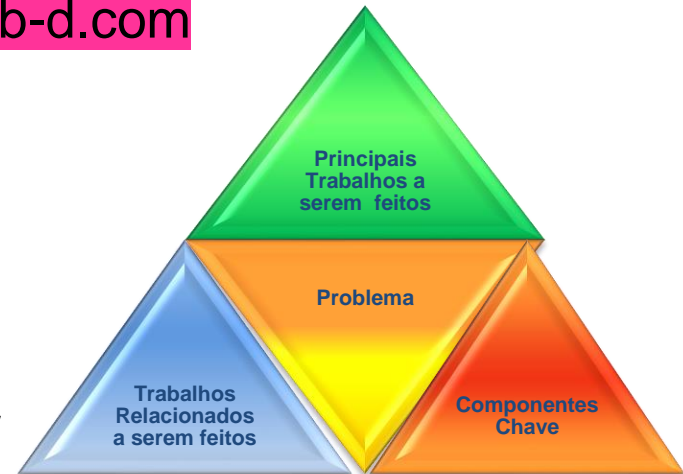
Estrutura de uma Declaração de Emprego:

Gerenciar minhas Finanças Pessoais em Casa

↑
Verbo de Ação

↑
Objeto da Ação

↑
Esclarecedor Contextual



Conceitos: Usable Security



THE
DEVELOPER'S
CONFERENCE

SEGURANÇA E USABILIDADE ENTRAM EM HARMONIA QUANDO UM SISTEMA INTERPRETA CORRETAMENTE OS DESEJOS (EXPECTATIVAS) DO USUÁRIO

Designing Effective Security UX: If It's Not Usable, It's Not Secure


Security / Privacy




Usability




Usable Security & Privacy




 Confidentiality
 Integrity
 Availability

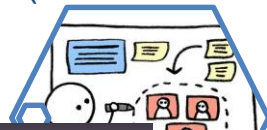
 Usage
 Fair Information Policy Practice

 Effectiveness
 Efficiency
 Accuracy

 Learnability
 Memorability
 Satisfaction

 Least Surprise
 Good Protection
 Consistent Placement of Controls

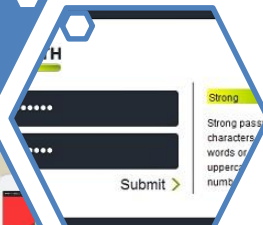
 Standardization of Policies
 Consistent Vocabulary
 Consistent Placement of Controls



DECISÕES
BASEADAS NAS
AÇÕES DO
USUÁRIO –
DESIGN DE
INTERAÇÃO

USABILIDADE:
MELHORAR O
ACESSO ÀS
OPERAÇÕES
COM EFEITOS
DESEJÁVEIS

ER OS
RIOS:
SÕES
ARES



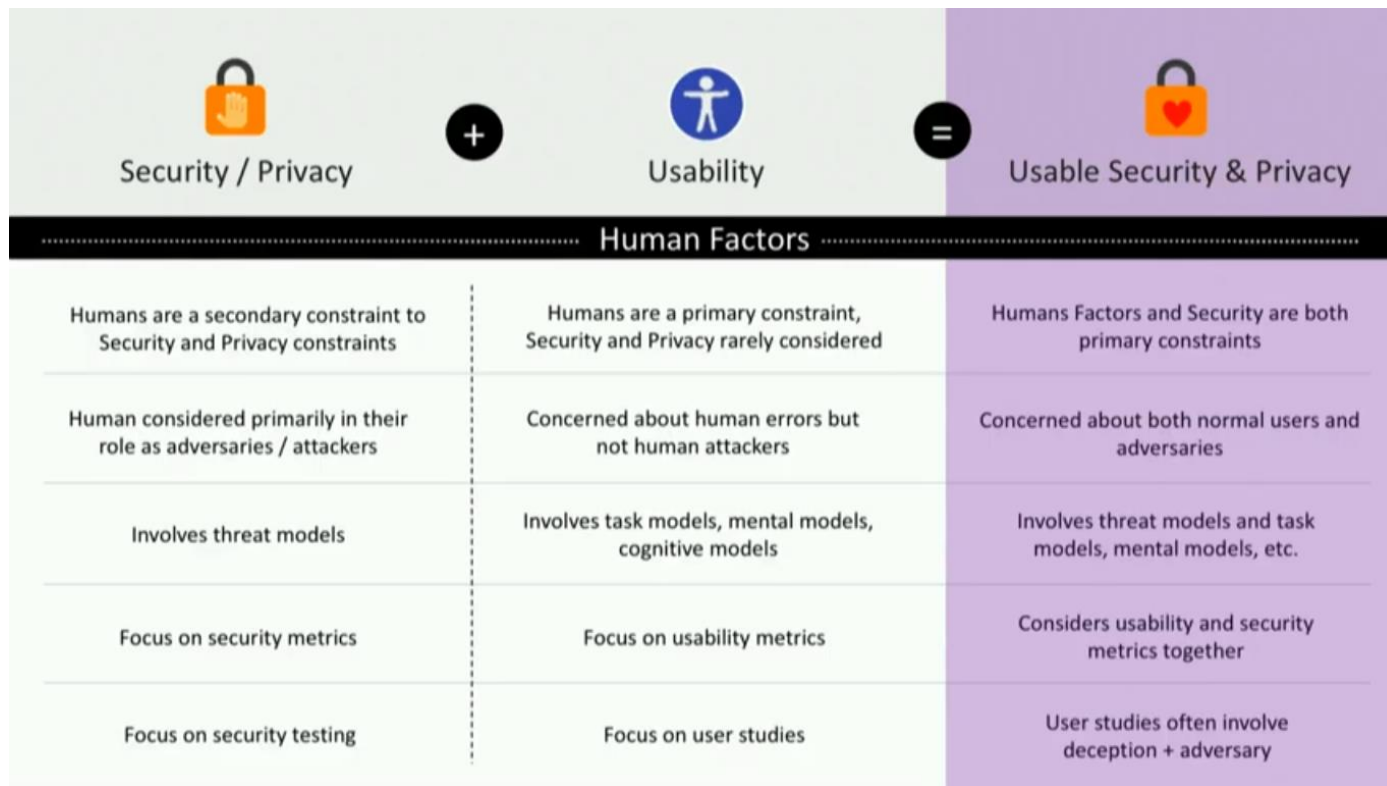
SEGURANÇA
EMBARCADA NO
DESIGN -
IMPLICITA SEM
GERAR
TAREFAS A MAIS



Conceitos: Usable Security



THE
DEVELOPER'S
CONFERENCE



Arquiteturas: Conceitos



- A ISO / IEC 42010: 2007 define “arquitetura” como:
- “A organização fundamental de um sistema, incorporada em seus componentes, suas relações uns com os outros e ao meio ambiente, e os princípios que governam seu design e evolução ”.
- O TOGAF abrange e estende essa definição. No TOGAF, “arquitetura” tem dois significados dependendo do contexto:
 - 1. Uma descrição formal de um sistema, ou um plano detalhado do sistema em um nível de componente para orientar sua implementação
 - 2. A estrutura dos componentes, suas inter-relações e os princípios e diretrizes governando seu design e evolução ao longo do tempo

Arquiteturas: Contexto



Negócios



A estratégia de negócios, governança, organização e principais processos e negócios. Abrange objetivos de negócios, funções ou recursos de negócios, funções e processos de negócios, etc.



Dados



A estrutura dos ativos e dados de dados lógicos e físicos de uma organização recursos de gestão. As estruturas de dados usadas por uma empresa e / ou seus aplicativos. Descrições de dados armazenados e em movimento. Mapeamentos desses artefatos de dados para qualidades de dados, aplicativos, locais etc.



Aplicações



Um modelo para os sistemas de aplicativos individuais a serem implantados, interações e seus relacionamentos com os principais processos de negócios da organização. 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.



Tecnológica

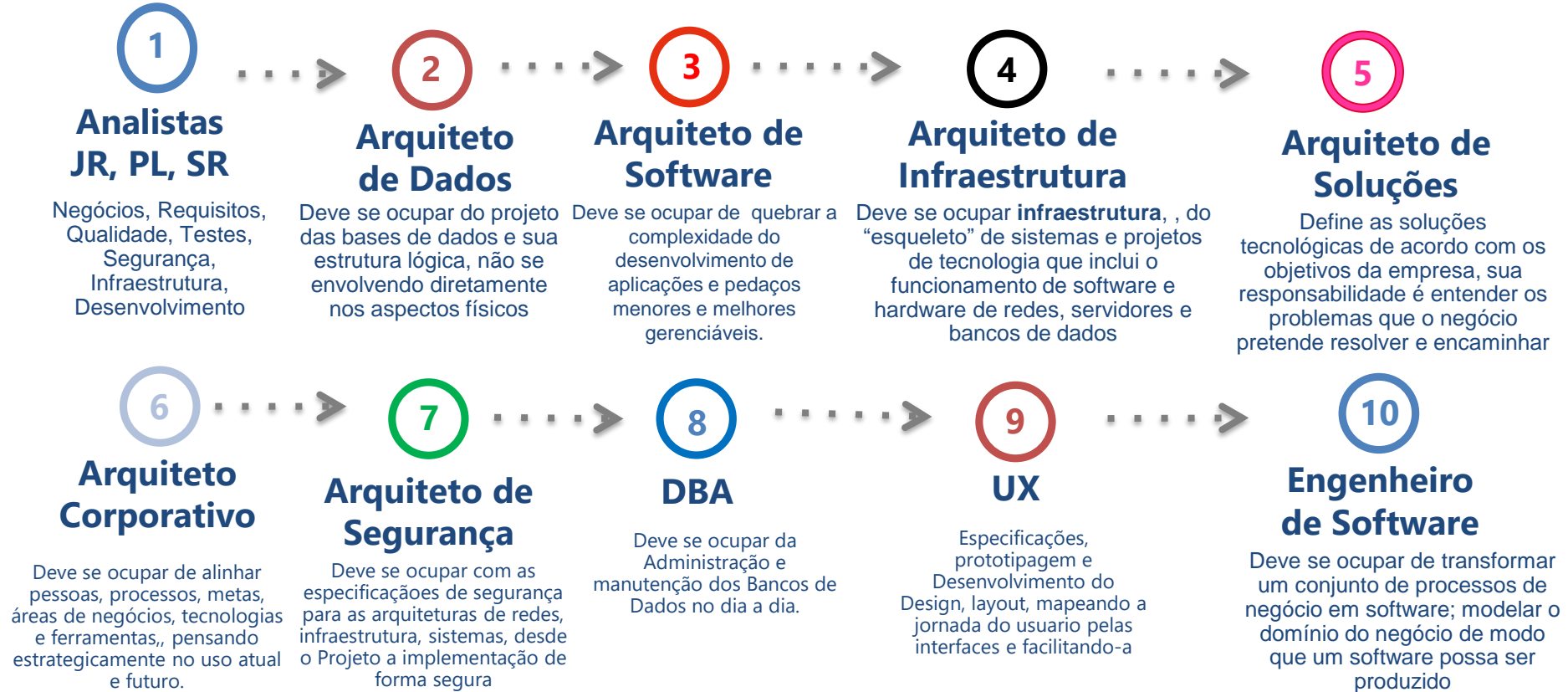


Os recursos lógicos de software e hardware necessários para suportar a implantação de serviços de negócios, dados e aplicativos. Isso inclui infraestrutura de TI, middleware, redes, comunicações, processamento e padrões. Estrutura e comportamento da infraestrutura de TI.

Arquiteturas: Papéis (Alguns)



THE
DEVELOPER'S
CONFERENCE



Contexto da LGPD

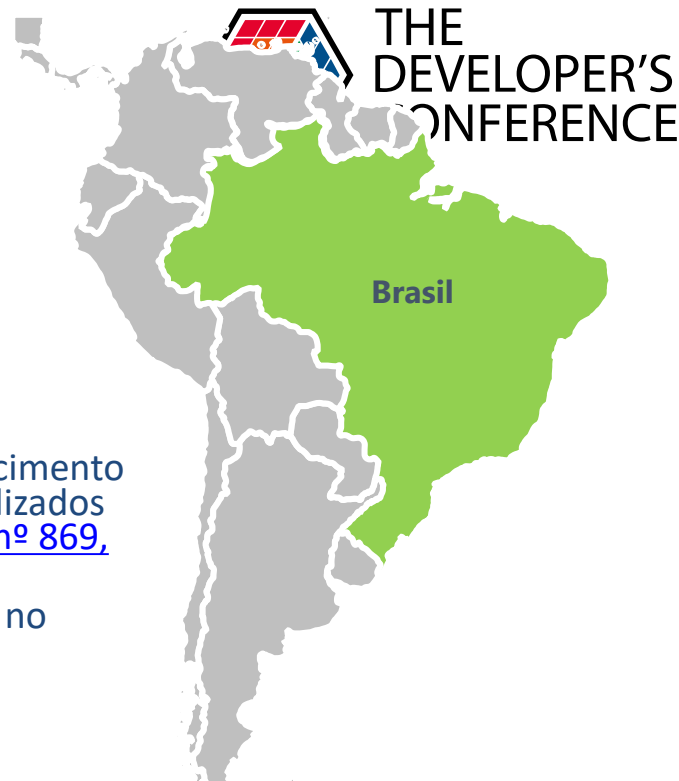
Art.3

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.

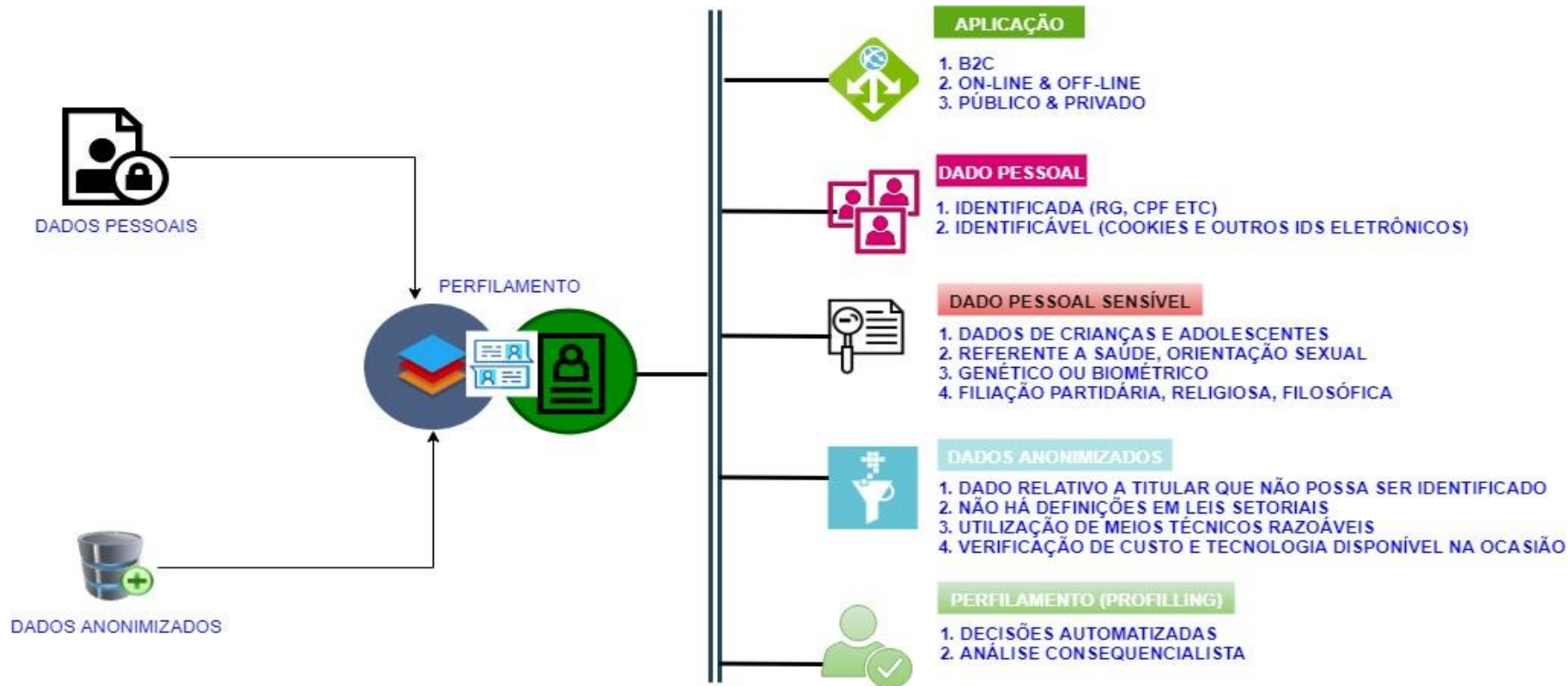
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.



Contexto da LGPD: Objetos e Escopo



THE
DEVELOPER'S
CONFERENCE

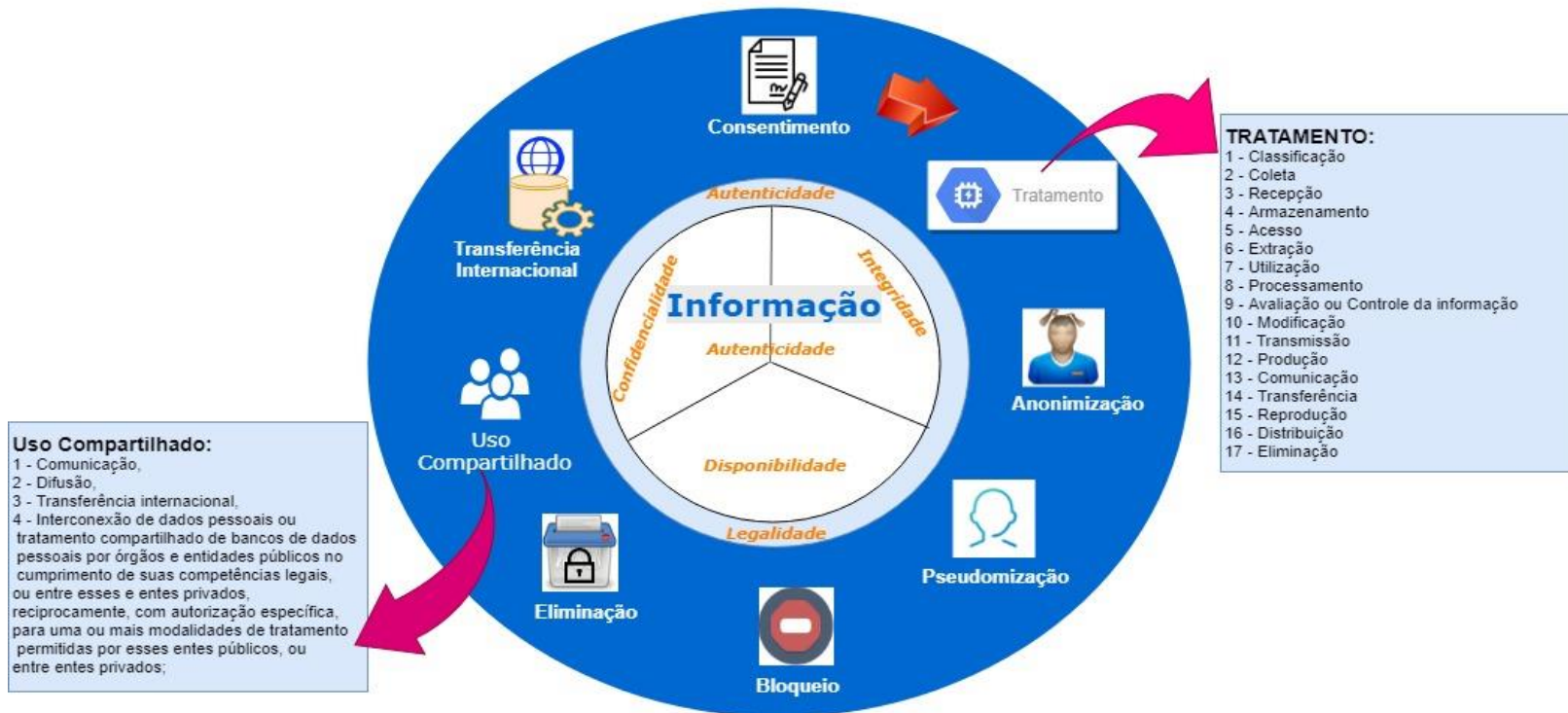


Contexto da LGPD: Operações



THE
DEVELOPER'S
CONFERENCE

Ciclo de Operações da Informação - LGPD



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



Quando o tratamento de Dados pessoais *for Condição para o fornecimento de produto ou serviço ou para o exercício de direito*, o Titular deverá ser informado com destaque sobre este fato:

O Consentimento:

- Deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas;
- Será considerado nulo caso as informações fornecidas ao Titular tenham conteúdo enganoso ou abusivo, ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca;
- Caso seja dado por escrito, deverá constar de cláusula destacadas das demais cláusulas contratuais;
- Vedado o tratamento de dados pessoais mediante Vício de Consentimento;

Contexto da LGPD: Deveres



THE
DEVELOPER'S
CONFERENCE



DPO

DATA
PROTECTION
OFFICER -
"ENCARREGADO"



DPIA

RELATÓRIO DE
IMPACTO



R.A

REGISTRO DAS
ATIVIDADES



P.DES

PRIVACY
BY DESIGN



CIRT

CENTRO DE
TRATAMENTO E
RESPOSTAS A
INCIDENTES -
"NOTIFICAÇÃO"



S.DES

SECURITY BY
DESIGN



GOV

GOVERNANÇA
DE DADOS



GRC

GOVERNANÇA
RISCOS E
COMPLIANCE



S.I

SEGURANÇA DA
INFORMAÇÃO



PADRÃO

PADRONIZAÇÃO
DE FORMATOS
DE ARQUIVOS
PARA ACESSO
A INFORMAÇÃO

Como Não Travar a Inovação?



THE
DEVELOPER'S
CONFERENCE



Como Não Travar a Inovação?



THE
DEVELOPER'S
CONFERENCE



NÃO FAÇA DA SEGURANÇA E
QUESTÕES DE COMPLIANCE UM
PUXADINHO NO FINAL DO
PROJETO...

OU UM DEPOIS “ A GENTE VÊ
DEPOIS, SE PEGAR” ...



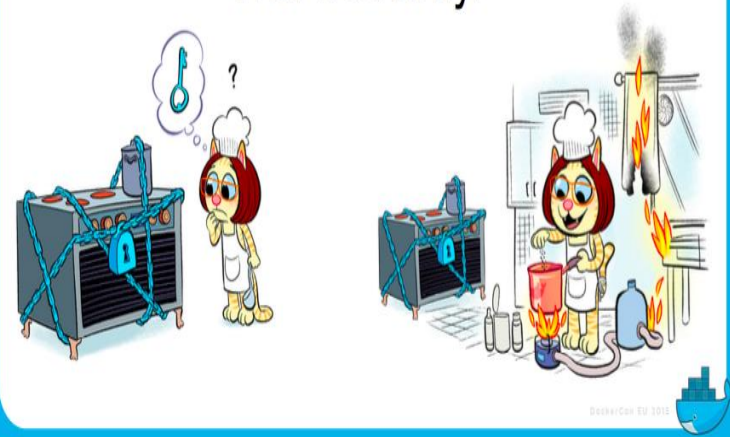
Como Não Travar a Inovação?



THE
DEVELOPER'S
CONFERENCE



Unusable security is
not security.



Princípios: Data Protection



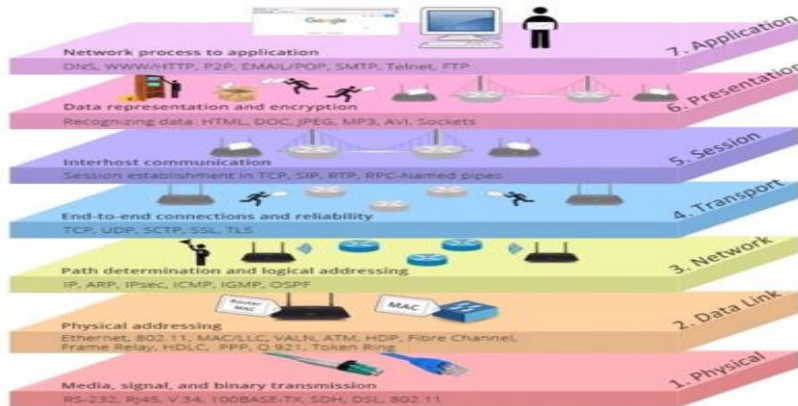
BY DESIGN:

“ 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 ESPECIFICO 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



Princípios: Privacy by Design e by Default



THE
DEVELOPER'S
CONFERENCE



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.

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



THE
DEVELOPER'S
CONFERENCE

1 - Minimizar a superfície de área de ataque

2 - Estabelecimento de Padrões

3 - Princípio do Menor Privilégio

4 – Princípio da Defesa em Profundidade

5 – Falhar com Segurança

6 - Não Confie nos Serviços

7 - Separação de deveres

8 - Evitar a segurança por obscuridade

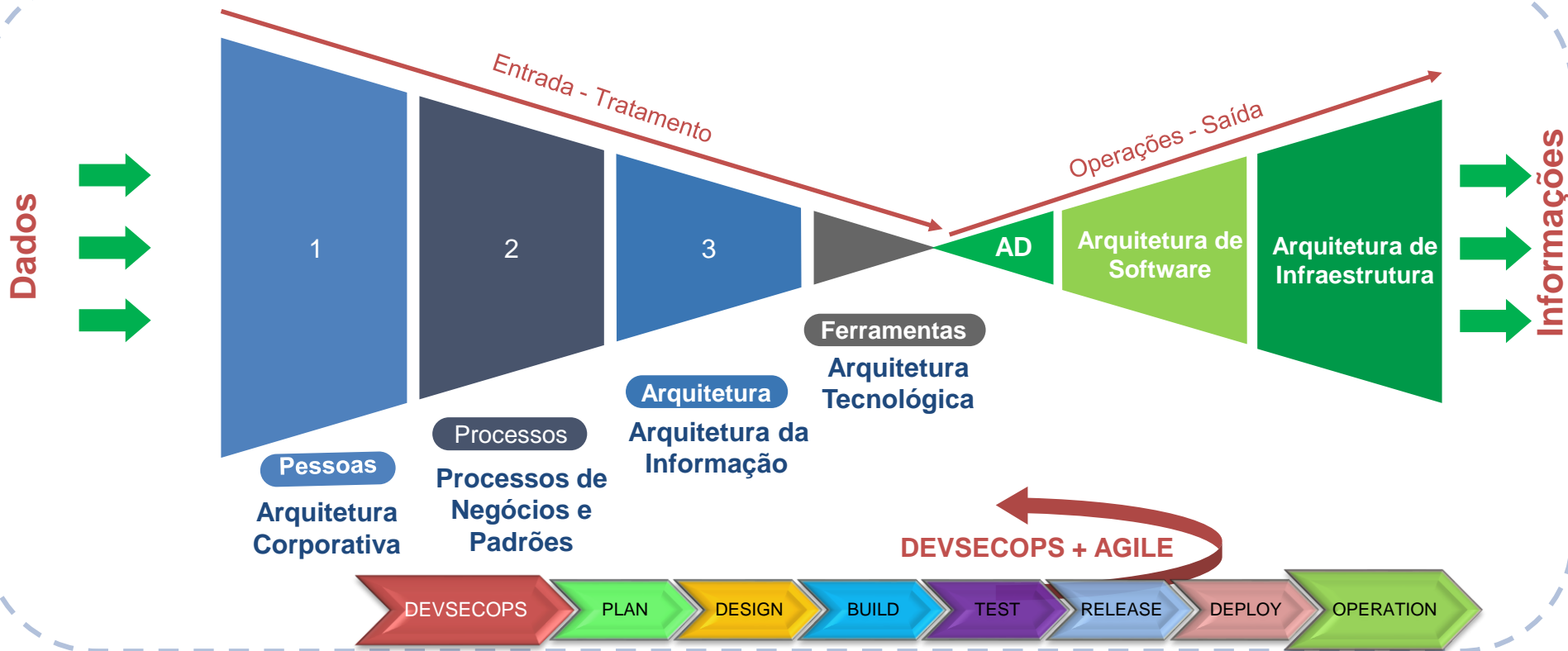
9 - Mantenha a Segurança simples

10 - Correção de Problemas de Segurança da maneira correta

Boas Práticas: by Design e by Default



THE
DEVELOPER'S
CONFERENCE



Boas Práticas: by Design e by Default



THE
DEVELOPER'S
CONFERENCE

Pesquisar

Definir

Ideação

Prototipação

Teste

Implementação

Eficácia

Eficiência

Envolvimento

Tolerância a erro

Facilidade de

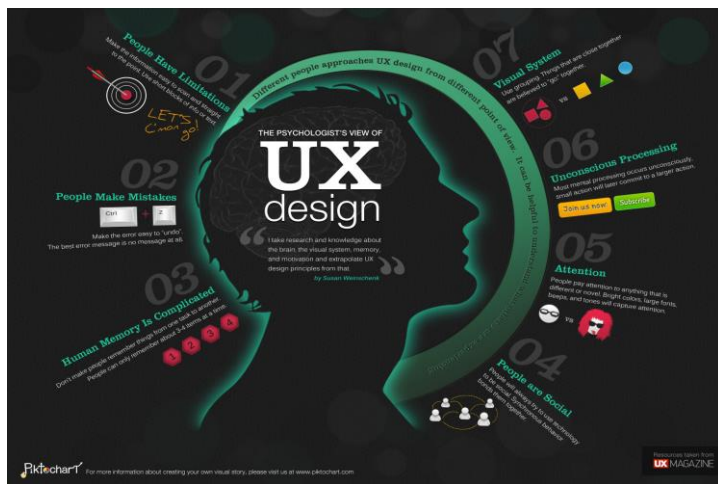
Aprendizado



Boas Práticas: by Design e by Default



THE
DEVELOPER'S
CONFERENCE



MÉTRICAS USABILIDADE

- VELOCIDADE
- EFICIÊNCIA
- FÁCIL APRENDIZADO (DIDÁTICO)
- FÁCIL MEMORIZAÇÃO
- PREFERÊNCIA DO USUÁRIO

UX METAS E MÉTRICAS

- FÁCIL DE ACHAR
- CREDIBILIDADE
- UTILIDADE
- ACESSIBILIDADE
- DESEJÁVEL: PROVER VALOR AO CLIENTE
- USABILIDADE
- ISO/IEC 9241-210:2019 HCD- ERGONOMIA DE SISTEMA DE INTERAÇÃO HUMANA

Boas Práticas: by Design e by Default



THE
DEVELOPER'S
CONFERENCE

PRIVACY AND
DATA
PROTECTION



Adotar uma abordagem de “PRIVACY FIRST” com todas as configurações padrão de sistemas e aplicativos;

Garantir que você não forneça uma opção ilusória para as pessoas relacionadas aos dados que você processará;

Não processe dados adicionais, a menos que o Titular decida que você pode;

Garantir que os dados pessoais não sejam automaticamente disponibilizados ao público ou terceiros, a menos que o Titular decida fazê-lo; e

Forneça às pessoas controles e opções suficientes para exercer seus direitos.

Boas Práticas: by Design e by Default



THE
DEVELOPER'S
CONFERENCE

Baseline de Informação

1 - Caso de uso – Definição de Estórias de Usuário

2 - Categorização dos Casos de Uso e Estórias do Usuário

3 - Detalhes da Estórias e Descrição dos Casos de Uso

Titulares dos Dados e Aplicações

4 - Aplicações Associadas com os Casos de Uso

5 - Titulares dos Dados associados aos casos de uso

Identificação e Gestão dos Dados, Técnicas e Base Legal

6 - Regulações – Leis

7 - Domínios e Proprietários

8 - Fluxo de Dados e Pontos de Contato

9 - Sistemas

Políticas, Controles e Serviços

10 - Controles

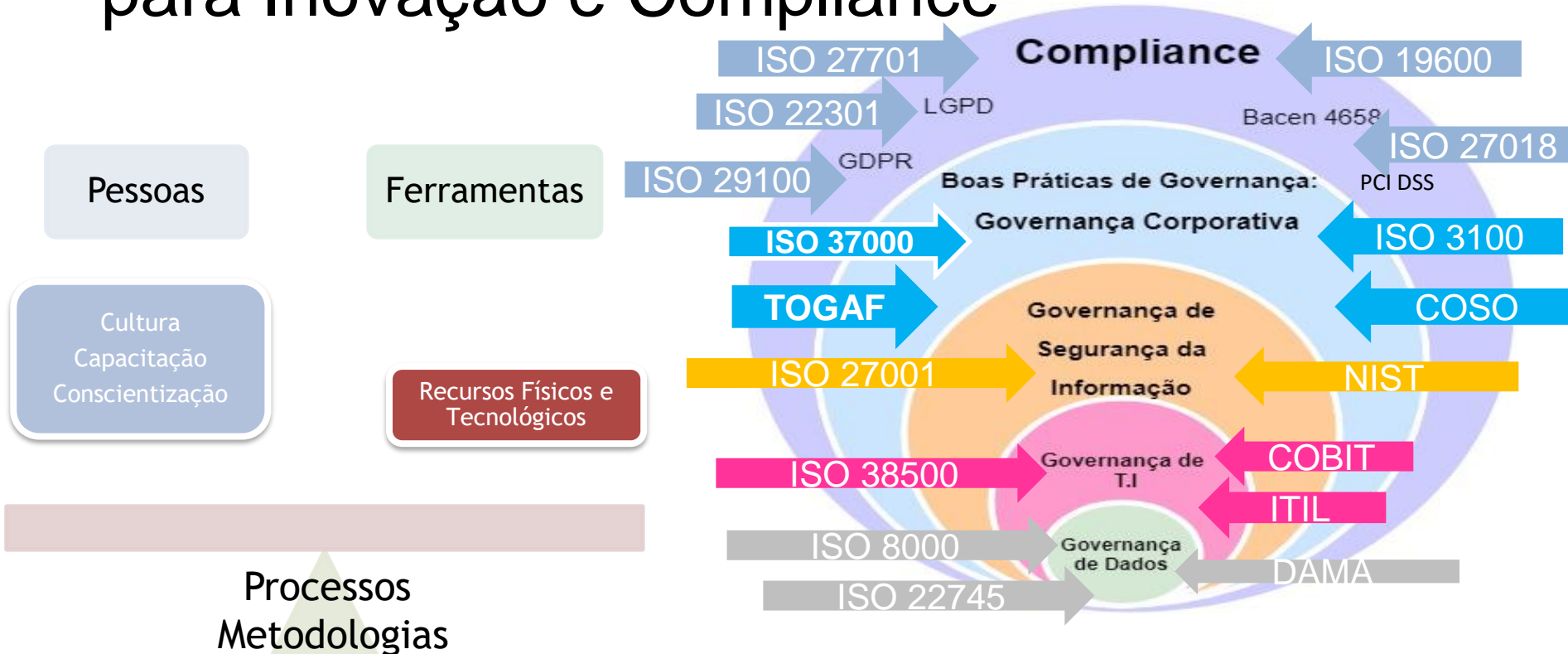
11 - Serviços

12 - Funções

Contribuições das Governanças para Inovação e Compliance



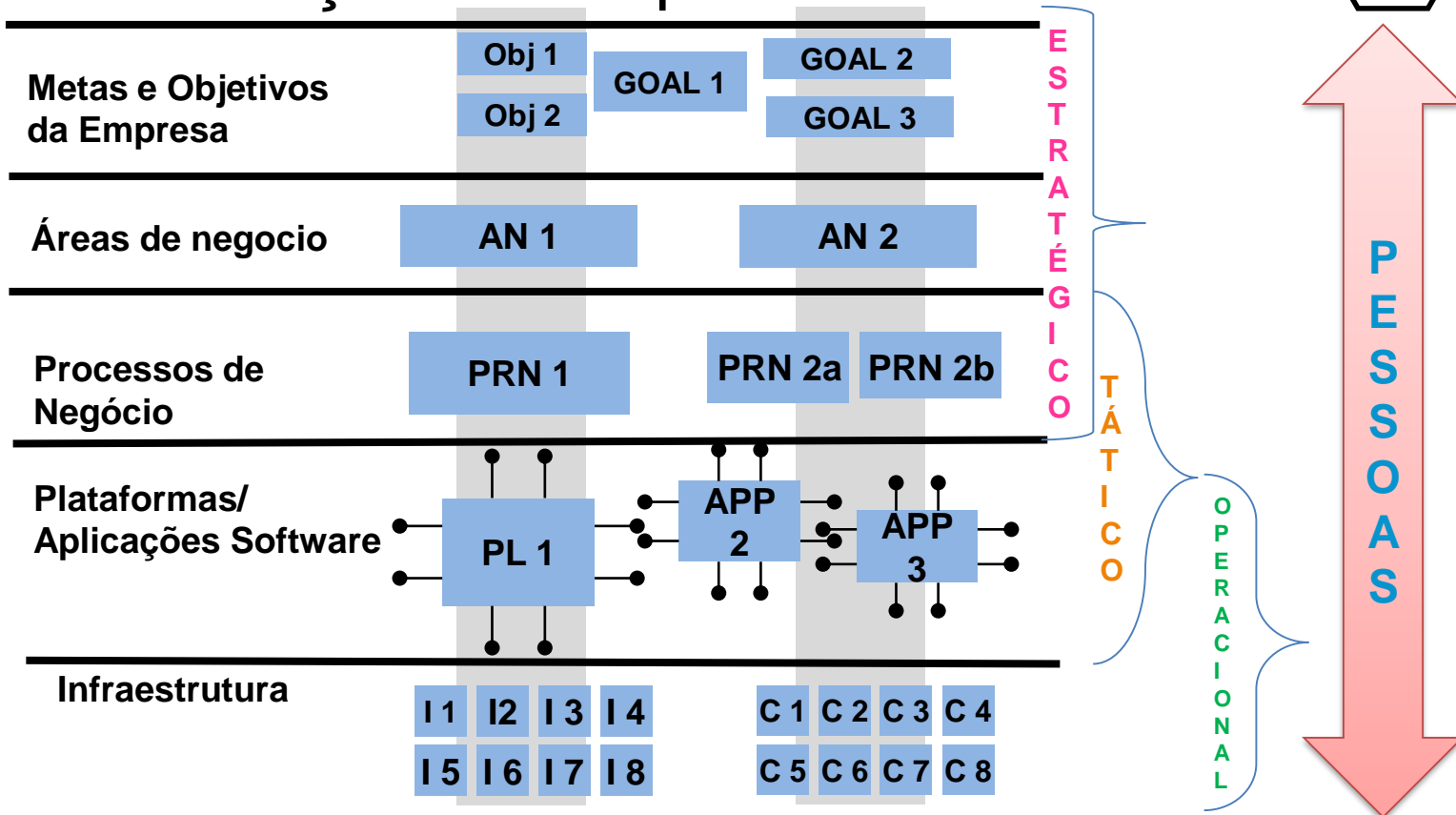
THE DEVELOPER'S CONFERENCE



Contribuições das Governanças para Inovação e Compliance



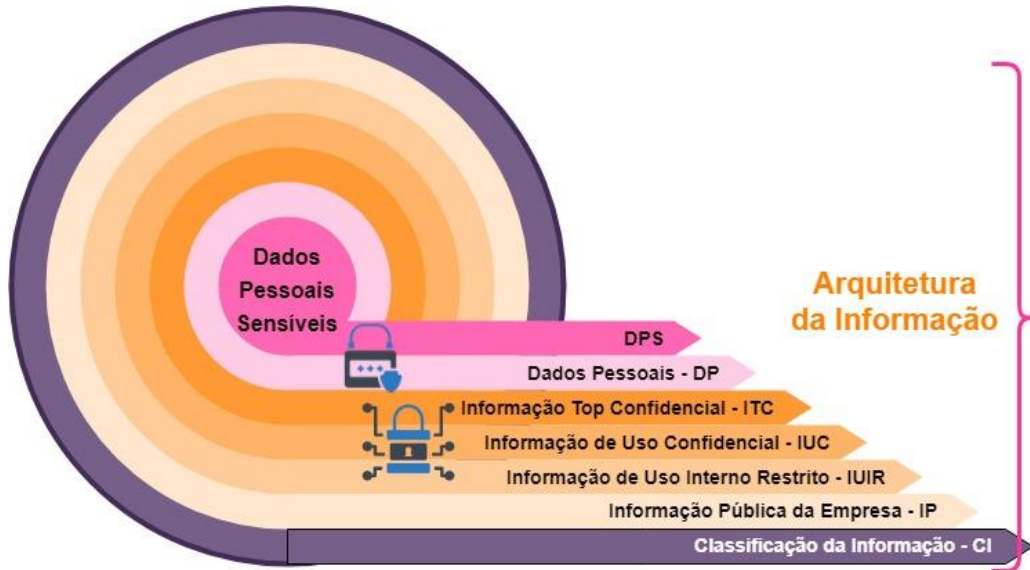
THE DEVELOPER'S CONFERENCE



Contribuições das Governanças para Inovação e Compliance



THE
DEVELOPER'S
CONFERENCE



Contribuições das Governanças para Inovação e Compliance



THE
DEVELOPER'S
CONFERENCE



Referências:



- > AGNER, Luiz. **Ergodesign e arquitetura de informação: trabalhando com o usuário**. Rio de Janeiro: Editora Quartet, 2ª 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://yourstory.com/2016/09/book-review-innovation-is-a-state-of-mind-innovation-is-good-business-but-it-can-also-be-good-life-new-book-gives-creative-tips>
- > <http://www.innovationmatrix.com/news/always-look-bright-side-ai>
- > <https://weheartit.com/entry/289642967>
- > <https://www.christenseninstitute.org/disruptive-innovations/>
- > <https://jobs-to-be-done.com/the-5-tenets-of-jobs-to-be-done-theory-ba58c3a093c1>
- > https://pt.wikipedia.org/wiki/Arquitetura_de_dados
- > <https://www.opengroup.org/togaf>
- > https://pt.wikipedia.org/wiki/Arquiteto_de_software
- > <https://www.linkedin.com/pulse/afinal-o-que-%C3%A9-arquitetura-de-solu%C3%A7%C3%B5es-ti-e-qual-nas/>
- > <https://www.slideshare.net/ulfmattsson/cloud-data-governance-risk-management-and-compliance-ny-metro-joint-cyber-security-conference-2014>
- > <https://www.linkedin.com/pulse/20140613155546-11856035-togaf-the-open-group-architecture-framework/>

KA-PING YEE. Artigo: “Guidelines and Strategies for SecureInteractionDesign”. Cap.30 pag 253 -280, 2005

<https://rebit.org.in/whitepaper/usable-security-identity-and-authentication>

<https://www.youtube.com/watch?v=DM8iYTBPVhQ>

<https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf>

<http://giftpicis.pw/Fail-4-Plumbing-Humor-or-should-we-say-quotpotty-humor-t.html>

<https://twitter.com/kasimerkan/status/630892630629613568>

<https://www.interaction-design.org/literature/article/an-introduction-to-usability>

<https://usabilla.com/blog/10-best-ux-infographics-2/>

<http://userexperienceproject.blogspot.com/2007/04/user-experience-wheel.html>

<http://www.gdprtoons.com/2017/10/gdpr-will-impact-many-us-businesses-by.html>

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>

<https://pbd.cs.kau.se/courses/24/pages/oasis-privacy-management-privacy-by-design-for-software-engineering>

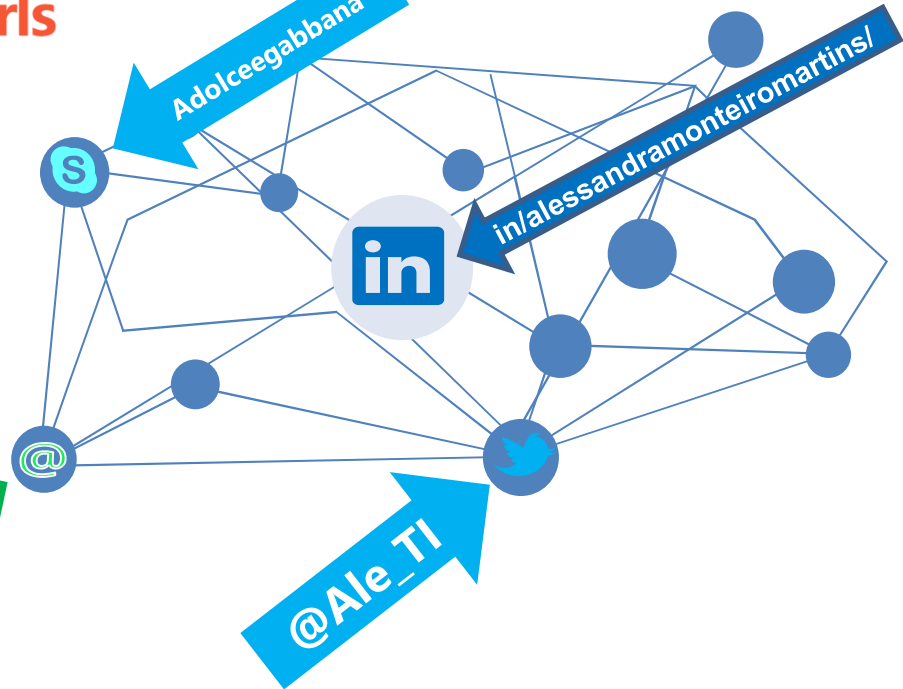
<https://www.anywherexchange.com/2017/12/azure-information-protection-end-user.html>

https://www.google.com/imgres?imgurl=https%3A%2F%2Fmiro.medium.com%2Fmax%2F2420%2F1*kXhhMLj8NXKj7f0857rUUw.jpeg&imgrefurl=https%3A%2F%2Fmedium.com%2Fanielledesign%2Fpuxadinho-anielle-design9f4dd2d357a&docid=Nt2bPriYpDa6zM&tbnid=FCvjW8k8cGRPKM%3A&vet=10ahUKEwivh5rMkpLIAhWmLLkGHSdDCb4QMwhyKAYwBg..i&w=1210&h=1756&bih=576&biw=1366&q=puxadinho&ved=0ahUKEwivh5rMkpLIAhWmLLkGHSdDCb4QMwhyKAYwBg&iact=mr&uact=8



OBRIGADA

[monteiomartins@bol.com.br](mailto:monteimartins@bol.com.br)





THE DEVELOPER'S CONFERENCE