
OWASP
Chapter
São Paulo

OWASP Chapter São Paulo

Uma Visão de Arquitetura da Informação para LGPD

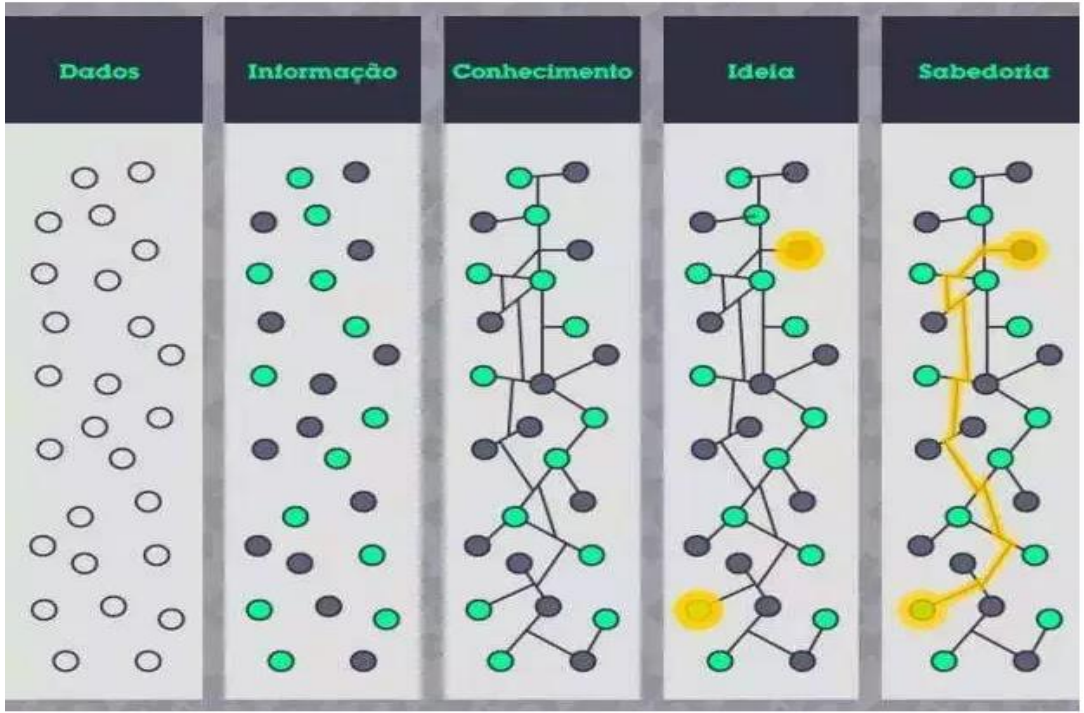
Roteiro:

1. Conceitos
2. A Lei
3. Princípios
4. Papéis e Responsabilidades
5. Como deveria ser sugestão de Organização…
6. Como poderá ser uma visão de Arquitetura…

1 –Conceitos: Dados X Informação

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.

1 –Conceitos: Governanças e Padrões

1 – 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.

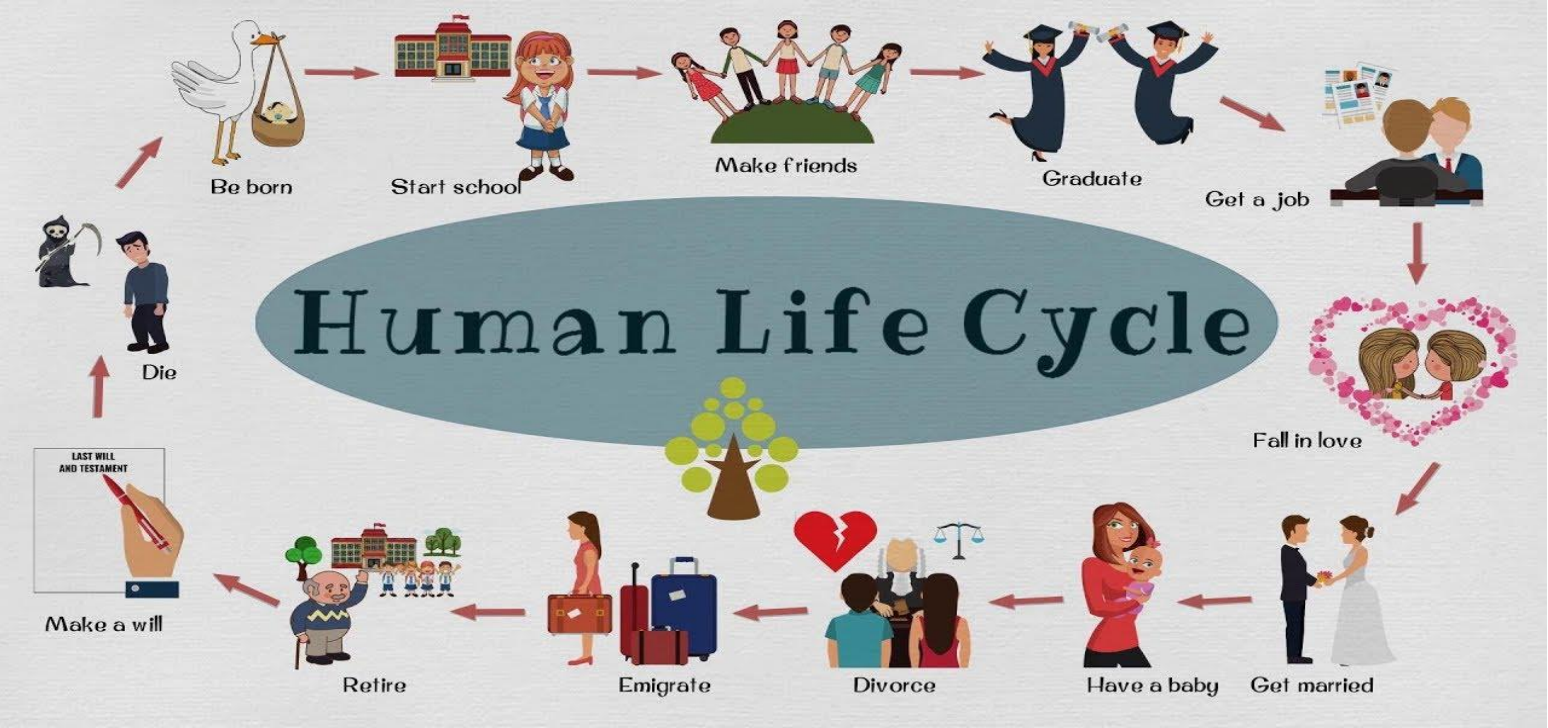
Aplicações

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

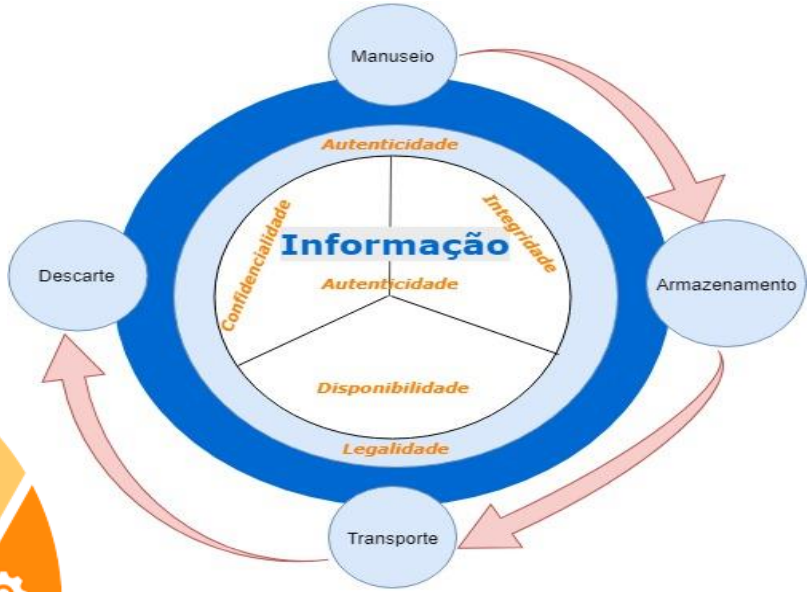
Estrutura e comportamento da infraestrutura de TI. Abrange os nós de cliente e servidor da configuração de hardware, os aplicativos de infraestrutura que são executados neles, os serviços de infraestrutura que eles oferecem aos aplicativos, os protocolos e as redes que conectam aplicativos e nós.

1 –Conceitos: Ciclos de Vida

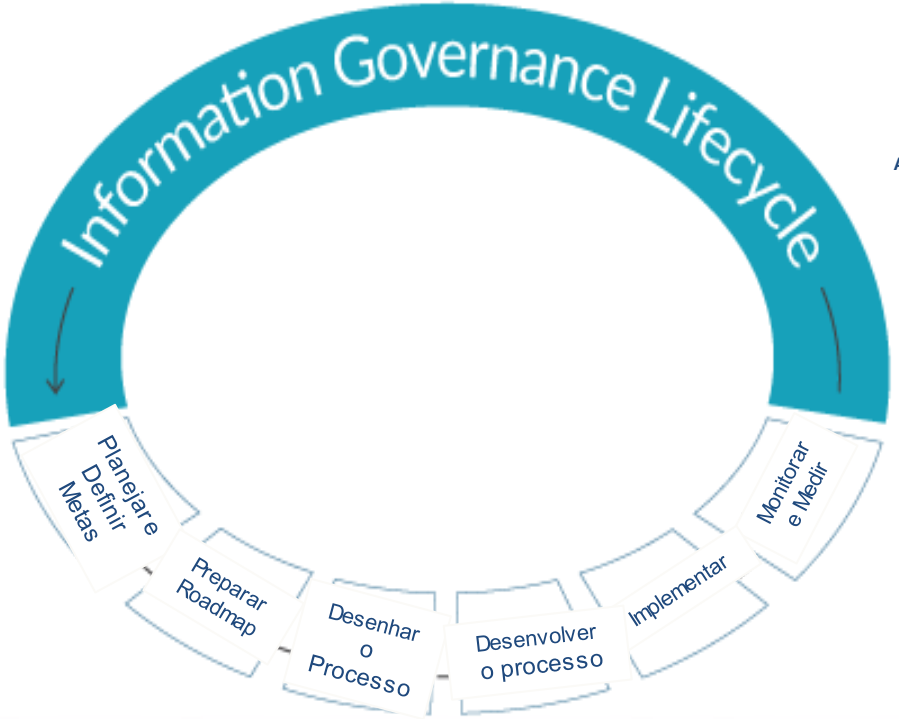


1 –Conceitos: Ciclos de Vida

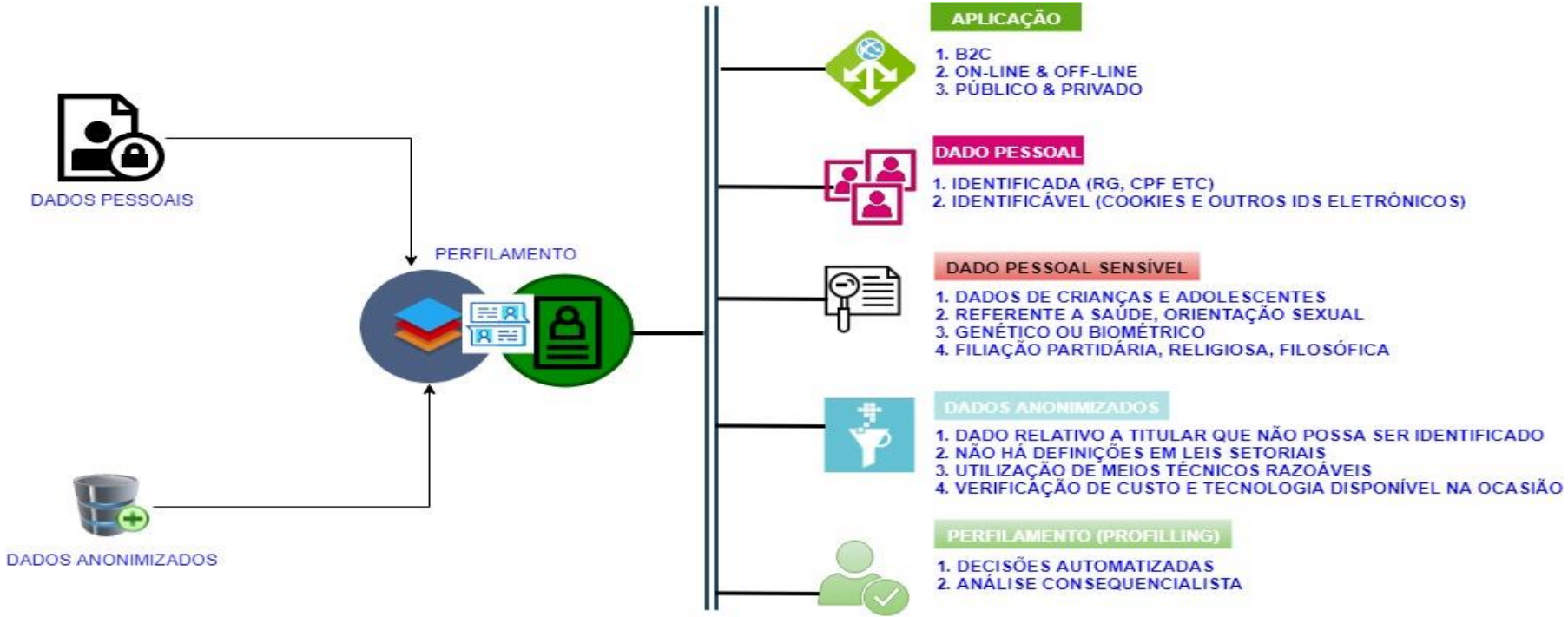
Ciclo de Vida do Dado



1 –Conceitos: Ciclos de Vida



2 – A Lei: Escopo



2 – A Lei: Contexto
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.

2 – A Lei Geral de Proteção de Dados: 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;

•**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;

Premissas:

Autorização

1 - Mediante fornecimento de consentimento pelo titular por escrito ou ou meio que manifeste a vontade do titular;

2 - Para atender os interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais;

3 - Mediante fornecimento de consentimento pelo titular ou responsável legal de forma específica e destacada para finalidades específicas;

10- Hipóteses de

Segurança Jurídica:

Validação de Modelos de Negócio,

Usos Secundário (Big Data):

Setor Privado - Legítimo Interesse;

Setor Público - Políticas Públicas;

Pesquisas sem fins lucrativos;

2 – A Lei Bases Legais: Dados Públicos

Art.7 § 3 º O tratamento de dados pessoais **cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.**

Art.7 § 4º É dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

Art.7 § 6º **A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei,** especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

2 – A Lei: Operações

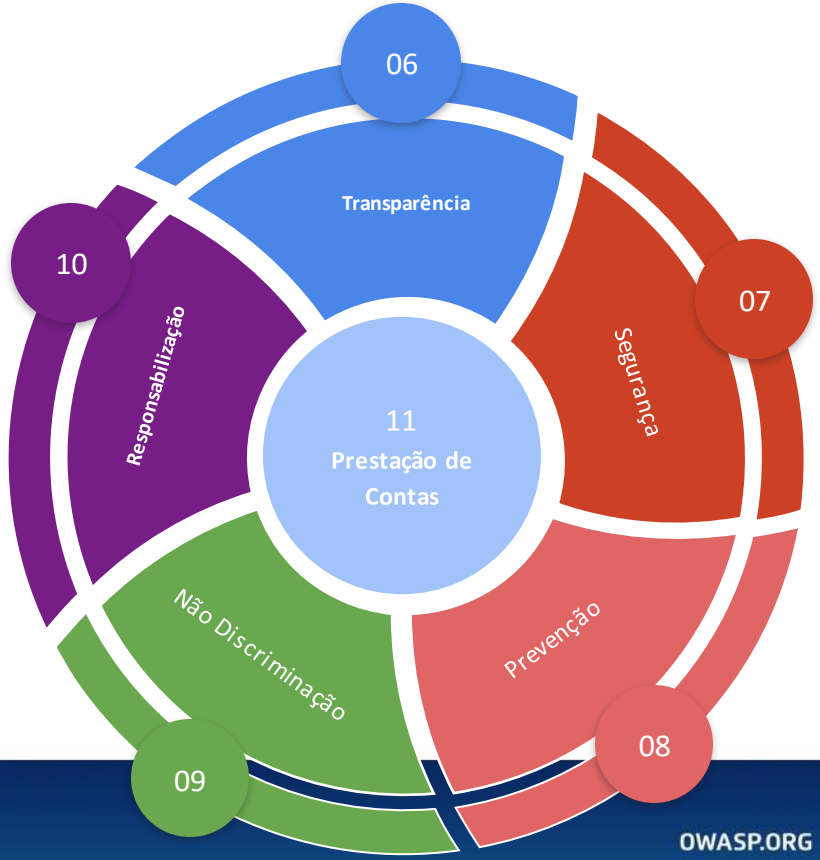
2 – A Lei: Direitos do Titular

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;**

- **Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.**

3 –Para o tratamento de dados devem ser observados os seguintes Princípios:



3 –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

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

3 –Princípio: Privacy by 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. 10 § 1º Quando o tratamento for baseado no legítimo interesse do controlador, **somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.**

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular **não podem ser utilizados em seu prejuízo.**

Art.8 § 3º É vedado o tratamento de dados pessoais **mediante vício de consentimento.**

§ 4º O consentimento deverá referir-se a finalidades determinadas, e **as autorizações genéricas para o tratamento de dados pessoais serão nulas.**

3 –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 seguros 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, ou seja, 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.

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

3 –Princípios: Security by Design

6. **Não Confie nos Serviços, ou seja, 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, ou seja, 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.

Art. 46 § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

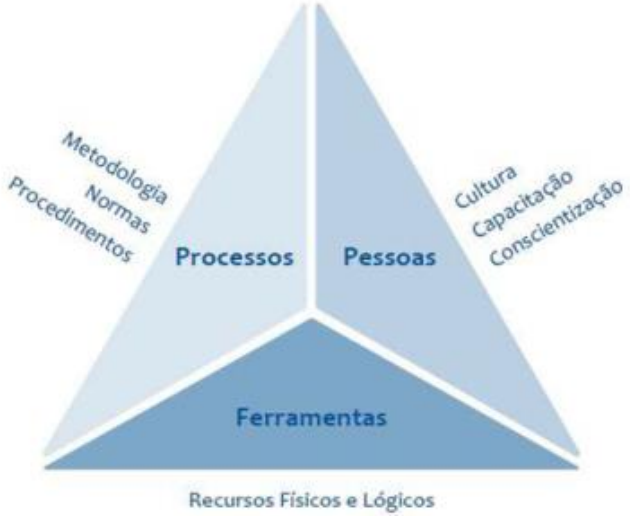
Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

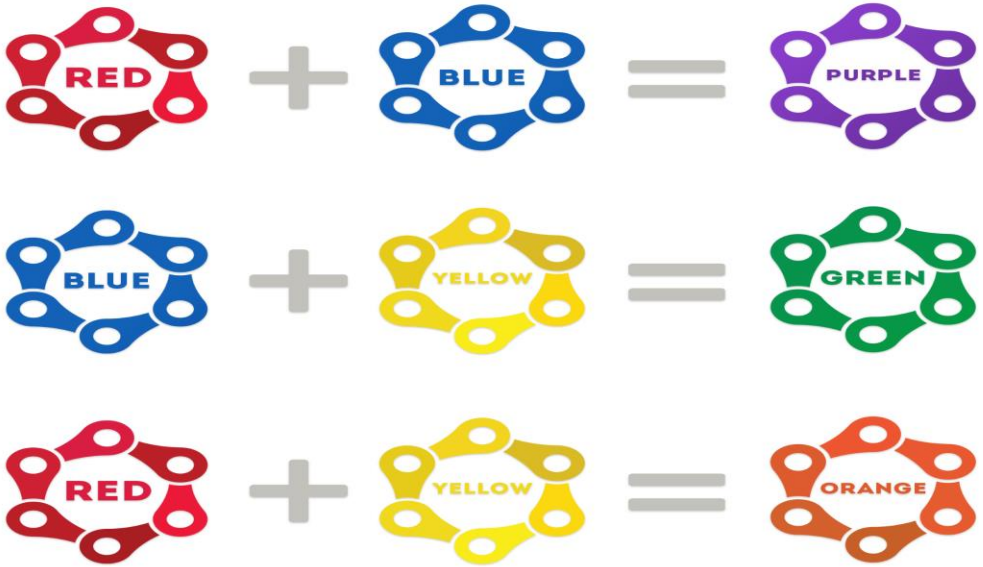
4 –Papéis e Responsabilidades

MATRIZ RACI							
Papéis	Titular (Pessoa Natural)	Controlador	Operador	Encarregado	Agentes de Tratamento	Orgão de Pesquisa	Autoridade Nacional
Operações | Responsabilidades							
tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;	C | I	R | A | C	R | A	I | A	R | A | C | I	R | A	A | C | I
anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;	I	R | A | C	R | C | I	I | A	R | A | C | I	R | A	A | I
consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;	C | I	R | A | I	R | C | I	I | A	R | A | C | I	R | A	A | I
bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;	C | I	R | A | I	R | A | I	I | A	R | A | C | I	R | A	A | I
eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;	C | I	R | A | I	R | A | I	I | A	R | A | C | I	R | A	A | I
transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;	C | I	R | A | C	R | C | I	I | A	R | A | C	R | A	A | C | I
Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;	C | I	R | A | C	R | C | I	I | A	R | A | C | I	R | A	A | C | I
Pseudominização	C | I	R | A | C	R | C | I	I | A	R | A | C	R | A	A | C | I
Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;	C | I	R | A | C | I	R | A	I | R	R | A | C	R | A	A | C | I

4 –Papéis e Responsabilidades: Deveres Agentes de Tratamento

4 –Papéis: uma visão de Pessoas + Processos + Ferramentas





4 –Papéis e Responsabilidades: uma visão de Times

Blue Team

Identificar

Gestão de Ativos

Gestão de Riscos

Controle de Danos

Resposta a Incidentes - SOC

MDM - DA

Segurança Defensiva

01

Orange Team

Proteger

Conscientização e Treinamento

Segurança de Dados

Procedimentos de Proteção

Codificação Segura

QA

02

Purple Team

Detectar

Identificar anomalias

Facilitar as Melhorias em defesa e detecção

Aprimorar as habilidades dos membros do time azul e vermelho – Heurísticas

ES, NOC

03

Red Team

Responder

Segurança Ofensiva

Ethical Hacker

Pentest

Exploração de Vulnerabilidades

ANS

04

Green Team

Recuperar

Melhorar a capacidade dos logs trabalhando com padrões e priorização de eventos importantes – AIOPS

Melhorar dados para forense digital e casos de resposta a incidentes

05

Yellow Team

Construir

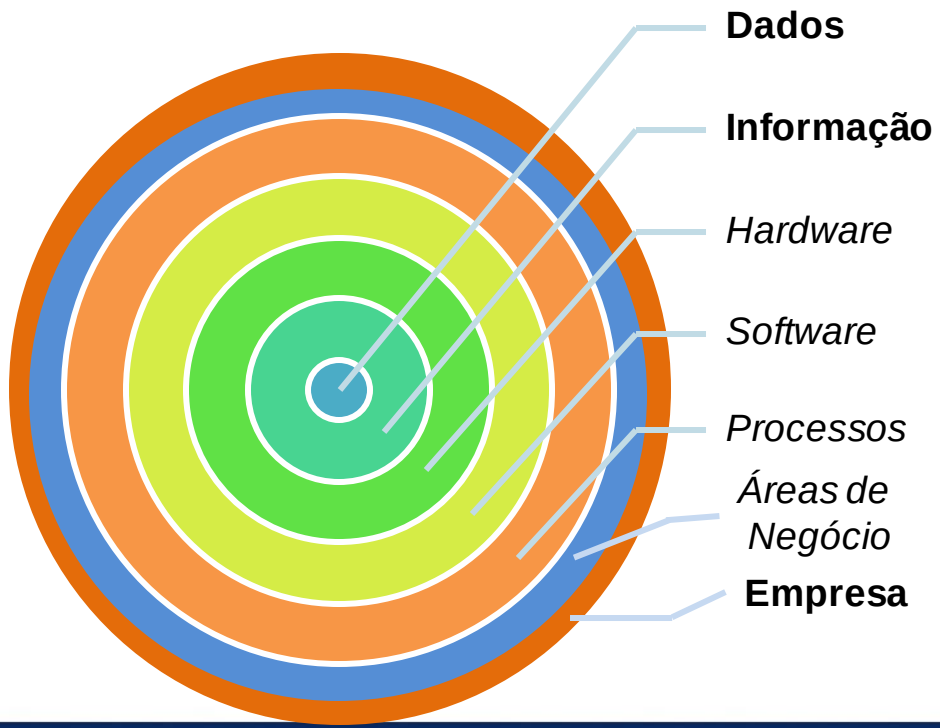
Arquitetos e Engenheiros de Software e Sistemas

Desenvolvedores de Aplicação

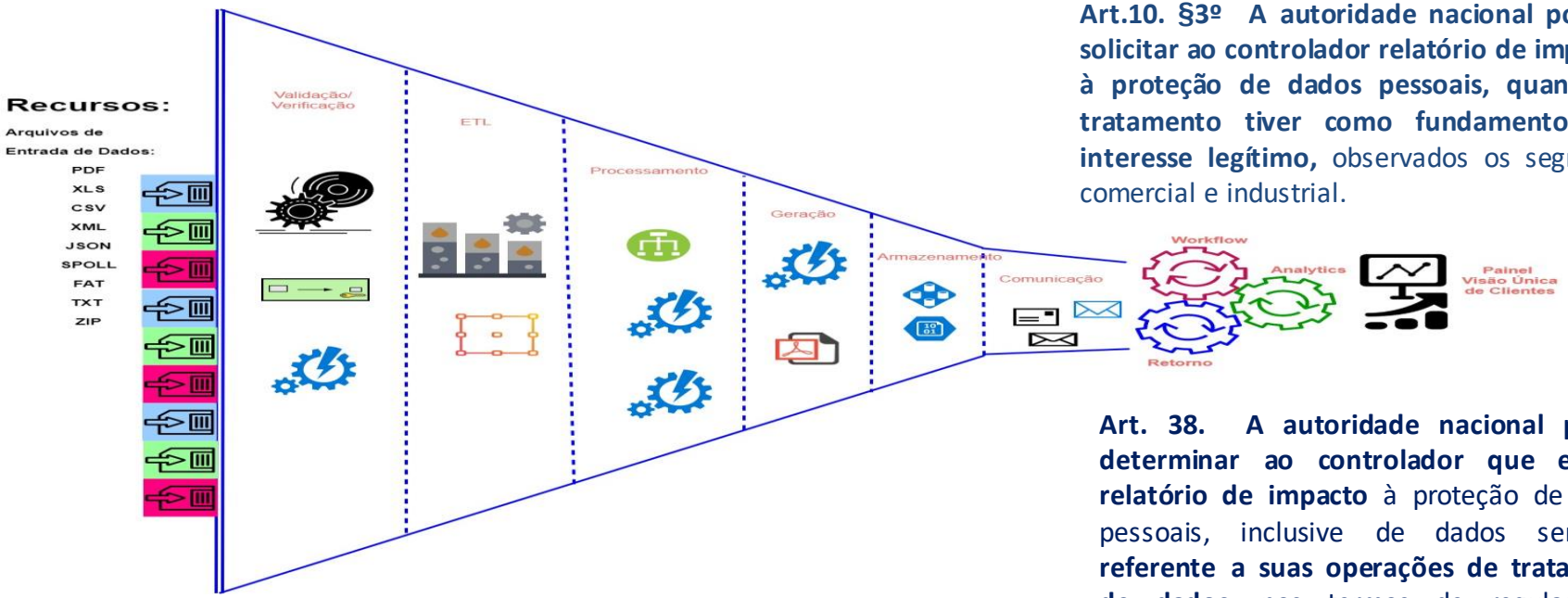
DBA , AN,

06

5 –Como deveria ser, sugestão de Organização



5 –Como deveria ser, sugestão de Organização



Art.10. §3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

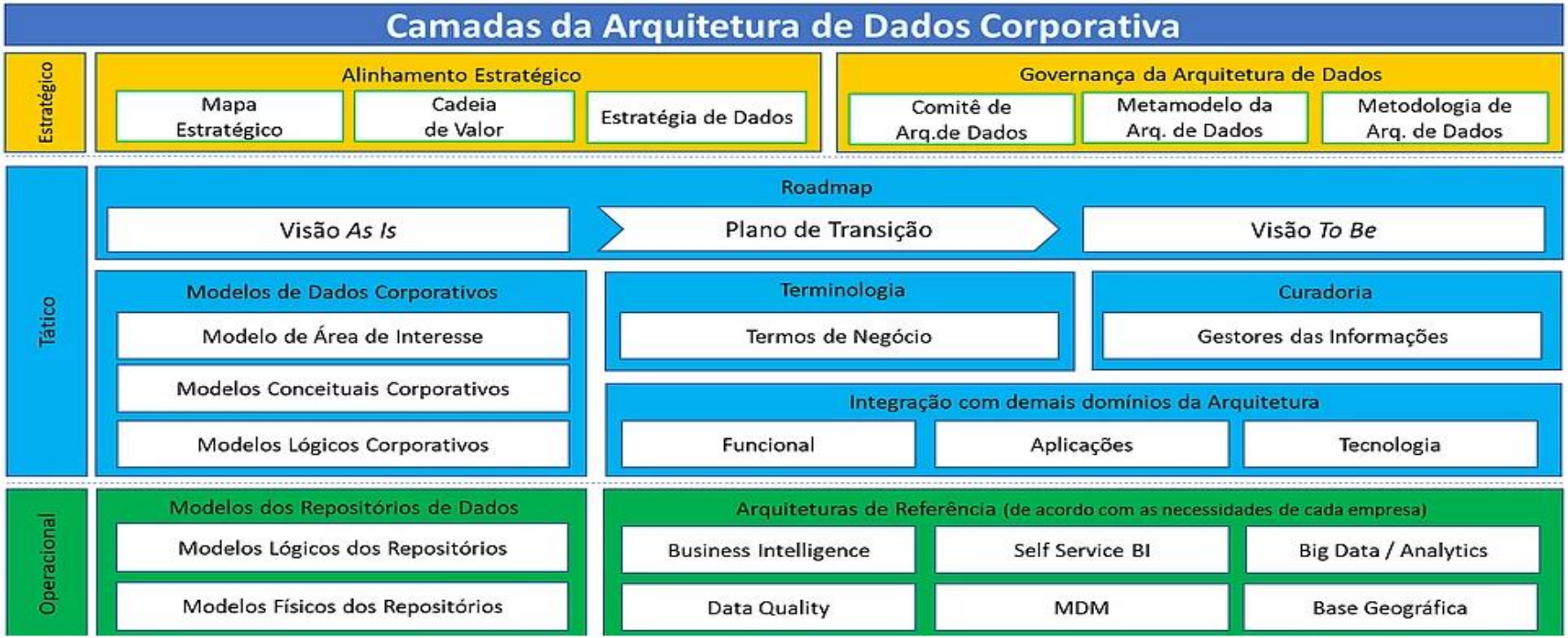
Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, **referente a suas operações de tratamento de dados,** nos termos de regulamento, observados os segredos comercial e industrial.

5 –Como deveria ser: sugestão de Organização

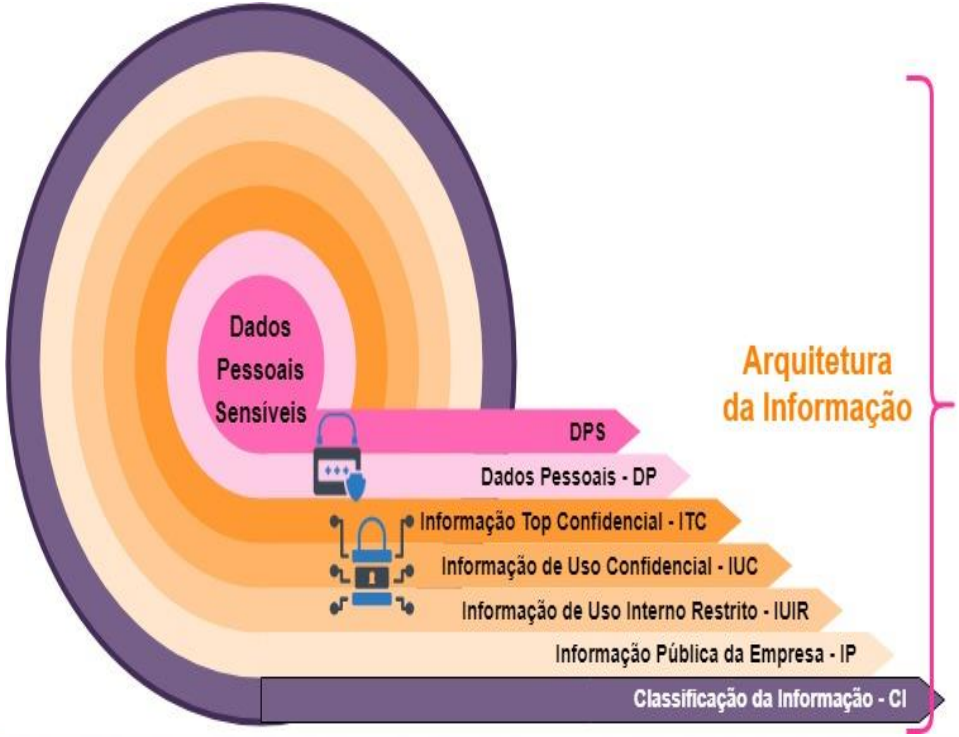
COMPLETUDE	Existe algum valor de dado faltando ou em um estado inutilizável?
CONFORMIDADE	Todas as expectativas de volume de dados estão conforme as especificações? Todos os valores estão no formato especificado?
CONSISTÊNCIA	Existem instâncias de dados provendo informações conflitantes sobre o mesmo 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?
DUPLICAÇÂO	Existem múltiplas representações desnecessárias do mesmo dado em diferentes ativos de dados?
INTEGRAÇÂO	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.

6 –Como poderá ser: uma visão de Arquitetura



6 –Como poderá ser: uma visão de Arquitetura



Arquitetura da Informação

Identificar

É preciso identificar os dados já existentes nos sistemas e bancos de dados existentes, identificar entradas, saídas, validações, verificar se possuem consetimento

Classificar

Após a identificação dos dados é preciso tipifica-los (on e off-line, Estruturado e Não estruturado), classifica-los quanto a sua sensibilidade e criticidade, e filtra-los quanto a sua origem e destino

Aplicar

Solicitar Consentimento aos Titulares Identificados e associa-lo aos seus respectivos dados
Aplicar Base Legal e Legítimo Interesse para os dados que não foi possível solicitar consentimento dos titulares, caso algum dado não seja passível do legitimo interesse ou base legal, segregar dados para avaliação jurídica e ANPD

Tratar

Tratar dados com as medidas de segurança necessárias conforme boas práticas e recomendações regulatórias.
Realizar as operações de tratamento de dados previstas em lei e conforme finalidades especificadas no consentimento dado pelo Titular.

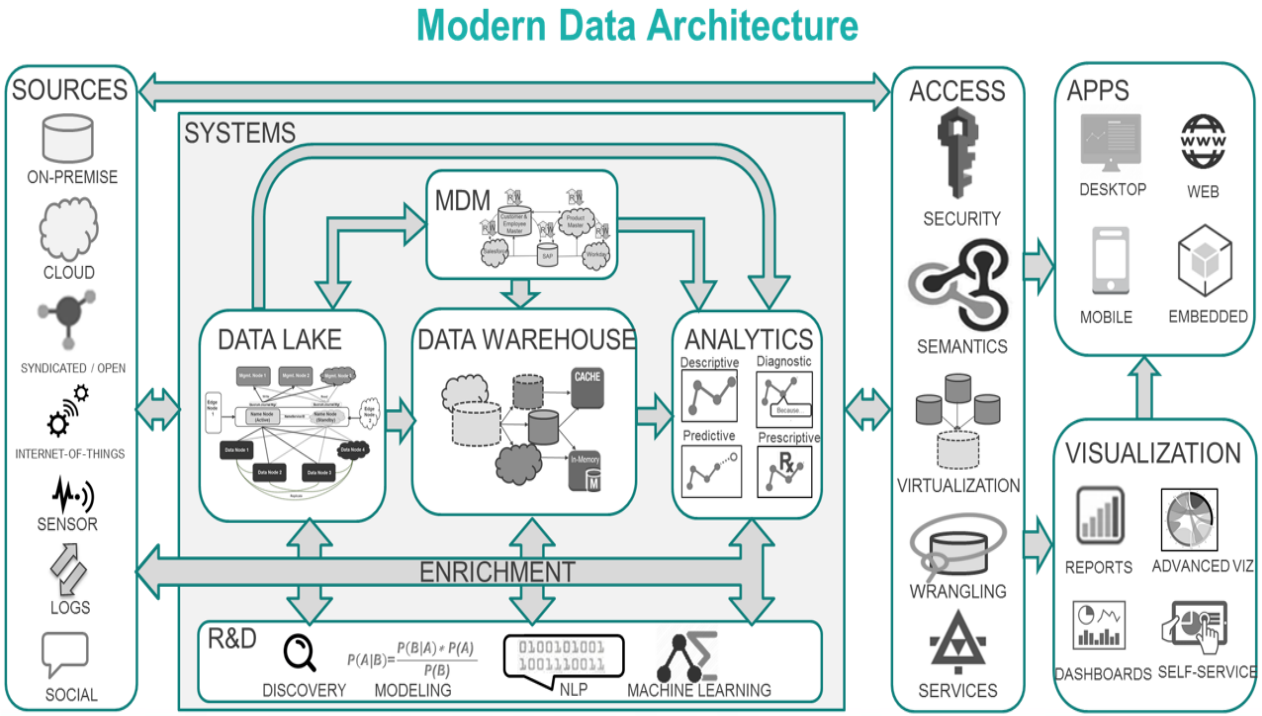
Proteger

Aplicar durante todo o ciclo de Vida das Informações e Dados, processos e medidas de controle e segurança, visando manter a disponibilidade, integridade, confidencialidade e privacidade dos dados enquanto durante período de ciclo de vida útil, ou seja, enquanto estiver vigente o contrato com o Titular dos Dados, ou estiver dentro da base legal ou regulatória

Descartar

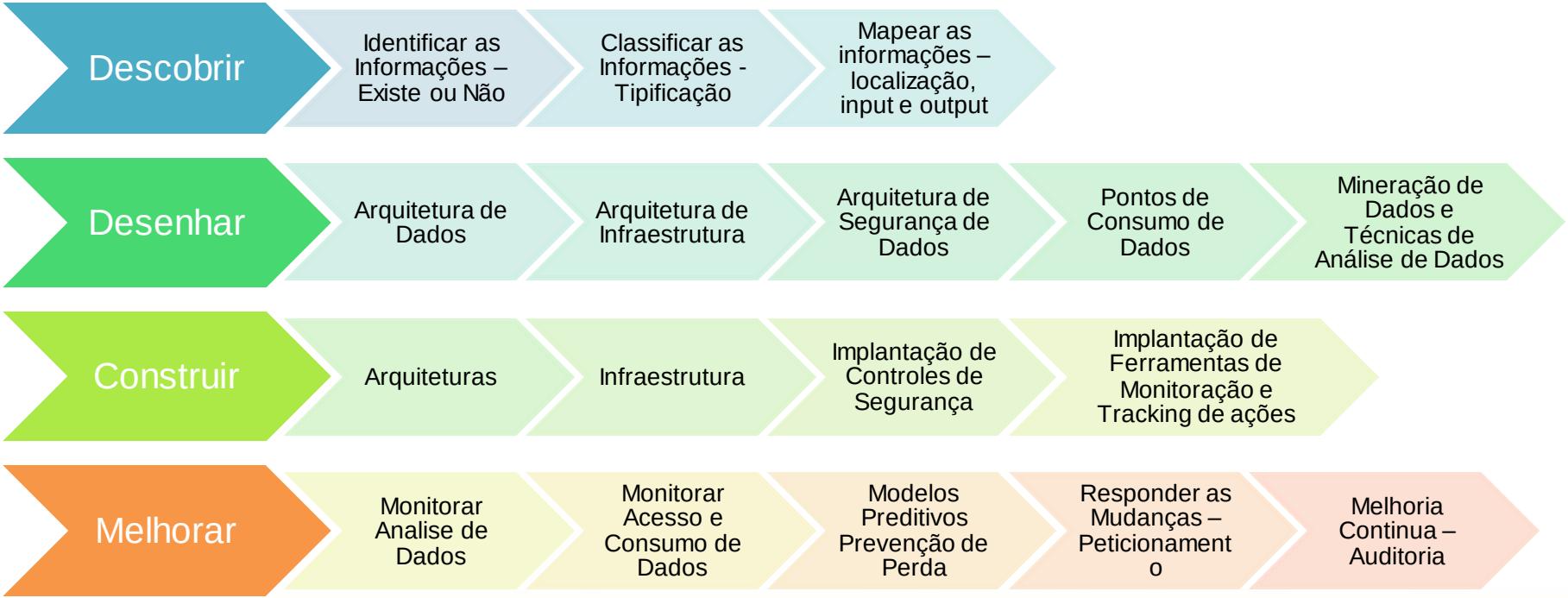
Após concluída a finalidade do tratamento ou mediante peticionamento do titular dos dados, as informações e dados devem ser excluídos, salvo se ainda estiver no período vigente de contrato, obrigação legal ou regulatória por parte dos Agentes de Tratamento. Esta eliminação deve ser feita de forma segura, e gerar um relatório de exclusão como evidencia do processo executado no caso de ter sido peticionado pelo Titular ou como medida de punição vinda de um órgão regulador, ou encerramento de contrato entre operador e controlador.

6 –Como poderá ser: uma visão de Arquitetura



Art.5 XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

6 –Como poderá ser: uma visão de Arquitetura



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

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.

OWASP
Open Web Application Security Project

Obrigado!

Adolceegabbana

in/alessandramonteiromartins/

@Ale_TI

FemmeIT
O JEITO FEMININO DE FALAR DE TI

Alessandra Martins
monteiromartins@bol.com.br