CCADON
Implementação da LGPD na Área de Dados

12/12/2022

Fundação Vanzolini

Apresentação

Razões de fazer o curso

À medida que as empresas coletam mais dados do que nunca, é fundamental que todos os profissionais possam ler, analisar dados e tomar as melhores decisões com eficiência. Esse oceano de dados guarda padrões complexos que, uma vez desvendados, se tornam fundamentais para decisões de negócio mais inteligentes. Profissionais, independente da área, que dominarem ferramentas de dados e possam usá-las para manipular, estruturar e arquitetar dados serão altamente demandados no mercado.

Razões deste módulo

O profissional tem que saber quais são as disposições legais que dão sustentação a sua atividade, os limites que devem ser obedecidos e como adequar as suas atividades a eles. Na vida profissional encontrará projetos novos que deverão nascer adequados à lei e também sistemas legados que precisará adequar. Logo, tem que ter conhecimentos administrativos e técnicos que permitam implementar as adequações.

Abreviações

Abreviações e siglas utilizadas

ABNT – Associação Brasileira de Normas Técnicas
AEPD – Agência Espanhola de Proteção de Dados
ANPD – Agência Nacional de Proteção de Dados Pessoais
CAPTCHA – Mecanismo de verificação do usuário de um site para impedir acesso por robôs
ISO – International Standard Organization
LGPD – Lei Geral de Proteção de Dados (Lei 13.709/2018)
MFA – Multifactor Authentication
NBR – Norma Brasileia
PDCA - Plan, Deliver, Check and Act
TI – Tecnologia da Informação
TIC – Tecnologia da Informação e Comunicação

Sumário

1. Conformidade com a LGPD no Tratamento dos Dados Pessoais

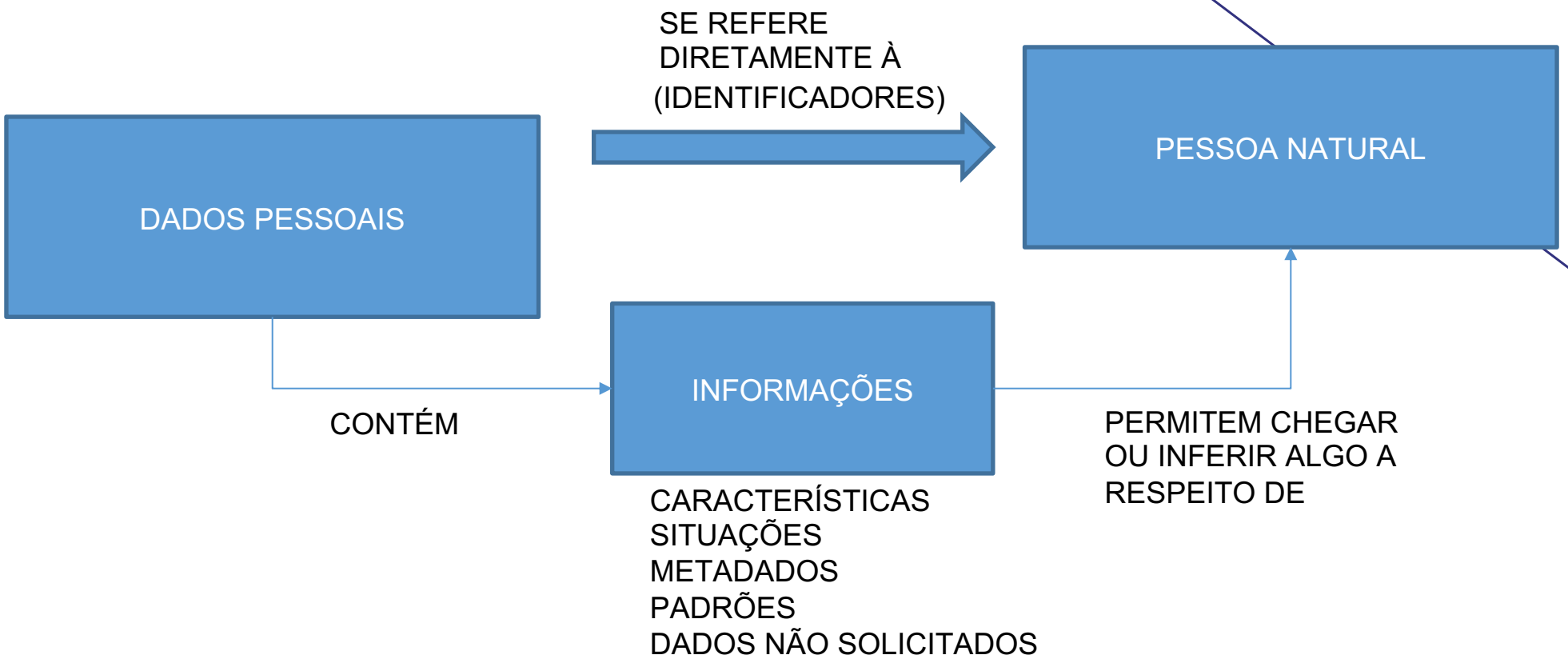
Contexto Tecnológico

Mudanças aceleradas na tecnologia, nas organizações e na sociedade

- Convergência Digital, Conectividade e Mobilidade
- Internet das Coisas
- Big Data e Inteligência Virtual
- Redes Sociais
- Realidade Virtual
- Realidade Aumentada
- Computação Quântica
- Nativos Digitais

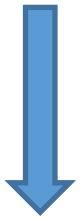
Dados Pessoais

O que caracteriza um conjunto de dados como sendo dados pessoais



Dados Pessoais Sensíveis

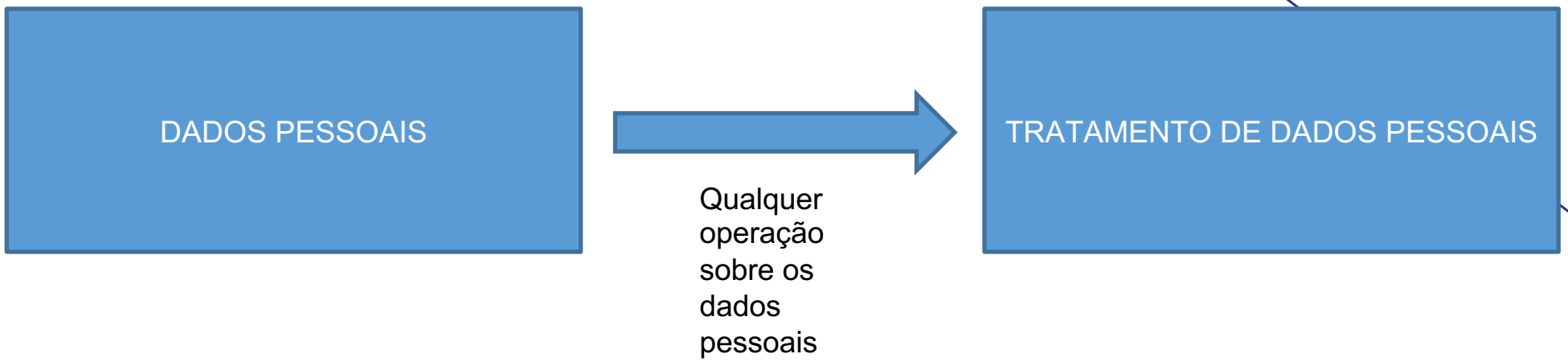
dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;



Atinge a esfera mais intima da vida da pessoa e pode sujeita-la à maiores riscos para os seus direitos e liberdades.

Tratamento de Dados Pessoais

Visão Técnica



Enriquecimento e Agregação de Dados

Atenção com as operações efetuadas em bases de dados

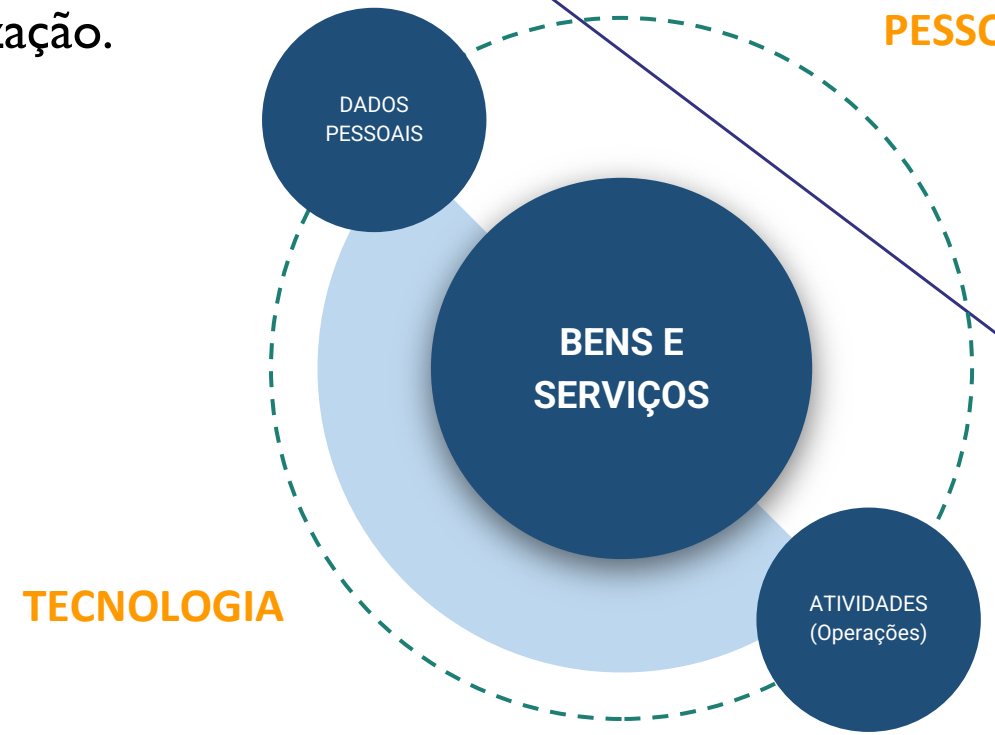
- A manipulação, estruturação e combinação de conjuntos de dados diferentes, originariamente não pessoais, com o enriquecimento dos dados coletados em outras fontes, pode agregar informações que permitam falar algo sobre pessoas naturais identificáveis e assim transformar a base resultante em base de dados pessoais;

- Bases com dados pessoais coletados e tratados de acordo com consentimento, contratos ou outras bases legais apropriadas, quando combinadas ou enriquecidas com informações de outras fontes, podem dar origem a novos conjuntos de dados pessoais cujo tratamento pode não estar em conformidade com os propósitos e condições originais apresentadas para os titulares;

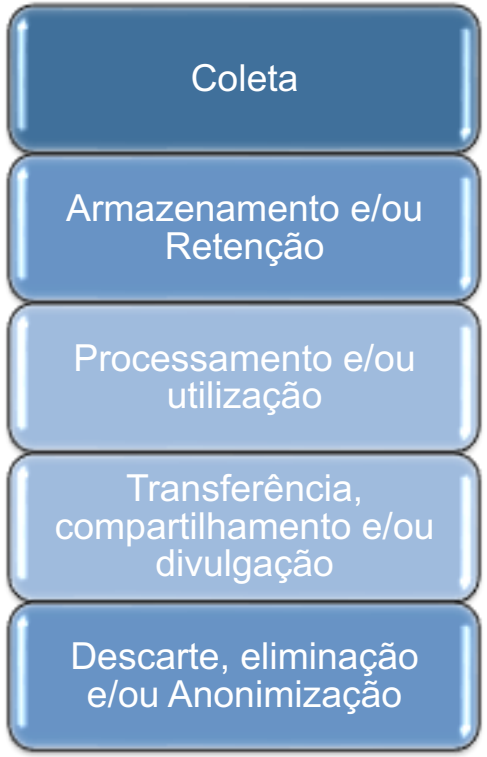
- Dados coletados em fontes públicas, normalmente estão divulgados lá com propósitos bem definidos, isso não significa que podem ser coletados e usados para outros fins com os quais o titular não concorde (não confundir dados tornado públicos por motivos específicos – por exemplo, nomes e salários divulgados com base na Lei de Acesso à Informação - com a aplicação do Art. 7º - § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados **tornados manifestamente públicos pelo titular**, resguardados os direitos do titular e os princípios previstos nesta Lei.);

- Os direitos dos titulares devem ser respeitados na coleta de dados pessoais com as técnicas de WEB SCRAPING. Há inclusive sites que bloqueiam o acesso por robôs por meio de técnicas de segurança como o CAPTCHA e, do ponto de vista de segurança da informação, burlar estas técnicas é uma violação de segurança. Assim, busque orientação jurídica antes de aplicar estas técnicas em seus projetos para não correr o risco de estar cometendo infrações contra a LGPD e outras leis como a dos crimes cibernéticos.

O tratamento dos dados pessoais ocorre nos processos de trabalho da organização.



Os dados pessoais passam por um ciclo de vida dentro dos processos de trabalho.



Condições básicas para que um processo de tratamento de dados pessoais possa ser executado (há disposições mais restritivas para dados de menores e dados pessoais sensíveis):

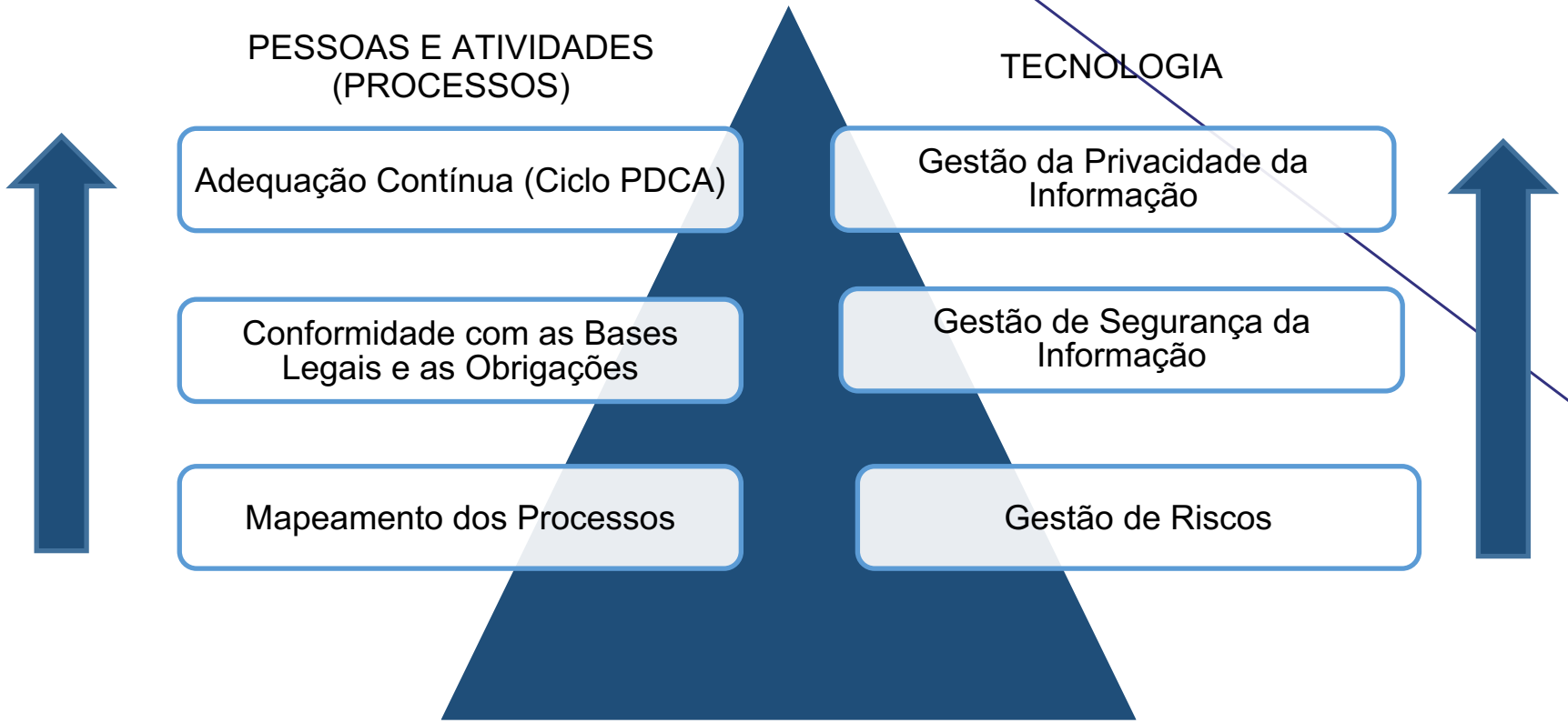
- mediante o fornecimento de consentimento pelo titular;
- para o cumprimento de obrigação legal ou regulatória pelo controlador;
- pela administração pública na execução de políticas públicas;
- para a realização de estudos por órgão de pesquisa;
- quando necessário para a execução de contrato ou seus procedimentos preliminares;
- para o exercício regular de direitos em processo judicial, administrativo ou arbitral
- para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- para a tutela da saúde (profissionais de saúde, serviços de saúde ou autoridade sanitária;
- interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

2. Eixos de Implementação da Conformidade

Medidas administrativas e técnicas de adequação dos processos de trabalho

JURÍDICO	PESSOAS E ATIVIDADES (ADMINISTRATIVO)	TÉCNOLOGIA
• Identificação, entendimento e aplicação de Leis, contratos, termos, convênios e regulamentações aplicáveis • Adequações em contratos, termos e convênios • Identificação das bases legais	• Planejamento, implantação, monitoração e melhoria contínua das atividades para atingir os fins da organização • Controle efetivo do ciclo de vida dos dados dentro de cada atividade • Adequação das atividades aos princípios de privacidade.	• Identificação, planeamento, implantação, operação e monitoração de ferramentas tecnológicas para a execução dos processos de trabalho da organização

Implementação da Adequação Administrativa e Técnica



As normas técnicas trazem orientação sobre as melhores práticas administrativas e técnicas em campos específicos do conhecimento.

Legislação de Proteção de Dados Pessoais

LGPD, GDPR, CCPA etc.

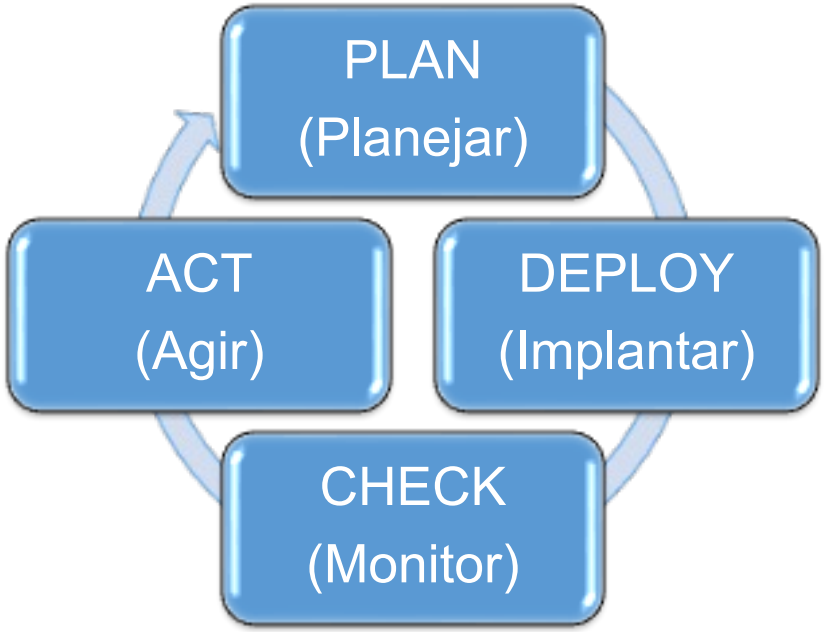
Sistemas de Tecnologia da Informação e Comunicação

Normas Técnicas Internacionais adotadas no Brasil (ABNT)

NBR ISO 29100 – Estrutura de Privacidade da Informação
NBR ISO 27001 – Sistema de Gestão de Segurança da Informação
NBR ISO 27701 – Sistema de Gestão de Privacidade da Informação

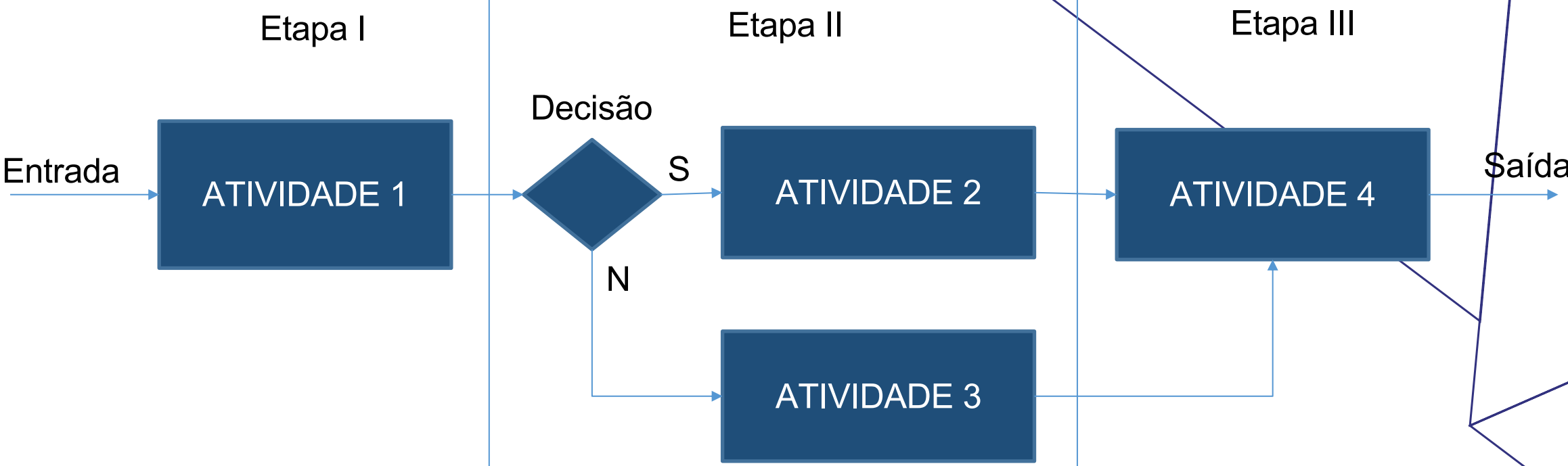
3. Ciclo PDCA

Conceito fundamental na gestão de processos de trabalho



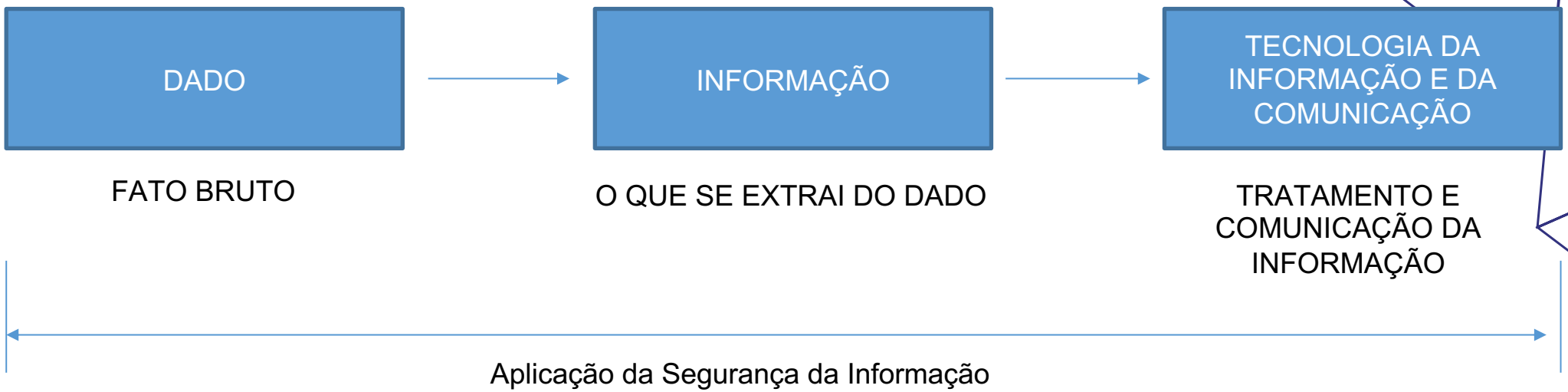
Documentando Processos

Desenhar os processos ajuda no planejamento e no controle

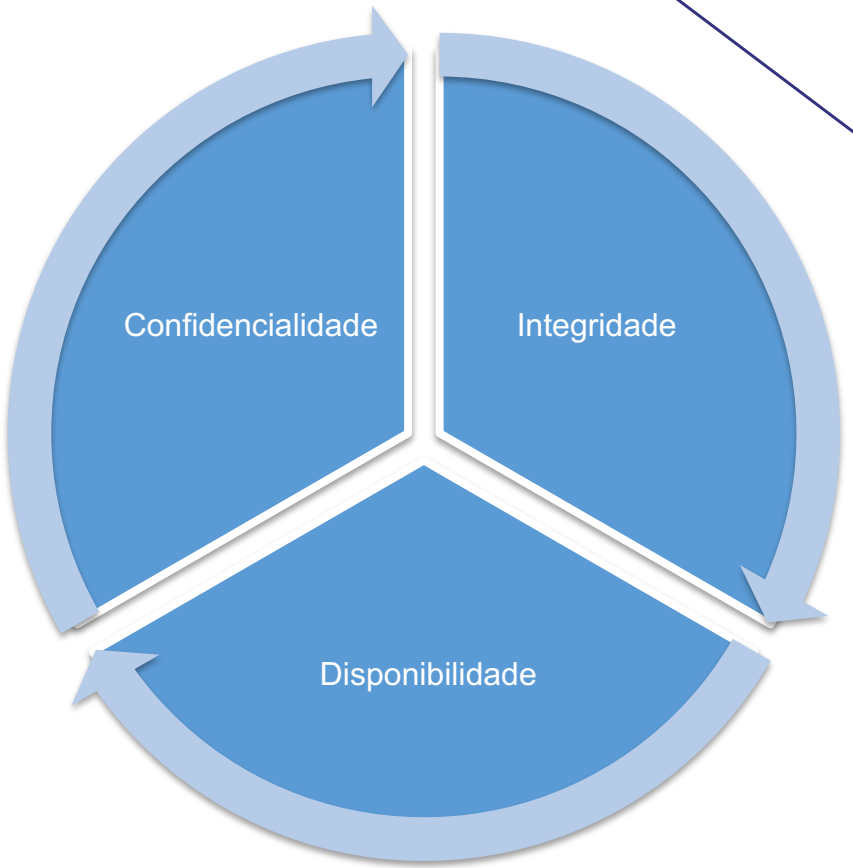


4. Segurança da Informação

Conceito técnico aplicado na implementação de medidas administrativas e técnicas em sistemas de tecnologia da informação e comunicação para garantir a confidencialidade, integridade e disponibilidade da informação.

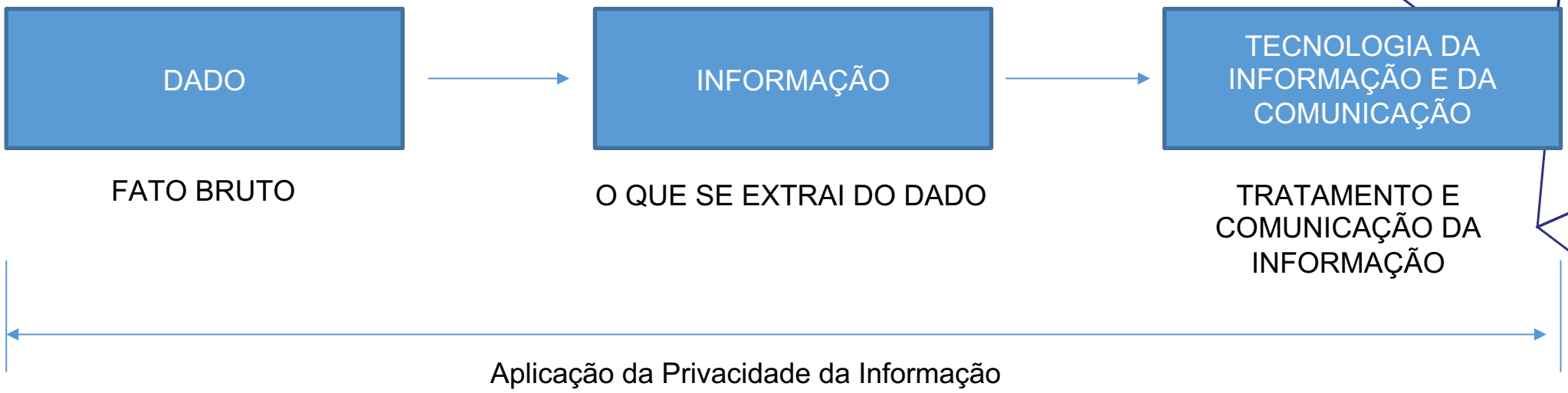


Princípios de Segurança da Informação



5. Privacidade da Informação

Conceito técnico aplicado na implementação de medidas administrativas e técnicas em sistemas de tecnologia da informação e comunicação para o respeito e proteção dos direitos de titulares de dados pessoais



Princípios de Privacidade

Lei Geral de Proteção de Dados (LGPD)

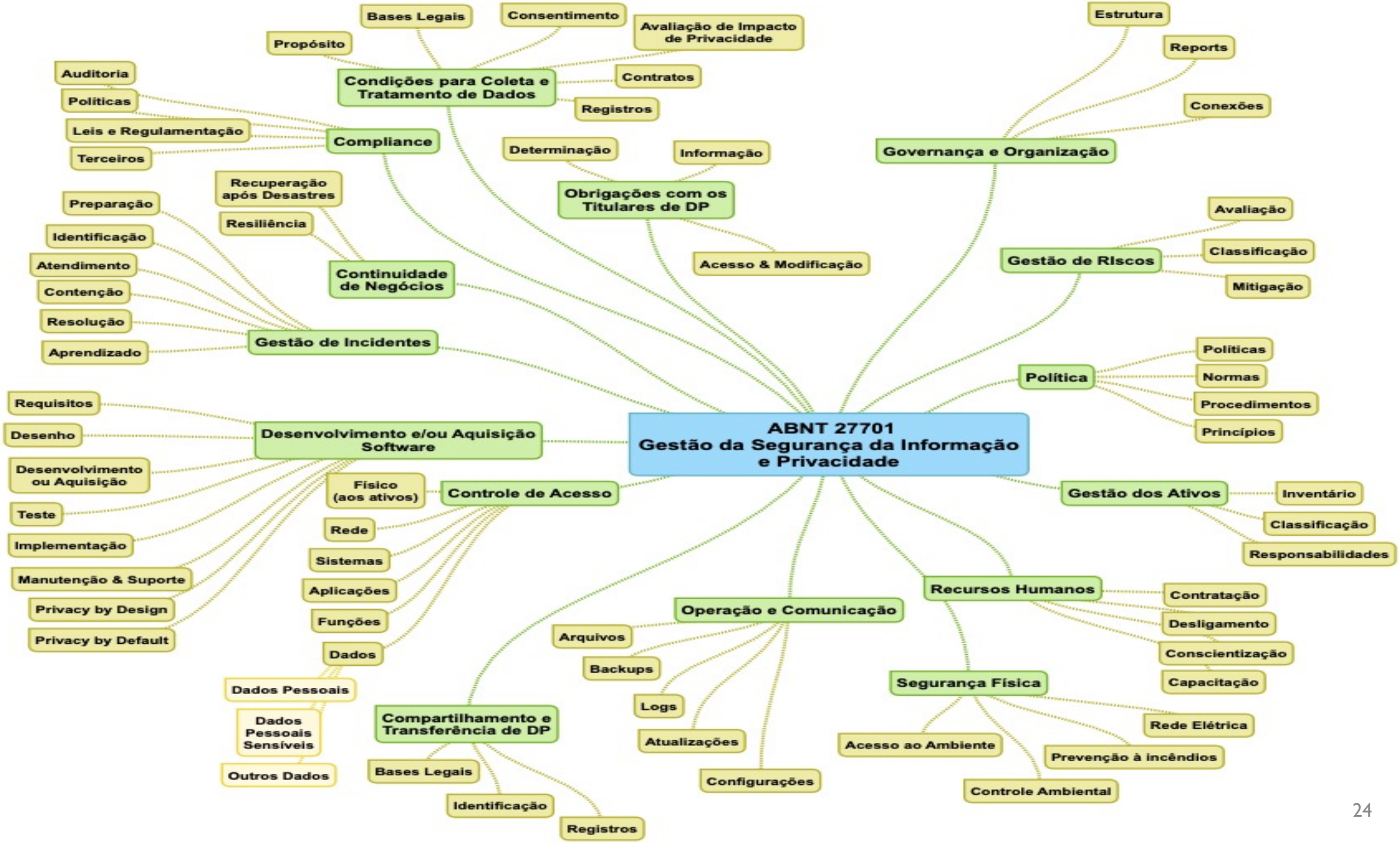
1 – Finalidade
2 – Adequação
3 – Necessidade
4 – Livre Acesso
5 – Qualidade
6 – Transparência
7 – Segurança
8 – Prevenção
9 – Não discriminação
10 - Responsabilização

Estrutura de Privacidade da Informação (NBR ISO 29100)

1 – Consentimento e Escolha
2 – Legitimidade e especificação de Propósito
3 – Limitação de Coleta
4 – Minimização do Tratamento
5 – Uso, retenção e limitação da retenção
6 – Precisão e qualidade
7 – Abertura, transparência e notificação
8 – Participação individual e acesso
9 – Segurança da Informação
10 – Compliance com a privacidade
11 - Responsabilização

Implementação da Privacidade da Informação

Norma ABNT	Controles (Medidas Técnicas e Administrativas)	Objetivo
NBR ISO 27001	Anexo A da NBR ISO 27001 (114 controles)	Garantir a confidencialidade, integridade e disponibilidade dos ativos da informação
NBR ISO 27701	Anexo A da NBR ISO 27701 (31 controles) para o agente de tratamento de dados pessoais com o papel de controlador no processo de tratamento de dados pessoais e Anexo B (18 controles)para o operador.	Condições para a coleta e o TDP Obrigações para com os titulares Privacy by Design e Privacy by Default Compartilhamento, transferência e divulgação de DP
NBR ISO 27005		Diretrizes para a Gestão de Riscos que orientará a implementação dos controles da NBR ISO 27001 e 27701


ABNT 27701
Gestão da Segurança da Informação e Privacidade
Condições para Coleta e Tratamento de Dados
Bases Legais
Consentimento
Avaliação de Impacto de Privacidade
Propósito
Contratos
Registros
Compliance
Auditoria
Políticas
Leis e Regulamentação
Terceiros
Obrigações com os Titulares de DP
Determinação
Informação
Acesso & Modificação
Continuidade de Negócios
Recuperação após Desastres
Resiliência
Gestão de Incidentes
Preparação
Identificação
Atendimento
Contenção
Resolução
Aprendizado
Governança e Organização
Estrutura
Reports
Conexões
Gestão de RIscos
Avaliação
Classificação
Mitigação
Política
Políticas
Normas
Procedimentos
Princípios
Gestão dos Ativos
Inventário
Classificação
Responsabilidades
Recursos Humanos
Contratação
Desligamento
Conscientização
Capacitação
Segurança Física
Rede Elétrica
Prevenção à incêndios
Controle Ambiental
Acesso ao Ambiente
Operação e Comunicação
Arquivos
Backups
Logs
Atualizações
Configurações
Compartilhamento e Transferência de DP
Bases Legais
Identificação
Registros
Controle de Acesso
Físico (aos ativos)
Rede
Sistemas
Aplicações
Funções
Dados
Dados Pessoais
Dados Pessoais Sensíveis
Outros Dados
Desenvolvimento e/ou Aquisição Software
Requisitos
Desenho
Desenvolvimento ou Aquisição
Teste
Implementação
Manutenção & Suporte
Privacy by Design
Privacy by Default

Papéis e Responsabilidades

Dentro de um sistema de gestão de privacidade da informação

- Alta Direção da Empresa – É a responsável em última instância pelo sistema de gestão de privacidade da informação;
- Comitê de Segurança da Informação e Privacidade – Apoio para a alta direção nas decisões estratégicas e no acompanhamento da segurança da informação e privacidade;
- Encarregado pelo Tratamento de Dados Pessoais (LGPD) - Papel definido na LGPD. O mercado tem usado a designação de DPO (Data Protection Officer - GDPR);
- Gestor de Segurança da Informação – Responsável pela confidencialidade, integridade e disponibilidade dos ativos da informação. O mercado costuma usar a designação em inglês CISO (Chief Security Information Officer);
- Todos os colaboradores são responsáveis por zelar pela segurança da informação e pela proteção de dados pessoais na sua esfera de atuação.

6 – Entendendo Riscos

Origem dos Riscos de Privacidade

EXISTÊNCIA DE AMEAÇA AOS DADOS PESSOAIS

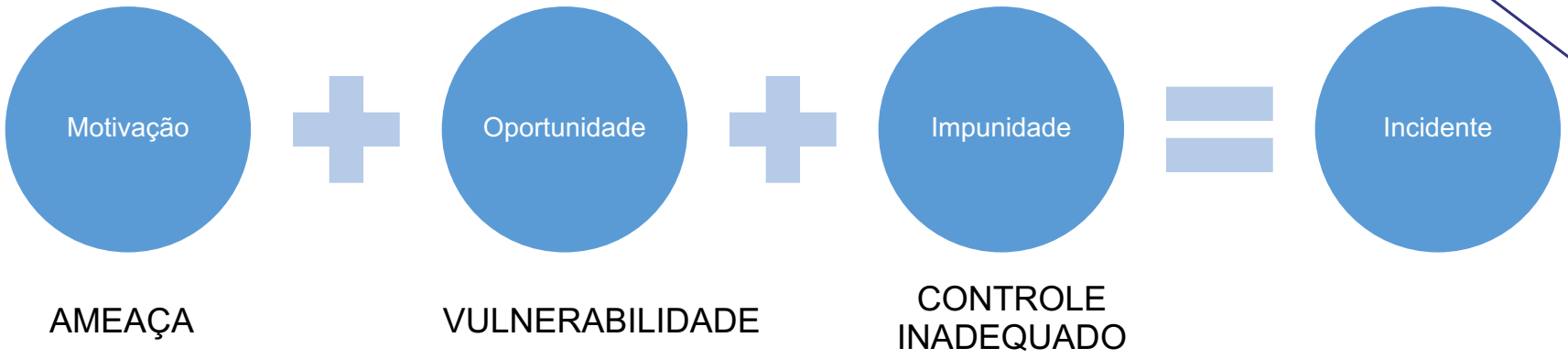
EXISTÊNCIA DE VULNERABILIDADE NOS PROCESSOS DE TRATAMENTO

CONTROLE INEFICAZ OU NÃO EXISTENTE

INCIDENTE

Incidentes Provocados por Ações Intencionais

Incidentes de segurança da informação e privacidade relacionados à ações mal-intencionadas ou criminosas



Incidente de Segurança da Informação

- Evento adverso que comprometa a confidencialidade, integridade ou disponibilidade de um ativo da informação da organização;

- Os dados pessoais tratados na organização estão entre os ativos da informação que podem ser comprometidos.

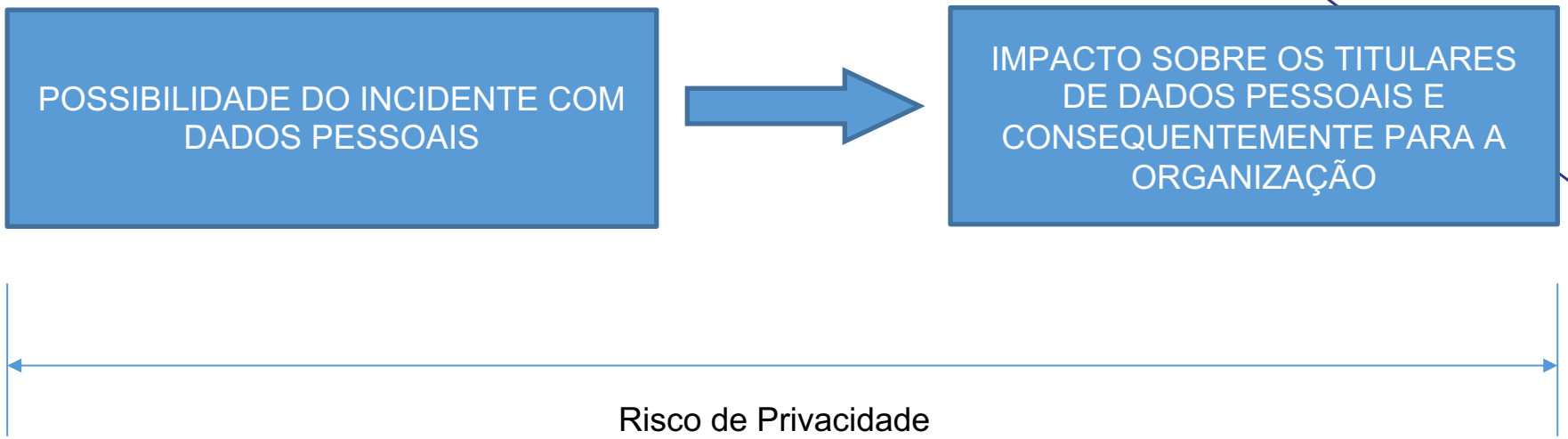
Incidente com Dados Pessoais

Fonte: Guia da ANPD

- Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.
- O art. 46 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) determina que os agentes de tratamento de dados pessoais 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.

Risco de Privacidade

Efeito da incerteza nos objetivos da organização



Vulnerabilidades

Alguns exemplos de vulnerabilidades que podem afetar os processos de tratamento de dados pessoais:

- Processos de trabalho mal desenhados ou mal documentados;
- Pessoal destreinado ou desmotivado;
- Falta de políticas de segurança da informação e de outros controles mínimos;
- Software e hardware desatualizados;
- Configurações de segurança não aplicadas ou aplicadas incorretamente;
- Direitos de acesso mal administrados;
- Ausência de segregação de funções em processos críticos;
- Falta de mecanismos de proteção contra malwares;
- Softwares com licenças irregulares ou pirata;
- Conexões com a Internet sem as devidas proteções;
- Ausência de monitoração do uso dos ativos de TI e do tratamento de dados pessoais;
- Falta de logs e trilhas de auditoria;
- Etc.

Ameaças

Alguns exemplos de ameaças para os processos de tratamento de dados pessoais:

- Falhas humanas, descuido, imperícia etc.;
- Erros operacionais;
- Fraudes, sabotagens e outras ações internas mal intencionadas;
- Roubo ou furto de equipamentos;
- Malwares;
- Ataques e outras ações mal intencionadas a partir de agentes externos;
- Espionagem industrial/comercial;
- Crime eletrônico em suas diversas formas;
- Sinistros como enchentes, incêndios, desabamentos etc.;
- Guerra cibernética.

Probabilidade de um Incidente

Como estimar a probabilidade da ocorrência de um incidente

- Histórico de ocorrências na organização ou em organizações similares;
- Avaliação dos especialistas sobre a facilidade de exploração das vulnerabilidades existentes;
- Nível e natureza das ameaças presentes.

Exemplo Ilustrativo

Probabilidade de incidente de vazamento de dados pessoais armazenados em mídia removível por motivo de roubo ou furto

1ª Situação – Dados armazenado em PEN DRIVE carregado pelo usuário na pasta que carrega diariamente da casa para o serviço

HISTÓRICO DE ROUBOS FURTOS: Alto
FACILIDADE DE SER ROUBADO/FURTADO: Alta
PRESENÇA DA AMEAÇA: Alta

→ **PROBABILIDADE ALTA**

2ª Situação – Dados armazenados em FITA de backup guardada em sala cofre no DATACENTER da empresa

HISTÓRICO DE ROUBOS FURTOS: Nenhum
FACILIDADE DE SER ROUBADO/FURTADO: Pouca ou nenhuma
PRESENÇA DA AMEAÇA: Baixa

→ **PROBABILIDADE BAIXA**

Impacto de um Incidente

Alguns exemplos de danos e riscos para os titulares de dados pessoais provocados por um incidente onde vazem seus dados financeiros críticos (CPF, nome, cartão de crédito, conta bancária etc.) ou dados pessoais sensíveis:

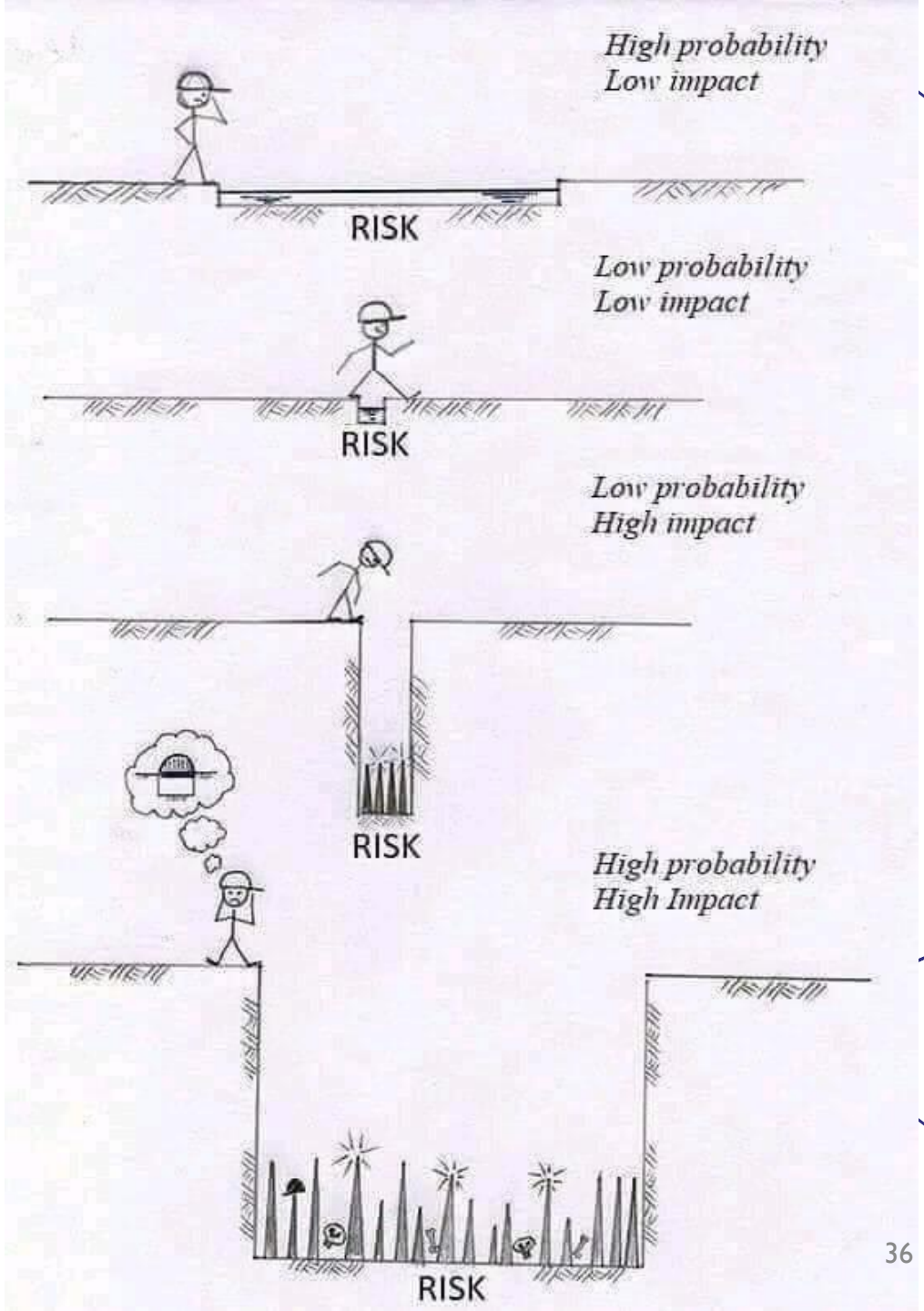
- Golpes financeiros
- Fraudes
- Sequestros, roubos, assaltos
- Discriminação
- Perseguição
- Exposição de sua vida privada
- Danos a sua imagem
- Manipulação
- Extorsão
- Chantagem

Nestes exemplos, todas as situações listadas seriam classificadas de IMPACTO ALTO para o titular

Analisando o Risco

Risco = Probabilidade x Impacto

RISCO ⟹ PERIGO



Fonte: Imagem postada no Linkedin por:

CSH **The Cyber Security Hub™**
226.267 seguidores

Classificação do Risco

Como classificar de forma subjetiva os riscos identificados

	Impacto Baixo 5	Impacto Médio 10	Impacto Alto 15
Probabilidade Alta 15	MÉDIO 75	ALTO 150	EXTREMO 225
Probabilidade Média 10	BAIXO 50	MÉDIO 100	ALTO 150
Probabilidade Baixa 5	MUITO BAIXO 25	BAIXO 50	MÉDIO 75

Classificação do Risco de Privacidade

Fonte: Guia da ANPD

- A probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade;

- Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

O que pode ser feito com o Risco de Privacidade

- **TRATAR** – Aplicar medidas jurídicas, administrativas e técnicas que modifiquem a possibilidade ou as consequências do cenário adverso;
- **TRANSFERIR** – Transferir as consequências do risco para outra parte, isto, normalmente significa contratar seguros;
- **ACEITAR** - Aceitar o risco como parte do negócio, estando a organização ciente da possibilidade da ocorrência do cenário adverso e pronta para lidar com as consequências;
- **EVITAR** – Deixar de fazer aquilo que traz o risco, do ponto de vista de negócios, normalmente significa deixar de prestar um serviço ou entregar um produto.

Tratamento de Riscos e Adequação LGPD

A existência das ameaças, das vulnerabilidades e da ineficácia dos controles, introduz a possibilidade de que os incidentes ocorram e cenários adversos, com impactos para a organização, bem como danos e riscos para os titulares de dados pessoais.

A gestão de riscos é a disciplina que permite à organização lidar com cenários de eventos futuros e seus impactos.

O risco é conceitualmente o efeito da incerteza sobre os objetivos da organização e é estimado com base na possibilidade da ocorrência e seus impactos. Organizações lidam com diferentes tipos de riscos operacionais, os de segurança são um deles.

Do ponto de vista da adequação LGPD, a gestão de riscos orienta a seleção e aplicação de medidas técnicas e administrativas que a colocam em conformidade com o art. 46 e definem seu sistema de gestão de privacidade da informação (SGPI)

7 – Implementação Administrativa e Técnica

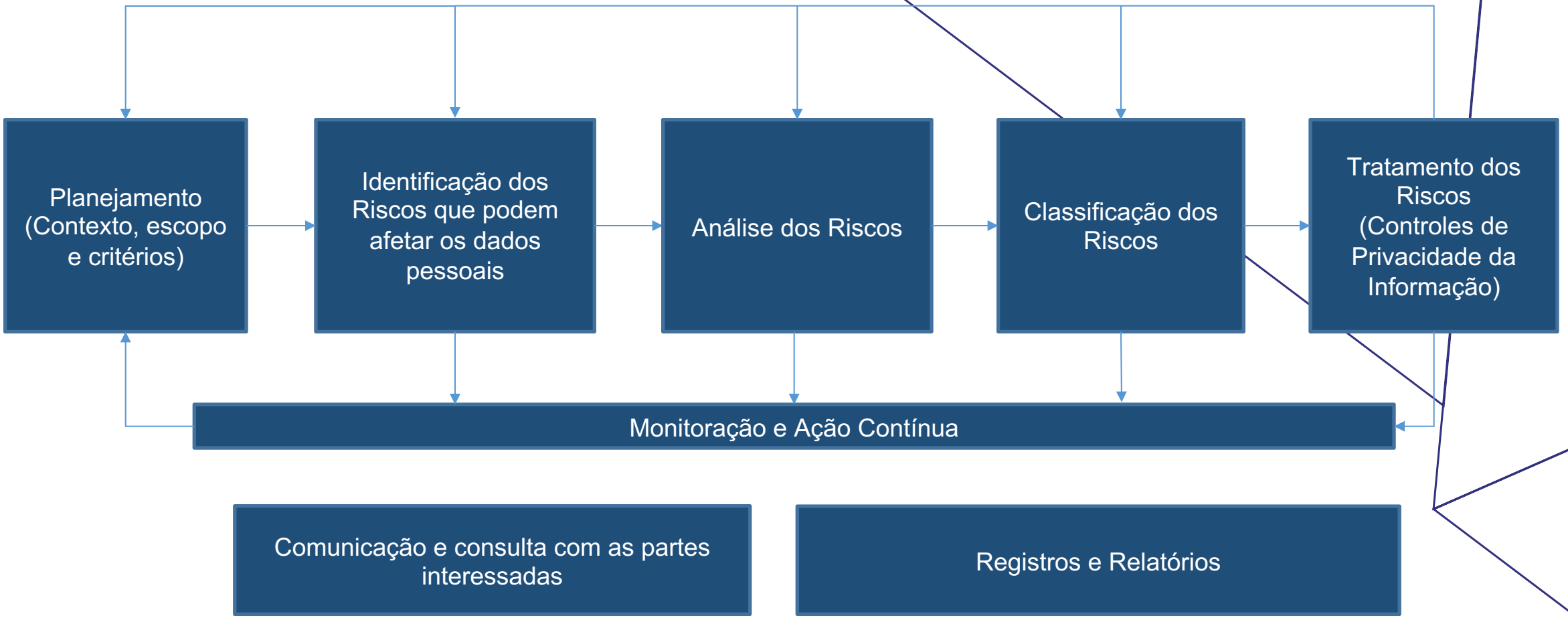
O processo de implantação das medidas administrativas e técnicas da LGPD é baseado na identificação, análise e tratamento dos riscos de segurança da informação e privacidade. Em suma se apoia na gestão de riscos.

Tem por base o mapeamento dos processos de tratamento de dados pessoais e seu diagnóstico, onde são avaliados os aspectos de aderência aos princípios e requisitos da lei.

Os pontos que não estão em conformidade com a lei introduzem os riscos.

O plano de tratamento dos riscos direciona a implementação da conformidade.

Processo de Implementação



Planejamento

Esta é a etapa mais importante para o sucesso da adequação

- O levantamento correto das características da organização, do escopo a ser tratado e dos critérios a serem empregados na identificação e classificação dos riscos, bem como nas condições para a sua aceitação ou tratamento, permite que as etapas seguintes sejam executadas de forma eficaz;

- Organizações diferentes tem características diferentes, escopos diferentes de aplicação e estão sujeitas as ameaças e vulnerabilidades de acordo com suas características e tem perfis de aceitação do risco diferentes;

- Esta etapa também envolve o mapeamento dos processos de dados pessoais, incluindo quais dados são tratados, em que condições, quem são seus titulares, quais os operadores e outras partes envolvidas.

Identificação

Riscos de Privacidade

Mapeamento dos dados pessoais e dos processos de tratamento em que estão inseridos;

Levantamento das ameaças, vulnerabilidades e deficiências nos controles de segurança existentes que podem resultar em cenários adversos (incidentes) com impactos negativas para à organização e/ou danos imediatos ou riscos para os titulares de dados pessoais.

Abordagem multidisciplinar, olhando para os três eixos: jurídico, processos e tecnologia.

Análise e Classificação dos Riscos

RISCO = PROBABILIDADE X CONSEQUÊNCIA

- Estima-se a probabilidade da ocorrência do evento adverso, tomando por base o nível de ameaça presenta, a facilidade de exploração da vulnerabilidade considerada e a eficácia dos controles de segurança existentes, de acordo com os critérios estabelecidos na fase de planejamento;

- Estima-se o impacto levando em conta os efeitos que a ocorrência terá para a organização (danos de imagem, interrupção de serviços, perda de faturamento, multas, indenizações, etc.) e os danos imediatos e riscos futuros para os titulares de dados pessoais eventualmente afetados pelo incidente, de acordo com os critérios estabelecidos na fase de planejamento;

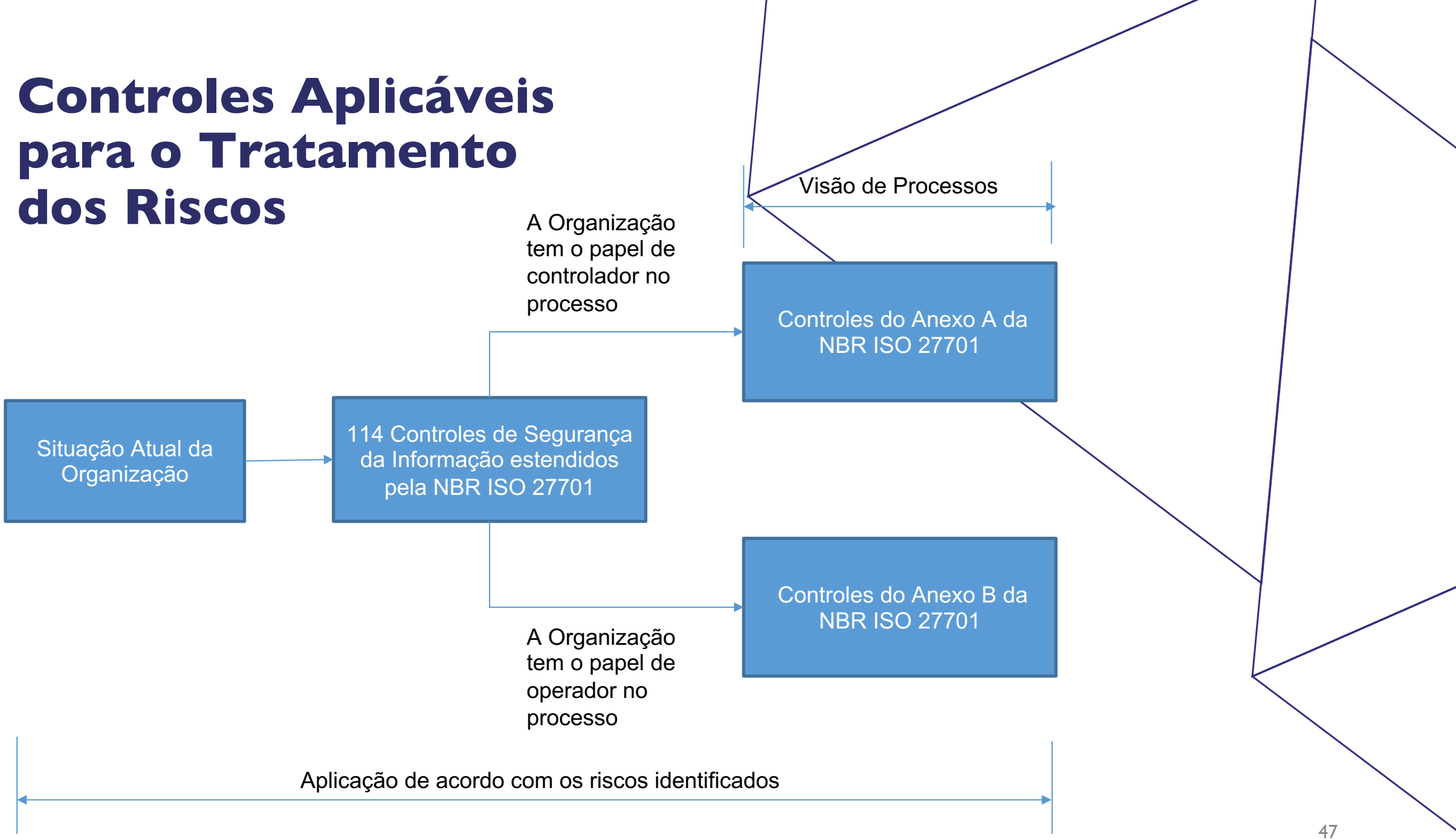
- A classificação do risco, ou seu nível, é determinado pela combinação da probabilidade e do impacto.

Tratamento

Tomada de decisão com base nos critérios previamente estabelecidos

Classificação/Nível do Risco	Prioridade no Tratamento	Recomendação
EXTREMO	A mais alta de todas	Não aceitar, tratar imediatamente
ALTO	Alta	Não aceitar, tratar rapidamente
MÉDIO	Média	Não aceitar, tratar assim que possível
BAIXO	Baixa	Não aceitar, o tratamento pode ser planejado para prazos mais longos
MUITO BAIXO	Sem prioridade	Aceitar até que surja ocasião para trata-lo

Controles Aplicáveis para o Tratamento dos Riscos



Controles Indicados pela ANPD

Aplicável para Agentes de Tratamento de Dados de **Pequeno Porte**
(corresponde a um subconjunto dos 114 controles da NBR ISO 27001)

- **Política de Segurança da Informação**: estabelecer uma política simplificada, realizar revisões periódicas, gerenciar contratos e aquisições com observância ao tratamento adequado dos dados pessoais.
- **Conscientização e Treinamento**: realizar campanhas e treinamentos para os colaboradores, informar e sensibilizar os colaboradores sobre as obrigações legais, informar aos funcionários sobre as regras de segurança.
- **Gerenciamento de Contratos**: estabelecer contratos com cláusulas de segurança da informação que assegurem a proteção dos dados pessoais, assinar termos de confidencialidade.
- **Controle de Acesso**: implantar um sistema de controle de acesso aplicável a todos os usuários; usar senhas fortes, implantar um gerenciamento adequado de senhas, proibir o compartilhamento de senhas, aplicar o princípio do mínimo privilégio, usar MFA para dados pessoais.
- **Segurança dos Dados Armazenados**: Limitar a coleta, usar criptografia para dados pessoais, evitar a transferência dos dados para dispositivos de armazenamento externo, inventariar a criptografar os dados nesses dispositivos; registro da destruição/descarte;
- **Segurança das Comunicações**: criptografia nas comunicações, proteção da rede interna por firewall, proteger o serviço de e-mail, remover dados sensíveis e outros dados pessoais desnecessariamente disponibilizados.
- **Gerenciamento de Vulnerabilidades**: atualização de software e hardware, varreduras periódicas;
- **Medidas para Dispositivos Móveis**: MFA, separar o uso dos dispositivos móveis daqueles de uso institucional, funcionalidades para apagar remotamente os dados.
- **Medidas para Serviços em Nuvem**: SLA de segurança dos dados armazenados, avaliar o atendimento aos requisitos de segurança, analisar os requisitos para o acesso do usuário, MFA.

8 – Tecnologia Aplicável

Exemplos de ferramentas disponíveis no mercado para implementação dos controles

- Plataformas de gestão de riscos corporativos e de segurança. Há muitas plataformas disponíveis no mercado brasileiro e internacional. Alguns exemplos:
  - Conformio (Advisera) - https://advisera.com/conformio/
  - Módulo Risk Manager - https://www.modulo.com.br/moduloriskmanager/
  - RIS – Redbelt - https://www.redbelt.com.br/plataformas-proprias/ris-risk-information-security
  - VsRisk – Vigilant Software - https://www.vigilantsoftware.co.uk/product/vsrisk

- Testes de invasão, para a identificação de vulnerabilidades na conexão da organização com Internet, que é um serviço prestado por várias empresas no Brasil, por exemplo:
  - Cherokee - https://www.cherokee.com.br/
  - RedBelt - https://www.redbelt.com.br/
  - Tempest - https://www.tempest.com.br

- Ferramentas diversas que implementam controles de segurança, como os scans de vulnerabilidades na rede, sistemas antivírus, firewalls, plataformas de gerenciamento de identidade, etc.

- Certificações pela Fundação Vanzolini nas normas NBR ISO 27001 e NBR ISO 27701 (validação externa dos processos de gestão de riscos de segurança da informação e privacidade)

Mapeamento de Dados Pessoais

Ferramentas disponíveis no mercado

- Existem várias ferramentas de mercado que auxiliam o Encarregado/DPO a manter um registro dos processos de tratamento de dados pessoais executados na organização. Este mapeamento ajudará na comunicação com a ANPD e com os Titulares, além de apoiar a gestão de riscos.

- Estas ferramentas variam de aplicações para a elaboração de fluxogramas até busca de dados pessoais em base de dados e serviços em nuvem.

- IBM, Microsoft, Amazon e Google são alguns dos fornecedores que disponibilizam ferramentas para encontrar e classificar os dados tratados em suas plataformas.

- A seleção e escolha da ferramenta adequada deve ser feita de acordo com as plataformas utilizadas na organização e a solução mais provável será uma combinação delas.

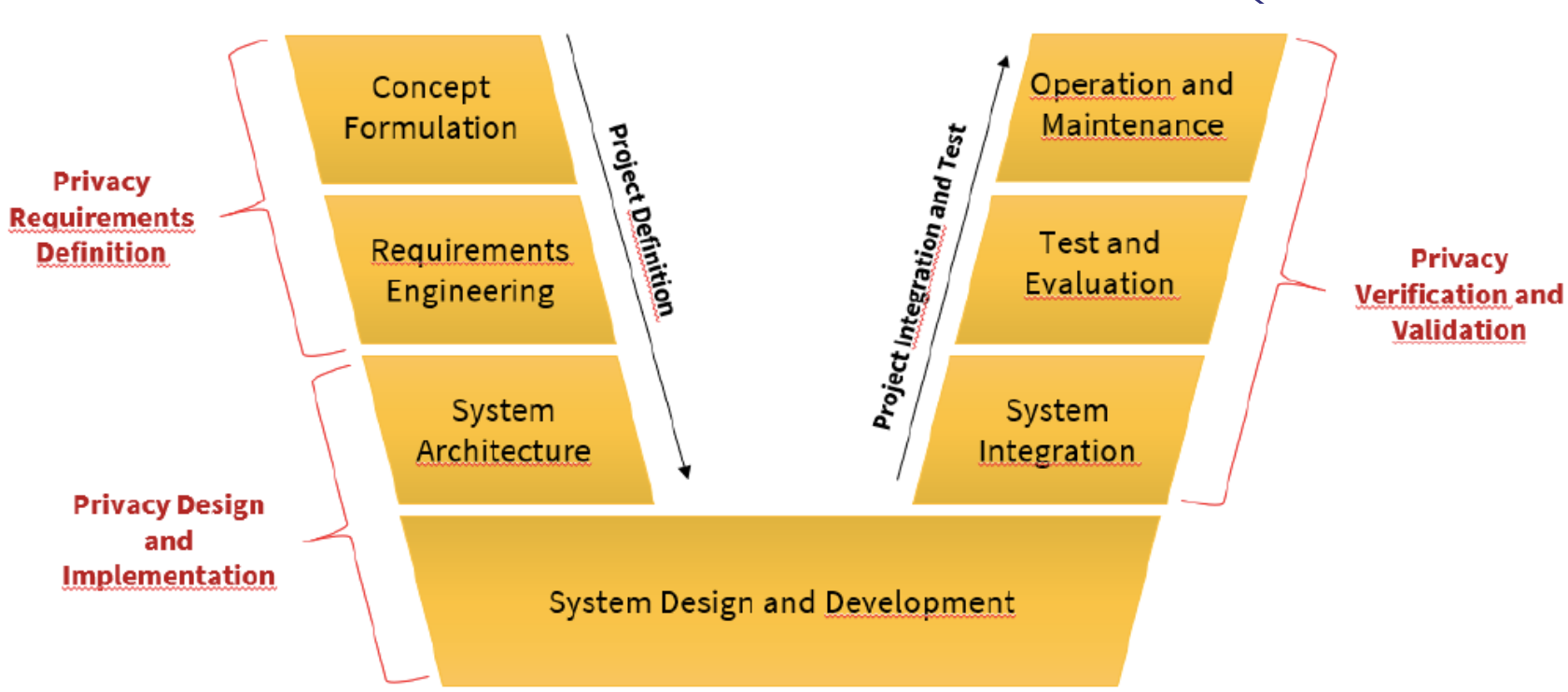
Desenvolvimento de Software

Os novos sistemas devem nascer em conformidade com a LGPD

PROTEÇÃO DA PRIVACIDADE DOS USUÁRIOS/TITULARES		
CONDIÇÕES PARA O TRATAMENTO	TRANSPARÊNCIA	CONTROLE
Limitação da coleta e do tratamento ao estritamente necessário Limitação do armazenamento e retenção ao estritamente necessário Segurança no tratamento	Conformidade legal, transparência e dentro do que é ético e justo Propósitos bem definidos e declarados	Limitação do tratamento ao propósito declarado Qualidade/precisão no tratamento Integridade e confidencialidade Responsabilização

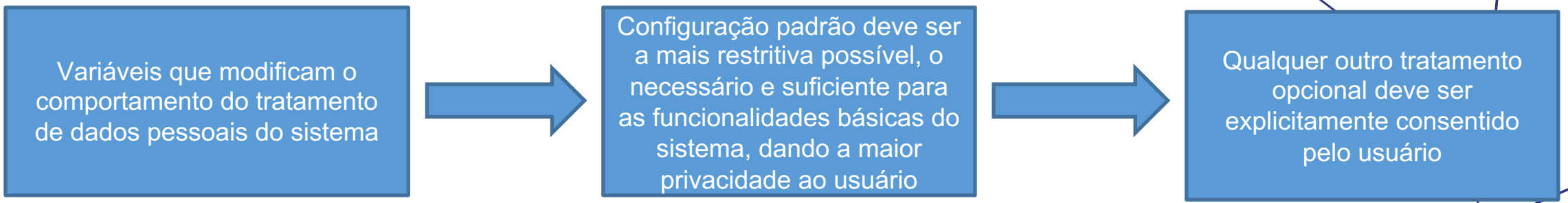
Privacy by Design

Projetando sistemas levando em conta os princípios e requisitos de privacidade (Fonte: AEPD)



Privacy by Default

Configurações de privacidade que permitem ao usuário adequar o sistema as suas preferências



Um exemplo da aplicação deste princípio é a opção pelo uso de cookies em página WEB. Por padrão, só devem ser habilitados os essenciais para o sistema

Cuidados na Aquisição de Sistemas

Aplica-se também a aquisição de plataformas ou uso de recursos contratados na nuvem

- Verificar se o sistema está em conformidade com a LGPD;
- Verificar se o sistema atende as normas de segurança da informação aplicáveis (NBR ISO 27001, NBR ISO 27002, NBR ISO 27017, NBR ISO 27018, NBR ISO 27701);
- Verificar se o sistema passou por auditorias e quais certificações de segurança o fornecedor possui;
- Verificar se estão claramente definidas as responsabilidades por controle de acesso, guarda de logs, backups, proteção dos dados pessoais, monitoração e tratamento de incidentes de segurança da informação;
- Verificar se estão claras as responsabilidades pelas operações de tratamento de dados pessoais executadas por meio do sistema e quais os registros de tratamento disponíveis;
- Verificar se há uma cadeia de fornecimento envolvida (sub operadores) e como estão definidas as responsabilidades pela proteção de dados pessoais nesta cadeia, inclusive se há transferência ou compartilhamento de dados pessoais para outros países;
- Verificar se está contratualmente claro o que será feito dos dados pessoais em caso de término ou cancelamento do contrato de prestação de serviços;
- Verificar que medidas o contrato prevê em caso de descontinuidade da operação do fornecedor;
- Verificar se o fornecedor tem ou terá acessos privilegiados aos dados pessoais armazenados no sistema e como esse acesso será controlado e monitorado.

9. Bibliográfia

ABNT – Norma técnica NBR ISO 27001
ABNT – Norma técnica NBR ISO 27005
ABNT – Norma técnica NBR ISO 27701
ABNT – Norma técnica NBR ISO 29100
AEPD (Agência Espanhola de Proteção de Dados) – A Guide to Privacy by Design
AEPD (Agência Espanhola de Proteção de Dados) – Guía de Protección de Datos por Defecto
ANPD – Comunicação de Incidentes de Segurança com Dados Pessoais
ANPD – Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado
ANPD – Segurança da Informação para Agentes de Tratamento de Pequeno Porte
ANPD – Guia Orientativo Cookies e Proteção de Dados Pessoais
GOV.BR – Guia de Boas Práticas para a Implementação na Administração Pública Federal
LGPD – Lei Geral de Proteção de Dados (Lei 13.709/2018)
REVISTA DOS TRIBUNAIS editora – Comentários ao GDPR
REVISTA DOS TRIBUNAIS editora – Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro

Contato

Carlos Alberto Iglesia Bernardo
Instrutor
carlos.bernardo@itsecure.com.br

Obrigado.

Fundação Vanzolini