

ATUANDO COMO ENCARREGADO DE DADOS

Luiz Felipe Vieira de Siqueira



Luiz Felipe Vieira de Siqueira

www.privacypoint.com.br

siqueira@privacypoint.com.br

Advogado

Sócio Privacy Point

DPO EXIN

Mestre em Direito Empresarial

Doutorando UFMG

Professor de Pós Graduação

Linkedin: <https://www.linkedin.com/in/luizfelipesiqueira/>

**privacy
point**



(31) 98589-0609



siqueira@privacypoint.com.br



privacypoint.com.br

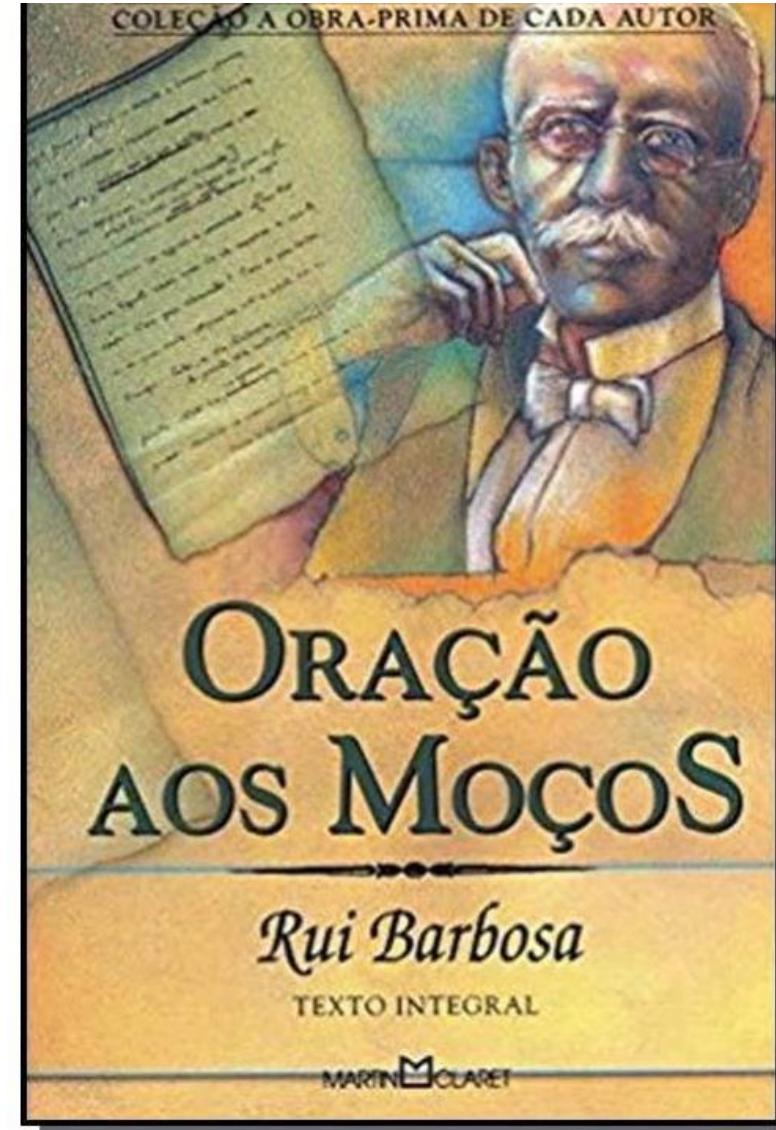
MARKETING JURÍDICO

Luiz Felipe Vieira de Siqueira

“Não fazer da
banca
balcão, ou da
ciência
mercatura”

Publicado em 1921

<https://www.amazon.com.br/Ora%C3%A7%C3%A3o-aos-Mo%C3%A7os-Rui-Barbosa/dp/8572325867>





https://aminoapps.com/c/breaking-bad-brasil/page/item/biografia-saul-goodman/aoee_qMT8IkLmzNgDbYj8WEG3VznebRwl

Ostentação

OAB suspende registro de advogado "ostentação" por posts nas redes

Criminalista também teria sido acionado para retirar qualquer postagem de ostentação das redes sociais no prazo de 24 horas.

Da Redação
Salvador, 5 de agosto de 2023
Atualizado em 7 de agosto de 2023 07:05

Compartilhar Comentar Siga-nos no Google News

O criminalista **Marcos Vinicius Borges**, conhecido por "advogado ostentação", foi suspenso preventivamente pela OAB/MT por conta dos conteúdos publicados em suas redes sociais. Segundo o jornal O Globo, a determinação permanecerá enquanto as publicações de viagens, carros e joias estiverem no perfil dele. Além disso, ele também foi acionado para retirar qualquer postagem de ostentação das redes sociais no prazo de 24 horas.



"Advogado ostentação" tem sua inscrição suspensa temporariamente pela OAB. (Imagem: Reprodução/Instagram/marcosviniciusborges)

<https://www.migalhas.com.br/quentes/391203/oab-suspende-registro-de-advogado-ostentacao-por-posts-nas-redes>

- **1ª onda: 1970-1990** – Sistemas Informatizados de pesquisa jurídica.
- **2ª onda: 1990-2012** – ferramentas de automação e montagem de documentos, softwares jurídicos, gestão de contratos automatizada, análise de dados de documentos e contratos.
- **3ª onda: 2012** – agora: machine learning, Inteligência Artificial, legal analytics, IaaS – infrastructure as a service, startups jurídicas.



Melbourne Law School

**Melbourne Legal Studies
Research Paper Series
No. 897**

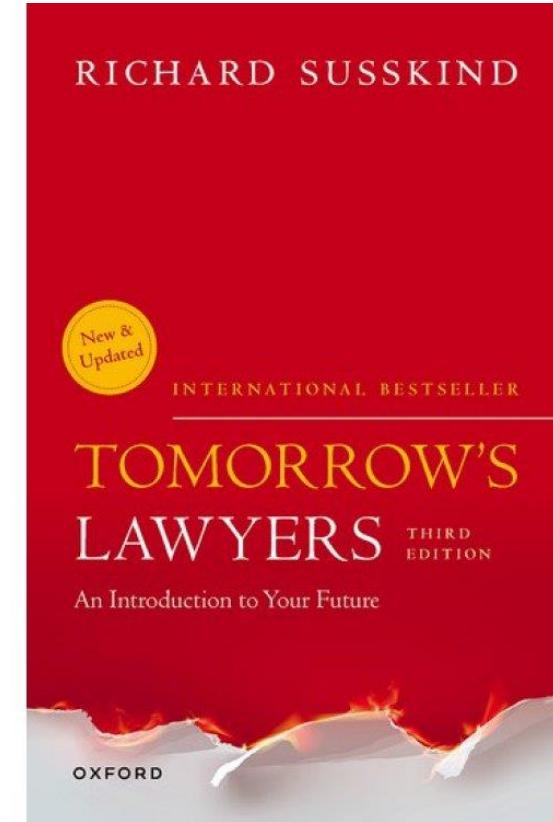
Legal Technology: The Great Disruption?

Julian Webb

Electronic copy available at: <https://ssrn.com/abstract=3664476>

FASES

- **Rejeição:** processo de descrença para as novas tecnologias
- **Informação:** processo de atenção e compreensão das novas tecnologias
- **Disrupção:** esmorecimento e transformação de hábitos de forma radical pelos Advogados, Escritórios, Departamentos Jurídicos e Cortes.



<https://bookpath.gr/p/tomorrows-lawyers-an-introduction-to-your-future>

LEI Nº 8.906, DE 4 DE JULHO DE 1994.

TÍTULO I

Da Advocacia

CAPÍTULO I

Da Atividade de Advocacia

Art. 1º São atividades privativas de advocacia:

I - a postulação a órgão do Poder Judiciário e aos juizados especiais

II - as atividades de consultoria, assessoria e direção jurídicas.

Alvaro de Azevedo Gonzaga
Karina Penna Neves
Roberto Beijato Junior

ESTATUTO DA ADVOCACIA *e* CÓDIGO DE ÉTICA E DISCIPLINA DA OAB

Comentados

- Indicação de julgados e normas correlatas
- Índice alfabético-remissivo do CED

Prefácio
Marcus Víncius Furtado Coelho
Apresentação
Pedro Estevam Serrano

De acordo com:
• Leis 14.365 e 14.508 de 2022 - Alterações no EAQAB

8ª edição
revista e atualizada



<https://www.livrariascuritiba.com.br/estatuto-da-advocacia-e-codigo-de-etica-e-disciplina-da-oab---comentados-lv503038/p>

CÓDIGO DE ÉTICA E DISCIPLINA OAB

Art. 5º O exercício da advocacia é incompatível com qualquer procedimento de mercantilização.

Art. 28. O advogado pode anunciar os seus serviços profissionais, individual ou coletivamente, com discrição e moderação, para finalidade exclusivamente informativa, vedada a divulgação em conjunto com outra atividade.



Alvaro de Azevedo Gonzaga
Karina Penna Neves
Roberto Beijato Junior

ESTATUTO DA ADVOCACIA *e* CÓDIGO DE ÉTICA E DISCIPLINA DA **OAB**

Comentados

- Indicação de julgados e normas correlatas
- Índice alfabético-remissivo do CED

Prefácio
Marcus Vinícius Furtado Coelho
Apresentação
Pedro Estevam Serrano

De acordo com:
• Leis 14.365 e 14.508 de 2022 - Alterações no EAQAB

8ª edição
revista e atualizada



<https://www.livrariascuritiba.com.br/estatuto-da-advocacia-e-codigo-de-etica-e-disciplina-da-oab---comentados-lv503038/p>

Provimento Nº 205/2021 – **Anexo ÚNICO** - OAB

Aplicativos para responder consultas jurídicas

Não é admitida a utilização de aplicativos de forma indiscriminada para responder automaticamente consultas jurídicas a não clientes por suprimir a imagem, o poder decisório e as responsabilidades do profissional, representando mercantilização dos serviços jurídicos.

Aquisição de palavra-chave a exemplo do Google Ads

Permitida a utilização de ferramentas de aquisição de palavra-chave quando responsável a uma busca iniciada pelo potencial cliente e desde que as palavras selecionadas estejam em consonância com ditames éticos. **Proibido o uso de anúncios ostensivos em plataformas de vídeo.**

Provimento Nº 205/2021 – Anexo ÚNICO - OAB

Correspondências e comunicados (mala direta);

O envio de cartas e comunicações a uma coletividade ("mala direta") é expressamente vedado. Somente é possível o envio de cartas e comunicações se destinadas a clientes e pessoas de relacionamento pessoal ou que os solicitem ou os autorizem previamente, desde que não tenham caráter mercantilista, que não representem captação de clientes e que não impliquem oferecimento de serviços.



<https://aoredordoburacotudoibeira.wordpress.com/2017/05/05/mala-direta-criando-etiquetas-de-enderecameto/>

Provimento Nº 205/2021 – Anexo ÚNICO - OAB

<https://blog.juriscorrespondente.com.br/chatbots-na-advocacia-o-guia-completo/>

Chatbot



Permitida a utilização para o fim de facilitar a comunicação ou melhorar a prestação de serviços jurídicos, não podendo afastar a pessoalidade da prestação do serviço jurídico, nem suprimir a imagem, o poder decisório e as responsabilidades do profissional. É possível, por exemplo, a utilização no site para responder as primeiras dúvidas de um potencial cliente ou para encaminhar as primeiras informações sobre a atuação do escritório. Ou ainda, como uma solução para coletar dados, informações ou documentos.



Provimento Nº 205/2021 – **Anexo ÚNICO** – OAB

- **Patrocínio e impulsionamento nas redes sociais:** Permitido, desde que não se trate de publicidade contendo oferta de serviços jurídicos.
- **Redes Sociais:** É permitida a presença nas redes sociais, desde que seu conteúdo respeite as normas do Código de Ética e Disciplina e do presente provimento.
- **Grupos de "whatsapp":** Permitida a divulgação por meio de grupos de "whatsapp", desde que se trate de grupo de pessoas determinadas, das relações do(a) advogado(a) ou do escritório de advocacia e seu conteúdo respeite as normas do Código de Ética e Disciplina e do presente provimento.
- **Lives nas redes sociais e Youtube:** É permitida a realização de lives nas redes sociais e vídeos no Youtube, desde que seu conteúdo respeite as normas do Código de Ética e Disciplina e do presente provimento.

EUA – permite publicidade de serviços advocatícios de forma mais ampla, apenas vedando-se desvios excessivos do ponto de vista da ética profissional.

Reino Unido e Austrália – mais liberal, permite-se até participação societária por terceiros no intuito de desenvolver escritórios e novas tecnologias.



<https://wizardofads.org/left-turn-to-albuquerque/>

Ação Civil Pública da OAB/RJ contra a Startup

LIBERFLY para que fosse condenada a se abster, definitivamente, de praticar qualquer ato de anúncio, de publicidade ou de divulgação de oferta de serviços jurídicos consistentes na angariação ou captação de clientela.

Sentença 1^a Instância: Condenou a LIBERFLY na obrigação de não fazer publicidade ou divulgação de oferta de serviços jurídicos.

Apelação: LIBERFLY alega que seu modelo de negócios é baseado na cessão de crédito e ativos judiciais. Até o momento, não foi julgada.

OAB/MG – Reclamação de Escritório Tradicional contra Startup de Privacidade e Proteção de Dados.



Início

Quem somos

Quando tenho direito?

Indique e Ganhe

Nosso Blog

Fale conosco

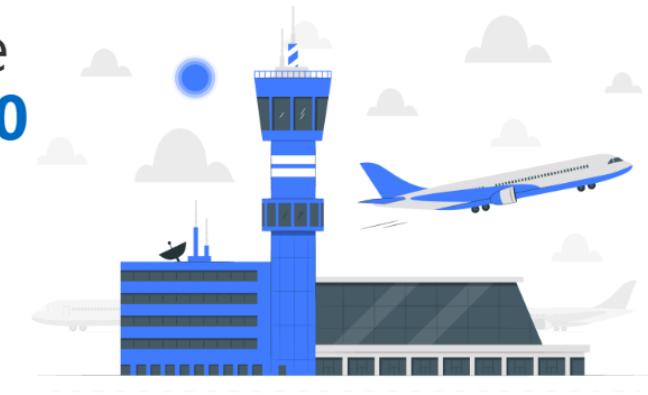
Avaliar agora

Problemas de Viagem?
Conte com a LiberFly e
receba até **R\$ 1.000,00**
para resolvê-los.

Se você passou nos últimos 5 anos por: **problemas de voo, hospedagem, viagens de ônibus e aluguel de carros**, tenha o seu caso analisado **gratuitamente** pela LiberFly e receba até R\$1.000,00 em 48 horas.

Avaliar meu caso agora

★ Mais de 100.000 clientes satisfeitos com a LiberFly
A LiberFly atende os consumidores que tiveram problemas de viagem ✓ Somos parceiros da OAB



www.liberfly.com.br



Marcas registradas pelo autor



**TRADICIONALISMO
IMPERA NA
ADVOCACIA**

TRADIÇÃO
OU
RESERVA DE MERCADO ?

TECNOLOGIAS DISRUPTIVAS E REGULAÇÃO DA ADVOCACIA: SINAIS RECENTES E PERSPECTIVAS

Marcos Luiz dos Mares Guia Neto

Mestrando em Direito Empresarial pela Universidade Federal de Minas Gerais –
UFMG. Advogado no Sergio Bermudes Advogados.

<https://www.dtibr.com/>

Autores

Ana Luisa Teotônio Josafá Simão
Arthur Salles de Paula Moreira
Bernardo Menicucci Grossi
Bruna de Paula Ferreira Costa
Cristiano Colombo
Giovanni Carlo Batista Ferrari
Gustavo Baião Vilela
Jessica Aparecida Soares
José Luiz de Moura Faleiros Júnior
Júlia Lio Rocha Camargo
Laurence Duarte Araújo Pereira
Luisa de Almeida Naves
Maique Barbosa de Souza
Marcela Adriana Carvalho Andrade
Marcos Luiz dos Mares Guia Neto
Marina Moretzsohn Chust Trajano
Matheus Puppe
Priscilla Menezes Santos Rodrigues
Rafael de Miranda
Renata Diniz de Souza
Sofia Bertolini Martinelli

Leonardo PARENTONI
Coordenador

Giovanni Carlo Batista Ferrari
José Luiz de Moura Faleiros Júnior
Tárik César Oliveira e Alves
Organização

**DIREITO,
TECNOLOGIA
E INOVAÇÃO**
vol. 4: *estudos de casos*



TÉCNICAS DE NEGOCIAÇÃO

Luiz Felipe Vieira de Siqueira

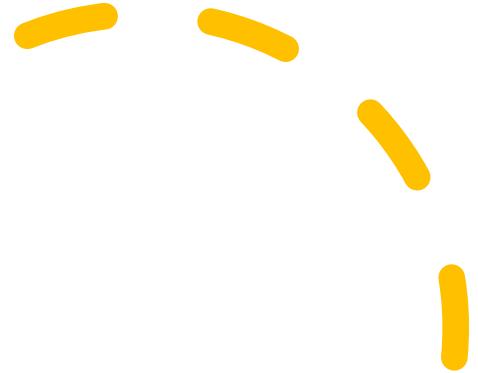
E-book

Técnicas infalíveis de negociação

Para advogados



JURISCORRESPONDENTE



<https://www.juriscorrespondente.com.br/>

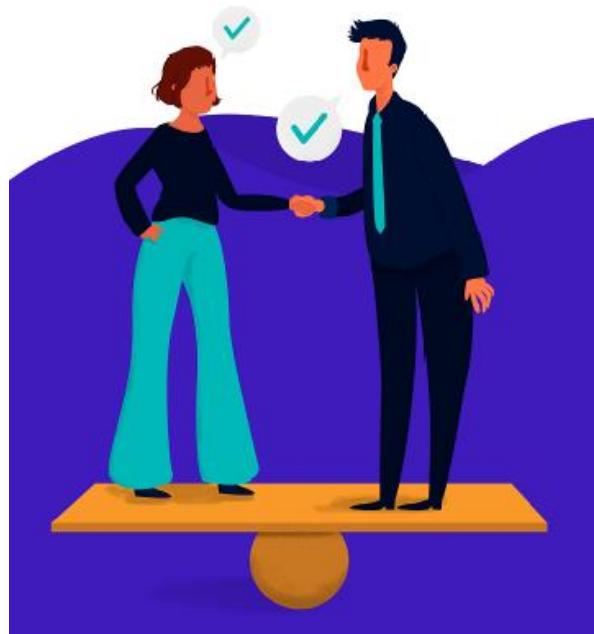
Projeto de Negociação de Harvard

Tipos de Negociador

Gentil	Firme	Por princípios
As partes são amigas	As partes são adversárias	As partes são solucionadores de problemas
O objetivo é o acordo	O objetivo é vencer	O objetivo é o acordo sensato, eficiente e amistoso
É gentil com a outra parte e com o dilema	É firme com a outra parte e com o dilema	É gentil com a outra parte e firme com o dilema
Aceita perder	Exige ganhar	Busca ganhos mútuos

Negociação Integrativa

e a era 4.0 do Direito



- Os princípios básicos da são:

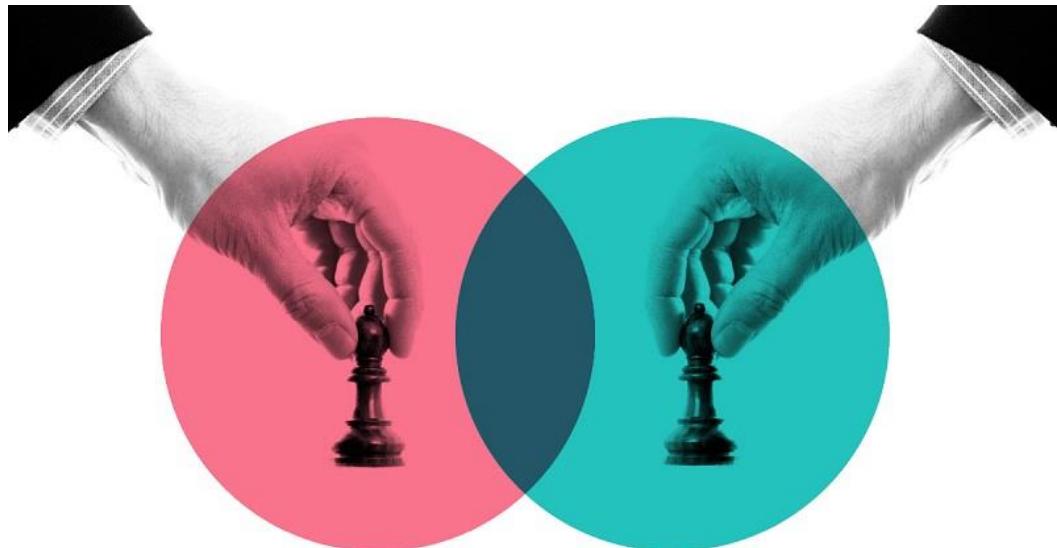
1. Separe as pessoas dos problemas;
2. Concentre-se nos interesses, não nas posições;
3. Crie opções de possibilidade de ganhos mútuos; e
4. Insista em critérios objetivo



<https://www.ibccoaching.com.br/portal/metas-e-objetivos/o-que-e-uma-relacao-ganha-ganha/>

TRÊS FASES DA NEGOCIAÇÃO

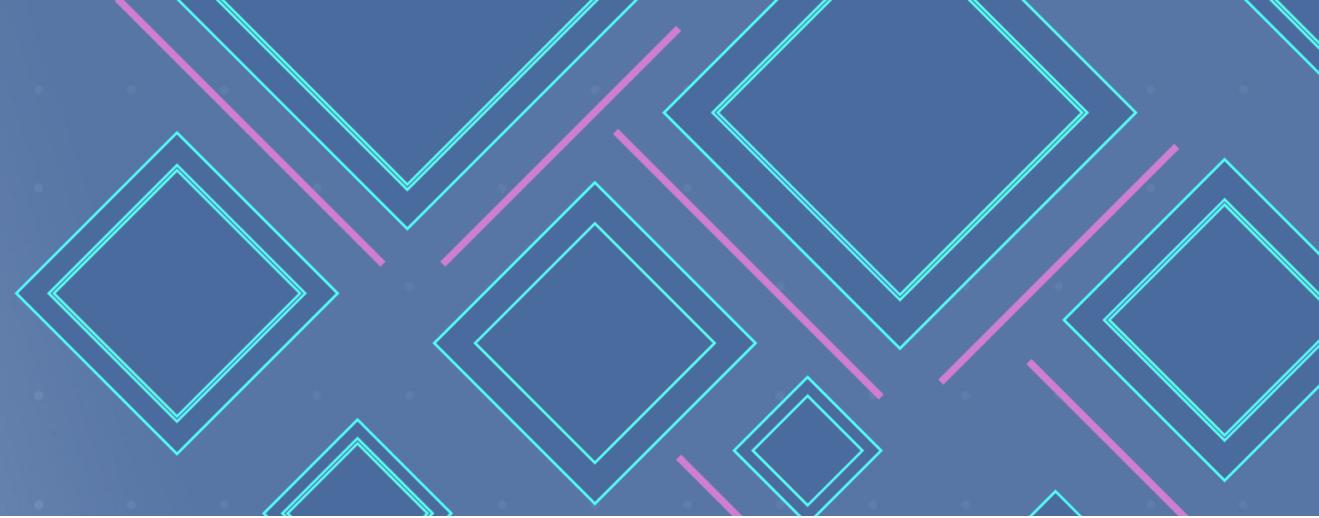
- **Primeira:** é a **análise**, onde você vai levar em conta a sua percepção, sentimentos, emoções e opções da outra parte, os seus interesses e já pensar em critérios objetivos para a futura negociação.
- **Segunda:** após o diagnóstico, partimos para o **planejamento**. É o momento de decidir como irá proceder, quais os interesses mais importantes, quais pontos discutir primeiro, quais são mais realistas etc.
- **Terceira:** a última fase é a discussão, fase em que **as partes se comunicam diretamente** e colocam em prática os quatro princípios da negociação. De preferência deve ser feita em um ambiente que favoreça o diálogo, seja neutro e que todos tenham as mesmas oportunidades de se expressar.



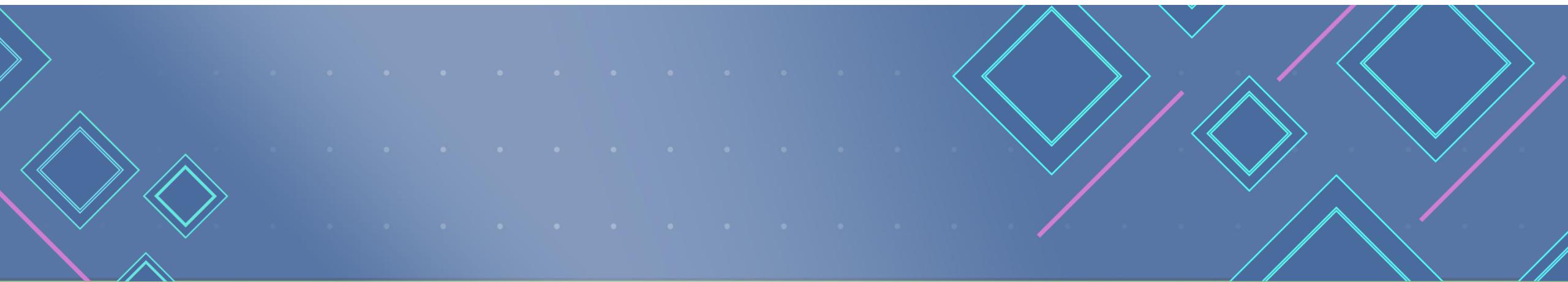
<https://lcmtreinamento.com.br/a-negociacao-e-o-mito-ganha-ganha/>



PUC Minas



GATILHOS MENTAIS



O que são gatilhos mentais?



<https://www.juridigital.com.br/gatilhos-mentais-na-advocacia/>

- Os gatilhos mentais podem estar contidos em **eventos ou circunstâncias externas que conseguem ativar determinada parte do cérebro, fazendo com que a pessoa responda a esse estímulo**, seja ele negativo ou positivo.
- Por meio de um **gatilho mental** a pessoa pode sentir **aspectos negativos, como ansiedade, pânico, desânimo, desespero, entre outras sensações**. Já quando os estímulos são positivos é possível que a pessoa sinta alegria, calma, confiança, entusiasmo e motivação.

GATILHOS MENTAIS

1. Reciprocidade

O gatilho da reciprocidade é bastante utilizado por políticos, pois ele proporciona às pessoas que recebem algo de alguém sem pedir nada em troca, o dever de retribuir o favor.

2. Autoridade

O gatilho da autoridade consiste em posicionar o seu negócio como referência no segmento em que atua.

3. Prova Social

O gatilho mental da prova social é uma ótima oportunidade para atrair e conquistar a confiança de novos clientes. Isso porque, essa estratégia consiste em destacar e promover clientes que tiveram sucesso com o seu produto ou serviço.



<https://www.maisweb.com.br/site1/index.php/blos/marketing-digital/127-13-principais-gatilhos-mentais-que-todo-empresario-produtor-de-conteudo-precisa-dominar>

GATILHOS MENTAIS

4. Princípio da novidade

Praticamente todo o ser humano possui grande curiosidade sobre aquilo que é novo, isso torna o gatilho da novidade um forte alinhado de vendedores e profissionais de marketing.

5. Escassez e urgência

O princípio da escassez e da urgência quando aplicado nas estratégias de marketing digital rende bastante resultados positivos.

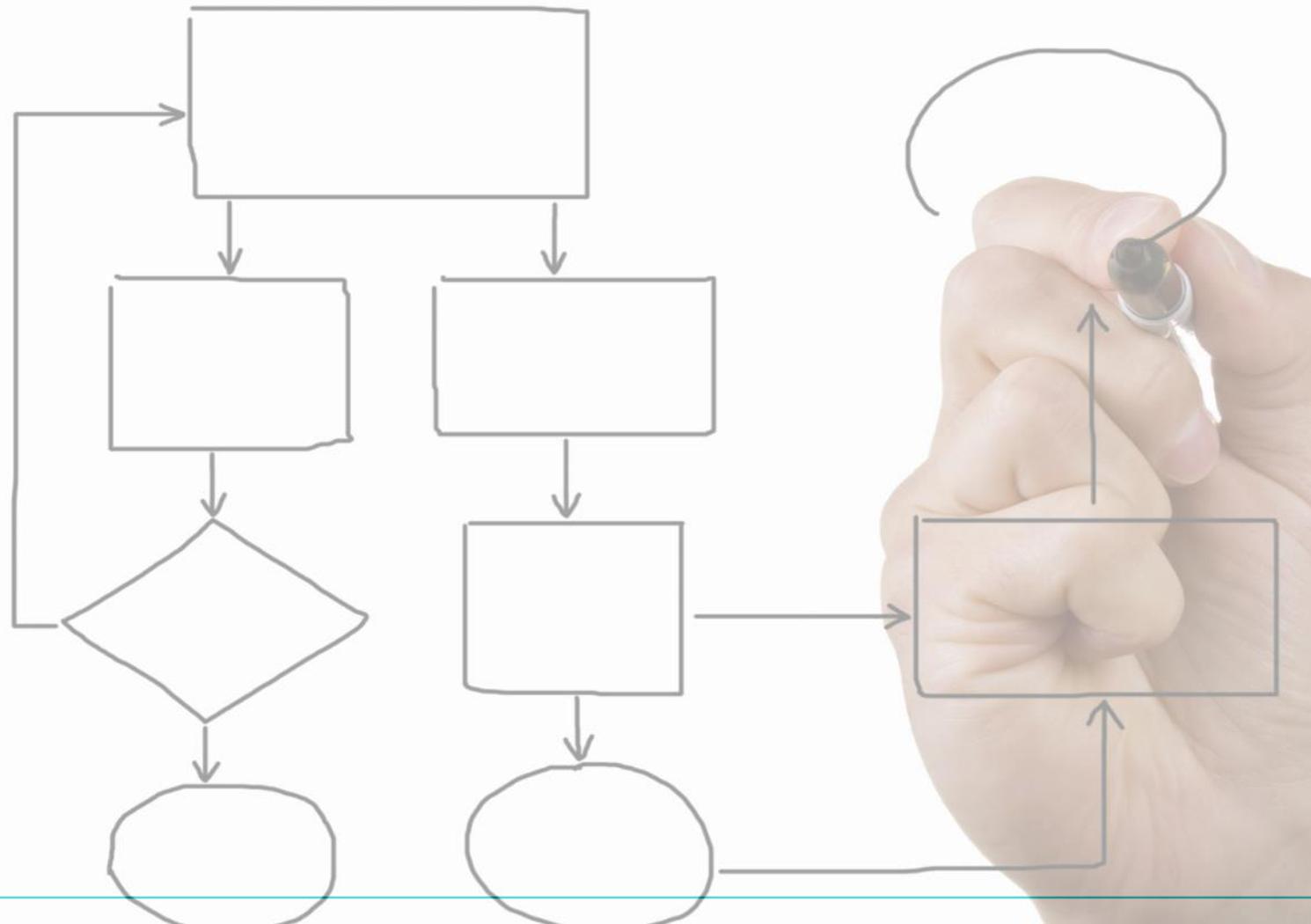


DATA MAPPING

Luiz Felipe Vieira de Siqueira

Mapeamento, Inventário de Dados Inventário de Sistemas e Análise de Risco

Mapeamento de Processos

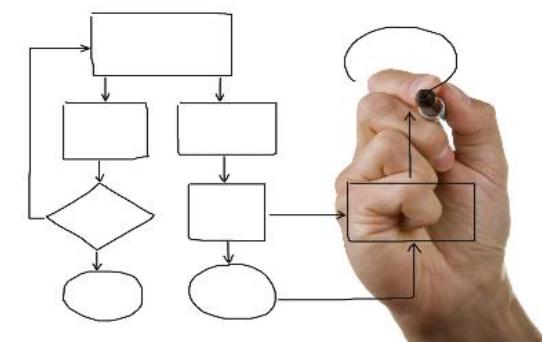


Fonte: Privacy Point

O que é mapeamento de processos?

Identificação da sequência lógica das atividades que compõem um processo e de outros elementos que interagem com o fluxo de trabalho.

Fonte: Privacy Point



Por que mapear processos?

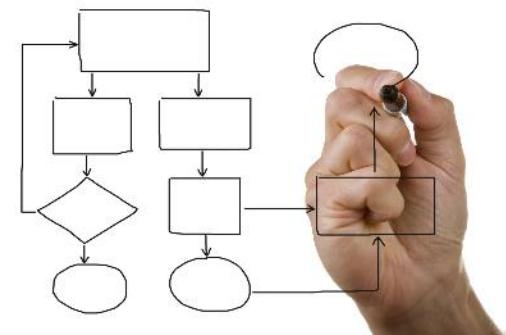
Melhorar os processos

Padronizar os processos

Transformar os processos

Documentar os processos

Compreender os processos



Tipos de processos

1

Processos Primários

Relacionados diretamente com a entrega de valor ao cliente final

2

Processos de Suporte

Apoiam os processos primários de gerenciamento

3

Processos de Gestão

Acompanha todos os outros processos

O que é um macroprocesso

Agrupamentos de **processos** necessários para a produção de uma ação ou desempenho de uma **atribuição** da organização.

Grandes **conjuntos de atividades** pelos quais a organização cumpre sua missão, gerando valor para o cliente/cidadão/usuário.

O que é um macroprocesso

Área: Departamento Pessoal

Admitir funcionário

Demitir funcionário

Fechar folha de pagamento

Registrar atestados

Programar férias, etc.

Níveis de mapeamento

Nível 1 ou Descritivo

Busca apenas alinhar o entendimento do processo entre os envolvidos, trazendo uma **visão básica do processo**.

Nível 2 ou Analítico

Destaca os eventos e tratamentos de exceção, fornecendo uma **visão mais técnica do processo**.

Nível 3 ou Executável

Detalha os serviços que serão implementados ou automatizados, trazendo uma **visão focada nos dados**.



Técnicas de mapeamento

Entrevistas

Fonte: Privacy Point



Técnicas de mapeamento

Questionários



Fonte: Privacy Point

Técnicas de mapeamento

Reuniões

Fonte: Privacy Point



Técnicas de mapeamento

Oficinas



Fonte: Privacy Point

Técnicas de mapeamento

Workshops

Fonte: Privacy Point



Fonte: Privacy Point

Técnicas de mapeamento

Observação



<https://vivaoftalmologia.com.br/doencas-dos-olhos/>

Técnicas de mapeamento

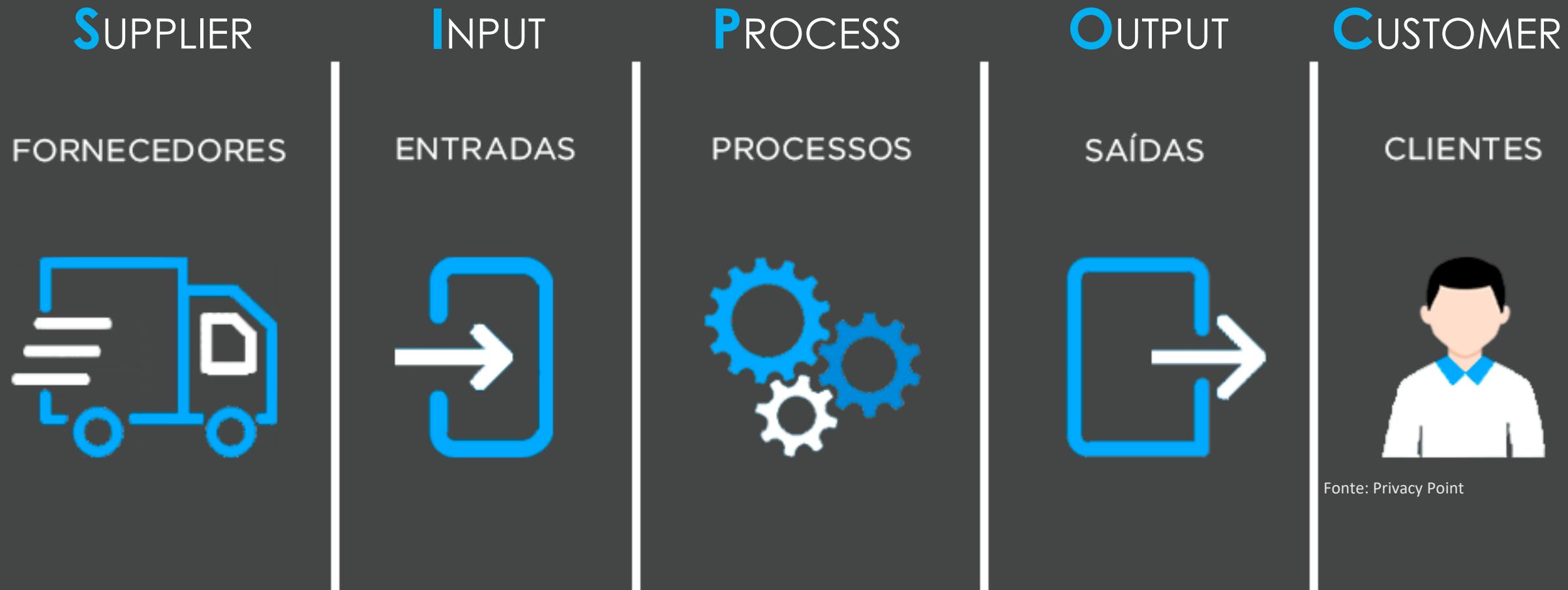
Análise documental



Fonte: Privacy Point

Técnicas de mapeamento

Matriz SIPOC



Técnicas de mapeamento

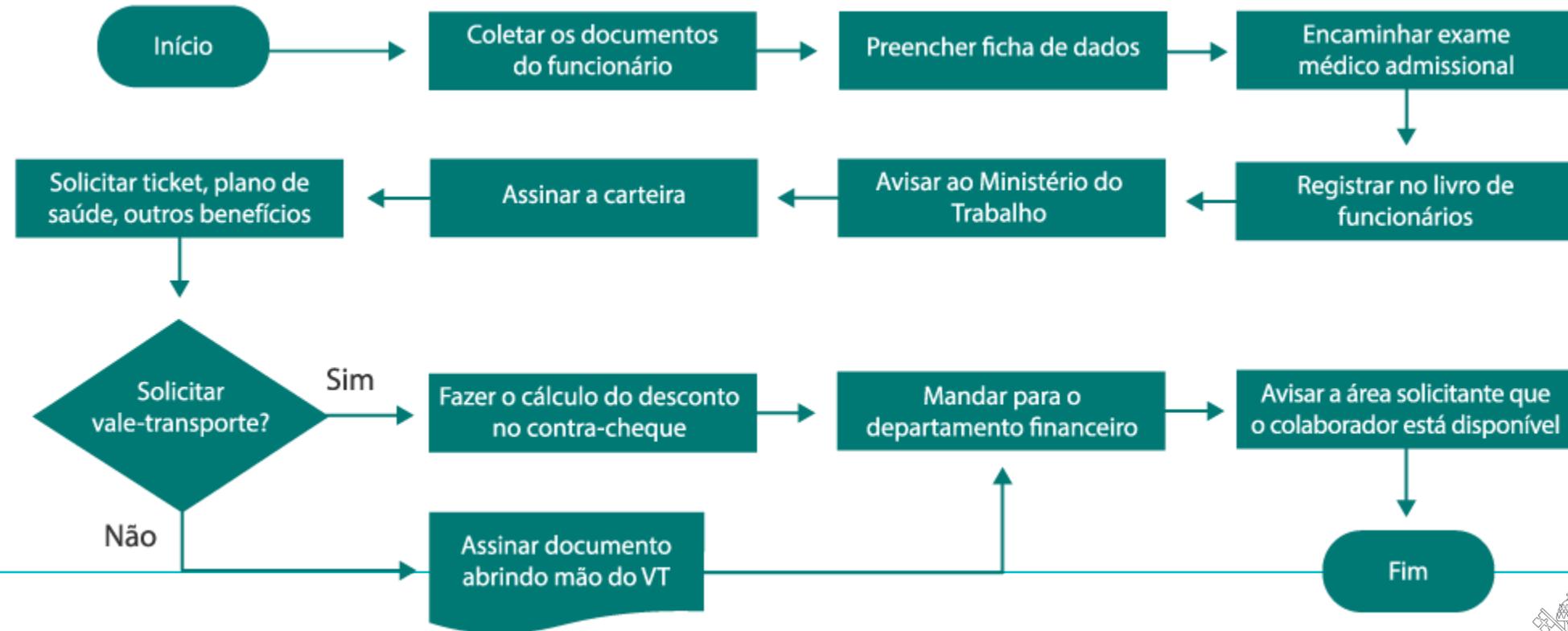
Diagrama de tartaruga



Fonte: Privacy Point

Técnicas de mapeamento

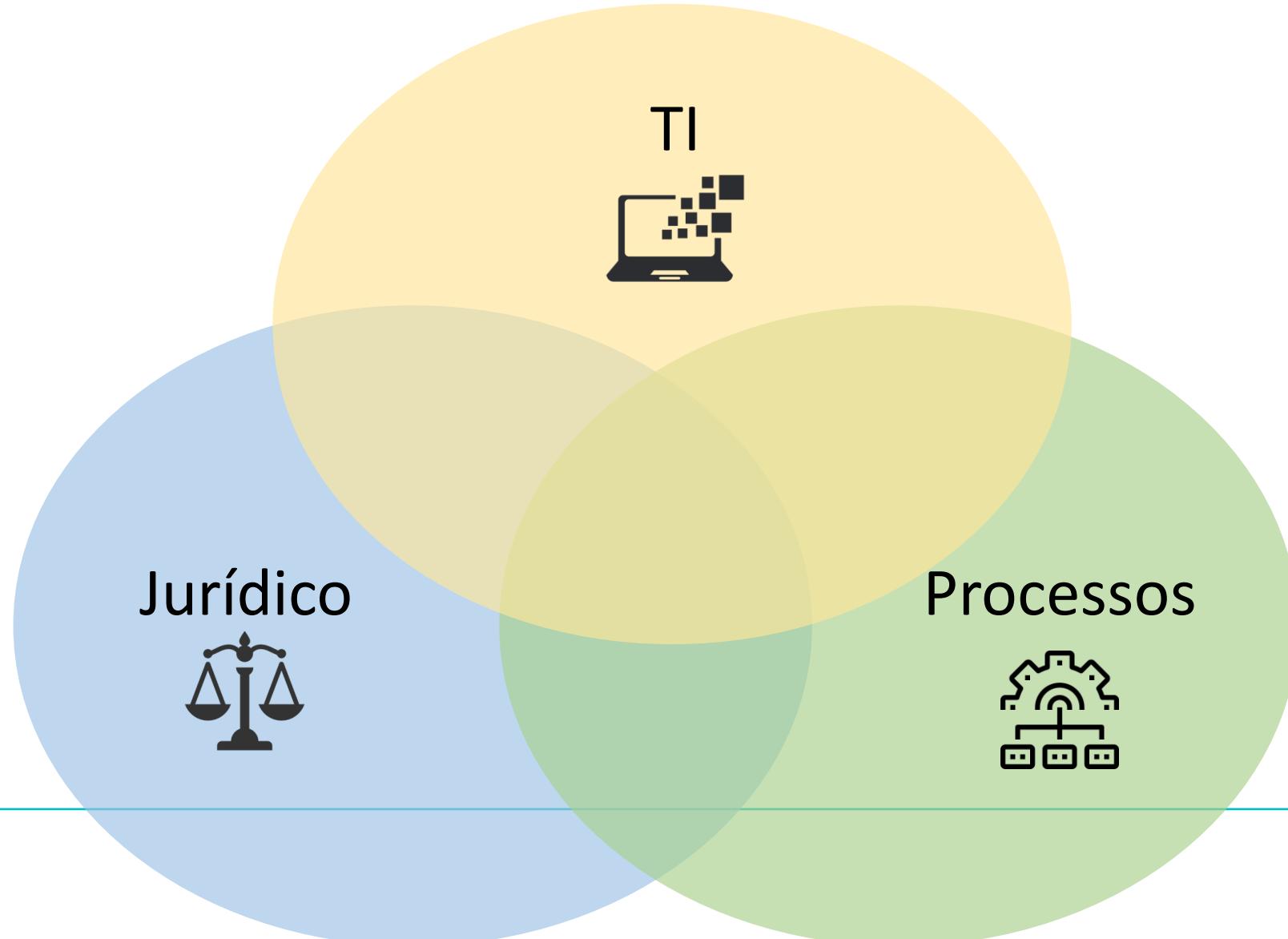
Fluxograma



O que é Data Mapping?

O data mapping se refere ao processo de rastreamento e catalogação dos dados **coletados** e **processados** por determinada organização.

Como fazer um Data Mapping



Como fazer um Data Mapping

Tipos de dados

Pessoal



Sensível



Crianças e adolescentes



Biométrico



Identificado



Identificável

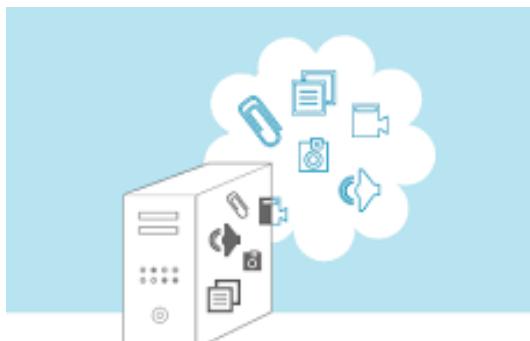


Fonte: Privacy Point

Como fazer um **Data Mapping**

Armazenamento

Local



Nuvem



Físico



Digital

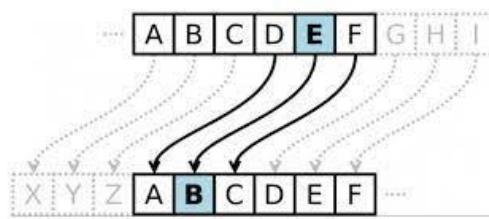


Fonte: Privacy Point

Como fazer um Data Mapping

Segurança

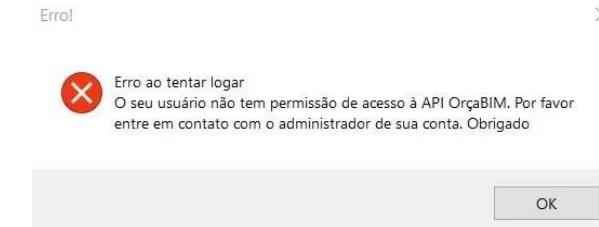
Criptografia



Backup



Permissão de acesso



Descarte



Compartilhamento



Fonte: Privacy Point

Como fazer um Data Mapping

Volumetria

Quantos processos
tratam os dados?

Qual o tamanho da
base?

Qual a frequência de
tratamento?

Fonte: Privacy Point



Como fazer um Data Mapping

Origem

Coleta direta com o titular

Coleta indireta com o titular

Recebimento por terceiros

Fonte: Privacy Point



Como fazer um Data Mapping

Tecnologia

Periféricos



Sistemas e fornecedores



Bancos de dados



Fonte: Privacy Point

Como fazer um Data Mapping

Transferência internacional

Avaliar as possibilidades de transferências internacionais de dados por meio de uso de plataformas *cloud*, *data centers centralizados*, transferências para sede ou filial no exterior.



Fonte: Privacy Point

Gestão de Riscos

O que é risco?

Um risco é um evento ou condição **incerta** que, se ocorrer, causará um efeito negativo ou positivo em um ou mais objetivos do projeto.

Gestão de Riscos

O que é matriz de risco?

A matriz de risco é um instrumento que facilita a **seleção de prioridades** para se empreender uma ação. Uma matriz de risco é uma **representação gráfica** e às vezes matemática da combinação da probabilidade de algo acontecer associado com a consequência potencial da ocorrência.

Gestão de Riscos

Como fazer uma matriz de risco?

- 1- Identificar os dados tratados;
- 2- Identificar o ambiente no qual os dados são tratados;
- 3- Para cada situação identificada, avaliar **probabilidade** de vazamento com base na maturidade quanto à ISO/IEC 27001 e o **impacto** com base na LGPD.

Gestão de Riscos

Como fazer uma matriz de risco?

		1	2	5	9	11		
		Muito Baixo	Baixo	Médio	Alto	Muito Alto		
Probabilidade	5 Muito Alto	5x5=25	5x2=10	5x1=5	5x9=45	5x11=55	1 à 3 Trivial	4 à 8 Tolerável
	4 Alto	4x5=20	4x2=8	4x1=4	4x9=36	4x11=44		
	3 Médio	3x5=15	3x2=6	3x1=3	3x9=27	3x11=33		
	2 Baixo	2x5=10	2x2=4	2x1=2	2x9=18	2x11=22		
	1 Muito Baixo	1x5=5	1x2=2	1x1=1	1x9=9	1x11=11		
Impacto								



Gestão de Riscos

Limitações de uma matriz de risco

É difícil definir as escalas com **precisão**

Seu uso é muito **subjetivo**

A classificação **dependerá** da forma como o ambiente foi descrito

Gestão de Riscos

Como apresentar?

Geral

Probabilidade	Muito Baixo	Baixo	Médio	Alto	Muito Alto
	5	6	10	0	0
Alto	35	43	87	7	4
Médio	75	85	154	22	18
Baixo	20	38	68	10	3
Muito Baixo	16	13	24	8	8

Impacto

Departamento

Área A

Probabilidade	Impacto de vazamento de dados				
	Muito Baixo	Baixo	Médio	Alto	Muito alto
Muito alto	5	6	10	0	0
Alto	32	40	78	6	4
Médio	63	61	122	20	18
Baixo	11	13	31	1	2
Muito Baixo	6	3	4	3	4

Área B

Probabilidade	Impacto de vazamento de dados				
	Muito Baixo	Baixo	Médio	Alto	Muito alto
Muito alto	0	0	0	0	0
Alto	0	0	5	0	0
Médio	0	7	13	1	0
Baixo	4	12	28	6	1
Muito Baixo	8	7	17	5	4

Área C

Probabilidade	Impacto de vazamento de dados				
	Muito Baixo	Baixo	Médio	Alto	Muito alto
Muito alto	0	0	0	0	0
Alto	3	3	4	1	0
Médio	12	17	19	1	0
Baixo	5	13	9	3	0
Muito Baixo	2	3	3	0	0

Dado tratado

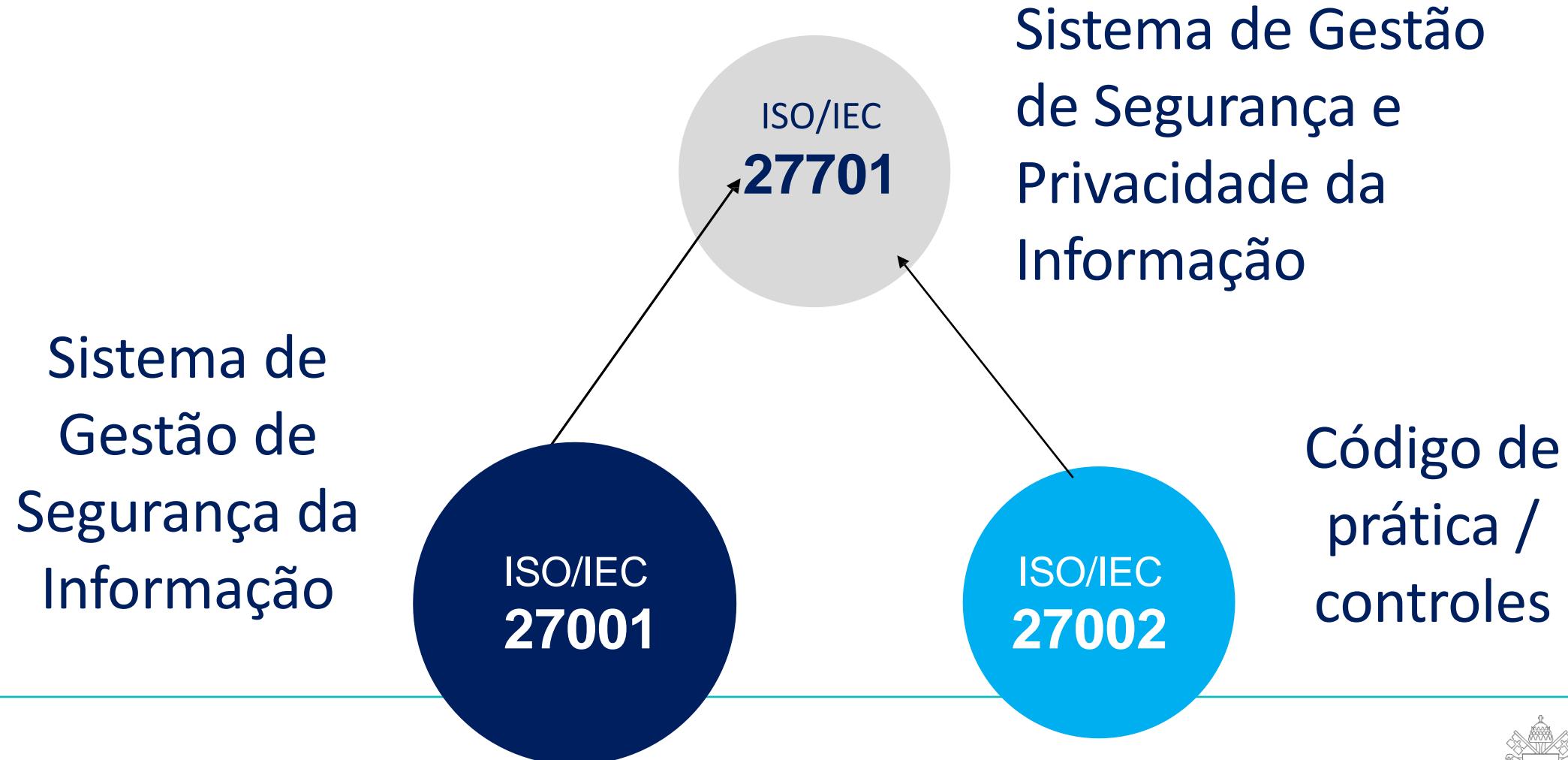
Risco de vazamento dos dados tratados

Dado	Probabil.	Impacto
CPF	Médio	Médio
Data de nascimento	Médio	Médio
E-mail corporativo	Médio	Muito baixo
Endereço	Médio	Médio
Nacionalidade	Médio	Baixo
Telefone corporativo	Médio	Muito baixo

Segurança da Informação

Luiz Felipe Vieira de Siqueira

FRAMEWORK ISO 27K



ISO 27701

- Participaram do seu desenvolvimento:
- CNIL (Agência Francesa), Comitê Europeu para a Proteção de Dados (e Autoridades de Proteção de Dados da UE).
- Norma foi desenvolvida com expectativa de
- satisfazer aos “*mecanismos de certificação*” referidos no artigo 42 do GDPR.
- **PORÉM, o Comitê Europeu para a Proteção de Dados ainda não reconheceu nenhum mecanismo de certificação para a GDPR.**



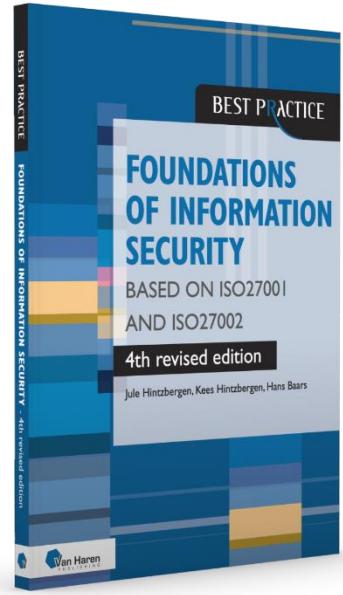
dreamstime.com

ID 225403353 © Iulian Dragomir

<https://pt.dreamstime.com/aguarde-e-veja-o-texto-no-selo-de-borracha-azul-esbranqui%C3%A7ado-do-carimbo-redonda-vintage-image225403353>

REFERÊNCIA

• FOUNDATIONS OF INFORMATION SECURITY – NORMAS ISO



- Baars, H., Hintzbergen, J., and Hintzbergen, K. Foundations of Information Security –Based on ISO 27001 and ISO 27002 Van Haren Publishing: 4th fully revised edition, 2023 [LINK PARA COMPRA VANHAREN](#)

- Normas da família ISO 27000

- Onde obter - [link](#)

DADO E INFORMAÇÃO



DADO: Descrição exata de algo ou algum evento. É a matéria-prima para geração de informação. Sozinho o dado não tem significado.



INFORMAÇÃO: Dados interpretados, dotados de relevância e propósito. (Peter Drucker)



CONHECIMENTO: Informação com valor adicionado pela mente humana - reflexão, síntese e contexto. “Conhecimento é informação eficaz em ação, focalizada em resultados. (Peter Drucker)



SABEDORIA: É modo como utilizamos esses conhecimentos adquiridos ao longo da vida.



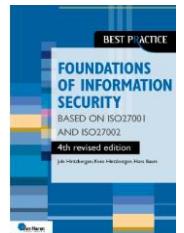
INFORMÁTICA: procedimento que converte dados em informação.

GESTÃO DA INFORMAÇÃO

SEGUNDO O AUTOR VAN HAREN

“A gestão da informação descreve o meio pelo qual uma organização planeja, coleta, organiza, utiliza, controla, dissemina e descarta suas informações de forma eficiente, e através da qual garante que o valor dessa informação seja identificado e explorado em toda a sua extensão”.

Referência: Foundations of Information Security, Van Haren



SEGURANÇA DA INFORMAÇÃO



PRESERVAÇÃO DO
CID



Confidencialidade



Integridade



disponibilidade da
informação.



Fonte: ISO /IEC 27000:2018

1. Princípio da Disponibilidade

A disponibilidade está relacionada ao tempo e à acessibilidade que se tem dos dados e sistemas da organização, esse princípio é de suma importância, pois, falhas de indisponibilidade comprometem o serviço prestado pela organização.

Através dos riscos associados a informação mapeados, a organização deve criar um plano de recuperação de dados, com um Plano de Continuidade de Negócios e recuperação de desastres (Disaster Recover), que serão colocados em prática de forma reativa a um incidente de segurança da informação.

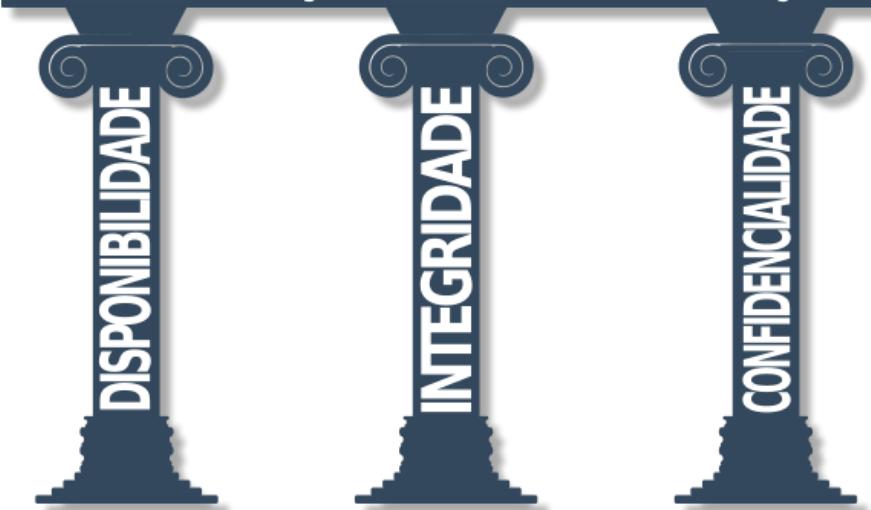
2. Princípio da Integridade

Integridade é que garante a veracidade da informação e restringe o acesso e/ou alteração da informação por pessoas não autorizadas, garante a completude e preservação da precisão da informação, para que não haja perda de partes da informação.

3. Princípio da Confidencialidade

A confidencialidade é o que garante o sigilo de informação e impede que elas não sejam roubadas ou acessadas por pessoas não autorizadas.

SEGURANÇA DA INFORMAÇÃO



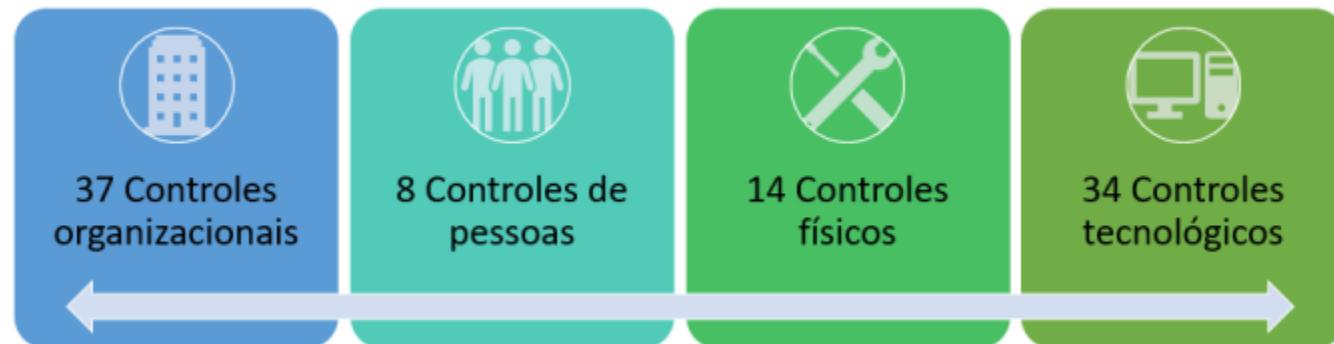
<https://qmsbrasil.com.br/wp-content/uploads/2021/06/iso-27001-iso-27701-compactado.pdf>

MEDIDAS DE SEGURANÇA

ISO 27002:2022

- ▶ Após uma análise de riscos são descritas as medidas de segurança. São controles realizados para evita, mitigar, transferir ou aceitar os danos aos ativos de informação.
- ▶ Os controles da ISO 27002 são referenciados no Anexo da ISO 27001.

93 Controles da nova ISO 27002



CONTROLES ORGANIZACIONAIS ISO 27002

37 Controles organizacionais

- 5.1 Políticas de segurança da informação
- 5.2 Papéis e responsabilidades pela segurança da informação
- 5.3 Segregação de funções
- 5.4 Responsabilidades da direção
- 5.5 Contato com autoridades
- 5.6 Contato com grupos de interesse especial
- 5.7 Inteligência de ameaças
- 5.8 Segurança da informação no gerenciamento de projetos
- 5.9 Inventário de informações e outros ativos associados
- 5.10 Uso aceitável de informações e outros ativos associados
- 5.11 Devolução de ativos
- 5.12 Classificação das informações
- 5.13 Rotulagem de informações
- 5.14 Transferência de informações
- 5.15 Controle de acesso
- 5.16 Gestão de identidade
- 5.17 Informações de autenticação
- 5.18 Direitos de acesso
- 5.19 Segurança da informação nas relações com fornecedores
- 5.20 Abordagem da segurança da informação nos contratos de fornecedores
- 5.21 Gestão da segurança da informação na cadeia de fornecimento de TIC
- 5.22 Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores
- 5.23 Segurança da informação para uso de serviços em nuvem
- 5.24 Planejamento e preparação da gestão de incidentes de segurança da informação
- 5.25 Avaliação e decisão sobre eventos de segurança da informação
- 5.26 Resposta a incidentes de segurança da informação
- 5.27 Aprendizado com incidentes de segurança da informação
- 5.28 Coleta de evidências
- 5.29 Segurança da informação durante a disruptão
- 5.30 Prontidão de TIC para continuidade de negócios
- 5.31 Requisitos legais, estatutários, regulamentares e contratuais
- 5.32 Direitos de propriedade intelectual
- 5.33 Proteção de registros
- 5.34 Privacidade e proteção de Dados Pessoais
- 5.35 Análise crítica independente da segurança da informação
- 5.36 Conformidade com políticas, regras e normas para segurança da informação
- 5.37 Documentação dos procedimentos de operação

8 Controles de pessoas

- 6.1 Seleção
- 6.2 Termos e condições de contratação
- 6.3 Conscientização, educação e treinamento em segurança da informação
- 6.4 Processo disciplinar
- 6.5 Responsabilidades após encerramento ou mudança da contratação
- 6.6 Acordos de confidencialidade ou não divulgação
- 6.7 Trabalho remoto
- 6.8 Relato de eventos de segurança da informação

CONTROLE DE PESSOAS

ISO 27002

14 Controles físicos

- 7.1 Perímetros de segurança física
- 7.2 Entrada física
- 7.3 Segurança de escritórios, salas e instalações
- 7.4 Monitoramento de segurança física
- 7.5 Proteção contra ameaças físicas e ambientais
- 7.6 Trabalho em áreas seguras
- 7.7 Mesa limpa e tela limpa
- 7.8 Localização e proteção de equipamentos
- 7.9 Segurança de ativos fora das instalações da organização
- 7.10 Mídia de armazenamento
- 7.11 Serviços de infraestrutura
- 7.12 Segurança do cabeamento
- 7.13 Manutenção de equipamentos
- 7.14 Descarte seguro ou reutilização de equipamentos

34 Controles tecnológicos

- 8.1 Dispositivos endpoint do usuário
- 8.2 Direitos de acessos privilegiados
- 8.3 Restrição de acesso à informação
- 8.4 Acesso ao código-fonte
- 8.5 Autenticação segura
- 8.6 Gestão de capacidade
- 8.7 Proteção contra malware
- 8.8 Gestão de vulnerabilidades técnicas
- 8.9 Gestão de configuração
- 8.10 Exclusão de informações
- 8.11 Mascaramento de dados
- 8.12 Prevenção de vazamento de dados
- 8.13 Backup das informações
- 8.14 Redundância dos recursos de tratamento de informações
- 8.15 Log
- 8.16 Atividades de monitoramento
- 8.17 Sincronização do relógio
- 8.18 Uso de programas utilitários privilegiados
- 8.19 Instalação de software em sistemas operacionais
- 8.20 Segurança de redes
- 8.21 Segurança dos serviços de rede
- 8.22 Segregação de redes
- 8.23 Filtragem da web
- 8.24 Uso de criptografia
- 8.25 Ciclo de vida de desenvolvimento seguro
- 8.26 Requisitos de segurança da aplicação
- 8.27 Princípios de arquitetura e engenharia de sistemas seguros
- 8.28 Codificação segura
- 8.29 Testes de segurança em desenvolvimento e aceitação
- 8.30 Desenvolvimento terceirizado
- 8.31 Separação dos ambientes de desenvolvimento, teste e produção
- 8.32 Gestão de mudanças
- 8.33 Informações de teste
- 8.34 Proteção de sistemas de informação durante os testes de auditoria

A norma ISO 27701:2020

Seção 1 – explica que esta norma é aplicável a qualquer tipo de organização.

Seção 2 – Refere-se a ISO/IEC 27000, a ISO/IEC 27001, a ISO/IEC 27002 e ISO/IEC 29100 como referências normativas.

Seção 3 – Refere-se a ISO/IEC 27000 e ISO/IEC 29100 como uma norma de termos e definições.

Seção 4 – Refere-se a ISO/IEC 27001 e ISO/IEC 27002 para detalhar a estrutura do documento.

Seção 5 - Define requisitos específicos de um sistema de gestão de privacidade da informação, de acordo com a ISO/IEC 27001.

Seção 6 – Define diretrizes específicas de um sistema de gestão de privacidade da informação, de acordo com a ISO/IEC 27002.

Seção 7 - Define as diretrizes para controladores.

Seção 8 – Define as diretrizes para operadores.

Anexo A – Uma lista de controles para controladores de DP. (Normativo)

Anexo B – Uma lista de controles para operadores de DP. (Normativo)

Anexo C – Mapeamento de controles para controladores de DP com os princípios da privacidade da ISO/IEC 29100. (Informativo)

Anexo D - Mapeamento de cláusulas da ISO/IEC 27701 com os artigos do GDPR (5 a 49 exceto 43). (Informativo)

Anexo E - Mapeamento de cláusulas da ISO/IEC 27701 com os requisitos da ISO/IEC 27018 para operadores de DP em nuvens públicas e ISO/IEC 29151 para controles e orientações adicionais para controladores de DP. (Informativo)

Anexo F – Detalhes sobre como aplicar a ISO/IEC 27701 com ISO/IEC 27001 e ISO/IEC 27002. (Informativo)

Anexo N/A – Mapeamento com a LGPD. (Informativo)

<https://qmsbrasil.com.br/wp-content/uploads/2021/06/iso-27001-iso-27701-compactado.pdf>



PUC Minas