WORKSHOP

O que é e como se adequar à Lei Geral de Proteção de Dados (LGPD)

omnisblue

AGENDA

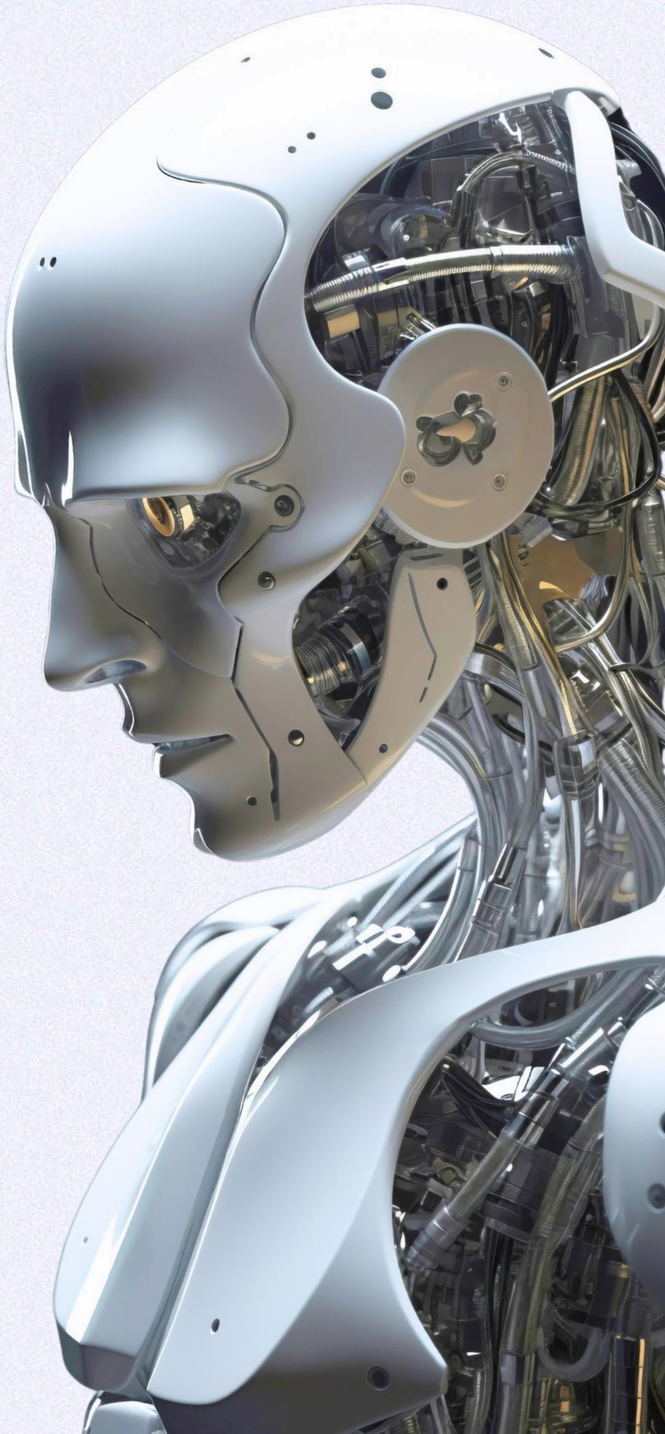
- O que é a LGPD
- Jornada de adequação à LGPD

omnisblue

+ 1 Mi
HORAS DE PROJETOS

30
ANOS

Expertise
GESTÃO PÚBLICA
LGPD



Framework Omnisblue

ADILSON TAUB JUNIOR

CEO | DPO Certified

+ 20 anos de experiência, ajudando empresas a resolver problemas com as ferramentas certas.

CERTIFICAÇÕES

Privacy & Security Management
- Data Protection Officer (DPO)
- Privacy and Data Protection Practitioner
- Privacy and Data Protection Foundation
- Information Security (ISO/IEC 27.001)

IT Governance and Service Management
- IT Service Management (ISO/IEC 20.000)
- ITIL V3 Fdn. Certified
- COBIT 4.1 Fdn. Certified
- ITIL V2 Fdn. Certified

Software Engineering
- Professional Scrum Product Owner (PSPO I)
- Professional Scrum Master (PSM I)
- Certified Scrum Professional
- Certified ScrumMaster
- Kanban Foundation KIKF
- IBM Certified Solution Designer (RUP)
- Certified Expert in BPM

CONTATO

/in/ataubjr/

adilson.taub@omnisblue.com

ACADÊMICO

Master of Business Administration - MBA
- Gestão Estratégica de Negócios

Formação Executiva
- Compliance Empresarial (FGV)

Pós-graduação
- Engenharia de Software

Graduação
- Processamento de Dados

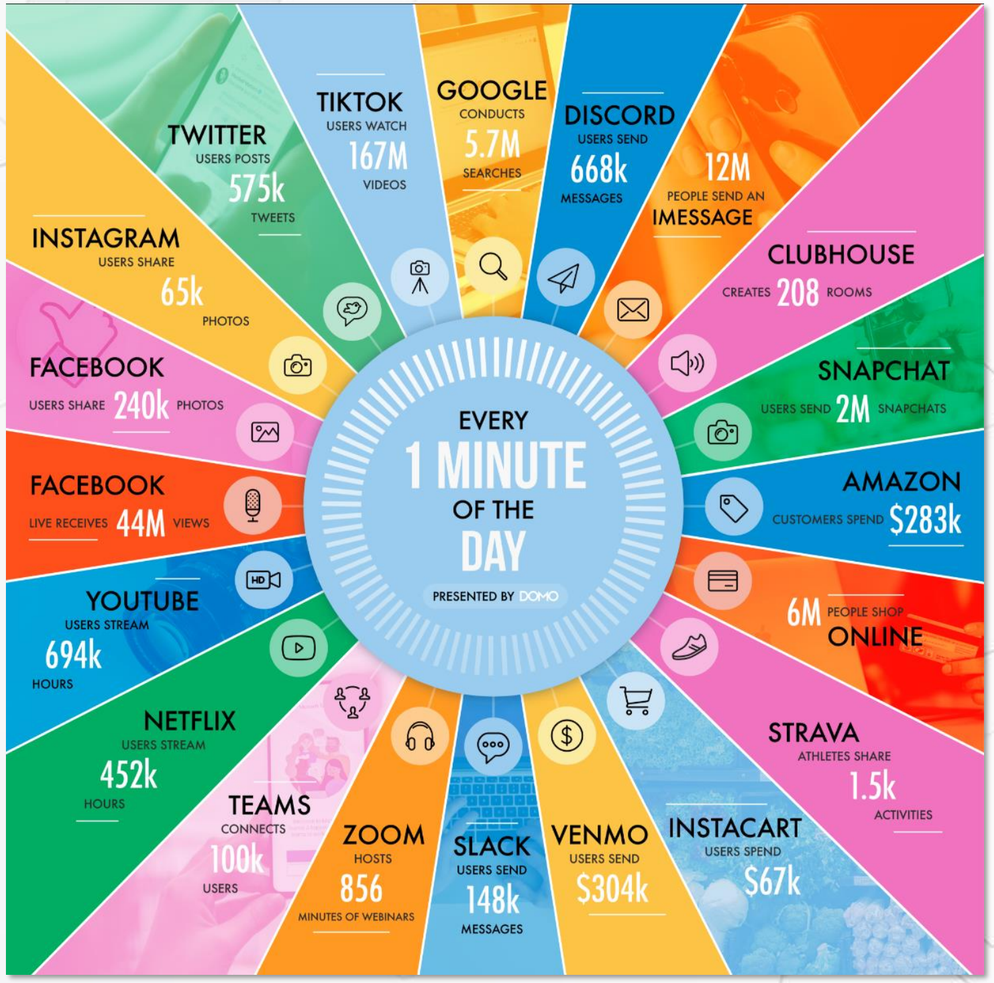
MAPA DE HABILIDADES

O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

E quais são seus principais parâmetros

omnisblue

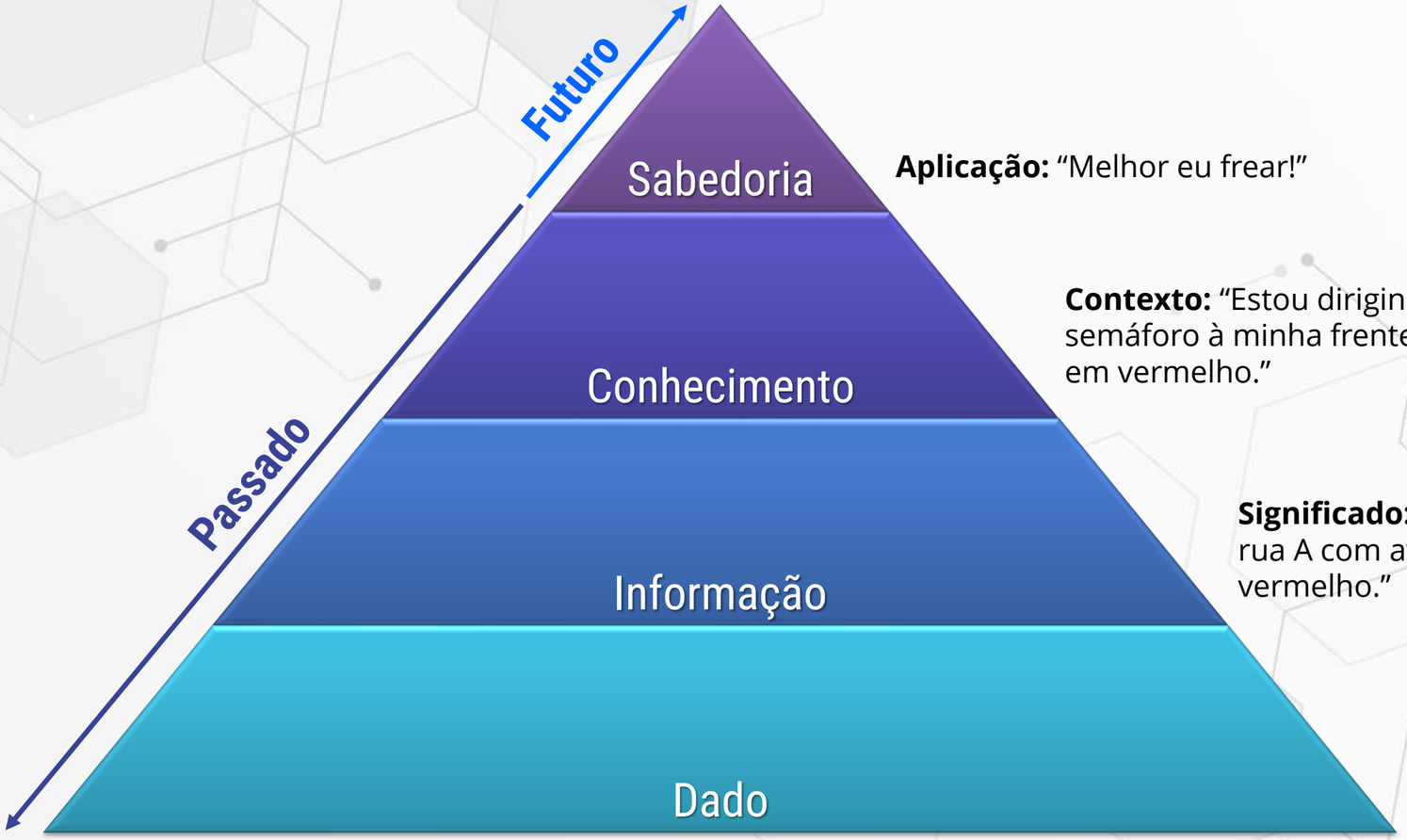
O VOLUME DE TRATAMENTO DE DADOS NA INTERNET



Fonte: Data Never Sleeps 9.0
(https://www.domo.com/learn/infographic/data-never-sleeps-9)

omnisblue

A GESTÃO DO CONHECIMENTO



Aplicação: “Melhor eu frear!”

Contexto: “Estou dirigindo um carro e o semáforo à minha frente acaba de acender em vermelho.”

Significado: “Semáforo na esquina da rua A com avenida B acendeu em vermelho.”

Parâmetro bruto: “Vermelho.”

omnisblue

OS DADOS PESSOAIS

Nome
CPF
RG
Sexo
Data de nascimento
Endereço
E-mail
....

Dado pessoal:
informação relacionada a pessoa natural identificada ou identificável.
(LGPD, Art. 5º)

omnisblue

PRIVACIDADE

“São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.”

Constituição Federal, Art. 5º, inciso X

omnisblue

HISTÓRICO DA LGPD

- Constituição Federal (Art. 5º)
- Lei de Acesso à Informação (Lei nº 12.527/2011)
- Lei de Crimes Cibernéticos (Lei nº 12.737/2012)
- Marco Civil da Internet (Lei n° 12.965/2014)
- *General Data Protection Regulation* - GDPR (EU 2016)
- *California Consumer Privacy Act of 2018* – CCPA (EUA 2018)
- Lei da Desburocratização (Lei n.º 13.726/2018)
- Resolução 4658 BACEN (2018)

omnisblue

OBJETIVO DA LGPD

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, *inclusive nos meios digitais*, por pessoa natural ou por *pessoa jurídica de direito público* ou privado, com o objetivo de *proteger os direitos fundamentais de liberdade e de privacidade* e o livre desenvolvimento da personalidade da pessoa natural.

- Promulgada em 14 de agosto de 2018
- Em vigor desde 18 de setembro de 2020
- Sanções começaram a ser aplicadas em 01 de agosto de 2021

omnisblue

FOLHA DE S.PAULO

Justiça já tem 600 decisões envolvendo lei de proteção de dados

Pedidos vão de exclusão de nomes na internet a remoção de informações no RH após demissão

Na Senacon, foram abertas 12 averiguações envolvendo proteção de dados desde setembro. Só no último mês, o órgão autuou quatro bancos, e a lista tende a crescer. Foram aplicadas multas a Itaú (R$ 9,6 milhões), Pan (R$ 8 milhões), BMG (R$ 5,1 milhões) e Cetelem (R$ 4 milhões).

Danos morais

Eletropaulo indenizará idosa por vazar dados pessoais a estranhos

A própria empresa notificou a consumidora do vazamento de dados decorrente da ação de criminosos.

terça-feira, 6 de julho de 2021

Cyrela é multada em R$ 10 mil por infração à Lei Geral de Proteção de Dados

Decisão é uma das primeiras referentes à nova lei, que entrou em vigor no dia 18.

Valor — Por Valor Online

30/09/2020 20h00 · Atualizado há 6 dias

BL CONSULTORIA DIGITAL

HOMEPAGE › PRIVACIDADE & PROTEÇÃO DE DADOS

LGPD / NOTICIAS SOBRE DIREITO DIGITAL / PRIVACIDADE & PROTEÇÃO DE DADOS

Instituição de Ensino é condenada por infração à LGPD

MPDFT AJUÍZA 1ª AÇÃO CIVIL PÚBLICA COM BASE NA LGPD

Publicado: 22/09/2020 às 7:27

Compartilhar Tweet

Iniciativa é contra empresa de informática especializada em comercializar dados cadastrais de usuários

O Ministério Público do Distrito Federal e Territórios ofereceu a primeira ação civil pública com pedido de tutela, baseada na Lei Geral de Proteção de Dados Pessoais, nesta segunda-feira, 21 de setembro. A lei, que entrou em vigor na sexta-feira, enquadra como lesiva a conduta de uma empresa sediada em Belo Horizonte (MG).

Homem pagará indenização de R$ 15.000,00 por divulgar dados pessoais sensíveis da ex-companheira. (LGPD).

A intimidade e a privacidade devem ser resguardadas, isso porque se constituem em direitos fundamentais da pessoa.

PRIVACIDADE

Ransomhack: um futuro problema envolvendo a LGPD?

Para evitar este e outros incidentes de segurança, o caminho é um só: investimento em cibersegurança

LGPD: sanções começam este ano

Em vigor desde o ano passado, LGPD começa a aplicar sanções a partir de agosto de 2021. Empresas precisam planejar sua governança de dados

O ESCOPO DA LGPD

É necessário **justificar** todos os tratamentos de Dados Pessoais que você realiza e encontrar **bases legais** que sustentem as rotinas de coleta, processamento, armazenamento e distribuição desses dados

Deve-se implementar medidas administrativas e técnicas de **segurança da informação**, para garantir a **Confidencialidade**, **Integridade** e **Disponibilidade** dos Dados Pessoais que você usa

Por fim, é preciso implantar **novos controles** operacionais e **modificar suas rotinas** atuais visando atender a todos os novos parâmetros legais em vigor, incluindo gerenciar os **Direitos dos Titulares**

omnisblue

PRINCÍPIOS A SEREM OBSERVADOS

omnisblue

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

i. **finalidade**: só se pode realizar tratamento de dados pessoais para fins explícitos e específicos, informados ao Titular de Dados;
ii. **adequação**: uma vez definido um fim, o mesmo dado pessoal não pode ser utilizado para outro fim;
iii. **necessidade**: só podemos utilizar o mínimo de dados necessários para cumprir a finalidade do tratamento;
iv. **livre acesso**: os titulares devem ter facilidades para consultar, gratuitamente, detalhes sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
v. **qualidade dos dados**: cabe ao Controlador garantir a exatidão e integridade dos dados do Titular;
vi. **transparência**: os titulares devem ter facilidades para consultar, gratuitamente, detalhes sobre a realização do tratamento e os respectivos agentes de tratamento;
vii. **segurança**: cabe ao Controlador fazer uso de medidas técnicas e administrativas para proteger os dados;
viii. **prevenção**: cabe ao Controlador adotar medidas para prevenir a ocorrência de incidentes envolvendo os dados;
ix. **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
x. **responsabilização e prestação de contas**: cabe ao Controlador comprovar o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia de suas medidas de segurança.

OS PAPÉIS PREVISTOS NA LGPD

Titular de Dados

- Pessoa física identificável
- É quem a LGPD busca garantir a privacidade
- Proprietária dos dados em tratamento

Controlador

- Pessoa física ou jurídica que é o maior responsável pelos dados dos Titulares
- É quem define as regras de segurança

Operador

- Pessoa física ou jurídica que realiza o tratamento de dados (ou parte dele) a pedido do Controlador
- Deve se adequar às regras definidas pelo Controlador

Encarregado (DPO)

- Ponto focal da LGPD dentro de um Controlador ou Operador
- Garante a adequada execução das rotinas de segurança
- Atende os Titulares e a ANPD

ANPD

- Autarquia federal que regulamentar a LGPD e garantie sua execução
- Audita Controladores e Operadores
- Aplica sanções

omnisblue

SANÇÕES POR DESCUMPRIMENTO

Art. 52 Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

i. **advertência**, com indicação de prazo para adoção de medidas corretivas;
ii. **multa simples,** de até 2% (dois por cento) do faturamento no seu último exercício totalizando até R$ 50.000.000,00 por infração;
iii. **multa diária**, observado o limite total da multa simples**;**
iv. **publicização da infração**;
v. **bloqueio dos dados pessoais**;
vi. **eliminação dos dados pessoais**;
vii. **suspensão parcial do funcionamento do banco de dados**;
viii. **suspensão do exercício da atividade de tratamento dos dados pessoais**;
ix. **proibição parcial ou total das atividades de tratamento de dados.**

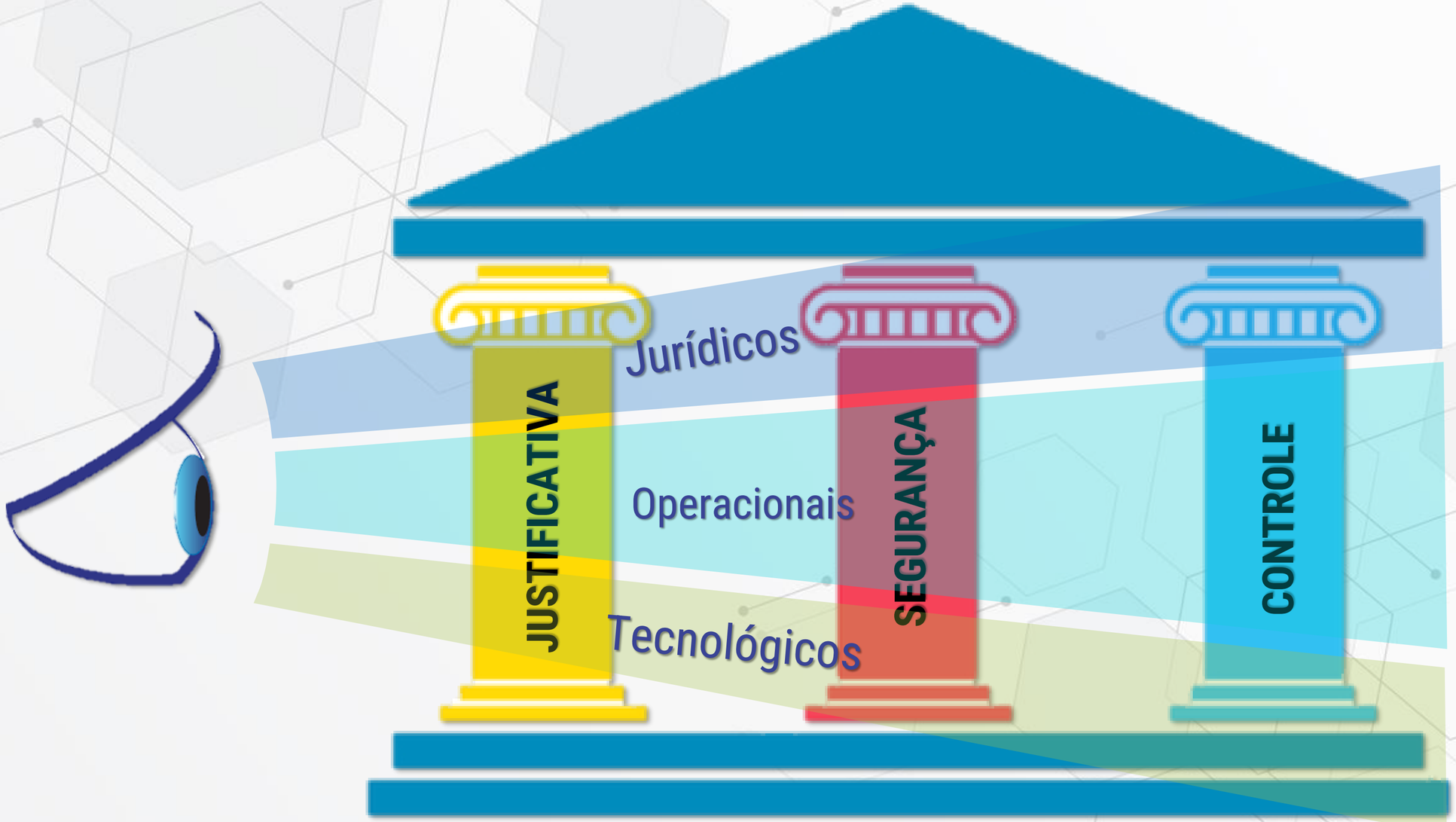
omnisblue

A JORNADA DE ADEQUAÇÃO À LGPD (LEI Nº 13.709/18)

E como fazemos para
trilhar esse caminho

omnisblue

OS PILARES DE ADEQUAÇÃO À LGPD



omnisblue

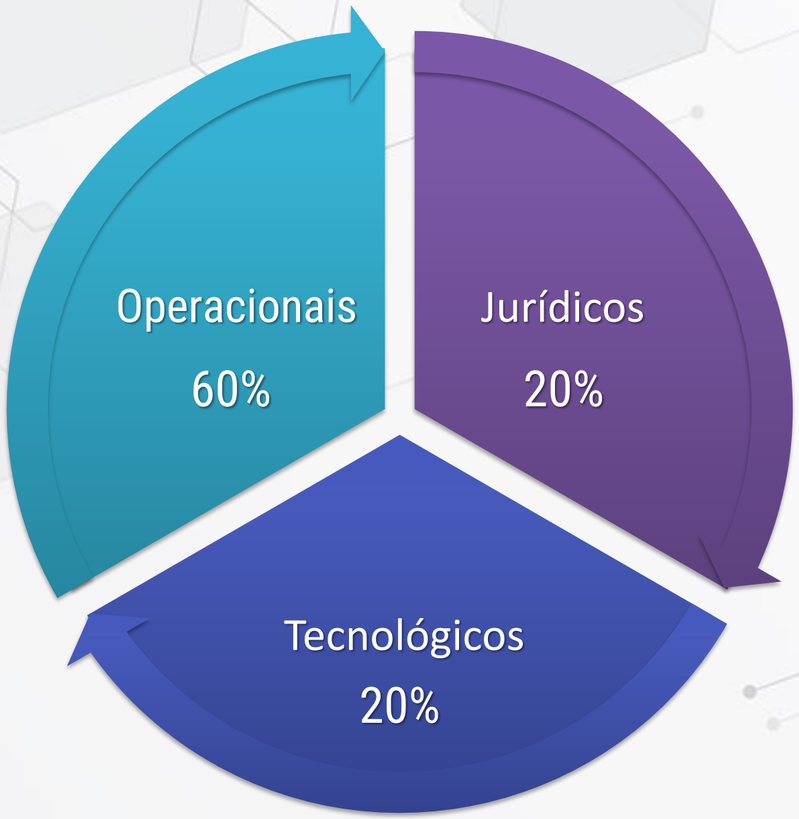
O QUE É UM SGPD

omnisblue

Sistema: Conjunto de elementos, concretos ou abstratos, intelectualmente organizados que interagem de tal forma que o resultado do todo não pode ser alcançado individualmente por suas partes.

Um **Sistema de Gestão/Gerenciamento de Proteção de Dados (SGPD)** é um conjunto de *papéis*, *atividades*, *documentos*, *controles* e *ferramentas* que, juntos, buscam gerenciam, organizam e garantem a **segurança de dados.**

OS ASPECTOS DE ADEQUAÇÃO À LGPD



Operacionais

- Ciclo de vida dos dados pessoais
- Finalidades de tratamento de dados
- Medidas *administrativas* de segurança (políticas)
- Processos previstos na LGPD
- Gestão de riscos operacionais

Jurídicos

- Hipóteses de tratamento de dados pessoais
- Fundamentos legais
- Gestão jurídica de contratos
- Gestão de riscos legais

Tecnológicos

- Gestão de ativos de informação
- Medidas *técnicas* de segurança
- Disponibilização de ferramentas para apoio ao SGPD
- Gestão de riscos tecnológicos

omnisblue

ETAPAS DE IMPLEMENTAÇÃO DE UM SGPD

Diagnóstico

- Mapear o ciclo de vida dos dados
- Mapear as bases legais
- Mapear medidas administrativas e técnicas de segurança
- Inventariar contratos
- Realizar análise inicial de impacto
- Criar plano de ação

Etapa 01
Preparação

Adequação

Etapa 02
Engajamento

- Definir papéis e responsabilidades
- Definir plano de comunicação
- Obter comprometimento geral
- Alocar DPO de adequação
- Realizar workshops iniciais

- Alterar processos
- Implantar novos processos
- Elaborar medidas administrativas de segurança
- Ajustar medidas técnicas de segurança
- Ajustar contratos
- Realizar capacitação completa

Etapa 03
Implementação

Operação

Etapa 04
Governança

- Alocar DPO de operação
- Gerenciar direito dos titulares
- Gerenciar riscos, incidentes e notificações
- Gerenciar DPIA
- Gerenciar operadores e controladores
- Gerenciar ANPD

- Manter medidas administrativas de segurança
- Manter medidas técnicas de segurança
- Monitorar e adaptar processos
- Monitorar ferramentas
- Reciclar conhecimento

Etapa 05
Melhoria contínua

omnisblue

DIAGNÓSTICO
1. PREPARAÇÃO

Principal Objetivo da Etapa: Elaborar o *Plano de Ação* com atividades claras e objetivas que deverão ser executadas posteriormente para garantir a adequação do controlador à LGPD.

Perguntas que devemos responder nessa etapa:

- Quais Dados Pessoais utilizamos e como eles trafegam por nossas rotinas?
- Por que utilizamos esses Dados Pessoais e como justificamos isso?
- Utilizamos apenas os Dados Pessoais minimamente necessários para cumprir nossos objetivos?
- Quais são os compromissos que nossa empresa assume em relação à privacidade e segurança de dados?
- Quais os níveis de Confidencialidade, Integridade e Disponibilidade dos nossos Ativos de Informação?
- Como está nosso website corporativos em relação à LGPD?
- Temos um DPO?
- Sob quais riscos de privacidade estamos atuando hoje? Como tratá-los?
- O que temos que fazer para cobrirmos as lacunas em relação à LGPD?

omnisblue

PASSO 01
ENCONTRAR OS DADOS PESSOAIS

Mapear os processos de negócio

- Usar modelagem BPMN
- Identificar atores
- Determinar objetivo e responsável de cada processo

Inventariar seus Ativos

- Classificar o tipo (físico ou eletrônico)
- Detalhar quem mantém o Ativo
- Associar aos processos de negócio

- Envolvimento do time de TI

Inventariar seus Artefatos e Dados

- Artefatos são documentos (físicos ou eletrônicos) que circulam pelos Ativos (devem ser associados)
- Dados pessoais estão dentro de Artefatos e podem ser reutilizados em vários artefatos

Classificar seus Dados Pessoais

- A LGPD classifica os dados pessoais em “normais” ou “sensíveis”
- O Decreto Federal 10.046 estende essa classificação e pode ser utilizado em conjunto

omnisblue

PASSO 02
JUSTIFICAR OS TRATAMENTOS DE DADOS

Elencar cada tratamento de dado

- Um processo pode ter “n” tratamentos em execução
- Identificar os detalhes sobre o ciclo de vida dos dados para cada tratamento
- Identificar parâmetros adicionais (como o uso de operadores, dados de crianças, compartilhamento e rotinas automatizadas)

Classificar as hipóteses

- Utilizar os incisos definidos no Art. 7º para dados normais
- Utilizar os incisos definidos no Art. 11º para dados sensíveis

- Envolvimento do time jurídico

Associar fundamentos legais

- Algumas hipóteses de tratamento podem exigir a indicação de fundamentos legais adicionais para justificar cada tratamento de dados

- Envolvimento do time jurídico

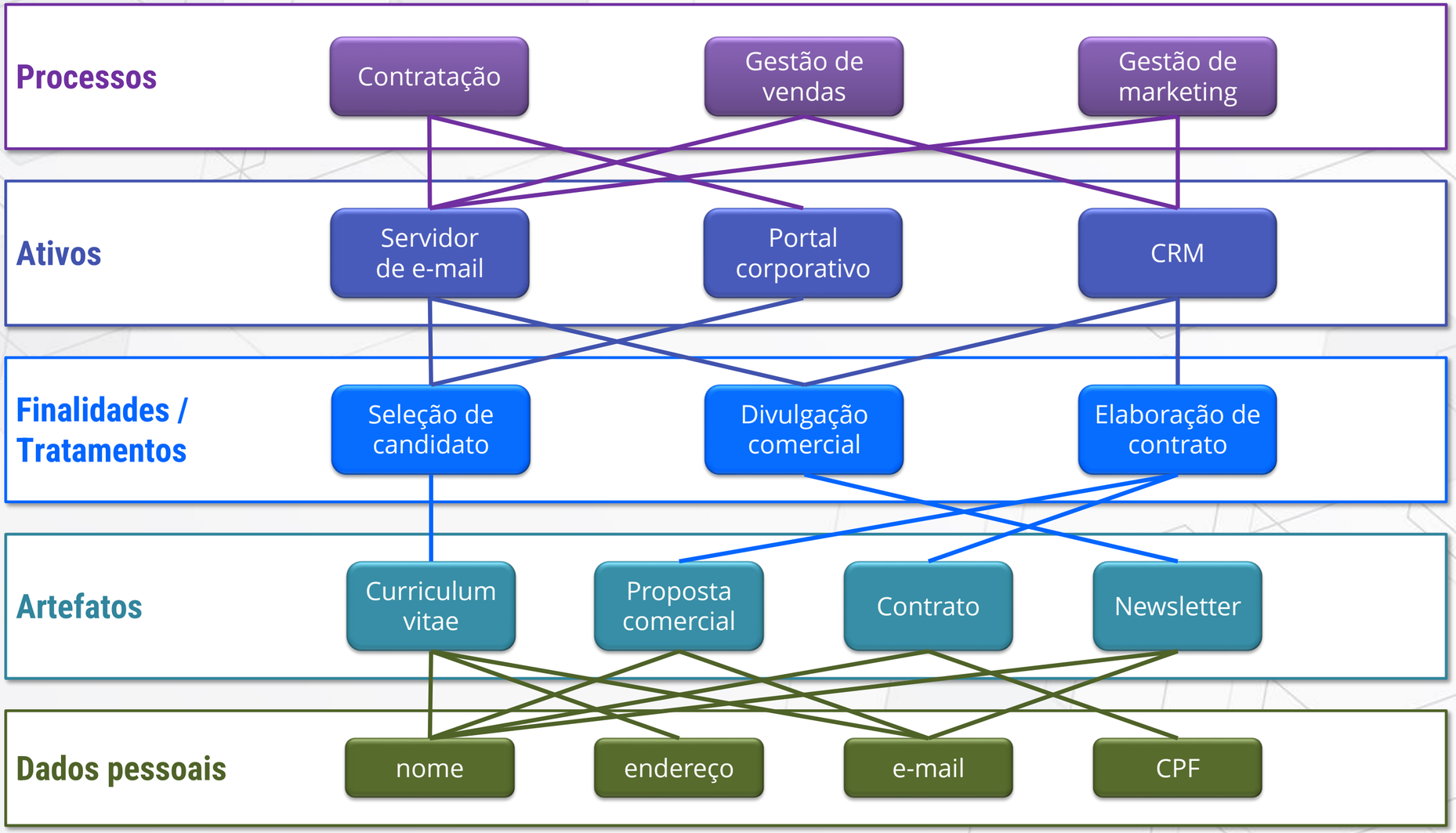
Analisar o princípio da Necessidade

- Para cada tratamento inventariado, é necessário indicar quais artefatos são utilizados e, dentro desses artefatos, quais dados pessoais são REALMENTE necessários para cumprir a finalidade do tratamento de dados

- Envolvimento do time jurídico

omnisblue

HIERARQUIA DA INFORMAÇÃO PESSOAL



PASSO 03
ANALISAR AS MEDIDAS ADMINISTRATIVAS

Analisar o alinhamento corporativo

- Verificar como o assunto “privacidade” é tratado na Governança Corporativa
- Entender como é aplicado os conceitos de “*privacy by design*” e “*privacy by default*” na empresa
- Envolvimento do time jurídico

Analisar as Políticas de Privacidade

- Documentos com foco EXTERNO que estabelecem os compromissos da empresa
- Analisar a exequibilidade e completude dos compromissos firmados
- Avaliar o nível de disseminação das políticas
- Envolvimento do time jurídico

Analisar as Políticas de Segurança

- Documentos com foco INTERNO que detalham regras e estratégias para a melhor gestão e segurança dos Ativos de Informação
- Analisar se essas políticas são compatíveis com as políticas de privacidade e de governança
- Envolvimento do time de TI

Analisar contratos

- Inventariar contratos que enderecem o tratamento de Dados Pessoais
- Analisar cláusulas contratuais com Titulares e Operadores
- Listar e associar terceiros envolvidos em tratamentos de Dados Pessoais
- Envolvimento do time jurídico

omnisblue

PASSO 04
ANALISAR AS MEDIDAS TÉCNICAS

A garantia da privacidade dos dados é obtida através da implementação de Medidas Técnicas de Segurança, tal como previstas nas Medidas Administrativas de Segurança

omnisblue

PASSO 05
ELENCAR RISCOS E CRIAR O PLANO DE AÇÃO

Analisar website corporativo

- Verificar se o website realiza adequadamente o tratamento de cookies
- Verificar a publicação da Política de Privacidade
- Verificar a publicização do DPO e do canal para atender Titulares de Dados

Elencar riscos

- Inventariar riscos de acordo com a situação atual
- Classificar o grau de impacto e a probabilidade de ocorrência de incidente
- Associar processos, ativos e tratamento de dados aos riscos
- Definir responsáveis e estratégias para cada risco

Emitir o primeiro DPIA

- Emitir o primeiro DPIA da empresa
- O documento será guardado como *baseline* do projeto e contará com as informações pré-adequação

Criar o Plano de Ação

- Definir todas as alterações operacionais, jurídicas e tecnológicas que a organização deverá implementar para completar sua adequação
- Envolvimento dos times jurídico e de TI

omnisblue

ADEQUAÇÃO
2. ENGAJAMENTO

Principal Objetivo da Etapa: Realizar o *onboarding* de todos os envolvidos nas mudanças que irão ocorrer e terminar a capacitação nos parâmetros da LGPD.

Perguntas que devemos responder nessa etapa:

- Quem será o responsável técnico pelas mudanças que estamos prestes a realizar?
- Quem será responsável por cada atividade prevista no Plano de Ação?
- Como iremos nos comunicar durante a execução das mudanças e quais são os pontos focais?
- Quais implicações que a falha do projeto pode trazer para a organização?

omnisblue

ATIVIDADADES DA ETAPA DE ENGAJAMENTO

Alocar DPO de adequação

Finalizar capacitação sobre LGPD

Definir papéis e responsabilidades

Definir um plano de comunicação

Obter compromissos

omnisblue

ADEQUAÇÃO
3. IMPLEMENTAÇÃO

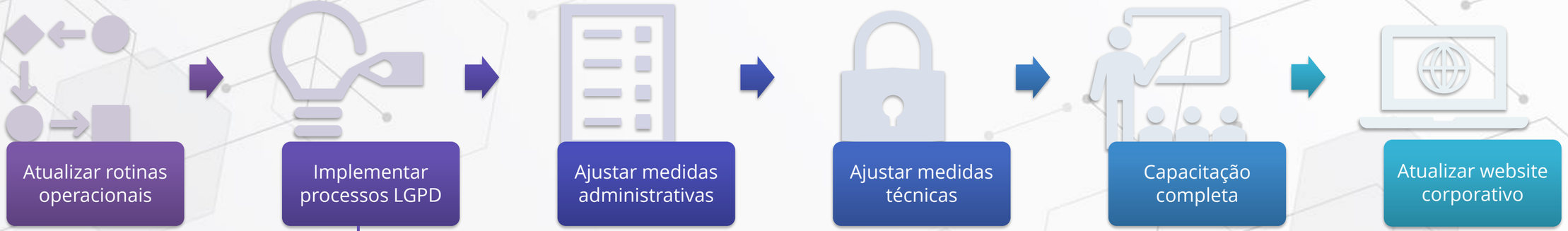
Principal Objetivo da Etapa: Colocar em prática todas as definições detalhadas no Plano de Ação e realizar mudanças operacionais, jurídicas e tecnológicas para adequar o Controlador à LGPD.

Perguntas que devemos responder nessa etapa:

- Como funcionam nossos processos atualizados?
- Como iremos atender nossos Titulares de Dados?
- Como iremos gerenciar riscos, incidentes e notificações?
- Como iremos gerenciar os consentimentos?
- Como o DPO irá emitir o DPIA?
- Quais são nossas novas políticas e cláusulas contratuais?
- Quais são os novos controles de segurança que irão gerenciar nossos Ativos de Informação?
- Quem é nosso DPO e como contatá-lo?

omnisblue

ATIVIDADADES DA ETAPA DE IMPLEMENTAÇÃO



- Gestão de Direitos dos Titulares
- Gestão de Riscos, Incidentes e Notificações
- Gestão de Consentimentos
- Emissão do DPIA

omnisblue

OPERAÇÃO
4. GOVERNANÇA

Principal Objetivo da Etapa: Garantir que o DPO execute suas obrigações e atenda aos requisitos estabelecidos na LGPD.

Atividades que o DPO irá realizar durante a etapa:

- Garantir atendimento aos Direitos dos Titulares de Dados;
- Atender solicitações, direcionar a operação e reciclar conhecimento sobre a gestão de privacidade e segurança de dados.
- Atender Operadores, direcionar estratégias e compromissos com a gestão de privacidade e segurança de dados nos contratos, auditar rotinas de tratamento de dados pessoais;
- Atender a solicitações da ANPD, demonstrar o status de adequação à LGPD;
- Emitir o DPIA, gerenciar riscos e monitorar ativos de informação (físicos e eletrônicos);
- Apoiar a TI na execução de estratégias e rotinas previstas na Política de Segurança;
- Registrar e acompanhar os desdobramentos de incidentes de segurança da informação, e notificar a ANPD e os Titulares de Dados quando for necessário.

omnisblue

OPERAÇÃO
5. MELHORIA CONTÍNUA

Principal Objetivo da Etapa: Permitir que o DPO mantenha todo o SGPD atualizado e em concordância com as novas realidades operacionais, jurídicas e tecnológicas da empresa e do mercado.

Atividades que o DPO irá realizar durante a etapa:

- Acompanhar as resoluções e regulamentações da ANPD e demais desdobramentos legais;
- Garantir que as Medidas Administrativas estejam sempre atualizadas, válidas e sejam conhecidas por todos;
- Apoiar a TI na melhoria e evolução das estratégias definidas na Política de Segurança;
- Atualizar os inventários, análises, Plano de Ação e o próprio SGPD sempre que houver mudança;
- Atualizar os processos de negócio LGPD e as ferramentas de apoio e recapacitar o time interno sempre que houver essas evoluções;
- Garantir, planejar, executar e gerenciar novos ciclos de execução de projetos de adequação à LGPD para maior abrangência do escopo de atendimento à Lei na empresa.

omnisblue

DÚVIDAS
DÚVIDAS
DÚVIDAS
DÚVIDAS
DÚVIDAS

omnisblue

LGPD | COMPLIANCE

WWW.OMNISBLUE.COM

OBRIGADO
OBRIGADO
OBRIGADO
OBRIGADO
OBRIGADO