CARTILHA

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

aesbe
Associação Brasileira das Empresas Estaduais de Saneamento

FICHA TÉCNICA

Diretor-Presidente

Marcus Vinícius Fernandes Neves (Cagepa)

Vice-Presidentes Regionais

Ricardo Soavinski (Saneago)

Armando do Valle (Cosama)

Neurisangelo Cavalcante de Freitas (Cagece)

Rogério Cedraz (Embasa)

Carlos Eduardo Tavares de Castro (Copasa)

Cláudio Stábile (Sanepar)

Conselho Fiscal

Roberta Maas (Casan)

James da Silva Serrador (Caer)

Roberto Sérgio Ribeiro Linhares (Caern)

Organização

Alberto Neto (Embasa)

Alixandro Jesus (Compesa)

Altair Alvarenga (Sanesul)

Ana Lyra (Cesan)

Carlos Brissac (Caema)

Dalton Ito (Sanepar)

Daniel Lyra (Caern)

Decio Malta (Sabesp)

Edmilson Neto (Caema)

Eliernandes Rodrigues (Caema)

Fabrício Vasconcellos (Copasa)

Felipe Souza (Cagece)

Graça Ahid (Caema)

Hellayne Thaís M. da Silva (Agespisa)

Humberto Barboza (Cedae)

Leonardo Montenegro (Cagepa)

Otávio Frota (Cagece)

Rodrigo Oliveira (Deso)

Romeu Souza N. Júnior (Cesan)

Ronaldo Melo Junior (Deso)

Thiago Santana Lopes (Caema)

Vitor Luiz (Saneago)

Waldeildo Júnior (Compesa)

Consultor convidado

Menndel Macedo (Menndel & Associados)

Projeto Gráfico, diagramação e revisão ortográfica

IComunicação

MEMBROS CTGE

AGESPISA
Paulo Roberto Araújo Couto

CAEMA
Angélica Maria Carnelosso
Cleison Gomes de Sá
Laís Alves Souza
Thiago Santana Lopes

CAER
Daniel Moraes Barreto
Gleidson Souza do Nascimento
Tony Carvalho Peixoto

CAERD
Jussiê da Silva Nogueira

CAERN
Nadja Bene Grangeiro de Sousa
Vilma Felix da Silva Araujo

CAESA
Carlos Jose dos Santos Filho

CAESB
Adeilde Matias C. de Araújo
Bruno Antonio Lisboa Cordeiro
Fuad Moura Guimarães Braga
Glaucilene de Oliveira Bertuli
Luiza Carneiro Brasil
Mauro Henrique Alves Coelho
Maxwell Simes de Souza Paiva
Pedro Cardoso de Santana Filho
Sandra Helena Thiesen Rios

CAGECE
Edênia Maria Torres Uchôa
Francisca Simone de Souza Arrais
Josestenne Bezerra do Amaral
Michele Arlinda Aguiar

CAGEPA
Márcia Lauriano da Silva
Marcus Vinicius Fernandes Neve
Riane de Lourdes Bezerra

CASAL
Marcelo Lima Moreira

CASAN
Carlos Alberto Coutinho
Filipe Alcioni Silva
Iris Lima Merizi

CEDAE
Mayná Coutinho Morais

CESAN
Gudson Lorencini
Karla Ponzo
Sergio Henrique Vieira Rabello

COMPESA
Marcela de Oliveira Henroz

COPASA
Elisangela Martins de Oliveira
Marcos Antunes de Castro

CORSAN
Alessandra Cristina
Fagundes dos Santos
Andréia Faleiro Lautert
Carina Oliveira da Cunha
Eliza Andréa Rambor
Fernanda Teixeira Escobar Silveira
Juliano Dertzbacher
Luiz Ricardo Monteiro
Mara Rubia Rodrigues Freitas
Samanta Popow Takimi
Savio Fernando Scherer

COSAMA
Kellen Pereira da Silva

COSANPA
Edilma R. Novaes de Moraes
Oberdan Pinheiro Duarte

DESO
Rodrigo Fernando Meneses
de Oliveira

SABESP
Dante Ragazzi Pauli
Janaina Barbosa de Souza
Sebastiana Alves da Silva
Rodrigues

SANEAGO
Diego Auguso Ribeiro Silva
Leyla Pereira Viana

SANEATINS
Marcelo Ferreira dos Santos

SANEPAR
Julio Cesar Chezanoski
Livia Regina L. M. Giordano Soares
Rita de Cassia G. Becher

SANESUL
Daniela Jimenez Cance
Marcia Helena Mello Santana

EMBASA
Dásio Câmara Neto
Rodrigo Lemos Valadares

COORDENADOR
Dásio Câmara Neto (Embasa)

SECRETÁRIO
Rodrigo Fernando Meneses de Oliveira
(Deso)

APRESENTAÇÃO

A Lei Geral de Proteção de Dados (LGPD), aprovada em agosto de 2018 e em vigor desde 2020 (Lei nº 13.709/2018), colocou o Brasil em posição de vanguarda mundial no que diz respeito à segurança da informação. O Congresso Nacional se inspirou na lei europeia GDPR (General Data Protection Regulation), uma das precursoras do tratamento de dados pessoais. Na prática, a LGPD dispõe sobre o tratamento de dados pessoais – inclusive nos meios digitais – por pessoa natural ou por pessoa jurídica de direito público ou privado. O objetivo é proteger os direitos fundamentais de liberdade e privacidade.

No âmbito empresarial – inclusive no âmbito da prestação dos serviços de saneamento básico – a LGPD também é importante ao exigir que negócios e organizações se adequem às práticas que confiram segurança na captação, armazenamento e utilização de dados de *stakeholders* (sejam clientes, fornecedores ou sociedade em geral). Além de contribuir para a boa imagem, a companhia que observa e cumpre as atuais regras de proteção de dados também evita as penalidades previstas na nova legislação.

Por tudo isso, a Aesbe preparou essa cartilha para que você possa entender tudo sobre a LGPD e como se adaptar às novas diretrizes. A cartilha foi fruto de um trabalho conjunto entre as empresas estaduais de saneamento representadas num grupo da Câmara Técnica de Gestão Empresarial (CTGE) da AESBE. Dentre elas, queremos destacar as contribuições da Companhia de Saneamento Ambiental do Maranhão (CAEMA), que disponibilizou seu plano de ações interno para adequação à LGPD, bem como cronogramas de atividades e descritivos a respeito das ações a serem executadas. Também destacamos o apoio da Companhia de Saneamento de Minas Gerais (COPASA), da Companhia de Saneamento Básico do Estado de São Paulo (SABESP), da Companhia de Saneamento do Paraná (SANEPAR), da Companhia de Água e Esgotos da Paraíba (CAGEPA) e demais companhias estaduais de saneamento representadas no grupo de trabalho.

Entre outros pontos, com esta cartilha você compreenderá princípios e conceitos como Dados Sensíveis, Controlador, Operador, Titular de Dados e DPO (Data Protection Officer, ou, simplesmente, Encarregado), além de entender a importância da implantação do Comitê Gestor de Segurança da Informação (CGSI) e um modelo de governança da proteção de dados pessoais numa entidade que lida diariamente com grandes volumes de dados de terceiros – como é o caso das companhias estaduais de saneamento de todo o país. Ao fim desta cartilha, você poderá acessar uma ferramenta para facilitar a execução e acompanhamento das ações de adequação à lei, o Trello, cujo modelo poderá ser replicado para a sua instituição, contendo as ações-macro, indicações de boas práticas e comentários de representantes de outras empresas de saneamento do Brasil. Boa leitura!

DESCRITIVOS DAS AÇÕES

Instituir o Comitê Gestor de Segurança da Informação (CGSI)

O Comitê Gestor de Segurança da Informação é uma unidade multissetorial, permanente, de natureza consultiva e propositiva, instituída para dar apoio à Diretoria Executiva no que tange à coordenação da formulação, implementação e revisão das Diretrizes da Política de Segurança e Proteção da Informação da companhia, com o intuito de promover a adequação à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018).

Definir oficialmente o Controlador (CNPJ), Operador (Equipe de TI), Encarregado (DPO) e Titulares de Dados (Clientes, Colaboradores e Prestadores de Serviços)

A LGPD institui responsabilidades específicas para cada nível de geração e/ou tratamento de dados:

- **Controlador** – é a Diretoria da Presidência, a quem compete a tomada de decisões referentes ao tratamento de dados pessoais e quem, por meio dos seus poderes e atribuições, delega as ações necessárias para operacionalizar a Lei Geral de Proteção de Dados na estrutura da companhia;
- **Operador** – é todo aquele que, durante a execução de suas atividades, tem contato com e/ou trata dados pessoais (tanto em meio físico quanto digital);
- **Titular de dados** – é toda pessoa a quem se referem os dados pessoais objetos de tratamento;
- **Encarregado (DPO – Data Protection Officer)** – é a pessoa física indicada pelo Controlador para atuar como canal de comunicação entre este, os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Criar/Revisar e Aprovar a Política de Proteção e Segurança da Informação

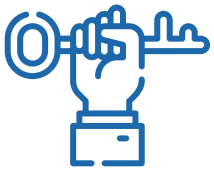
Documento aprovado pela Alta Gestão, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da LGPD no âmbito da companhia.

Criar/Revisar Política de Privacidade

A Política de Privacidade é o documento que contém o conjunto de conceitos e diretrizes que descrevem as práticas adotadas pelo site – ou aplicação – em relação às informações dos usuários (dados pessoais). O objetivo é esclarecer ao visitante/usuário como e com qual finalidade seus dados serão utilizados.

Criar/Revisar Política de Divulgação de Informações

A Política de Divulgação de Informações tem como finalidade definir as diretrizes que envolvem o uso e a divulgação de informações que, por sua natureza, possam suscitar ato ou fato relevante – com o intuito de evitar o uso indevido de informações sensíveis.



Elaborar Modelo dos Termos de Confidencialidade

Termo de Confidencialidade é um documento entre duas partes que visa proteger dados estratégicos de ambas. Assim, a parte contratada assume o compromisso de não divulgar as informações (sigilo) às quais terá acesso em determinado projeto ou por algum período específico. Os mais usuais são direcionados aos funcionários e prestadores de serviço, ao encarregado de dados, a convênios, entre outros.

Sugere-se que o modelo-base dos Termos de Confidencialidade esteja incluído como anexo à Política de Proteção e Segurança da Informação, aprovada pela Alta Gestão da companhia.

Criar Política de Dados Pessoais

A Política de Dados Pessoais visa definir as diretrizes e o compromisso da organização perante seus clientes, colaboradores e parceiros quanto ao uso dos seus dados pessoais, informando-lhes de forma clara e inequívoca o contexto em que serão coletados e tratados. Essa política pode ser unificada à Política de Privacidade (o que é muito comum), tornando-se "Política de Privacidade e Proteção de Dados".

Criar a Política de Gestão Documental (com a Tabela de Temporalidade dos Dados Físicos e Digitais)

A Política de Gestão Documental estabelece as diretrizes e orientações gerais para a estruturação do Processo de Gestão de Documentos e Informações nos arquivos corporativos e institucionais. Ela contém o conjunto de procedimentos e operações técnicas referentes à produção, à tramitação, ao uso, à avaliação e ao arquivamento de documentos, visando à eliminação ou ao recolhimento para armazenamento permanente.

Criar/Revisar Normativas de Segurança da Informação

Neste quadro estão contidas as normativas relacionadas às aplicações diretas das diretrizes definidas pela Política de Proteção e Segurança da Informação. As normativas – resolução, POPs, normas, rotinas etc. – deverão refletir a Lei Geral de Proteção de Dados (LGPD, lei nº 13.709/2018) no âmbito de atuação dos setores para criar um cenário de segurança jurídica, assegurando a integridade do tratamento de dados.

Monitorar e Cobrar a Atualização do Portal de Transparência

O objetivo dessa ação é promover a harmonização da Lei nº 12.527 (LAI) com a Lei nº 13.709 (LGPD), criando o que é comumente chamado no meio jurídico de "Diálogo das fontes". Isto é possível haja vista a constante revisitação ao portal da transparência da companhia, com o intuito de verificar se todos os dados pessoais publicados são realmente necessários para o cumprimento dessa obrigação legal, conforme o Princípio da Necessidade, preconizado pelo art. 6º, III, da LGPD.

Mapear Contratos Existentes por Diretoria

Esta ação tem como objetivo o levantamento dos contratos ativos na companhia, por centro de responsabilidade, para futura aditivação – ou apostilamento – da cláusula contratual referente à adequação à Lei Geral de Proteção de Dados.

Mapear Convênios Existentes

Esta ação tem como objetivo o levantamento dos convênios ativos na companhia, para futura aditivação – ou apostilamento – da cláusula contratual referente à adequação à Lei Geral de Proteção de Dados.

Executar o *Data Mapping* para Dados Digitais

O *Data Mapping* é o mapeamento dos tipos de dados pessoais tratados no âmbito da companhia, com seus responsáveis e processos associados. Esse mapeamento pode ser executado de forma manual, lógica ou até por meio da utilização de softwares de terceiros.

As informações mapeadas, associadas à tabela de temporalidade – contida na Política de Gestão Documental, e as bases legais (definidas pelo setor jurídico da Empresa) fundamentam a construção do Relatório de Impacto Sobre Dados Pessoais.

Executar o *Data Mapping* para Dados Físicos (Gestão Documental)

O *Data Mapping* é o mapeamento dos tipos de dados pessoais tratados no âmbito da companhia, com a descrição dos responsáveis e processos relacionados. Esse mapeamento pode ser executado de forma manual, lógica ou até por meio da utilização de softwares de terceiros (caso a gestão documental na Empresa seja um processo integralmente informatizado).

Essa ação normalmente é coordenada pelo setor de Biblioteca/Arquivo da companhia, que, por meio da Política de Gestão Documental, institui as diretrizes para controle e armazenamento dos documentos relacionados.

As informações mapeadas, associadas à tabela de temporalidade – contida na Política de Gestão Documental – e as bases legais (definidas pelo jurídico da Empresa), fundamentam a construção do Relatório de Impacto Sobre Dados Pessoais.

Definir as Bases Legais para Cada Dado Mapeado

No processo de adequação à Lei nº Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018), é de suma importância a análise e o cumprimento das hipóteses – mencionadas no art. 7° e no art. 13 – que viabilizam o tratamento de dados pessoais na execução dos serviços da companhia. Logo, caso a empresa trate os dados fora de alguma das dez bases legais descritas na lei, ela está sob o risco de incorrer no tratamento ilegal. As mencionadas prerrogativas da Lei são: Consentimento (ver art. 9°); Obrigação Legal; Políticas Públicas; Pesquisa; Execução de Contrato; Tutela pela Saúde e Proteção da Vida; Legítimo Interesse; Proteção ao Crédito.

Homologar

- **Política de Privacidade –** Aprovação da Política de Privacidade pela Alta Gestão da companhia.
- **Política de Divulgação de Informações –** Aprovação da Política de Divulgação de Informações pela Alta Gestão da companhia.
- **Termos de Confidencialidade para os Operadores, Encarregado e Titulares de Dados –** Aprovação dos Termos de Confidencialidade para os operadores, encarregado de dados (DPO) e titulares de dados pela Alta Gestão da companhia.
- **Cláusula Contratual –** Aprovação da Cláusula Contratual pela Alta Gestão da companhia.
- **Política de Dados Pessoais –** Aprovação da Política de Dados Pessoais pela Alta Gestão da companhia.
- **Termos de Confidencialidade para os Convênios –** Aprovação dos Termos de Confidencialidade para os convênios pela Alta Gestão da companhia.
- **Política de Gestão Documental –** Aprovação da Política de Gestão Documental pela Alta Gestão da companhia.
- **Normativas de Segurança da Informação –** Aprovação das Normativas de Segurança da Informação pela Alta Gestão da companhia.

- **Portal de Transparência –** Aprovação das informações a serem adicionadas no Portal de Transparência pelos setores responsáveis, tal qual a Alta Gestão da companhia e/ou órgãos externos (Secretaria de Transparência do Estado, Secretaria do Governo, Secretaria de Planejamento etc.).

- **Plano de Comunicação da LGPD para a ANPD –** Aprovação do Plano de Comunicação da Lei Geral de Proteção de Dados pela Alta Gestão da companhia.

Elaborar Cláusula Contratual Referente à Adequação à LGPD

De acordo com a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018), todo contrato que perpassa o tratamento (físico ou digital) de dados pessoais deve conter uma cláusula que defina os direitos e atribua as responsabilidades para ambas as partes a respeito da gestão da informação de cunho sensível. No caso dos contratos já existentes, assinados previamente à homologação da cláusula, o processo de adequação à LGPD requer sua inclusão, por aditivação ou apostilamento do documento.

Criar Termos de Confidencialidade Específicos para os Operadores, os Colaboradores e o Encarregado

Os Termos de Confidencialidade devem estar direcionados ao tipo de relação entre ambas as partes, definindo as diretrizes relacionadas ao sigilo no que se refere ao tratamento de dados pessoais. Com responsabilidades bem definidas, estabelece-se uma gestão mais clara e objetiva da tramitação de informações sensíveis na companhia.

Aditivar/Apostilar os Contratos Ativos, Incluindo a Nova Cláusula

Após a aprovação da Cláusula Contratual pela Alta Gestão da companhia, o setor responsável (normalmente a área de contratos ou jurídica) deve analisar o mapeamento dos contratos e iniciar a aditivação/apostilamento da cláusula. É importante que haja uma comunicação aberta entre as partes às quais se refere o contrato, para que ambas estejam a par das alterações nos procedimentos e/ou rotinas contidas na cláusula.

Criar Aviso de Privacidade

O Aviso de Privacidade tem como objetivo esclarecer, de forma simples, transparente e objetiva, como se dá o tratamento das informações pessoais na utilização dos serviços da companhia. Ele descreve os tipos de dados pessoais que serão coletados, além das suas finalidades, os seus possíveis compartilhamentos com terceiros e as medidas adotadas para armazenamento e segurança da informação.

Criar Plano de Comunicação da LGPD para a Internet

Esta ação refere-se à criação de um cronograma específico ao setor de Comunicação para gerar informes – *pop-ups*, notícias, vídeos, postagens em redes sociais etc. – a respeito da Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) direcionados aos clientes.

Criar Rotinas de Treinamentos e Sensibilização a Respeito da LGPD e seus Desdobramentos para os Colaboradores

De acordo com a LGPD, todos os colaboradores devem ser capacitados para incorporar as diretrizes de Segurança da Informação (contidas na Política de Proteção e Segurança da Informação e seus produtos derivados) a suas rotinas, com a finalidade de adequar suas atividades aos novos fluxos de responsabilidade.

Assim, o setor de Recursos Humanos deve criar cronogramas específicos para treinamento contínuo de todos os funcionários informando-os a respeito da lei e seus respectivos desdobramentos no âmbito da companhia.

Disponibilizar o Portal de Transparência

Após a aprovação do conteúdo do Portal de Transparência, o setor de Tecnologia da Informação deverá disponibilizar o link para seu acesso (de forma clara) no site da companhia.

Para Cada Convênio Ativo, Incluir, no Termo de Cooperação, o Termo de Confidencialidade

Após a aprovação do Termo de Confidencialidade pela Alta Gestão da companhia, o setor responsável (normalmente a área de contratos ou jurídica) deve analisar o mapeamento dos convênios e iniciar a inclusão do termo a este destinado.

É importante que haja uma comunicação aberta entre as partes a que se referem o convênio, para que ambas estejam a par das alterações nos procedimentos e/ou rotinas que decorrem da inclusão do termo.

Criar o Formulário de Tratamento de Dados Pessoais (com Área, Nome do Processo, Objetivo Do Processo, Responsável pelo Dado, Dados Pessoais Envolvidos, Forma de Coleta, Saídas, Interfaces, Sistemas, Responsáveis e Bases Legais)

O Formulário de Tratamento de Dados Pessoais deve ser preenchido pelo titular de dados (ou responsável/representante legal) para solicitação de informações referentes à existência e ao tratamento de dados pessoais.

Os dados coletados a partir do formulário serão tratados exclusivamente para o atendimento e registro da solicitação do titular, no legítimo interesse das partes. Essas informações serão de uso restrito pelo encarregado de dados (DPO) e pelos demais envolvidos diretamente na solicitação, permanecendo armazenados por tempo indeterminado, sem acesso pelos demais usuários da companhia, exceto no caso de necessidade de consulta para demandas decorrentes do próprio atendimento.

Recomenda-se que o DPO tenha definido também o fluxo de resposta às solicitações para facilitar a gestão dessas demandas e trazer mais celeridade à atividade.

Criar Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é o instrumento criado e constantemente atualizado pelo encarregado de dados (DPO), o qual contém os riscos inerentes às liberdades civis e aos direitos fundamentais referentes ao tratamento de dados pessoais na companhia, bem como às ações de mitigação/contingenciamento e aos responsáveis por elas.

Esse documento é de posse do controlador, podendo ser requisitado pela Agência Nacional de Proteção de Dados (ANPD) durante fiscalização e/ou processos de auditoria.

Criar Plano de Comunicação da LGPD para a ANPD

Nesse plano devem ser estabelecidas as diretrizes e estratégias de comunicação com a ANPD, principalmente no que se refere às respostas aos incidentes de vazamento ou comprometimento dos dados dos titulares.

Recolher Assinaturas para cada Contrato Aditivado

Recolhimento das assinaturas após cada aditivação/apostilamento dos contratos previamente mapeados.

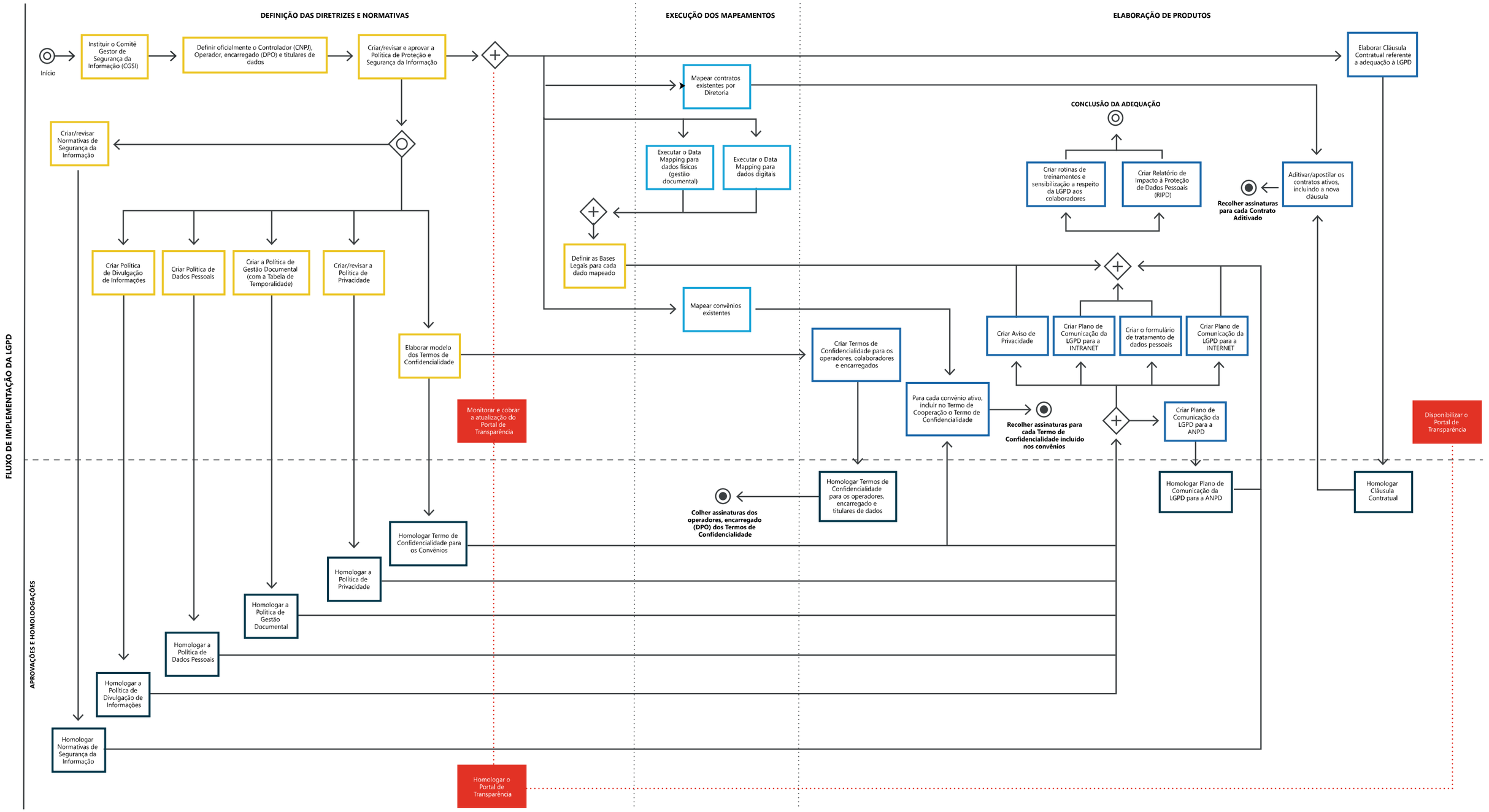
Colher Assinaturas dos Operadores e do Encarregado (DPO) dos Termos de Confidencialidade

Recolhimento das assinaturas dos Termos de Confidencialidade por parte dos operadores e encarregado de dados (DPO).

Recolher Assinaturas para Cada Termo de Confidencialidade Incluído nos Convênios

Recolhimento das assinaturas de ambas as partes para cada inclusão do Termo de Confidencialidade no Termo de Cooperação

FLUXOGRAMA


DEFINIÇÃO DAS DIRETRIZES E NORMATIVAS
EXECUÇÃO DOS MAPEAMENTOS
ELABORAÇÃO DE PRODUTOS
FLUXO DE IMPLEMENTAÇÃO DA LGPD
APROVAÇÕES E HOMOLOOGAÇÕES
Início
Instituir o Comitê Gestor de Segurança da Informação (CGSI)
Definir oficialmente o Controlador (CNPJ), Operador, encarregado (DPO) e titulares de dados
Criar/revisar e aprovar a Política de Proteção e Segurança da Informação
Criar/revisar Normativas de Segurança da Informação
Criar Política de Divulgação de Informações
Criar Política de Dados Pessoais
Criar a Política de Gestão Documental (com a Tabela de Temporalidade)
Criar/revisar a Política de Privacidade
Elaborar modelo dos Termos de Confidencialidade
Monitorar e cobrar a atualização do Portal de Transparência
Homologar Termo de Confidencialidade para os Convênios
Homologar a Política de Privacidade
Homologar a Política de Gestão Documental
Homologar a Política de Dados Pessoais
Homologar a Política de Divulgação de Informações
Homologar Normativas de Segurança da Informação
Homologar o Portal de Transparência
Mapear contratos existentes por Diretoria
Executar o Data Mapping para dados físicos (gestão documental)
Executar o Data Mapping para dados digitais
Definir as Bases Legais para cada dado mapeado
Mapear convênios existentes
Criar Termos de Confidencialidade para os operadores, colaboradores e encarregados
Para cada convênio ativo, incluir no Termo de Cooperação o Termo de Confidencialidade
Recolher assinaturas para cada Termo de Confidencialidade incluído nos convênios
Colher assinaturas dos operadores, encarregado (DPO) dos Termos de Confidencialidade
Homologar Termos de Confidencialidade para os operadores, encarregado e titulares de dados
CONCLUSÃO DA ADEQUAÇÃO
Criar rotinas de treinamentos e sensibilização a respeito da LGPD aos colaboradores
Criar Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
Criar Aviso de Privacidade
Criar Plano de Comunicação da LGPD para a INTRANET
Criar o formulário de tratamento de dados pessoais
Criar Plano de Comunicação da LGPD para a INTERNET
Criar Plano de Comunicação da LGPD para a ANPD
Homologar Plano de Comunicação da LGPD para a ANPD
Recolher assinaturas para cada Contrato Aditivado
Aditivar/apostilar os contratos ativos, incluindo a nova cláusula
Elaborar Cláusula Contratual referente a adequação à LGPD
Homologar Cláusula Contratual
Disponibilizar o Portal de Transparência

ESTRUTURA DPO E SEGINFO

Estrutura de Proteção de Dados Pessoais

Onde deve estar lotado o DPO e qual a sua estrutura. São três opções recomendadas:

- Como gerência/superintendência específica, com equipe de trabalho própria, abaixo do CEO da organização. Em estrutura independente, o DPO consegue não ter conflito de interesses e exercer as atribuições previstas na lei de forma independente;
- Como função gratificada, ou assessoria, dentro da estrutura de *compliance* da organização. Nesta posição, pode o DPO utilizar dos recursos da estrutura do *compliance* para favorecer o cumprimento das atividades e atribuições previstas na lei;
- Com função gratificada ou assessoria, dentro de uma área que não desempenhe condição de conflito de interesses em relação às funções atribuídas e realizadas.

Estrutura de Segurança da Informação

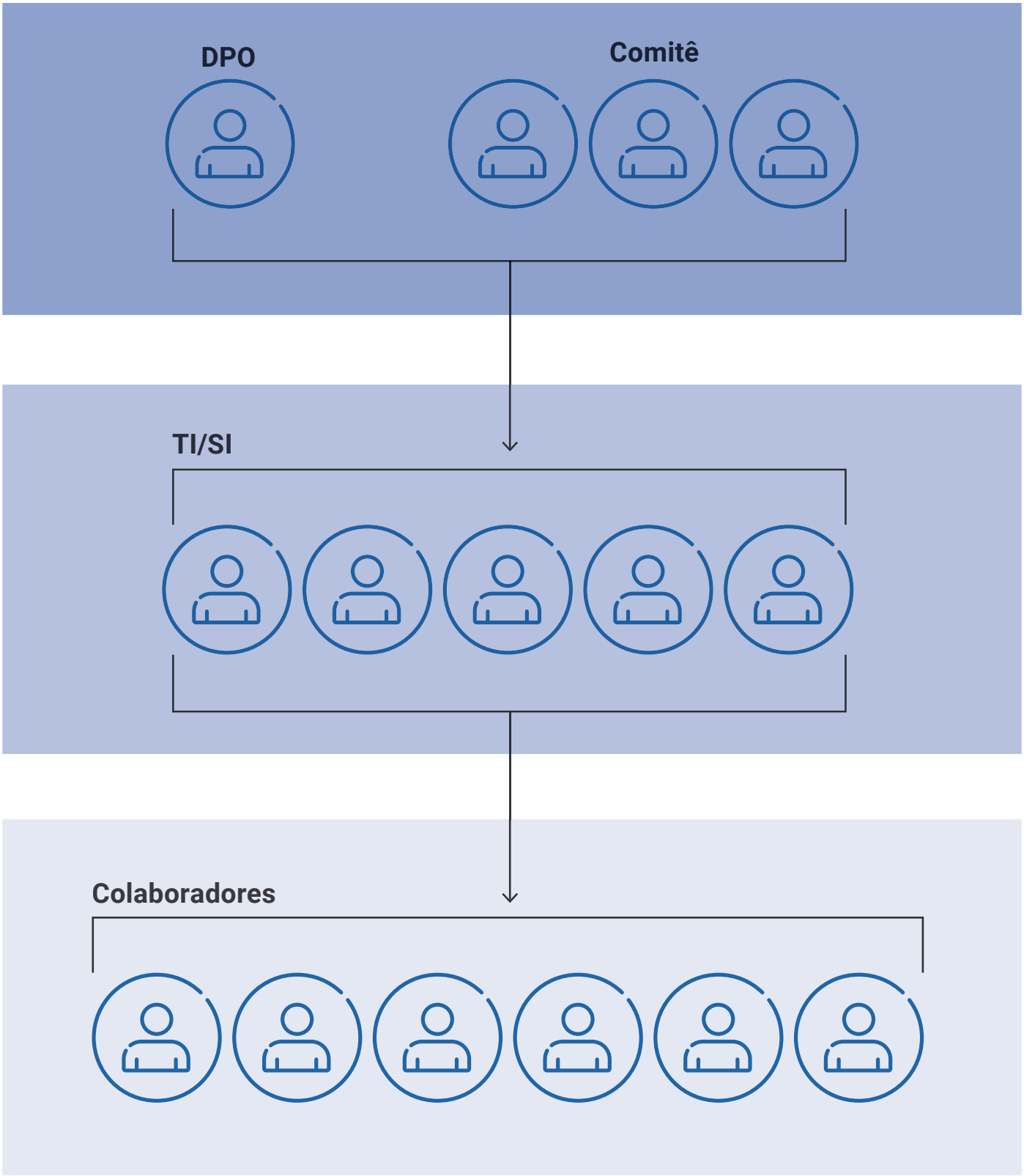
Onde deve estar a estrutura de segurança e qual o perfil da equipe. A estrutura de Segurança da Informação deve ser área específica da TI da organização. Se a TI tem gerências para desenvolvimento, atendimento de usuário e outras, a área de Segurança deve ser uma delas. Para executar seu trabalho, deve-se agrupar os profissionais de redes, *firewall*, antivírus, conectividade, *proxy*, e demais aparatos tecnológicos para que gerenciem a estrutura de segurança da empresa.

A área deve existir para garantir os investimentos centralizados e necessários, além de evitar *cyber* ataques e exposição de dados e estrutura da organização. Por esta razão, recomenda-se que a empresa garanta o reconhecimento desta área e também invista na aquisição de soluções de segurança, as quais devem ser consideradas investimentos na gestão e na imagem.

Para mais, é importante ressaltar que a ISO 27.001 (Organização Internacional de Normalização) e suas séries reportam a necessidade da existência de estrutura própria de gestão da segurança da informação nas empresas. Ela considera, inclusive, a contratação de testes de rede e de profissionais de mercado com experiência em gestão ativa do parque tecnológico.

Portanto, é bem verdade que as Organizações que possuem a TI em nível de diretoria tendem a enfrentar menos problemas para alinhar os seus investimentos e custeio de TI às necessidades de negócio das empresas.

MODELO DE GOVERNANÇA DA PROTEÇÃO DE DADOS PESSOAIS



FERRAMENTA PARA EXECUÇÃO E CONTROLE DAS AÇÕES DE ADEQUAÇÃO À LGPD

Um dos produtos das atividades do Grupo de Trabalho da LGPD foi a elaboração de um quadro na ferramenta Trello, contendo desde as ações e descritivos, até comentários, indicações de boas práticas e compartilhamento de experiências entre empresas de saneamento no Brasil.

O objetivo é não só facilitar o planejamento, execução e acompanhamento das ações relacionadas a adequação à LGPD através do fornecimento de um modelo de plano de trabalho, como também criar um espaço interativo de trocas, para impulsionar o avanço das empresas nacionais de saneamento no que diz respeito ao alcance da conformidade à lei.

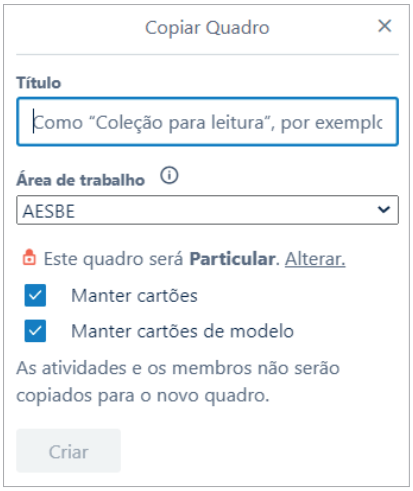
SAIBA MAIS
Aponte a câmera do celular e utilize o Trello como ferramenta de gestão para o planejamento da LGPD.

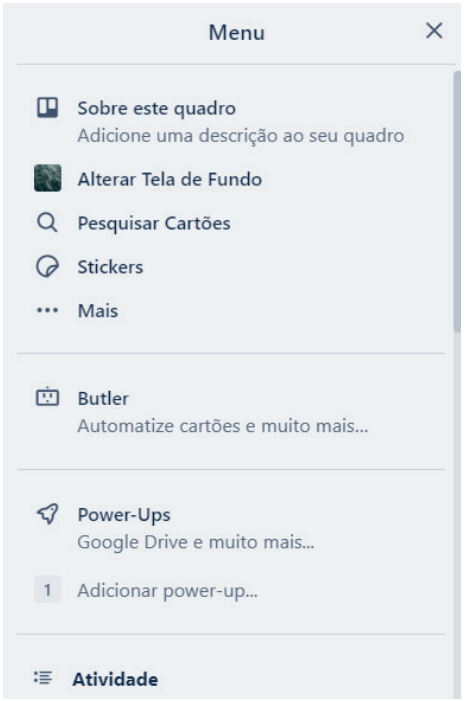
A seguir, estão relacionados os passos para replicação (cópia) do quadro em questão. Recomenda-se que sejam analisados item a item deste plano de trabalho para verificar as diretrizes e ações que se alinham - ou não - com o modelo de negócio e estrutura organizacional da sua empresa. Em alguns casos, será necessário a criação (ou remoção) de ações específicas, seguidas de atividades que corroborem para o alcance da conformidade no âmbito empresarial.

Recomenda-se também que os representantes de cada empresa entrem em contato com a Câmara Técnica de Gestão Empresarial (CTGE) para a inclusão no Grupo de Trabalho da LGPD, caso haja interesse na inserção de comentários e/ou questionamentos nos cartões das ações.

O nosso foco é alcançarmos juntos este objetivo de estabelecer um ambiente de maior segurança de dados no setor de saneamento do Brasil. Contamos com vocês!

Aqui estão os itens a serem analisado na cópia do quadro, como a seleção da área de trabalho onde ele será incluído e demais configurações relacionadas a permissões de acesso e cartões.





Replicação do quadro para uso interno

Acompanhamento das ações e inclusão de comentários em cada cartão.

CONCLUSÃO

O Grupo de Trabalho da Lei Geral de Proteção de Dados, em nome da Câmara Técnica de Gestão Empresarial (CTGE), agradece a todos que somaram para a confecção desta cartilha, em especial aos representantes da Companhia de Saneamento Ambiental do Maranhão (CAEMA) e das demais concessionárias, que não pouparam esforços para consolidar o conteúdo deste instrumento.

Como grupo, incentivamos que as Diretorias das empresas estaduais de saneamento indiquem membros para compor nosso corpo técnico, com o objetivo de alavancar o alcance e impacto das atividades relacionadas à proteção de dados e segurança da informação.

Os próximos passos do grupo de trabalho são a criação e publicação de uma cartilha complementar – voltada ao saneamento nacional – para a implementação e obtenção do certificado ISO/IEC 27001, o qual descreve a padronização do gerenciamento de segurança da informação, visto que boa parte das diretrizes desta ISO já está abarcada no processo de conformidade à Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

Concluímos reafirmando o papel da Associação Brasileira das Empresas Estaduais de Saneamento (AESBE) na garantia e manutenção da legalidade dos processos finalísticos nos níveis estratégico, tático e operacional das empresas prestadoras do serviço de abastecimento de água e esgotamento sanitário no Brasil.

Com a colaboração de todos, alcançaremos a universalização dos serviços de saneamento de forma justa, equalitária, assegurando também o sigilo das informações sensíveis e dos dados pessoais dos nossos clientes – o povo brasileiro.

aesbe
Associação Brasileira das Empresas
Estaduais de Saneamento