Guia básico de adequação à LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

PROJETO DE EXTENSÃO

DISCIPLINA DE TÓPICOS INTERDISCIPLINARES

UNISM FACULDADE DE CIÊNCIAS JURÍDICAS DE SANTA MARIA

Elaborado por:
Andrei Nichele Reses
Andressa Batista dos Santos
Carlos Roberto Gaida
Claudio Dalla Porta
Elpídio da Rosa Moreira
Fabio Santos de Oliveira
Guilherme Howes Neto
Fagner Paim da Silva
João Antonio Farias
Luciano Silva Bonacorso
Kellen Machado Lamperth
Maria Luísa Beck da Rocha
Miguel Armando Bick
Otavio Dutra Dias
Ronei Silva dos Santos
Roberto Oliveira do Nascimento
Samuel Coitinho Oliveira
Samuel Souza Rodrigues
Thamires da Silva Santos
William de Souza Lima
Vinísios Soares Neto
Vinicios Alves Marques

GRADUAÇÃO EM DIREITO

Professora da Disciplina: Me. Joelma da Silva Machado de França
Direção Geral: Drª Nara Suzana Stainr
Coordenação Acadêmica: Me. Claudete Fogliato Ribeiro
Design: Luciano Bitencourt Dielo

GUIA BÁSICO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PARA ORGANIZAÇÕES PRIVADAS

A Lei Geral de Proteção de Dados, Lei 13.709/2018, entrou em vigor em setembro de 2020, sendo que suas sanções administrativas passaram a ser exigíveis a partir de 1° de agosto de 2021, a fim de haver tempo hábil para a adequação das empresas e organizações.

A legislação visa, sobretudo, proteger os dados pessoais, que pertencem aos seus titulares, estabelecendo que para o tratamento desses dados por parte das empresas ou organizações, deve haver obrigatoriamente transparência acerca do uso que é feito com tais informações pessoais.

TITULARES DE DADOS

São as pessoas naturais a quem se referem os dados pessoais objetos do tratamento.

DADO PESSOAL

Informação relacionada a pessoa natural identificada ou identificável.

LISTA DE ABREVIATURAS E SIGLAS:

LGPD - LEI GERAL DE PROTEÇÃO DE DADOS / Lei 13.709/2018

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

RIPD – RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

GDPR (General Data Protection Regulation) - Regulamento Geral de Proteção de Dados da União Europeia, em vigor desde 25 de maio de 2018.

DESSA FORMA, A LEI INCIDE SOBRE TODOS OS CNPJ, SEM EXCEÇÃO. CASO SUA EMPRESA AINDA NÃO ESTEJA DEVIDAMENTE ADEQUADA, JÁ PASSOU DA HORA, POIS SUA ORGANIZAÇÃO JÁ SE ENCONTRA EXPOSTA ÀS SANÇÕES PREVISTAS NESSA LEI FEDERAL.

ATENÇÃO AGENTES DE PEQUENO PORTE!

A ANPD PUBLICOU UMA RESOLUÇÃO QUE SIMPLIFICOU O REGULAMENTO DE APLICAÇÃO DA LGPD PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE, MICROEMPRESAS E STARTUPS. DE ACORDO COM A RESOLUÇÃO, TAIS AGENTES:

- Não são obrigados a indicar o Encarregado pelo tratamento de dados pessoais, desde que disponibilizem um canal de comunicação com o titular de dados;

- Deverão adotar medidas de segurança da informação para proteção dos dados pessoais, no entanto, podem ter uma política simplificada de segurança da informação, desde que eficaz;

- Terão prazo dobrado para: atendimentos de solicitações dos titulares, comunicação com à ANPD e ao titular sobre a ocorrência de incidentes de segurança, apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento, entre outros prazos.

A lei prevê a necessidade de implementação de uma Governança sobre a Segurança da Informação, tema relevante na agenda mundial, demandando investimento afim de se adequar a essa realidade. Para tanto, faz-se necessário, em especial, pessoas qualificadas, como é o caso do Encarregado de Dados, alteração de processos, ferramentas que garantam a segurança das informações, criação de canais de comunicação com os titulares, treinamento de colaboradores, fornecedores e parceiros e eventualmente, contratação de consultorias.

A seguir, sugerimos 6 passos a serem percorridos no Processo de Adequação a LGPD:

1º CONSCIENTIZAÇÃO P A P

DA PRESIDÊNCIA A PORTARIA DA ORGANIZAÇÃO

A alta gerência deve considerar a relevância da LGPD, tendo em vista:

• **Relações mais transparentes e fortalecimento do reconhecimento no mercado.** A Lei prevê maior transparência aos titulares acerca da utilização das suas informações pessoais, sendo também, uma oportunidade para as empresas se aproximarem de seus colaboradores, clientes e fornecedores, demostrando comprometimento e responsabilidade com os dados que lhe foram confiados.

• **Agenda global**, com a chegada da 4ª REVOLUÇÃO INDUSTRIAL ou Revolução Digital 4.0 as mais diversas áreas do comércio, indústria e serviços passarão por adequações em suas atividades que implicarão em investimentos em tecnologias, sendo **o tratamento dos dados pessoais vital para a manutenção dos negócios.**

• **Segurança Jurídica**, a Lei unifica todas as regras relacionadas à privacidade no país, sendo essencial para manter o mercado brasileiro "na mesma página" que os demais mercados do mundo. Na esteira da criação do GDPR, países podem restringir as negociações, quando o país de origem ou destino dos dados não possuir legislação de proteção de dados adequada, tornando-se indispensável que o Brasil se adaptasse.

• **Retorno sobre o investimento.** A Lei prevê a eliminação de informações irrelevantes, como leads perdidos, assim o marketing conseguirá adaptar com maior facilidade suas mensagens de acordo com as necessidades e hábitos específicos de um público claramente definido.

• **Segurança da Informação:** A empresa deverá criar políticas internas de Segurança da Informação, o que favorecerá para a redução dos riscos do uso inadequado de informações pessoais, bem como de invasões, violações, vazamento de dados, ou o uso dos dados de forma diversa da finalidade proposta na política de privacidade, os chamados incidentes de segurança.

• O artigo 52 da LGPD prevê as sanções administrativas decorrentes da inadequação a Lei, sendo que as multas podem chegar a 2% do faturamento anual da empresa ou organização por infração, limitada a R$50.000,000,00 (cinquenta milhões de reais). Mas a multa, que também pode ser diária, é o menor dos danos, já que a empresa pode ser impedida de usar os dados temporariamente ou em definitivo, a depender das peculiaridades do caso concreto. Além disso, a Autoridade Nacional de Proteção de Dados, órgão fiscalizador, também poderá dar publicidade ao fato ocorrido o que poderá acarretar em perda de credibilidade no mercado.

OS COLABORADORES DEVERÃO RECEBER O DEVIDO TREINAMENTO A FIM DE SEREM CAPACITADOS NO QUE TOCA AO TRATAMENTO DE DADOS EM CONFORMIDADE COM A LGPD

• A Alta Gerência deve nomear o Encarregado de Dados, podendo também ser denominado de Data Protecttion Officer (DPO), termo emprestado da Lei Europeia (GDPR).

• Após, deverá ser realizado um **Treinamento específico** com o objetivo de disseminar uma cultura de proteção de dados entre colaboradores e prestadores de serviços, sendo fundamental que todos compreendam a responsabilidade em gerir dados pessoais, o que é a LGPD e como ela repercutirá no cotidiano de cada um, enquanto profissionais e cidadãos. **Mudanças exigem planejamento, prática e persistência. Seja criativo para engajar as pessoas e busque os recursos necessários para atingir os objetivos da organização.**

• Melhor seria, que o treinamento fosse ministrado pelo **Encarregado de Dados**, pessoa que deve ser indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, podendo ser contratado por CLT ou através de um contrato de prestação de serviços.

• **Controlador** a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, que é o caso das empresas.

• **Operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, é o caso, por exemplo de um escritório de contabilidade que presta serviço para uma determinada empresa.

• Ambos, controlador e operador, são denominados pela Lei, como **Agentes de Tratamento de Dados.**

• Após o Treinamento, deverá ser formado um **Comitê de Privacidade**. O Encarregado é o responsável por tal formação, trata-se da equipe que auxilia na implementação da LGPD, regulamentando o tratamento dos dados pessoais.

Não será possível levar o projeto a termo, se não houver o apoio incondicional da Alta Gerência.

2ª MAPEAMENTO DE DADOS

Após a Equipe de Comitê de Privacidade ser estabelecida, treinada e engajada, a primeira atividade será mapear todos os processos da empresa que realizam tratamento de dados pessoais, sob a supervisão do Encarregado de dados.

As Atividades Do Encarregado De Tratamento De Dados Pessoais consistem em:

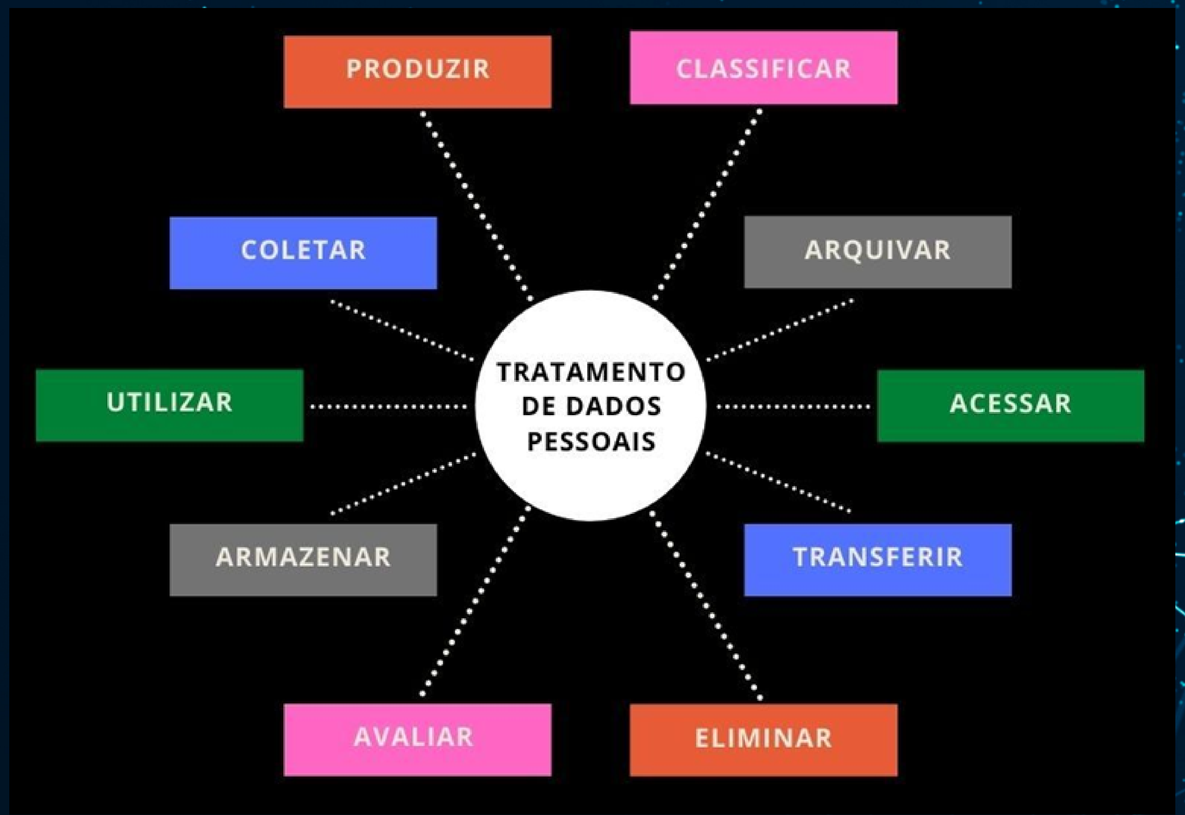
- Receber as comunicações dos titulares, através de um canal próprio para isso e gratuito e respondê-las de acordo com o prazo estipulado pela Lei.

- Atuar na comunicação com a ANPD, como no caso de reportar incidentes de segurança;

- Realizar a gestão do processo de Adequação da empresa à LGPD, ou o aculturamento.

Empresas com procedimentos operacionais descritos irão otimizar o tempo na fase de Mapeamento de Dados, uma vez que a documentação dos processos interno possibilita visualizar os dados pessoais utilizados nos mesmos. Se esse não for o caso, será necessário mapear todos os processos e identificar quais dados pessoais foram usados, que é o mesmo que tratados, em cada etapa.

Mas, o que é tratar dados pessoais, afinal?



De qualquer forma, faz-se necessário criar uma planilha ou um documento padronizado, a fim de que toda a equipe obtenha resultados semelhantes durante esse levantamento.

A seguir sugerimos um modelo, escaneie o QR CODE e faça o dowload:

PLANILHA
MODELO DE MAPEAMENTO

O modelo proposto na tabela anterior abrange pontos da LGPD que necessitam ser levantados e avaliados. No entanto, cada empresa tem suas peculiaridades, sendo recomendado que se façam as adaptações de acordo com a realidade da organização que será adequada.

É durante esse levantamento que deve se dar atenção especial à descrição da **finalidade**, ou seja, para que, **com qual objetivo, a empresa realiza o tratamento de dados**. A finalidade é fundamental para identificar a **hipótese de tratamento** que dará embasamento legal para o tratamento de dados realizado pela sua empresa.

Dica: Cada finalidade deve estar associada a uma hipótese de tratamento

O objetivo dessa etapa também possibilita mapear se os princípios estabelecidos pela LGPD estão sendo cumpridos nas atividades de tratamento de dados, que deverão observar a boa-fé, bem como os demais princípios a seguir:

FINALIDADE: realização do tratamento para propósitos legítimos, específicos, explícitos e informados previamente ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

ADEQUAÇÃO: compatibilidade do tratamento de dados com as finalidades específicas informadas previamente ao titular, de acordo com o contexto do tratamento;

NECESSIDADE: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

LIVRE ACESSO: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

QUALIDADE DOS DADOS: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

TRANSPARÊNCIA: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;

SEGURANÇA: utilização de medidas 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 difusão;

PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

NÃO DISCRIMINAÇÃO: impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.;

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

3ª DIAGNÓSTICOS

De acordo com os levantamentos obtidos na etapa anterior, é hora de identificar o grau de maturidade da empresa em face das exigências preconizadas pela LGPD, sendo a Lei também uma oportunidade para estabelecer melhorias com relação a governança corporativa, pois estipula que a governança dos dados dever estar integrada com a **governança corporativa. Então, devemos identificar quais processos devem ser adequados á LGPD, bem como, os novos processos que deverão ser criados em conformidade com a Lei.**

Ocorre que nem mesmo a LGPD se encontra completamente adequada, sendo que muitos artigos ainda carecem de regularização pela ANPD, estima-se que o processo de Adequação pode levar de 6 meses a 3 anos, a depender das peculiaridades da organização

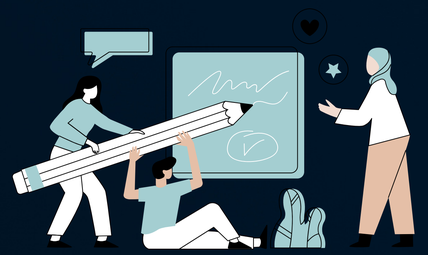
Mas, a Lei já deixou evidente a necessidade de todos os processos da empresa serem regidos sob a ótica da gestão da proteção de dados e da segurança da informação. Portanto, todos os processos que foram diagnosticados à margem desses conceitos devem ser adequados.

Deve ser criada uma cultura de privacidade na empresa, a fim de ser permanentemente revista com ações de melhorias provenientes de sugestões e incidentes reportados pelos envolvidos.

Importa que todos sigam BOAS PRÁTICAS DE PROTEÇÃO DE DADOS. Outro relevante conceito trazido pela lei é o *privacy by design* , em que proteção de dados pessoais é pensada desde a concepção do produto ou serviço até a sua concepção. Por isso, busque instituir esse processo em seus novos projetos também.

Note-se que a LGPD não incide somente sobre a proteção de dados no meio digital, mas também em meios físicos. Assim, faz-se imprescindível uma revisão nos processos físicos, bem como a eliminação de quaisquer riscos à proteção de dados.

4º PLANEJAMENTO DO PROCESSO DE ADEQUAÇÃO



Agora vamos identificar, planejar as soluções acerca dos **processos que precisam ser criados ou modificados** no que toca as mudanças nas operações e no comportamento que a empresa precisa implementar, bem como, estabelecer os prazos para tanto.

Entre tais mudanças, faz-se necessária a elaboração da documentação exigida pela Lei, no que se refere, em especial:

Documentos a serem elaborados ou aditados:

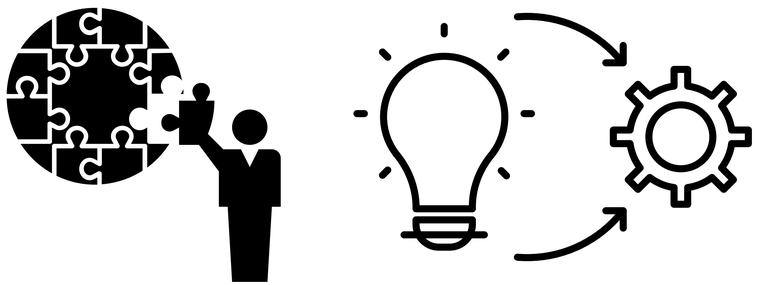
1 - Termos de compromisso com a segurança: empresas que atuam como os controladores devem enviar aos seus operadores.
2 - Cronograma de gestão: é necessário e importante ter um cronograma para assim acompanhar as ações de adequação.
3 - Plano de gestão de incidentes: é responsável por comunicar os incidentes se ocorrerem.
4 - Política de privacidade interna: este documento tem como primordial assegurar a privacidade do público interno de uma empresa (colaboradores, fornecedores).
5 - Política de privacidade externa: diferente da privacidade interna, esta tem como foco os titulares dos dados pessoais externos (clientes), deve ser clara e fácil de se encontrar para facilitar a compreensão dos mesmos.
6 - ***Data Mapping ou ROPA*****:** mapeamento de dados pessoais coletados e tratados nas empresas, onde ocorre o rastreamento e inventário dos mesmos.
7 - Plano de ação com gerenciamento de riscos: é basicamente medidas que são tomadas antes de qualquer risco acontecer, prevenindo que ocorra possíveis ameaças.
8 - Política de segurança da informação: a segurança da informação é o pilar da proteção e privacidade dos dados coletados. Exemplo: anonimização dos dados, criptografia, armazenamento físico adequado, entre outras.
9 - Plano de comunicação e treinamentos: A comunicação e o treinamento são essenciais para que não ocorra nada de forma equivocada.
10 - Relatório de impacto: algumas atividades tem um risco mais alto do que outras e por isso é primordial que constem no RIPD (relatório de impacto de proteção de dados.)

Também é a hora de definir qual será o mecanismo oferecido ao titular, para que ele possa, nos termos da Lei, solicitar informações, modificações, ou mesmo exclusões de seus dados por meio de um canal de relacionamento com o Encarregado de dados. Tal meio deve ser gratuito e facilitado.

Aos colaboradores, que também são titulares de dados, devem ser realizadas ações para demonstrar como os seus dados são tratados pela empresa (quem trata, como trata, qual a finalidade, qual a hipótese de tratamento).

Então, é hora de desenvolver um Cronograma de Implementação dos processos que necessitam ser criados para dar continuidade a Adequação da sua empresa a LGPD!

5º IMPLEMENTAÇÃO



Mais do que nunca, é hora de colocar em prática todos os processos que foram criados no Cronograma de Implementação, de forma a cumprir-se os prazos previamente estabelecidos, a seguir citamos alguns desses processos:

Atendimento das solicitações dos titulares, Registro de Operações de Tratamento de dados, Relatório de Impacto à Proteção de Dados, Atenção ao consentimento e guarda de provas, Gestão de riscos, Plano de contingência, Conformidade de fornecedores, Política de Segurança da Informação, entre outros.

6º MONITORAMENTO E CONTROLE

Enfim, chegamos à conclusão do Projeto de Adequação à LGPD, sendo esse o passo inicial para a implantação de uma cultura de proteção de dados na empresa.

A etapa de Monitoramento e Controle pode ser realizada pelo Comitê de Privacidade (auditoria interna) ou por uma consultoria (auditoria externa).

Para que se atinja o escopo da LGPD, é imprescindível que a empresa passe a adotar um modelo de gestão com fundamento na proteção de dados, que uma vez incorporado, seja continuamente melhorado, com foco em:

1 - Atualização constante;
Sempre fique por dentro das atualizações da lei ou adequações que ela poderá sofrer.

2 - Revisão constante de dados e processos;
Para chegar à *compliance*, todos os dados pessoais da empresa tiveram que estar catalogados, e vários processos tiveram que sofrer alterações.

3 - Desenvolvimento com privacidade por design;

Reforce com suas equipes, especialmente as de TI e a de Segurança da Informação, a importância do uso deste conceito, para manutenção de sistemas já existentes, e para elaboração de novos sistemas ou módulos.

4 - Resposta a Solicitações de Usuários;

As solicitações dos usuários poderão acontecer a qualquer momento. E a empresa está obrigada a acatar a solicitação, e tratar de cumpri-la, ou, pelo menos, dar resposta adequada, em tempo hábil.

5 - Resposta a Solicitações da ANPD;

De igual forma, a ANPD poderá solicitar, a qualquer momento, dados específicos sobre a conformidade da empresa em relação a LGPD. Esteja preparado para estas respostas.

6 - Treinamento e Conscientização de Colaboradores;

Prepare seus colaboradores para que entendam questões básicas de segurança, formas de proteger-se, formas de proteger a empresa etc.

7 - Monitoração Constante;

Procure criar métodos ou processos automatizados que monitorem, de forma constante, alguns aspectos mensuráveis da situação da empresa em relação à LGPD. Existem diversas ferramentas que podem ser utilizadas no processo de implementação da melhoria contínua, tais como Kaizen, Ciclo PDCA, Six Sigma, Lean Thinking, entre outras, com suas respectivas vantagens e aplicações.

8 - Resposta à Incidentes;

Deve-se prever os métodos que a empresa utilizará, em primeiro lugar, para mitigar os danos do incidente. Logo, os procedimentos de comunicação aos titulares de dados, e à ANPD, sobre o ocorrido.

9 - Prestação de Contas;

Isto se faz, normalmente, através da preparação de um relatório de incidente, para a ANPD, e um comunicado de prestação de contas, ao titular.

10 - Documentação adequada.

Para manter a empresa em conformidade, sem dúvida, um dos pontos administrativos mais notáveis, é a questão da documentação, conforme já tratamos anteriormente.

Dessa forma, a sua empresa estará cumprindo o propósito de criar um sistema de gestão da proteção de dados e da segurança da informação, que tem por objetivo tornar a relação entre a empresa e os titulares dos dados que lhe foram confiados, mais transparente e segura, cumprindo os requisitos da Lei Geral de Proteção de Dados.

O sistema de gestão da proteção de dados e da segurança da informação, começa s ser implantado com o Projeto de Adequação à LGPD, devendo ser incorporado ao sistema de gestão da empresa e reavaliado constantemente para melhorias contínuas.

A implantação desse sistema pode ser longa e trabalhosa, e sua manutenção exige disciplina e persistência. Contudo, os benefícios trazidos por ele irão elevar a sua empresa a outro nível na gestão de um de seus mais importantes ativos: os dados.

DESEJAMOS QUE TENHA ÊXITO NA SUA IMPLANTAÇÃO E MANUTENÇÃO.

Guia básico de adequação à

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

PROJETO DE EXTENSÃO

DISCIPLINA DE TÓPICOS INTERDISCIPLINARES

SANTA MARIA, RIO GRANDE DO SUL SETEMBRO DE 2022