Série Proteção de Dados

7 LEGÍTIMO INTERESSE

VEIRANO ADVOGADOS



Este é o sétimo capítulo da Série Proteção de Dados. Clique aqui para acessar o cap. 6.



Em 2023, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou "LGPD") completa 5 anos de sua publicação – agora também com a possibilidade de aplicação das sanções administrativas pela ANPD, que se estende desde agosto de 2021. A Autoridade Nacional de Proteção de Dados ("ANPD") tem atuado ativamente para fomentar a discussão e disseminar os conceitos, práticas e princípios de privacidade e proteção de dados, com a publicação de diversos materiais para conscientização e regulamentação da LGPD desde a sua criação.

O Veirano Advogados tem acompanhado e participado das discussões relacionadas a estes temas. Por isso, nosso time de Proteção de Dados & Privacidade preparou a **Série Proteção de Dados**, na qual serão realizadas publicações periódicas sobre diferentes temas relacionados à privacidade, trazendo não somente os conceitos da LGPD, mas também publicações da ANPD sobre o tema, considerações relevantes, dentre outros conteúdos.

A Base Legal do Legítimo Interesse

Conforme mencionado de forma resumida no Capítulo 5, o Legítimo Interesse é uma base legal aplicável apenas para o Tratamento de Dados Pessoais não-sensíveis. Em outras palavras, o fundamento de um interesse legítimo do Controlador (ou de algum terceiro) **não** pode ser usado como fundamento para tratar Dados Pessoais Sensíveis.

Segundo a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - "LGDP"), Dados Pessoais Sensíveis são "*origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*".



Lembre-se:

Dados sensíveis NÃO poderão ser tratados com base no legítimo interesse.

O Legítimo Interesse é uma das dez bases legais previstas na LGDP para Tratamento de Dados Pessoais. Esta é a hipótese de Tratamento considerada mais flexível e, portanto, a mais controversa.

Tendo isso em vista, e levando em conta que a Autoridade Nacional de Proteção de Dados ("ANPD") ainda não estabeleceu diretrizes específicas com relação à referida base legal, deve-se ter bastante cuidado ao aplicá-la. De acordo com Agenda Regulatória da ANPD para o biênio 2023-2024, publicada pela Portaria ANPD nº 35, de 4 de novembro de 2022, a publicação de documento orientando o público sobre as bases e hipóteses legais de aplicação da LGDP deverá ocorrer ainda na Fase 1, ou seja, ainda em 2023.

Adiantamos que é incorreto o pensamento de que o Legítimo Interesse se aplica quando as demais bases legais não são aplicáveis. De forma alguma esta hipótese deve ser entendida como uma espécie de "cheque em branco".

Nos termos da LGPD, o Legítimo Interesse do Controlador somente poderá fundamentar o Tratamento de Dados Pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

- Apoio e promoção de atividades do Controlador.

E

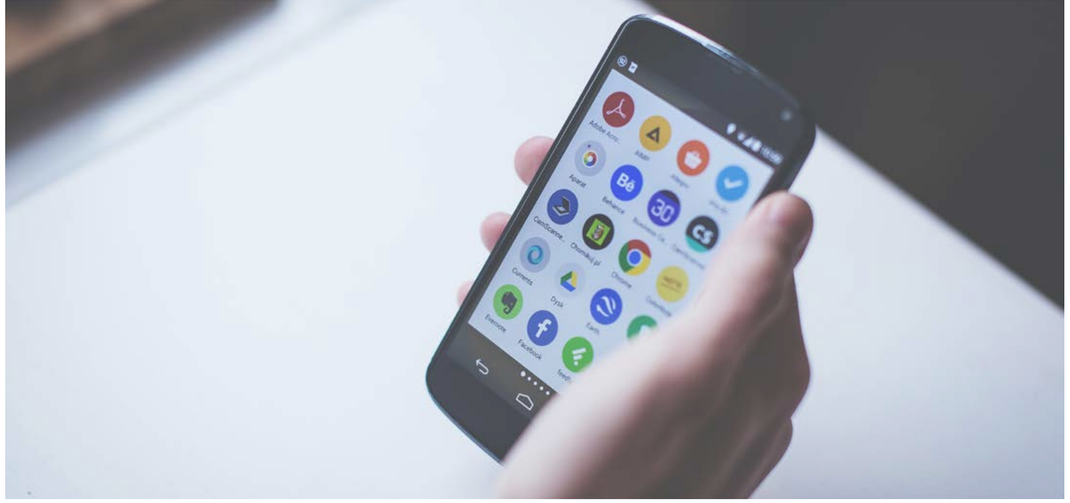
- Proteção, em relação ao Titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos da LGPD.

Em atenção do princípio da necessidade previsto na LGPD, quando o Tratamento for baseado no Legítimo Interesse do Controlador, somente os Dados Pessoais estritamente necessários para a finalidade pretendida poderão ser Tratados, devendo o Controlador adotar medidas para garantir a transparência do Tratamento.

Além disso, a escolha do Legítimo Interesse deve, necessariamente, estar atrelada a critérios de segurança e previsibilidade. Como o seu uso está baseado em riscos, é importante que, preventivamente, o Controlador realize testes e elabore a documentação adequada.

Assim sendo, para garantir que a sua empresa não utilizará o Legítimo Interesse de forma precipitada e incorreta, a própria LGPD determina que a sua utilização seja precedida da realização do **Teste de Ponderação**, mais conhecido como *Legitimate Interest Assessment*, ou, de forma simplificada, "LIA", que será explicado a seguir.





Teste de Ponderação e Relatório de Impacto à Proteção de Dados Pessoais

Elaboração do LIA - Teste de Ponderação

O *Legitimate Interest Assessment* (LIA) não foi expressamente previsto pela LGPD, nem pelo Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* – "GDPR"), apesar de existir orientações nesse sentido por parte das autoridades competentes na União Europeia.

Segundo as diretrizes da *Information Commissioner's Office* ("ICO"), que regula a proteção de Dados Pessoais no Reino Unido, como o Legítimo Interesse pode ser aplicado em uma ampla gama de circunstâncias, o Controlador é quem possui o ônus de equilibrar seus interesses legítimos e a necessidade de tratar os Dados Pessoais em respeito aos direitos e liberdades do Titular. Tudo isso levando em consideração as circunstâncias particulares do caso concreto.

Para tanto, recomenda-se a elaboração do LIA, que, por sua vez, é subdividido em três etapas: **(1)** finalidade; **(2)** necessidade; e **(3)** ponderação.



Em linhas gerais, o LIA consubstancia a finalidade e a adequação da base legal para determinada atividade de Tratamento, assegurando que você esteja em conformidade com a LGPD e em cumprimento com o princípio da responsabilidade e da prestação de contas previsto na LGPD.

Pode-se resumir as três etapas da seguinte forma:

Finalidade.

Primeiramente, para ser válido, o Legítimo Interesse somente poderá ser utilizado para **finalidades legítimas** de Tratamento de Dados Pessoais, tomando como base situações concretas, tais como: prevenção de fraude, segurança patrimonial e marketing direto. Em outras palavras, isso quer dizer que situações meramente hipotéticas não podem ser abarcadas pelo Legítimo Interesse por carecer do fator concretude.

Alguns exemplos de perguntas para verificar se uma determinada finalidade é legítima:

» Qual a finalidade do Tratamento?

» Qual o benefício que você pretende obter com o Tratamento?

» Algum terceiro se beneficia do Tratamento? De qual maneira?

» Existem benefícios públicos mais amplos para o Tratamento?

» Qual a importância desses benefícios?

» Qual seria o impacto caso você não pudesse seguir com o Tratamento?

» O Tratamento pode ser considerado antiético ou ilegal de alguma forma?

Necessidade.

Além disso, quando o Tratamento for baseado no Legítimo Interesse do Controlador, somente os Dados Pessoais **estritamente necessários** para a finalidade pretendida poderão ser tratados, devendo tal Tratamento ser pertinente, proporcional e não excessivo. Desta forma, o Controlador deverá adotar medidas para garantir a transparência do Tratamento baseado em seu interesse legítimo.

Alguns exemplos de perguntas para confirmar a necessidade estrita:

» O Tratamento é proporcional com a finalidade pretendida?

» Existe uma forma menos onerosa para atingir a finalidade pretendida?

» O Tratamento realmente ajuda a atingir o interesse almejado?

» É uma maneira razoável de fazer isso?

» Existe outra maneira menos invasiva para se obter o mesmo resultado?

Ponderação.

Por fim, deve-se **equilibrar** as finalidades legítimas e os Dados Pessoais estritamente necessários com os direitos e liberdades do Titular de Dados, identificando possíveis impactos e riscos atrelados.

Alguns exemplos de perguntas para auxiliar com a ponderação:

» Você está tratando Dados Pessoais de crianças ou de pessoas que podem ser consideradas vulneráveis?

» Existe uma expectativa razoável do Titular em ter seus Dados Pessoais tratados desta maneira e para essa finalidade?

» Qual é a natureza do seu relacionamento com o Titular?

» Algum dos Dados Pessoais é confidencial ou privado?

» Você está confiante em explicar o Tratamento ao Titular?

» É provável que o Titular se oponha ou ache o Tratamento intrusivo?

» Qual é o impacto potencial ao Titular?

- Você pode adotar alguma salvaguarda para minimizar o impacto?
- Você pode oferecer algum mecanismo de opt-out para o Titular?

Esta última etapa do balanceamento é fundamental para a verificar se o Tratamento realmente não afeta os direitos e liberdades fundamentais do Titular, nem contraria suas legítimas expectativas.

Após a elaboração do LIA

Após as perguntas acima serem respondidas, lembrando que este é um rol não exaustivo de perguntas, o Controlador chegará à conclusão com relação a possibilidade de uso da base legal do Legítimo Interesse. Como consequência lógica, não sendo possível justificar o Tratamento nas três esferas – finalidade, necessidade e ponderação – o Legítimo Interesse não poderá ser usado.

Como mencionado anteriormente, o Legítimo Interesse é uma hipótese controversa, portanto, sempre recomendamos que o LIA seja realizado com o objetivo de assegurar que a base legal do Legítimo Interesse pode ser aplicada ao caso concreto.

Por fim, mas não menos importante, recomenda-se a adoção de salvaguardas adicionais que sejam aptas a limitar os riscos para o Titular. Dentre essas medidas, destacamos a realização de processos de pseudoanonimização e criptografia dos Dados Pessoais, a minimização de coleta de Dados Pessoais e atualização constante de avisos de privacidade, que servem como um atestado de transparência da empresa com relação ao Tratamento conferido aos Dados Pessoais de Titulares, dentre outras políticas de segurança.

Elaboração do RIPD

Nos termos da LGPD, a ANPD poderá solicitar ao Controlador a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais ("RIPD"), também chamado de *Data Processing Impact Assessment* ("DPIA"). Mais recentemente, no dia 06 de abril de 2023, a ANPD publicou uma série de perguntas e respostas ("Q&A") com o objetivo de orientar e esclarecer a sociedade sobre o RIPD. Ressaltamos que o processo de regulamentação do tema está em andamento, conforme previsto na Agenda Regulatória da ANPD para o biênio 2023-2024, de modo que obrigações e parâmetros adicionais poderão ser estabelecidos pela ANPD futuramente.

Os principais pontos apresentados no Q&A foram os seguintes:

O que é o RIPD, quem deve elaborá-lo e como fazê-lo?

Em linhas gerais, o RIPD é uma documentação, de responsabilidade do Controlador, que contém a descrição dos processos de Tratamento de Dados Pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de Dados Pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do Titular. O RIPD deve conter, também, as medidas, salvaguardas e mecanismos de mitigação dos riscos apontados.

Existem, ainda, algumas situações em que o RIPD pode ser exigido pela ANPD. A própria LGPD menciona as seguintes hipóteses:

- Operações de Tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.
- Quando o Tratamento tiver como fundamento a hipótese de Legítimo Interesse.
- Para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD.
- Para Controladores em geral, quanto às suas operações de Tratamento, incluindo as que envolvam Dados Pessoais Sensíveis.

Entende-se, portanto, que as seguintes situações ensejarão a elaboração do RIPD pelo Controlador:

(1) Para atender à determinação da ANPD.

OU

(2) Em atenção ao princípio da responsabilização e prestação de contas, ao verificar que o Tratamento a ser realizado pode implicar em **alto risco** à garantia dos princípios gerais de proteção de Dados Pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do Titular.

O RIPD deve conter, no mínimo, os seguintes elementos*:

A descrição dos tipos de Dados Pessoais coletados ou tratados.

+

A metodologia usada para o Tratamento e para a garantia da segurança das informações.

+

A análise do Controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

*Caso o RIPD seja requerido pela ANPD, poderão ser solicitados elementos adicionais.

Quando um Tratamento deve ser considerado como de alto risco?

Sobre este tema, novos entendimentos devem ser publicados pela ANPD, mas até lá, o Tratamento será considerado de alto risco se for verificada, no caso concreto, a presença de, ao menos, um Critério Geral e de um Critério Específico conforme abaixo apresentado.

- Critérios Gerais (sendo apenas 01 necessário):
  - Larga escala
  - Afetar significativamente interesses e direitos fundamentais do Titular.
- Critérios Específicos (sendo apenas 01 necessário):
  - Uso de tecnologias emergentes ou inovadoras
  - Vigilância ou controle de zonas acessíveis ao público

› Decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais

› Utilização de Dados Pessoais Sensíveis ou de Dados Pessoais de crianças, de adolescentes e de idosos.



***Larga escala**: quando o tratamento abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

****Afetar significativamente interesses e direitos**: quando o tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Atenção: A lista de Critérios Gerais e Específicos não é exaustiva, de modo que, em conformidade com o princípio da responsabilização e prestação de contas, cabe ao Controlador avaliar a existência de alto risco em situações diferentes das indicadas.

Outros pontos de atenção sobre o RIPD: quantidade, atualizações e gestão de risco.

Ressaltamos que, como regra, um único RIPD deve corresponder a cada projeto/processo do Controlador que contenha um conjunto de operações de Tratamento voltadas para uma mesma finalidade. No entanto, a depender do caso concreto, se o Controlador realizar múltiplas operações de Tratamento similares em termos de natureza, finalidade e riscos, é razoável que seja elaborado apenas um RIPD que inclua todas essas operações em conjunto.

De toda forma, recomenda-se ao Controlador a revisão contínua do RIPD, em especial, quando houver fatos novos que possam ensejar mudanças nos riscos identificados, tais como alteração nas operações de Tratamento, identificação de novos fatores de risco, agravamento dos fatores de risco anteriormente identificados, ou em caso de novas regulamentações ou orientações emitidas pela ANPD.

Por fim, a LGPD também prevê a possibilidade de que o Controlador, para cumprimento dos princípios da segurança e da prevenção, implemente programa de governança em privacidade, devendo incluir, por exemplo, políticas e salvaguardas adequadas com base em processos de avaliação sistemática de impactos e riscos à privacidade.

RIPD | RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

1. Identificar os agentes de tratamento e o encarregado.
2. Identificar outras partes interessadas / envolvidas.
3. Avaliar a justificativa da necessidade de elaborar ou atualizar o relatório.

É NECESSÁRIO ELABORAR OU ATUALIZAR O RIPD?

- NÃO
  10. Monitorar e atualizar.
  9. Coletar comentários e aprovações.
  8. Estabelecer medidas, salvaguardas, e mecanismos de mitigação de riscos.
  7. Avaliar os riscos identificados.
  6. Analisar os princípios da LGPD.
- SIM
  4. Descrever o tratamento de dados.
  5. Analisar a base legal.

Por fim, note que o LIA e o RIPD possuem finalidades claramente distintas quando se trata da base legal do Legítimo Interesse:

» **LIA**: tem como objetivo determinar se uma empresa ou organização pode tratar Dados Pessoais utilizando o Legítimo Interesse como base legal, de acordo com a finalidade, necessidade e ponderação do Tratamento.

» **RIPD**: tem como objetivo descrever os processos de Tratamento de Dados Pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais do Titular, bem como medidas, salvaguardas e mecanismos de mitigação de risco, ou seja, é entendido como uma exceção.



Comunicações de Marketing e o Legítimo Interesse

Muito se questiona sobre a aplicabilidade do Legítimo Interesse como base legal para o Tratamento de Dados Pessoais com a finalidade de efetuar comunicações de marketing. O principal motivo desta preocupação é que algumas formas de comunicação de marketing podem não ser legítimas se não cumprirem outros padrões legais ou éticos ou códigos de prática deste setor.

Desta forma, se o marketing for realizado em conformidade com a LGPD e demais normas do setor, em atenção aos elementos abaixo, é provável que a atividade seja justificada pelo Legítimo Interesse. São eles:

a. Existir uma relação prévia entre a empresa e o Titular.

b. A empresa visar oferecer produtos e serviços estritamente similares aos previamente contratados pelo Titular.

c. Ser dada ao Titular a opção de não receber novas comunicações de marketing no futuro (*opt-out*).

Com relação ao LIA e a necessidade da opção de *opt-out*, para atividades envolvendo marketing direto, frisamos que, dado que o Titular possui o direito de se opor ao Tratamento, é mais difícil para o Controlador "passar" no Teste de Ponderação se não for dada ao Titular a opção clara de optar por não receber novos contatos.

Hipótese: Segundo este racional, se uma loja envia comunicações de marketing para um cliente antigo sobre um produto similar ao que ele já adquiriu no passado, em observância aos critérios listados, entende-se que o Legítimo Interesse pode ser utilizado como justificativa.

Em qualquer caso, deve ser garantida a esse mesmo cliente a possibilidade de *opt-out*, ou seja, de se manifestar contrariamente ao recebimento de novas comunicações de marketing pela loja. Caso o opt-out seja acionado, a loja não poderá continuar o Tratamento para esta finalidade, pois o Legítimo Interesse não será mais aplicável.

Na hipótese acima, o Tratamento pelo Controlador, em princípio, "passou" no LIA, mas por um motivo posterior foi contestado pelo Titular, impedindo a permanência do uso do Legítimo Interesse. Este cenário, não significa que o Controlador não poderá mais tratar Dados Pessoais para esta finalidade, no entanto, para que o Tratamento possa ocorrer em linha com a legislação aplicável, deve estar pautado em outra base legal (i.e., consentimento). Sobre a base legal do consentimento recomendamos a leitura completa do Capítulo 6.



Com este Capítulo 7, buscamos trazer os principais pontos de atenção com relação à escolha do Legítimo Interesse pelo Controlador. Como pode ser observado, esta base legal é um tanto quanto desafiadora e ainda traz muitos questionamentos sobre a sua aplicação.

Dada tamanha controvérsia do tema, a ANPD se antecipou e publicou o Q&A que mencionamos anteriormente. Mesmo com algumas perguntas já esclarecidas, a previsão da Agenda Regulatória da ANPD para o biênio 2023-2024 é de que este assunto volte a ser comentado e, principalmente, regulamentado de maneira mais efetiva.

Até lá, ressaltamos mais uma vez que, em todo qualquer caso que envolva o uso desta base legal, é fundamental que o Controlador tenha como norte os princípios da LGPD já detalhados no Capítulo 5, principalmente o princípio da transparência, e mantenha suas políticas e mecanismos de segurança sempre atualizados.



VEIRANO ADVOGADOS

A Experiência Veirano conta com uma abordagem holística, multidisciplinar e orientada para negócios. A fim de suprir todas as necessidades relacionadas à LGPD, nosso time de Proteção de Dados & Privacidade desenvolveu diversos formatos de projetos, que compreendem diferentes escopos de trabalho para atender demandas específicas de cada um dos nossos clientes:

1. Adequação completa

Com a atuação de uma equipe multidisciplinar, este projeto é destinado aos clientes que possuem como objetivo identificar e avaliar todas as atividades de Tratamento realizadas pela sua empresa e, a partir disso, identificar as vulnerabilidades e estruturar um plano de ação para criação de um programa de privacidade, proteção de dados embasado em pilares jurídico, processuais, de segurança da informação e governança corporativa.

2. *DPO as a service*

Neste modelo, assumimos a função de Encarregado (DPO) em nome do cliente. Para isso, alocamos um profissional para executar as atividades de gestão e monitoramento do programa de proteção de dados e privacidade do cliente.

3. Assessoria em M&A

Criado para assessorar clientes nos processos de auditoria legal de operações de fusão e aquisição, com o propósito de identificar questões de natureza jurídica relevantes (*red-flags*) e mitigar riscos relacionados à proteção e segurança de Dados Pessoais da empresa-alvo.

4. LGPD Pocket

Uma assessoria "pocket" para a adequação das atividades e/ou dos produtos desenvolvidos pela empresa, independentemente de seu porte ou linha de negócios, com um número reduzido de entregáveis.

5. LGPD on Demand

O LGPD on Demand é direcionado às organizações que desejam contar com uma assessoria multidisciplinar jurídica, de segurança da informação e governança corporativa, com atuação pontual e específica, relacionada a proteção de dados pessoais.

6. LGPD Legal Helpdesk

O Helpdesk foi criado para assessorar clientes em consultas e demandas sobre proteção de dados dentro de um pacote mensal de horas, seja antes, durante ou após o processo de adequação inicial.

7. Task Force para avaliação e comunicação de incidentes de segurança (VA Cybersecurity)

Assessoria jurídica específica e multidisciplinar para aspectos relacionados à suspeita ou ocorrência de um Incidente de Segurança, de acordo com as instruções mais atualizadas da ANPD e demais leis e regulamentos aplicáveis ao tema.

8. Representação em ações administrativas e judiciais envolvendo proteção de dados

Representação de clientes em ações ou potenciais ações administrativas e/ou judiciais em matéria de proteção de dados.

9. Análise de decisões administrativas e judiciais sobre proteção de dados

Monitoramento periódico de decisões proferidas em processos judiciais e administrativos, a fim de apresentar o entendimento das autoridades e os impactos para a empresa ou setor econômico ao cliente de forma resumida.

10. Elaboração e atualização de relatório de impacto à proteção de dados

A ANPD poderá solicitar ao Controlador o Relatório de Impacto à Proteção de Dados Pessoais (“RIPD” ou, em inglês, “DPIA”). Nossa equipe possui expertise no tema, e pode auxiliar com a elaboração e atualização do RIPD.

11. Desenvolvimento de workshops

Elaboração e aplicação de treinamentos sobre os principais conceitos de privacidade e proteção de dados para capacitação de seus colaboradores.

12. Playbook para negociação de contratos comerciais

Elaboração de *playbooks* para negociação e contratos comerciais, para facilitar e agilizar processos internos de equipes comerciais, técnicas e jurídicas.

13. Handbook para resposta aos titulares

Elaboração de materiais para auxiliar as empresas no atendimento tempestivo das solicitações dos titulares, bem como no procedimento a ser seguido pela empresa na resposta ao titular, conforme o modelo de negócio da companhia.

14. Transferência internacional de dados

Ajudamos clientes a entender o contexto da transferência internacional, adequá-la ao fundamento legal aplicável, avaliar requisitos de localização de dados, aditar contratos, elaborar e revisar acordos intragrupo e, de forma geral, responder consultas relacionadas à harmonização da legislação estrangeira com a brasileira.

15. Auditoria de privacidade e proteção de dados

Realizamos auditorias para avaliação do nível de maturidade da companhia, apresentando recomendações para mitigação de risco.

16. Elaboração e revisão de documentos pertinentes ao setor financeiro

Nosso time tem expertise em elaborar políticas de segurança em conformidade com as regulamentações específicas de segurança da informação do Banco Central, além de responder consultas sobre o tema.

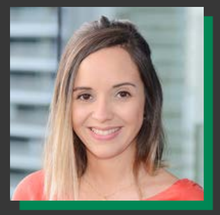
Estamos à disposição caso tenha dúvidas ou precise de informações adicionais



FÁBIO PEREIRA
+55 11 2313 5906
fabio.pereira@veirano.com.br



CINTIA ANDRADE
+55 21 3824 4655
cintia.andrade@veirano.com.br



DENISE LOUZANO
+55 11 2313 5912
denise.louzano@veirano.com.br



ISABEL HERING
+55 11 2313 5726
isabel.hering@veirano.com.br



PAOLA LORENZETTI
+55 11 99976 8480
paola.lorenzetti@veirano.com.br



ROBERTA MEDINA
+55 21 3824-4661
roberta.medina@veirano.com.br

Disclaimer: Este material foi atualizado pela última vez em 27 de abril de 2023 e publicado em 28 de abril de 2023. Para informações mais atualizadas, entre em contato conosco.