Relatório de Impacto à Proteção de Dados Pessoais

Serviço de disponibilização de dados corporativos para contatos comerciais.

SPEEDIO

Elaborado por:

POSSA

CONSULTORIA EM COMPLIANCE
DE PROTEÇÃO DE DADOS

Sumário

1. Objetivos

O relatório de impacto está previsto na LGPD como medida de governança para processos de tratamento de dados pessoais que possam oferecer riscos aos titulares.

Desse modo, o presente documento irá analisar todos os aspectos do fluxo de tratamento de dados pessoais referente ao serviço de disponibilização de dados corporativos para contatos comerciais, a fim de mapear os riscos para os titulares de dados pessoais e as respectivas medidas de mitigação aplicáveis.

Pretende-se avaliar o potencial impacto e a possibilidade de incidentes de segurança e ofensas à legislação de proteção de dados frente às medidas de mitigação adotadas.

2. Metodologia

O presente instrumento foi incorporado ao ordenamento jurídico brasileiro através da importação do *Data Protection Impact Assessment* previsto no *General Data Protection Regulation* da União Europeia.

Por tal motivo a metodologia utilizada tem como base os seguintes documentos da *Commission Nationale de l'Informatique et des Libertés*, Autoridade Nacional de Proteção de Dados da França:

- Guideline "PRIVACY IMPACT ASSESSMENT (PIA) 1: METHODOLOGY";
- Guideline "PRIVACY IMPACT ASSESSMENT (PIA) 2: TEMPLATE"
- Guideline "PRIVACY IMPACT ASSESSMENT (PIA) 3: KNOWLEDGEBASES"
- Guideline "SECURITY OF PERSONAL DATA PROCESSING FOR PMES" - ENISA

A respectiva metodologia demanda alto nível de detalhamento de todos os aspectos legais e técnicos dos processos de tratamento de dados pessoais que envolvem o fluxo de dados do respectivo processo, isso inclui uma análise do contexto do tratamento de dados, avaliação da necessidade e proporcionalidade da utilização de tais dados, identificação dos riscos aos titulares e quais as medidas necessárias para mitigar os impactos.

3. Necessidade de elaborar o Relatório

O relatório de impacto à proteção de dados (RIPD) está previsto nos arts. 5º e art. 38 da Lei Geral de Proteção de Dados Pessoais. É um instrumento que visa

descrever as atividades de tratamento, os possíveis riscos aos titulares e as medidas necessárias para mitigar danos em casos em que o tratamento de dados pessoais possa gerar impactos às liberdades civis e aos direitos fundamentais dos titulares.

Embora a Autoridade Nacional de Proteção de Dados do Brasil (ANPD) não tenha delimitado os tipos de operações que necessitam do desenvolvimento de um RIPD – Relatório de Impacto à Proteção de Dados, é aconselhável o desenvolvimento do documento, visto que a autoridade poderá solicitar a elaboração do RIPD a qualquer momento ao Controlador.

Seguindo as orientações emitidas pelo *Article 29*[1], órgão consultivo europeu independente em matéria de proteção de dados e privacidade, um dos critérios para avaliar a necessidade de elaborar um relatório de impacto para determinada operação é se há ou não tratamento de dados em larga escala e a combinação de diferentes conjuntos de dados. A Autoridade de Proteção de Dados do Reino Unido (ICO) considera que para análise da existência do tratamento de dados em larga escala é necessário avaliar: o número de titulares envolvidos, o volume dos dados, a variedade de dados, a duração do tratamento e a extensão geográfica.[2]

No presente caso, os dados estão sendo utilizados a partir da ampla coleta de informações disponíveis publicamente na web e há combinação de várias fontes de dados pelas empresas que fornecem serviços de *scraping* sobre dados de acesso público e dados tornados manifestamente públicos pelos próprios titulares em suas redes sociais. Com isso, é possível que o tratamento de dados pessoais, por envolver um grande número de titulares e a combinação de várias fontes de dados, resultem em riscos aos indivíduos. Surge, portanto, a necessidade de elaborar este documento para mitigar os impactos.

---

[1] **Dados tratados em grande escala:** o RGPD não define o que constitui grande escala, contudo o considerando 91 fornece alguma orientação. Em qualquer caso, o Grupo de Trabalho do Artigo 29.º recomenda que os seguintes fatores, em especial, sejam considerados quando se determina se o tratamento é ou não efetuado em grande escala: a. o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente; b. o volume de dados e/ou a diversidade de dados diferentes a tratar; c. a duração da atividade de tratamento de dados ou a sua pertinência; d. a dimensão geográfica da atividade de tratamento. **Estabelecer correspondências ou combinar conjuntos de dados**: por exemplo, com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados. Disponível em: https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf. Acesso em: 29 nov. 2022.

[2] Avaliações de impacto de proteção de dados (DPIAs). Information Comissioner's Office. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when12. Acesso em: 29 de nov. 2022.

4. Descrição e contexto do tratamento

4.1. Natureza

O respectivo tratamento de dados ocorre a partir da coleta de informações disponíveis publicamente na Internet. Existem duas categorias de dados pessoais que podem ser coletadas nesse processo: dados de acesso público e dados disponíveis publicamente pelo próprio titular.

A coleta de dados de acesso público é realizada por meio da extração de informações que estão disponíveis abertamente ao público e que são divulgadas por terceiros, através de sites governamentais, sites corporativos ou outras plataformas que disponibilizem esse tipo de dado. Além disso, existe a captação de dados tornados manifestamente públicos pelos próprios titulares em mídias sociais, por exemplo, no LinkedIn, onde é possível visualizar informações profissionais e de contato do colaborador de uma determinada organização.

Em todos os casos, as informações são utilizadas para que a Speedio possa prestar seus serviços relativos à disponibilização de dados corporativos aos seus clientes (empresas), a fim de que eles tenham insumos suficientes para prospectar ativamente novos clientes para seus negócios. Sendo assim, o acesso aos dados pessoais será disponível a Speedio e compartilhado com os clientes que contratarem seu serviço de disponibilização de dados corporativos.

Para a captação dos dados, a Speedio conta com tecnologia de Big Data e Inteligência Artificial, além do apoio de empresas parceiras que são responsáveis por coletar os dados que estão disponíveis na Internet e repassá-los a ela, a fim de que avalie as informações que são pertinentes para prestação de seus serviços.

Atualmente, os dados que são tratados permanecem disponíveis ininterruptamente na base de dados, a menos que o titular requeira a eliminação dos dados, momento em que é realizado o procedimento de exclusão das informações solicitadas, conforme procedimentos “220118 - Exclusão de dados - Procedimento Operacional Padrão (POP)” e “211124 - Modelo Resposta LGPD”.

Por fim, ressalta-se que a Speedio se preocupa com a segurança dos dados pessoais que são tratados, e é por esse motivo que a empresa desenvolveu sua Política de Segurança da Informação e estabeleceu medidas aptas a proteger os dados, tais como: criptografia, contratação de auditores externos, gestão de vulnerabilidades, backups, entre outros.

4.2. Escopo

Para o presente fluxo de tratamento, utiliza-se apenas dados de natureza comum que sejam acessíveis publicamente. Não há uso de dados com alto nível de sensibilidade, como a 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.

O tratamento de dados limita-se a dados de identificação e dados de contato dos titulares que sejam colaboradores e decisores de empresas, o uso das informações é exclusivamente para prospecção ativa de clientes.

Entretanto, é evidente que a atividade de tratamento envolve uma enorme volumetria de dados capazes de identificar pessoas. Sendo assim, é imprescindível que exista um alto controle e proteção das informações processadas, a fim de evitar danos e impactos aos titulares envolvidos no processo.

4.3. Contexto

Considerando que a coleta de dados advém de variadas fontes disponíveis on-line, não existe um contexto específico e uma relação previamente estabelecida entre o responsável pelo tratamento e os titulares.

Ocorre que a Speedio somente coleta dados de pessoas com a finalidade de permitir o conhecimento sobre uma determinada estrutura corporativa, **não sendo objeto dos serviços** a criação de perfis profissionais dos titulares ou qualquer outro processo de definição de perfil que consista em avaliar certos aspectos pessoais de uma pessoa física para prever, por exemplo, seu desempenho profissional.

Assim, considerando que para essa finalidade existem tratamentos de dados pessoais de forma instrumental, é necessário que garantias sejam concedidas aos indivíduos, caso não concordem com o tratamento, isso inclui procedimentos para exclusão dos dados, direito de acesso as informações, entre outros direitos previstos no art. 18 da LGPD.

4.4. Finalidade

A finalidade do tratamento dos dados é fornecer informações sobre outras empresas, através de dados tornados públicos por titulares que trabalham para essas instituições. Essas informações são repassadas aos clientes da Speedio mediante prestação de serviço, a fim de que sejam utilizados em situação de relação corporativa, beneficiando não só as empresas envolvidas, como também os próprios

titulares de dados pessoais que podem estar interessados na oferta do serviço ou produto fornecido para suas contratantes.

Ressalta-se que a Speedio é considerada Controladora de dados pessoais no processo de criação e estruturação de banco de dados com informações sobre relações corporativas e contatos profissionais dos titulares que estão em sua base de dados.

A tabela abaixo descreve os dados, duração e formas de armazenamento:

Tipos de Dados	Descrição dos Dados	Armazenamento	Prazos de Armazenamento
Dados corporativos	Nome completo, e-mail corporativo, telefone corporativo, cargo exercido na empresa.	Base de dados AWS, Azure, Hetzner e Contabo	Indeterminado, a menos que o titular solicite a exclusão dos dados.

5. Princípios

5.1. Princípio da finalidade, adequação e necessidade

O princípio da finalidade estabelece que os dados só podem ser tratados para propósitos legítimos, específicos, explícitos e informados, sem um tratamento posterior que desvie das finalidades previamente determinadas.

A partir da análise do tratamento, observa-se que a operação está relacionada ao fornecimento de dados atualizados sobre contatos corporativos, a fim de que as empresas que contratem a ferramenta da Speedio possam seguir com seus processos de prospecção ativa de clientes de maneira facilitada, ou seja, a empresa que contrata a plataforma da Speedio tem acesso a dados corporativos de clientes ideais (colaboradores e decisores de empresas). Assim, a empresa que utiliza a base de dados de *leads* da Speedio consegue um meio de contatar um colaborador de determinada organização para fornecer seus serviços e produtos.

A Speedio não possui controle sobre a finalidade para qual seus clientes utilizam os dados pessoais.

Os dados são tratados unicamente para a finalidade de fornecimento de informações corporativas pela Speedio, cabendo a cada empresa contratante delimitar a finalidade do tratamento que ocorrerá posteriormente.

Ademais, considera-se legítima a finalidade do tratamento, uma vez que a base legal que autoriza o tratamento é o interesse legítimo do Controlador, conforme justificativa apresentada no item 6 deste documento.

Outrossim, o princípio da finalidade deve ir além das disposições previstas na LGPD, outras legislações que possam interferir no tratamento precisam ser analisadas.

Em relação ao aspecto da transparência mediante informações explícitas e claras, a finalidade necessita ser comunicada ao titular de modo que não gere ambiguidades ou imprecisões que possam acarretar dúvidas sobre a finalidade do tratamento. Para evitar tal situação, é pertinente a elaboração de um Aviso de Privacidade que informe de maneira clara e objetiva as finalidades pelas quais os dados estão sendo utilizados, a fim de garantir transparência.

É, também, dever dos clientes da Speedio, como Controladores, elaborarem Avisos de Privacidade e dar transparência sobre os tratamentos realizados com os dados que obtêm acesso em consequência do serviço contratado.

Quanto ao princípio da adequação, a LGPD define que as atividades de tratamento devem ser compatíveis com as finalidades informadas ao titular de acordo com o contexto do tratamento. Nessa situação, há compatibilidade do tratamento com a finalidade identificada e com o contexto do tratamento. Os dados coletados são utilizados apenas para fornecer o serviço da Speedio, que permite aos seus clientes a identificação da estrutura corporativa e contatos internos para relações comerciais, dentro do contexto de marketing *outbound*.

Por fim, nota-se que há um nível alto de compatibilidade da operação com o princípio da necessidade, o qual estabelece que os dados devem ser pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Apesar da coleta de dados de acesso público na Internet que podem fugir das expectativas razoáveis dos titulares, as informações que compõem a base de dados são limitadas, apenas ocorre o tratamento de dados pessoais relativos a nome, e-mail corporativo, telefone corporativo e cargo, pois sem a coleta desses dados não é possível entrar em contato com *leads* úteis para oferta de produtos ou serviços que possam ser do interesse da empresa cujos titulares são relacionados.

5.2. Princípio da transparência, livre acesso e qualidade dos dados

Os princípios da transparência e do livre acesso determinam que os responsáveis pelo tratamento de dados pessoais devem garantir aos titulares previsibilidade em relação a utilização de suas informações e consulta gratuita e facilitada sobre os dados que estão sendo tratados pela Speedio.

Para garantir o cumprimento dos princípios, é fundamental a disponibilização de um Aviso de Privacidade aos titulares, preferencialmente, no site da empresa. O Aviso precisa descrever como é realizado o tratamento de dados, em conformidade com o art. 9º da LGPD e deverá classificar quais os tipos de dados pessoais são tratados, ter a identificação do controlador, finalidades específicas, bases legais, formas de armazenamento e compartilhamento de dados, direitos dos titulares e meios de comunicação com o Encarregado para atendimento de dúvidas e possíveis requisições.

Além disso, o titular precisa ter livre acesso aos seus dados, ou seja, é necessário que exista algum instrumento capaz de possibilitar o acompanhamento das informações que estão sendo utilizadas pela Speedio, a fim de que o titular tenha controle das suas informações pessoais e possa solicitar, quando necessário, correções e atualizações na base de dados, garantindo a qualidade dos dados.

São recomendadas as soluções da One Trust para exercício de direitos dos titulares.

6. Bases Legais

Inicialmente, vale destacar que a base legal diz respeito somente ao processo de tratamento de dados pessoais que ocorre desde a coleta dos dados de plataformas, estruturação e disponibilização para terceiros (clientes da Speedio). Para contatos e outros tipos de tratamentos que podem ser realizados pelos clientes, a base legal deverá ser definida por eles.

Embora o art. 7º, § 4º da LGPD dispense a necessidade de solicitar o consentimento para coleta de dados manifestamente públicos pelos titulares, não significa que o tratamento dessa categoria de dado possa ser realizado sem respaldo e sem garantias aos titulares, mesmo com a dispensa do consentimento, se faz necessário o enquadramento em uma das hipóteses previstas no art. 7º da LGPD.

O *Article 29,* em seu parecer sobre conceito de interesses legítimos do responsável pelo tratamento dos dados, enfatiza que:

> Não é correto concluir, por exemplo, que o facto de alguém ter manifestamente tornado públicas certas categorias específicas de dados nos termos do artigo 8.o, n.o 2, alínea e), é – sempre e por si só – condição suficiente para permitir qualquer tipo de tratamento de dados, sem uma avaliação do equilíbrio entre os interesses e os direitos em jogo, tal como exigido no artigo 7.o, alínea f).

Diante disso, a base legal que melhor se encaixa na finalidade e no contexto do tratamento é o legítimo interesse do Controlador, visto que os dados são coletados para integrarem uma base de informações de contato corporativo e

disponibilizadas aos clientes da Speedio, a fim de que possam prospectar ativamente novos clientes nos seus respectivos negócios.

A situação descrita enquadra-se na prática de Outbound Marketing, trata-se de um processo de prospecção ativa a potenciais clientes e os benefícios do tratamento estão diretamente relacionados a promoção das atividades da empresa na divulgação de seus serviços e produtos. Assim, é imprescindível a adoção do *LIA – Legitimate Interests Asssessment* (Avaliação de Legítimo Interesse) a fim de que seja balanceado os interesses legítimos da organização e dos titulares que estão sujeitos ao tratamento.

7. Direitos dos titulares

Os direitos do titular de dados pessoais estão previstos em dois pontos da LGPD: art. 9° (obrigação de informação antes da coleta dos dados) e art. 18 (obrigação de informação mediante requerimento do titular de dados pessoais).

O dever de informação com base no art. 9° deve estar consubstanciado no Aviso de Privacidade, conforme já exposto. Os direitos previstos no art. 18 são exercidos mediante requisição ao Encarregado de Dados, os dados de identificação do responsável estarão evidentes no Aviso de Privacidade a fim de facilitar a comunicação.

Devido a disponibilização de dados corporativos e das constantes atualizações na base de dados que consolida as informações, é fundamental que seja desenvolvido um mecanismo capaz de excluir efetivamente os dados quando o titular fizer o pedido de exclusão. Recomenda-se a geração de um registro interno das solicitações para questões de controle e prestação de contas da Speedio, tendo em vista que a Speedio apenas coleta os dados e realiza a estruturação. A utilização para contatos ou outras finalidades é feita por parte das empresas-clientes que também possuem acesso aos dados e devem ser responsáveis por estabelecerem controles para o exercício de direitos dos titulares.

É válido mencionar que nem sempre as requisições dos titulares poderão ser atendidas, mas, caberá ao Encarregado responder as solicitações dos titulares demonstrando as justificativas em caso de não atendimento das demandas em um prazo razoável de atendimento. Os setores, em conjunto, avaliarão o requerimento e prosseguirão com a resposta ao titular ou então buscarão auxílio jurídico.

8. Definição dos agentes de tratamento

De acordo com o art. 5º, inc. VI e VII da LGPD, o controlador é a pessoa jurídica ou física que toma as decisões sobre o tratamento e define as finalidades e os meios

do tratamento, enquanto o operador é o agente de tratamento responsável por tratar os dados em benefício do Controlador e de acordo com as instruções fornecidas por ele.

No caso concreto, a Speedio é considerada Controladora exclusivamente para o processo de coleta dos dados através de *scraping*, a estruturação da base de dados relativos às empresas que os titulares representam e a disponibilização de acesso à essas informações em um dashboard próprio com limitações de acesso conforme o tipo de serviço contratado.

São as empresas contratantes dos serviços da Speedio que detém o poder de usar a base de dados da maneira como acharem melhor, inclusive, definindo quem serão os titulares de dados a partir da definição do perfil ideal de clientes para a empresa, aplicando filtros para localizar determinados perfis de consumo na plataforma, além de decidir quais meios serão utilizados para prospectar seus clientes, por exemplo, por e-mail, telefone ou outro mecanismo de comunicação. A Speedio não participa do processo de prospecção ativa, se limitando apenas ao fornecimento dos dados devido a prestação de serviços.

O Guia Orientativo sobre Agentes de Tratamento da ANPD[3] elucida que o Controlador sempre irá determinar os aspectos essenciais do tratamento, o que inclui a definição da finalidade para realizar o tratamento e a base legal que justifica o uso dos dados.

Assim, as organizações que usam a base de dados da Speedio devem estabelecer quais dados corporativos serão usados e quais são as finalidades do tratamento, de acordo os critérios para prospecção de clientes e promoção de suas atividades comerciais. A Speedio não possui controle sobre a maneira como os dados serão utilizados por seus clientes, apenas fica encarregada de buscar fontes de dados corporativos atualizadas e consolidar em um banco de dados como fornecimento de seus serviços.

[3] O terceiro ponto a ser considerado diz respeito à definição dos elementos decisórios que se caracterizam como "principais" ou "essenciais" e que, por isso, devem permanecer sob o domínio do controlador. Dentre esses elementos decisórios principais, destaca-se a definição da finalidade do tratamento, que será sempre estabelecida pelo controlador, a quem compete, em conformidade com as disposições da LGPD, estipular os objetivos que justificam a realização do tratamento, bem como a sua respectiva base legal. Considere os seguintes exemplos de decisões do controlador, segundo a finalidade do tratamento: utilização de dados pessoais para o pagamento de empregados, a realização de uma pesquisa com clientes, a promoção de uma campanha de marketing, o armazenamento seguro de informações ou a emissão de passagens aéreas. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

Ainda, a ICO, Autoridade de Proteção de Dados do Reino Unido[4], emitiu orientações sobre utilização de dados pessoais no contexto de marketing B2B e enfatiza que se o agente utiliza dados de acesso público para suas próprias finalidades, será considerado como Controlador de Dados e, consequentemente, estará responsável pela adequação as normas de proteção de dados.

> If you use **publicly available personal data for your own purposes, you are a controller** and take on full responsibility for compliance with data protection legislation for that personal data.

Ademais, a Speedio conta com o apoio de parceiros de negócios, que são empresas responsáveis pela coleta dos dados de acesso público na Internet e que repassam as informações a fim de que a Speedio faça a avaliação e inclua em sua base de dados. Para essa relação, considera-se que as empresas que fornecem os dados são operadores, agindo em nome da Speedio, mas devendo observar as diretrizes de coleta.

Por fim, ressalta-se que a configuração dos agentes de tratamento deve ser analisada de acordo com a realidade fática e não apenas com parâmetros legais, conforme elucidado pela autoridade:

> A identificação do controlador deve partir do conceito legal e dos parâmetros auxiliares indicados neste Guia, sempre considerando o contexto fático e as circunstâncias relevantes do caso. O papel de controlador pode decorrer expressamente de obrigações estipuladas em instrumentos legais e regulamentares ou em contrato firmado entre as partes. Não obstante, a efetiva atividade desempenhada por uma organização pode se distanciar do que estabelecem as disposições jurídicas formais, razão pela qual é de suma importância avaliar se o suposto controlador é, de fato, o responsável pelas principais decisões relativas ao tratamento.

Resumo da definição dos agentes de tratamento envolvidos:

a) **Controladores (Singulares):** clientes da Speedio e Speedio,
b) **Operador:** empresas que fornecem serviços técnicos de *scraping*

OOO Não Aplicável OOO Insatisfatório OOO Planejar Melhoria OOO Aceitável

Controles para cumprimento dos princípios	Avaliação
Finalidade: propósitos legítimos, específicos, explícitos e informados	OOO

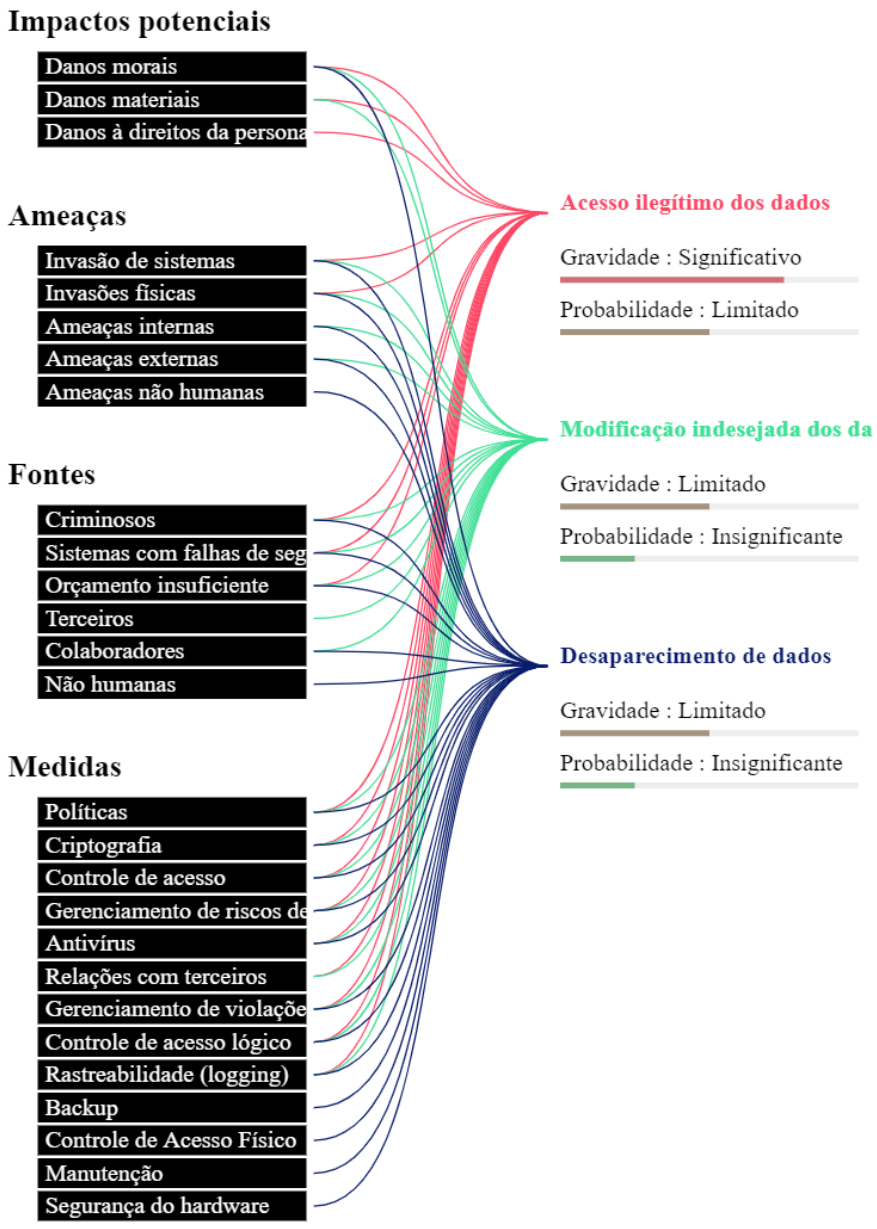
[4] Disponível em: https://ico.org.uk/for-organisations/direct-marketing/business-to-business-marketing/

Base legal: legalidade do processamento, proibição de uso indevido	OOO
Necessidade: adequada, relevante e limitada	OOO
Qualidade dos dados: precisos e atualizados	OOO
Duração do armazenamento: limitada	OOO
Informações para os titulares de dados (transparência)	OOO
Obtenção de consentimento	OOO
Exercer o direito de acesso e direito à portabilidade de dados	OOO
Exercendo os direitos de retificação e eliminação	OOO
Exercer direito de oposição (opt-out)	OOO
Agentes de tratamento: identificados e regidos por um contrato	OOO

9. Riscos

9.1. Elementos e natureza de riscos

Os riscos avaliados são classificados com base no tipo de impacto ao dado pessoal, sendo eles: a quebra da confidencialidade através do acesso ilegítimo, quebra da integridade através da modificação indesejada, ou falta de disponibilidade através do desaparecimento dos dados.



9.2. Descrição dos impactos

O conceito de impacto está relacionado ao resultado decorrente da verificação de um determinado evento de segurança, evento este que gera consequências direta e indiretas, vejamos:

Tipo	Definição
Danos morais	É o conjunto de ações que podem causar danos morais ou mentais ao interessado, como depressão, fobias, assédio, etc. A natureza é de tal ordem que o titular sofre constrangimentos, seja de ordem privada, seja de ordem pública, mas restritos à esfera moral. Exemplos: crises de ansiedade, abalos psicológicos, sensação de invasão de privacidade, etc.
Danos materiais	É o conjunto de ações que podem causar prejuízos econômicos, patrimoniais, empregatícios, etc. O titular sofrerá danos de valor pecuniário, possíveis de serem comprovados e mensurados objetivamente. Exemplos: fraudes, roubos de identidade e extorsão.
Danos à direitos da personalidade	Os impactos na vida do titular são gravíssimos, afetando sua liberdade, dignidade, privacidade, entre outros direitos da personalidade.

9.3. Descrição das ameaças

Considera-se como ameaças os meios pelos quais os riscos se concretizam, é a causa potencial de um evento indesejado, que pode resultar em dano para um sistema, organização e indivíduos.

Tipo	Descrição
Invasão de sistemas	As invasões são propositais e normalmente por criminosos buscando vulnerabilidades para serem exploradas. Exemplo: ransomware através de phishing.
Invasões físicas	Criminosos que invadem espaços físicos para subtrair equipamentos/arquivos físicos na infraestrutura que armazena a base de dados.
Ameaças externas	As ameaças externas referem-se a acessos no sistema realizados por pessoas fora da organização. Por exemplo: uma empresa terceirizada autorizada, utilizando seu acesso privilegiado a informações acessadas ilegitimamente.
Ameaças internas	As ameaças internas referem-se a ações de colaboradores internos da empresa que podem ocasionar em um evento indesejado, como colaboradores negligentes que realizam procedimentos de maneira

	errônea e concretizam riscos. Exemplo: colaborador inadvertidamente apaga ou modifica os dados que devem ser armazenados na base de dados.
Ameaças não humanas	Na hipótese de ocorrer algum incêndio, explosão, inundação que consiga atingir e comprometer a infraestrutura física e todas as informações pessoais contidas no equipamento ou na base de dados.

9.4. Descrição das medidas de mitigação

As medidas indicadas abaixo têm como objetivo evitar ou reduzir que as situações de riscos em relação aos dados biométricos se concretizem.

Tipo	Descrição
Políticas	Criação de Políticas de Segurança de Informação bem como Política de Privacidade que define os procedimentos necessários para garantir a segurança e a proteção dos dados pessoais. Vide 210407 - Política de Privacidade.
Criptografia	Conjunto de técnicas desenvolvidas para proteger as informações de modo que apenas o emissor e receptor consigam compreendê-las. Hoje toda comunicação cliente-servidor é criptografada (SSL) e o acesso se dá somente por certificados individuais (RSA Key). Toda nossa comunicação servidor-servidor é também criptografada, seja ela SSH ou HTTPS. O acesso se dá somente por certificados individuais (RSA Key), não permitimos o acesso a servidores somente com senha e login. Utilizamos ferramentas específicas para esse gerenciamento do processo formal de registro, cancelamento e atribuição de direitos de acesso aos nossos ambientes
Controle de acesso	É a garantia de que apenas os indivíduos autorizados tenham acesso aos recursos necessários. O acesso lógico, o controle do acesso físico e o uso da informação da empresa devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao cargo ou função.
Gerenciamento de riscos de privacidade	Elaboração de procedimentos para os processos de Gerenciamento de Incidente e do Grupo de Resposta a Incidente de Segurança, sempre atentando-se para a necessidade de comunicação a órgãos reguladores específicos por conta de obrigações específicas e as orientações/informações pontuais. A Política de Privacidade pode estabelecer os requisitos mínimos relativos a incidentes de segurança dos dados pessoais. Atualmente, nosso protocolo exige que caso ocorra algum incidente ou suspeita de incidente, cada líder do time técnico da empresa se reúna juntamente com o CEO para decidir a solução a ser produzida. Atualmente esse comitê é formado por 4 pessoas.

Gerenciamento de violações de dados pessoais	Elaboração de Política de Segurança da Informação e Política de Privacidade que possuam diretrizes para a gestão de incidentes de segurança da informação.
Backup	Os equipamentos onde dados e informações são coletados/gerados devem estar conectados a sistemas com suporte para backup, a base que armazena os dados pode incluir backups periódicos, exemplo: backups diários de modificações e semanal completo. Somos extremamente rigorosos nos nossos backups, trabalhamos com 3 redundâncias, variando o provedor, a localidade física e formato do backup. A maioria dos backups são realizados diariamente, alguns a cada 2 horas, e outros a cada 3 dias, isso varia de acordo com a frequência de atualizações nos bancos de dados.
Controle de acesso lógico	Métodos para definir e atribuir perfis de usuários, meios de autenticação implementados, como: as regras aplicáveis às senhas (duração mínima, caracteres necessários, duração da validade, número de tentativas falhadas antes que o acesso à conta seja bloqueado, etc.). Orientamos os colaboradores a não anotarem nenhuma senha de qualquer acesso a qualquer sistema em qualquer ambiente, meio ou software que não seja seguro. As senhas devem ser guardadas em meios que exijam autenticação e que sejam criptografados (orientamos os colaboradores e prestadores de serviço em como fazer). Além disso orientamos que as senhas sejam trocadas a cada 6 meses por uma combinação de letras, números e caracteres especiais e que seja diferente de qualquer utilizada anteriormente.
Relações com terceiros	Todos os acessos à bases de dados da empresa por outras empresas e clientes devem possuir contratos que estipulem as responsabilidades de terceiros no tratamento de dados pessoais. A depender da sensibilidade do serviço que contratamos exigimos NDA e cláusulas específicas de responsabilidade sob o nosso dado.
Rastreabilidade (logging)	Os sistemas devem possuir suporte para logs de monitoramento, a fim de registrar todas as atividades realizadas neles e identificar a origem dos registros. Hoje trabalhamos com 3 níveis de registro de logs: temos um serviço de terceiro que captura qualquer anomalia, bug ou problema no nível de aplicação. Utilizamos também uma ferramenta para leitura constante dos principais logs em buscas de padrões, comportamentos e comandos de anomalia, bug ou problema. Além disso mantemos os logs de acesso aos servidores e banco de dados com ações, registros de data e hora e usuário originador.
Antivírus	Possuir licença de sistemas antimalware que realizem atualizações automáticas.
Controle de Acesso Físico	Elaboração de políticas para garantir a segurança física da infraestrutura.
Manutenção	Elaboração de políticas que descrevam como a manutenção física do hardware é gerida.
Segurança do hardware	Controles relacionados à segurança física da infraestrutura, como exemplo: áreas com equipamentos que são essenciais para o

	funcionamento dos serviços prestados serão acessadas somente mediante chave dos que possuem o direito de acesso.

10. Danos à atributos da informação

10.1. Acesso ilegítimo aos dados (confidencialidade)

10.1.1. Possíveis impactos ao titular de dados pessoais

O acesso ilegítimo aos dados pessoais pode gerar desde sofrimentos limitados na ordem moral até constrangimentos à sua personalidade, quando utilizados por criminosos, por exemplo. Eles também podem gerar danos de ordem material pois podem causar impactos pecuniários aos titulares.

10.1.2. Ameaças principais

- **Invasão de sistemas:** as invasões são propositais e normalmente por criminosos buscando vulnerabilidades para serem exploradas, por exemplo: criminosos que conseguem acessar o sistema que armazena a base de dados.
- **Invasões físicas:** criminosos que invadem espaços físicos para subtrair equipamentos/arquivos físicos na infraestrutura que processa a base de dados.

10.1.3. Fontes de risco

- Criminosos
- Sistemas com falhas de segurança
- Orçamento insuficiente

10.1.4. Controles para mitigação de riscos

- **Políticas:** Criação de Políticas de Segurança de Informação bem como Política de Privacidade que define os procedimentos necessários para garantir a segurança e a proteção dos dados pessoais.

- **Criptografia:** Conjunto de técnicas desenvolvidas para proteger as informações de modo que apenas o emissor e receptor consigam compreendê-las.

- **Controle de acesso:** É a garantia de que apenas os indivíduos autorizados tenham acesso aos recursos necessários. O acesso lógico, o controle do acesso físico e o uso da informação da empresa devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao cargo ou função.

- **Gerenciamento de riscos de privacidade:** Elaboração de procedimentos para os processos de Gerenciamento de Incidente e do Grupo de Resposta a Incidente de Segurança, sempre atentando-se para a necessidade de comunicação a órgãos reguladores específicos por conta de obrigações específicas e as orientações/informações pontuais. A Política de Privacidade pode estabelecer os requisitos mínimos relativos a incidentes de segurança dos dados pessoais.

- **Antivírus:** Possuir licença de sistemas antimalware que realizem atualizações automáticas.

- **Relações com terceiros:** Todos os acessos à bases de dados da empresa por outras empresas devem possuir contratos que estipulem as responsabilidades de terceiros no tratamento de dados pessoais.

- **Gerenciamento de violações de dados pessoais:** Elaboração de Política de Segurança da Informação e Política de Privacidade que possuam diretrizes para a gestão de incidentes de segurança da informação.

- **Controle de acesso lógico:** Métodos para definir e atribuir perfis de usuários, meios de autenticação implementados, como: as regras aplicáveis às senhas (duração mínima, caracteres necessários, duração da validade, número de tentativas falhadas antes que o acesso à conta seja bloqueado, etc.).

- **Rastreabilidade (logging):** Os sistemas devem possuir suporte para logs de monitoramento, a fim de registrar todas as atividades realizadas neles e identificar a origem dos registros.

10.1.5. Gravidade de danos ao titular

SIGNIFICATIVO

Em casos de acesso ilegítimo aos dados pessoais a gravidade do dano será considerada significativa, uma vez que os dados de acesso público dos titulares, por mais que estejam disponíveis abertamente, são agregados com dados de várias origens e podem gerar inferências que ultrapassem a expectativa razoável dos titulares para tratamento destinados ao marketing.

A Constituição Federal assegura a todos que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, garantido o direito a indenização pelo dano material ou moral decorrente de sua violação. Nos casos de acesso ilegítimo, os titulares podem sofrer danos relacionados a sentimentos de ansiedade, desconforto e prejuízos, se houver tentativas de chantagem, roubo de identidade ou fraude.

Entretanto, pelo fato de o tratamento de dados pessoais ser limitado e ter sido classificado como dados comuns relativos a nome, e-mail, telefone e cargo, não representam um alto risco aos titulares, como nos casos de dados sensíveis, os quais podem gerar discriminações. Com isso, diminui-se a probabilidade de gerar impactos significativos aos titulares.

A fim de assegurar que os dados sejam devidamente protegidos, medidas precisam ser tomadas, a Speedio já vem adotando alguns controles, como a criptografia e o controle de acesso da base de dados para garantir a confidencialidade das informações.

10.1.6. Probabilidade de risco

LIMITADO

A probabilidade do risco é limitada, uma vez que a Speedio já adota medidas de mitigação no nível de políticas, sistemas e controles para evitar acessos indevidos, independentemente da fonte do risco. Contudo, é importante o monitoramento constante dos mecanismos de segurança empregados na operação para assegurar que estão em pleno funcionamento devido a tentativas de acesso não autorizado dos dados.

10.2. Modificação de dados (integridade)

10.2.1. Possíveis impactos ao titular de dados pessoais

- **Danos morais:** A natureza é de tal ordem que o titular sofre constrangimentos, seja de ordem privada, seja de ordem pública, mas restritos à esfera moral. Exemplos: crises de ansiedade, abalos psicológicos, sensação de invasão de privacidade, etc.
- **Danos materiais:** O titular sofrerá danos de valor pecuniário, possíveis de serem comprovados e mensurados objetivamente. Exemplos: fraudes, roubos e extorsão.

10.2.2. Ameaças principais

- **Invasão de sistemas:** as invasões são propositais e normalmente por criminosos buscando vulnerabilidades para serem exploradas, como exemplo: vulnerabilidades em sistemas e ransomware.
- **Invasões físicas:** criminosos que invadem espaços físicos para subtrair equipamentos/arquivos físicos na infraestrutura que armazena a base de dados.
- **Ameaças internas:** as ameaças internas referem-se a ações de colaboradores internos da empresa fornecedora que podem ocasionar em um evento indesejado, como colaboradores negligentes que realizam procedimentos de maneira errônea e concretizam riscos.

Exemplo: colaborador inadvertidamente apaga ou modifica os dados que devem ser armazenados na base de dados de cadastros.

- **Ameaças externas:** as ameaças externas referem-se a acessos no sistema de monitoramento realizados por pessoas fora da organização. Por exemplo: uma empresa terceirizada autorizada, utilizando seu acesso privilegiado a informações acessadas ilegitimamente.

10.2.3. Fontes de risco

- Criminosos
- Terceiros
- Colaboradores
- Sistemas com falhas de segurança
- Orçamento insuficiente

10.2.4. Controles para mitigação de riscos

- **Políticas:** Criação de Políticas de Segurança de Informação bem como Política de Privacidade que define os procedimentos necessários para garantir a segurança e a proteção dos dados pessoais.
- **Criptografia:** Conjunto de técnicas desenvolvidas para proteger as informações de modo que apenas o emissor e receptor consigam compreendê-las.
- **Controle de acesso:** É a garantia de que apenas os indivíduos autorizados tenham acesso aos recursos necessários. O acesso lógico, o controle do acesso físico e o uso da informação da empresa devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao cargo ou função.
- **Gerenciamento de riscos de privacidade:** Elaboração de procedimentos para os processos de Gerenciamento de Incidente e do Grupo de Resposta a Incidente de Segurança, sempre atentando-se para a necessidade de comunicação a órgãos reguladores específicos por conta de obrigações específicas e as orientações/informações pontuais. A Política de Privacidade pode estabelecer os requisitos mínimos relativos a incidentes de segurança dos dados pessoais.

- **Antivírus:** Possuir licença de sistemas antimalware que realizem atualizações automáticas.
- **Relações com terceiros:** Todos os acessos à bases de dados da empresa por outras empresas devem possuir contratos que estipulem as responsabilidades de terceiros no tratamento de dados pessoais.
- **Gerenciamento de violações de dados pessoais:** Elaboração de Política de Segurança da Informação e Política de Privacidade que possuam diretrizes para a gestão de incidentes de segurança da informação.
- **Controle de acesso lógico:** Métodos para definir e atribuir perfis de usuários, meios de autenticação implementados, como: as regras aplicáveis às senhas (duração mínima, caracteres necessários, duração da validade, número de tentativas falhadas antes que o acesso à conta seja bloqueado, etc.).
- **Rastreabilidade (logging):** Os sistemas devem possuir suporte para logs de monitoramento, a fim de registrar todas as atividades realizadas neles e identificar a origem dos registros.

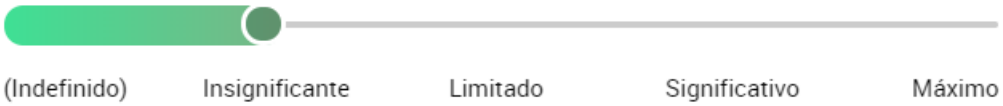
10.2.5. Gravidade de danos ao titular

LIMITADO

Na hipótese de modificação de dados, há riscos em relação aos dados que são disponibilizados na base de dados da Speedio, os quais podem afetar os clientes que usam os dados na prospecção ativa e venda de seus serviços e produtos. Sendo assim, os impactos atingiriam tanto as empresas que usam a base de dados, pois teriam dificuldades de prospectar os clientes ideais, quanto os próprios titulares, tendo em vista a violação de privacidade que pode gerar danos morais, como sensação de invasão de privacidade baseada em inferências e dados que não correspondem à realidade.

Para mitigar tais riscos, é importante o backup periódico das bases que armazenam os dados corporativos, medida que já vem sendo adotada pela empresa, diminuindo-se consideravelmente a probabilidade do risco.

10.2.6. Probabilidade de risco



INSIGNIFICANTE

A empresa já vem implementando medidas de segurança para evitar a ocorrência de eventos indesejados, tais como: medidas de mitigação no nível de políticas e controles de acessos.

Para mitigar tais riscos, é importante o backup periódico das bases que armazenam os dados corporativos, medida que já vem sendo adotada pela empresa, diminuindo-se consideravelmente a probabilidade do risco. A Speedio argumenta que é extremamente rigorosa nos nossos backups, trabalhando com 3 redundâncias, variando o provedor, a localidade física e formato do backup. A maioria dos backups são realizados diariamente, alguns a cada 2 horas, e outros a cada 3 dias, isso varia de acordo com a frequência de atualizações nos bancos de dados.

10.3. Desaparecimento de dados (disponibilidade)

10.3.1. Possíveis impactos ao titular de dados pessoais

- **Danos morais:** A natureza é de tal ordem que o titular sofre constrangimentos, seja de ordem privada, seja de ordem pública, mas restritos à esfera moral. Exemplos: crises de ansiedade, abalos psicológicos, sensação de invasão de privacidade, etc.

10.3.2. Ameaças principais

- **Invasão de sistemas:** as invasões são propositais e normalmente por criminosos buscando vulnerabilidades para serem exploradas, como exemplo: vulnerabilidades em sistemas e ransomware.
- **Invasões físicas:** criminosos que invadem espaços físicos para subtrair equipamentos/arquivos físicos na infraestrutura que armazena a base de dados.
- **Ameaças internas:** as ameaças internas referem-se a ações de colaboradores internos da empresa que podem ocasionar em um evento indesejado, como colaboradores negligentes que realizam

procedimentos de maneira errônea e concretizam riscos. Exemplo: colaborador inadvertidamente apaga ou modifica os dados que devem ser armazenados na base de dados de cadastros.

- **Ameaças externas:** as ameaças externas referem-se a acessos no sistema de monitoramento realizados por pessoas fora da organização. Por exemplo: uma empresa terceirizada autorizada, utilizando seu acesso privilegiado a informações acessadas ilegitimamente.
- **Ameaças não humanas:** na hipótese de ocorrer algum incêndio, explosão, inundação que consiga atingir e comprometer a infraestrutura física e todas as informações pessoais contidas no equipamento ou na base de dados.

10.3.3. Fontes de risco

- Criminosos
- Funcionários
- Sistemas com falhas de segurança
- Orçamento insuficiente
- Não humanas (desastres naturais)

10.3.4. Controles para mitigação de riscos

- **Políticas:** Criação de Políticas de Segurança de Informação bem como Política de Privacidade que define os procedimentos necessários para garantir a segurança e a proteção dos dados pessoais.
- **Controle de acesso:** É a garantia de que apenas os indivíduos autorizados tenham acesso aos recursos necessários. O acesso lógico, o controle do acesso físico e o uso da informação da empresa devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao cargo ou função.
- **Gerenciamento de riscos de privacidade:** Elaboração de procedimentos para os processos de Gerenciamento de Incidente e do Grupo de Resposta a Incidente de Segurança, sempre atentando-se para a necessidade de comunicação a órgãos reguladores específicos por conta de obrigações específicas e as orientações/informações pontuais. A Política de Privacidade pode estabelecer os requisitos mínimos relativos a incidentes de segurança dos dados pessoais.

- **Antivírus:** Possuir licença de sistemas antimalware que realizem atualizações automáticas.
- **Relações com terceiros:** Todos os acessos à bases de dados da empresa por outras empresas devem possuir contratos que estipulem as responsabilidades de terceiros no tratamento de dados pessoais.
- **Gerenciamento de violações de dados pessoais:** Elaboração de Política de Segurança da Informação e Política de Privacidade que possuam diretrizes para a gestão de incidentes de segurança da informação.
- **Controle de acesso lógico:** Métodos para definir e atribuir perfis de usuários, meios de autenticação implementados, como: as regras aplicáveis às senhas (duração mínima, caracteres necessários, duração da validade, número de tentativas falhadas antes que o acesso à conta seja bloqueado, etc.).
- **Rastreabilidade (logging):** Os sistemas devem possuir suporte para logs de monitoramento, a fim de registrar todas as atividades realizadas neles e identificar a origem dos registros.
- **Controle de Acesso Físico:** Elaboração de políticas para garantir a segurança física da infraestrutura.
- **Manutenção:** elaboração de políticas que descrevam como a manutenção física do hardware é gerida.
- **Segurança do hardware:** Controles relacionados à segurança física da infraestrutura, como exemplo: áreas com equipamentos que são essenciais para o funcionamento dos serviços prestados serão acessadas somente mediante chave dos que possuem o direito de acesso.

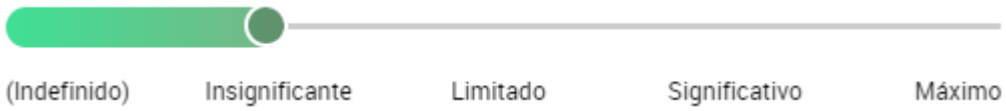
10.3.5. Gravidade de danos ao titular

LIMITADO

Os riscos em caso de desaparecimento dos dados serão limitados, visto que os dados são somente utilizados para contato com os titulares, o desaparecimento de dados impactaria as empresas que acessam a base de dados visto que encontrariam dificuldades em prospectar seus clientes e há impactos na esfera moral aos titulares que incluem sensação de perda de controle de seus dados.

Dentre as medidas de segurança aptas a evitar a ocorrência de desaparecimento dos dados, destaca-se a realização periódica dos backups a fim de evitar maiores prejuízos.

10.3.6. Probabilidade de risco

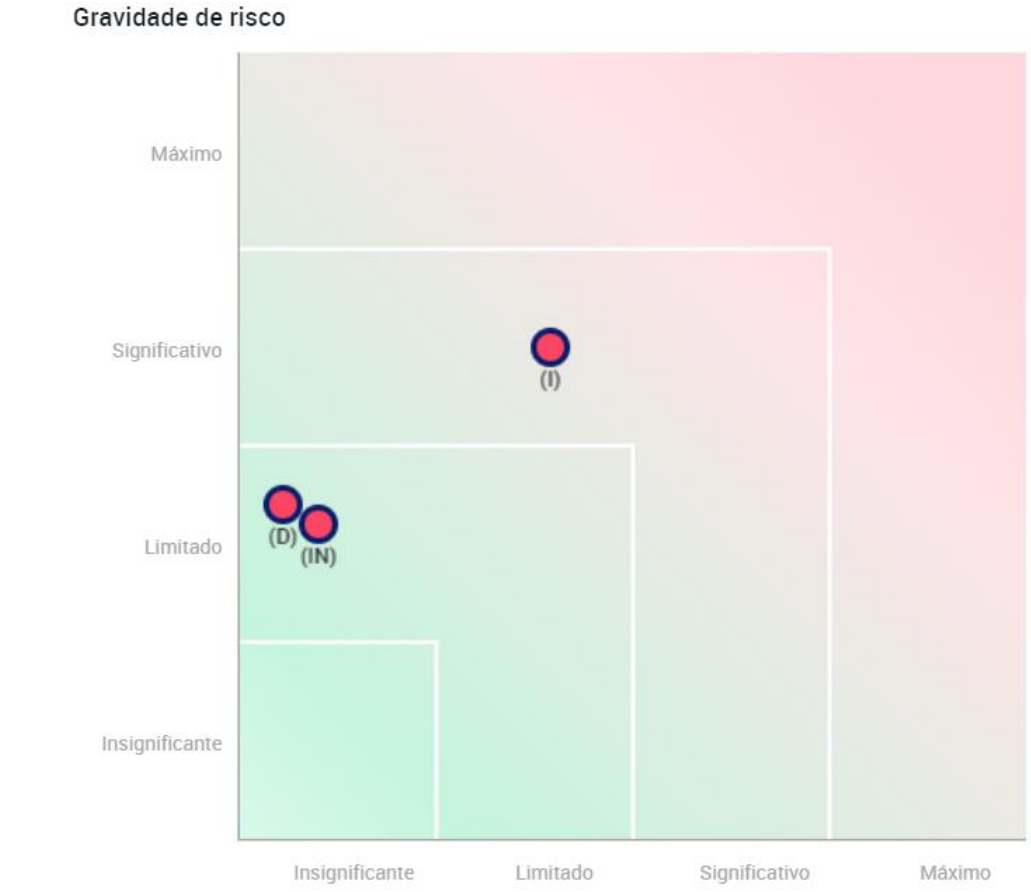


INSIGNIFICANTE

A empresa já vem implementando medidas de segurança para evitar a ocorrência de eventos indesejados, tais como: medidas de mitigação no nível de políticas e controles de acessos.

Para mitigar tais riscos, é importante o backup periódico das bases que armazenam os dados corporativos, medida que já vem sendo adotada pela empresa, diminuindo-se consideravelmente a probabilidade do risco. A Speedio argumenta que é extremamente rigorosa nos nossos backups, trabalhando com 3 redundâncias, variando o provedor, a localidade física e formato do backup. A maioria dos backups são realizados diariamente, alguns a cada 2 horas, e outros a cada 3 dias, isso varia de acordo com a frequência de atualizações nos bancos de dados.

11. Visão Geral



- Medidas existentes ou planeadas
- Com as medidas corretivas implementadas
- Acesso (i)legítimo aos dados
- Modificação (in)desejada dos dados
- Desaparecimento dos dados

05/12/2022

12. Resumo

Diante das análises, são sugeridas as seguintes medidas:

Observação	Medidas recomendadas
Empresas que prestam serviços de *scraping* devem estar limitadas à coleta de dados de indivíduos no contexto corporativo e garantir a observância dos Termos de Usos das plataformas.	Aditivos contratuais com as respectivas previsões.
Os clientes da Speedio são Controladoras para os usos dos dados que possuem acesso, devendo assumir as respectivas obrigações dessa espécie de agente de tratamento.	Inserção de cláusulas relativas à relação entre Controladores no contrato padrão da Speedio.
Transparência facilitada para os titulares.	Criação de um "Portal da Privacidade" nos moldes das empresas que foram objeto de *benchmark.*
Possiblidade facilitada de eliminação de dados pessoais com mecanismos que impeçam a reinserção do mesmo dado.	Adoção de sistema automatizado nos moldes das empresas que foram objeto de *benchmark*.

13. Conclusão

A Speedio utiliza os dados de acesso público em detrimento dos seus serviços comerciais relacionados a disponibilização de dados corporativos, a fim de que as empresas que contratem os serviços possam realizar marketing outbound e prospectar clientes ativamente, de acordo com o perfil que se encaixa melhor com a empresa.

Vale ressaltar que o uso de dados disponíveis publicamente deve estar compatível com as finalidades originárias que geraram a disponibilização pública dos dados. Dessa forma, é importante avaliar a expectativa razoável do titular em relação ao tratamento, a fim de evitar danos a privacidade e proteção de dados.

No presente caso, a Speedio é considerada Controladora para o processo de coleta de dados pessoais, estruturação de perfis corporativos e disponibilização para clientes conforme o tipo de serviço contratado. Sendo assim, cabe aos usuários da base de dados da Speedio, clientes da empresa, como Controladores, ao estabelecer outras finalidades, indicar as respectivas bases legais e demais garantias relacionadas a proteção de dados.

Ademais, considerando-se que a Speedio possui parceiros de negócio que realizam *scraping* de dados públicos, é imprescindível que sejam estabelecidas contratualmente as respectivas responsabilidades no tratamento de dados pessoais, recomenda-se, também, a realização de auditoria nos fornecedores de dados de acesso público para avaliação da conformidade com a LGPD.

Cabe ressaltar que é necessário que transparência aos titulares e a possibilidade de exercerem seus direitos, como o direito de exclusão dos dados e o direito de acesso a informações, visto que o tratamento de dados pode não ser esperado pelos titulares. Além disso, se faz necessário adotar medidas de mitigação que visem diminuir a probabilidade da ocorrência do dano, garantindo a possibilidade da utilização dos dados pessoais.

Ademais, existem riscos relativos aos Termos de Uso das plataformas em que os dados são coletados através de sistemas de *scraping*. Algumas das empresas e instituições que disponibilizam dados abertos ou tornados públicos pelos titulares proíbem essas práticas perante direitos de propriedade industrial e intelectual, gerando riscos de ordem comercial. Assim, as empresas responsáveis por fornecer os sistemas de *scraping* devem estar contratualmente obrigadas à Speedio de verificar a relação com essas plataformas.

Ainda, é fundamental realizar o acompanhamento frequente em relação as medidas de conformidade legal e mitigação de riscos que as empresas fornecedoras de dados adotam, bem como acompanhar possíveis modificações nos processos

internos da Speedio que impactem o tratamento de dados, a fim de garantir efetivo controle sobre a segurança do tratamento dos dados pessoais.

Brasília, 06 de dezembro de 2022

Alisson Possa
Possa Consultoria LTDA