RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

Belo Horizonte, 15 de janeiro de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor
15/01/2024	1.0	Conclusão da primeira versão do relatório	Comitê Interno de Privacidade

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador	
Codemge – Companhia de Desenvolvimento de Minas Gerais; Codemig – Companhia de Desenvolvimento Econômico de Minas Gerais.	
Operador	
Empregados, colaboradores, terceirizados, fornecedores e demais parceiros de negócio com os quais a Codemge e a Codemig possuam relações jurídicas.	
Encarregado	
Patrícia Sanglard Fadlallah	
E-mail Encarregado	**Telefone Encarregado**
privacidade@codemge.com.br	(31) 3916-8100

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

A Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – passou a vigorar em setembro de 2020. Ela prevê regras para que os dados das pessoas sejam protegidos de uso indevido. Foi promulgada, portanto, para regulamentar o tratamento dessas informações e preservar os direitos fundamentais de liberdade e de privacidade, bem como a livre formação da personalidade e a dignidade de cada indivíduo.

A Lei abarca o tratamento de dados pessoais, dispostos em meio físico ou digital, por pessoa física ou jurídica de direito público ou privado. Engloba, assim, um amplo conjunto de operações que podem ocorrer em meios manuais ou eletrônicos.

Nesse contexto, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) consiste na documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, conforme conceito trazido pelo artigo

5º, inciso XVII da LGPD. Trata-se, pois, de um documento basilar para demonstrar como é feito o tratamento de dados pessoais pela Codemge, desde a forma como são coletados, tratados, usados e eventualmente compartilhados, até as medidas adotadas para mitigar riscos que possam afetar os titulares desses dados.

O conteúdo mínimo do RIPD é indicado pelo parágrafo único do artigo 38:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A própria LGPD prevê casos em que o RIPD deverá ou poderá ser solicitado:

- para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
- quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados);
- a qualquer momento sob determinação da ANPD (art. 38).

No caso da Codemge, os dois últimos pontos acima respaldam a necessidade, eminentemente preventiva, de elaboração do RIPD.

Além dos casos específicos previstos pela LGPD, é indicada a elaboração ou a atualização do Relatório sempre que houver mudanças que possam causar impacto na privacidade dos dados pessoais, resultante de:

- Novas tecnologias, serviços ou iniciativas em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
- Necessidade de rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise à formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12, § 2º);
- Tratamento de dado pessoal sobre “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 (LGPD, art. 5º, II);

- Processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);
- tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);
- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);
- tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);
- tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);
- alterações nas leis e regulamentos aplicáveis a privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.;
- reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Como os itens acima podem integrar a realidade de uma empresa pública como a Codemge, o RIPD é fundamental para assegurar a conformidade da Companhia à LGPD.

2.1 – COMITÊ INTERNO DE PRIVACIDADE

Em conformidade com a LGPD, a Companhia criou, em agosto de 2020, um Comitê Interno de Privacidade (CIP), para promover a adequação legal da Empresa. O Comitê é uma equipe multidisciplinar formada atualmente por integrantes das áreas de Auditoria, Comunicação, Gestão de Riscos, Integridade, Jurídico, Recursos Humanos e Tecnologia da Informação da Codemge.

A partir do plano de ação proposto pelo CIP, processos internos foram revistos, sistemas foram adequados, e uma Política de Privacidade foi elaborada em consonância com a LGPD e a Lei de Aceso à Informação (LAI). Essa Política disciplina o tratamento de dados pessoais de cidadãos, empregados e parceiros e está disponível no site da Codemge (codemge.com.br) e no da sua subsidiária, Codemig (codemig.com.br).

Ambos os portais contam com página específica sobre Proteção de Dados, oferecendo informações diversas sobre o assunto e canal de contato com o público. Os dois sites também exibem mensagem aos usuários acerca dos *cookies* usados – pequenos arquivos de texto que podem ser salvos no dispositivo do usuário ao visitar uma página na internet.

Em agosto de 2023, a LGPD completou cinco anos, ocasião na qual a Codemge lançou cartilha sobre o tema para os empregados. Já em outubro, a Empresa lançou a versão da cartilha para o público externo, em especial fornecedores (disponível no site codemge.com.br), contendo diretrizes relacionadas à LGPD e à proteção de dados pessoais para suas contratadas. Ambas as peças (para os públicos interno e externo) integram o escopo de ações do projeto de adequação da Codemge à Lei nº 13.709/2018.

3 – DESCRIÇÃO DO TRATAMENTO

O tratamento de dados pessoais abarca toda operação efetuada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação/controle da informação, modificação, comunicação, transferência, difusão ou extração, conforme art. 5º, X da LGPD.

O tratamento pode ocorrer apenas quando o titular ou o responsável legal consentir, de maneira específica e destacada, para finalidades determinadas, ou sem o consentimento para situações previstas no artigo 7º da Lei Geral de Proteção de Dados Pessoais.

No caso de dados pessoais sensíveis, o tratamento pode se dar somente quando o titular ou o responsável legal consentir, de maneira específica e destacada, para finalidades determinadas, ou sem o consentimento para certas situações previstas no artigo 11, inciso II, da LGPD.

O tratamento de dados pessoais pelo Poder Público deve estar sempre associado a uma finalidade pública, que seja:

- legítima, isto é, lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal, que autorize o tratamento;
- específica, de forma que a partir da finalidade seja possível delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais;
- explícita, ou seja, expressa de uma maneira clara e precisa;
- informada, isto é, disponibilizada em linguagem simples e de fácil compreensão e acesso ao titular dos dados.

Dessa forma, o tratamento de dados pessoais pelo Poder Público, incluindo a divulgação pública de dados pessoais, deve ser realizado em conformidade com as disposições da LGPD. Devem ser observadas as normas que garantem a proteção integral dos dados pessoais, a autodeterminação informativa e o respeito à privacidade dos titulares durante todo o ciclo do tratamento. Além de observar os princípios previstos na Lei e verificar a base legal aplicável ao tratamento, é preciso assegurar os direitos dos titulares e adotar medidas de prevenção e segurança, a fim de evitar a ocorrência de incidentes.

No contexto da Codemge, considerando as atividades por ela desenvolvidas, as hipóteses autorizativas do tratamento de dados pessoais mais utilizadas para o tratamento são:

- cumprimento de obrigação legal;
- legítimo interesse;
- consentimento;

- execução de contrato ou de procedimentos preliminares relacionados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral.

Já no caso das exceções para manutenção de dados pessoais após o término do tratamento, a base legal mais utilizada pela Codemge é o cumprimento de obrigação legal ou regulatória.

Cabe pontuar que, considerando a fragilidade do uso do legítimo interesse, a Codemge desenvolveu um teste de proporcionalidade para verificar a adequada utilização dessa base legal. Nesse teste, são avaliadas a legitimidade e a necessidade do uso, bem como aplicada a regra de balanceamento e verificação de atendimento às salvaguardas.

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, do escopo, do contexto e da finalidade** do tratamento. O objetivo principal é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, com subsídios para avaliação e tratamento de riscos.

3.1 – DESCRIÇÃO DO TRATAMENTO

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e finalidade** do tratamento.

A LGPD (art. 5º, X) considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

3.1.1 – HISTÓRICO

Tendo em vista a necessidade de adequação da Companhia à LGPD, a Codemge inicialmente promoveu a capacitação de um grupo multidisciplinar de empregados, composta por integrantes dos setores de tecnologia da informação, jurídico, auditoria interna, compliance e recursos humanos. A equipe participou, em junho de 2019, do "Curso de Extensão: Proteção de Dados Pessoais e Privacidade - Teoria e Prática" ministrado pelo *Data Privacy* Brasil, empresa reconhecida por difundir e inovar no conhecimento sobre privacidade e proteção de dados no país.

Em julho de 2019, foi instituído na Companhia o Comitê Interno de Privacidade, responsável por conduzir os trabalhos de adequação da Codemge à legislação de proteção de dados, cuja composição englobava os colaboradores certificados pelo *Data Privacy*, atuando como multiplicadores, juntamente com integrante da assessoria de comunicação e da gerência administrativa (Gerad).

O grupo foi responsável por estudar as exigências e os impactos da nova lei para a Companhia e propor plano de trabalho para implementação das ações necessárias. O primeiro passo consistiu na realização de reuniões personalizadas com diretorias, gerências e comissões da empresa, no intuito de conscientizar sobre a relevância da norma publicada, além de sensibilizar sobre a importância da atuação de todos para o alcance da conformidade. Além disso, foram realizados *benchmarkings* com outras estatais de renome para conhecimento do andamento dos trabalhos de adequação à LGPD nessas organizações, como: Banco de Desenvolvimento de Minas Gerais (BDMG), Companhia Energética de Minas Gerais (Cemig), Companhia de Saneamento de Minas Gerais (Copasa) e Companhia de Saneamento do Paraná (Sanepar).
Em seguida, com o subsídio de informações de todas as áreas técnicas da Companhia, foi realizado o mapeamento de dados pessoais tratados no desenvolvimento das atividades da Codemge. A partir do mapeamento, definiram-se como prioridades três braços de atuação, considerando a adequação: nos contratos (jurídico); normativos da casa, incluindo a elaboração da política de privacidade (integridade); e sistemas de informação, intranet e sites institucionais (tecnologia da informação).
Em 2020 e 2021, a Codemge passou por diversas mudanças na estrutura decisória, incluindo rearranjo integral do organograma e trocas na formação do Comitê Interno de Privacidade.

Em 30 junho de 2022, foram designados os atuais componentes do Comitê, que conta com:

- Patrícia Sanglard Fadlallah - Encarregado/*Data Protection Officer*/DPO (Gerência de Integridade, Conformidade e Gestão de Riscos – Gicor)
- Érica Rosália de Jesus Parreiras - Coordenadora (Gicor)
- Cláudia Patrocínio Veloso (Gerência de Tecnologia e Inteligência de dados – Getid)
- Denise Lobato de Almeida (Gerência de Direito Administrativo – Gedad)
- Juliana Lúcia Mascarenhas Gomes Ferreira (Auditoria Interna – Audit)
- Marcello Pereira Machado (Gerência de Comunicação – Gerco)
- Ronaldo José Madureira (Gerência de Recursos Humanos – Gerhu)
- Suellen Silva de Almeida (Gerência de Comunicação – Gerco)

A primeira ação do novo Comitê consistiu em estudar o planejamento anterior com o objetivo de identificar, dentre as atividades programadas, quais haviam sido efetivamente realizadas, quais precisavam ser executadas e quais tinham perdido aderência considerando o novo contexto. Além disso, a verificação incluiu o estudo de atividades não previstas, mas importantes para a Companhia no entendimento do grupo.

3.1.2 – AÇÕES POR SEGMENTO DE ATUAÇÃO

3.1.2.1 – EIXO JURÍDICO

No que se refere à atuação do jurídico, constatou-se a realização:

(i) Elaboração de minuta do Termo de Ciência sobre o tratamento de dados e LGPD para os empregados da Codemge o qual, em consideração à recomendação da Gerência de Direito Administrativo, por meio do Parecer Jurídico, optou-se por não levar a ação adiante;
(ii) Elaboração de minuta de aditivo dos contratos, com inclusão de Termo Aditivo com cláusulas de observância obrigatória à privacidade de dados. A redação do documento foi aprovada pela Gerência de Direito Administrativo – Gedad, por meio do Parecer Jurídico;
(iii) Encaminhamento da minuta final de aditivo a todas as Gerências da Codemge, via Comunicação Interna, para adequação dos contratos vigentes da Companhia que ainda não possuam cláusula específica de proteção de dados pessoais, no âmbito de cada Gerência. O Comitê entendeu ser mais produtivo a emissão da minuta final já aprovada a todos os contratos, com análise pontual dos contratos que demandem atuação mais específica.

3.1.2.2 – EIXO INTEGRIDADE E GESTÃO DE RISCOS

No tocante a integridade, o realizado consistiu em:

(i) Elaboração da Instrução Normativa 59 (Gestão dos Normativos Internos) e da Cartilha de orientação da criação e revisão de normativos. Aquele documento determinou a obrigatoriedade de inclusão de cláusulas relativas à observância da LGPD nas normas da Companhia e este mesmo trouxe as regras para padronização das cláusulas;
(ii) Coordenação junto às gerências e comissões/comitês da Companhia da revisão para adequação dos normativos internos da Codemge;
(iii) A Companhia possui 75 normativos internos, sendo que 73 destes estão adequados e 1 está em processo de revisão e aprovação, totalizando 97,33% dos normas da Codemge adequadas à LGPD;
(iv) Coordenação junto às gerências e comissões/comitês da Companhia da adequação dos formulários internos da Codemge;
(v) Ação concluída, com 100% dos formulários internos utilizados pelas gerências da Companhia aderentes à LGPD;
(vi) Revisão da Política de Privacidade, apresentada ao Conselho de Administração em 13/12/2022;
(vii) Consulta ao jurídico com a finalidade de subsidiar os trabalhos, envolvendo a elucidação de questões legais dúbias e sua aplicabilidade à Companhia, como, por exemplo, os limites de atendimento à Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011) frente à LGPD;
(viii) Reuniões com escritórios de advocacia referência no mercado no quesito proteção de dados para apresentação dos serviços por estes oferecidos e solicitação de orçamento para estudo da viabilidade de contratação de consultoria para o projeto de adequação da Codemge;
(ix) Promoção de palestras com a Dra. Patrícia Peck Pinheiro e o com Dr. Luiz Gustavo Miranda para fomentar a discussão sobre a LGPD e incentivar a conscientização da Empresa;

(x) Coordenação da elaboração, revisão e publicação da Instrução Normativa nº 57, Norma de Resposta a Pedidos de Titulares e Incidentes LGPD, aprovada em 23 de agosto de 2022;
(xi) Contratação de curso de capacitação em LGPD para o Comitê e outros colaboradores da Companhia, a ser ministrado pela Fundação João Pinheiro em novembro e dezembro de 2023;
(xii) Participação em eventos e fóruns de discussão com integrantes de órgãos da Administração Pública e do setor privado para realização de benchmarkings e aprimoramento das atividades de proteção de dados desenvolvidas na Codemge;
(xiii) Atuação como consultoria a outras gerências da Companhia envolvendo questionamentos quanto à adequação de procedimentos, projetos e atividades desenvolvidas na Codemge à legislação e boas práticas de proteção de dados.

3.1.2.3 – EIXO TECNOLOGIA DA INFORMAÇÃO

No braço de atuação de tecnologia da informação, verificou-se a realização:

(i) Revisão da Política de Segurança da Informação e normativas associadas e adequações para a LGPD;
(ii) Habilitação de trilhas de auditoria e geração de relatórios para consulta dos logs de acesso;
(iii) Relatório de atividades do Comitê Interno de Privacidade de 2022;
(iv) Implantação da Dupla autenticação na nuvem *Microsoft office* 365;
(v) Aquisição de *notebooks* com o recurso de criptografia;
(vi) Migração do servidor de arquivos para Prodemge;
(vii) Migração do servidor de antivírus para *DataCenter* Prodemge com interface publicada na internet;
(viii) Piloto do uso de certificado digital *web free - lestsencript;*
(ix) Piloto de login com biometria nos *notebooks* da empresa;
(x) Contratação de consultoria especializada para diagnóstico de riscos e vulnerabilidades no ambiente tecnológico da Codemge, tendo como produto final um plano de ação com medidas curto, médio e longo prazo;
(xi) Elaboração da matriz de riscos de segurança cibernética.

3.1.2.4 – EIXO COMUNICAÇÃO

Na esfera de comunicação, foram desenvolvidas diversas ações – entre as principais, estão:

(i) Manutenção de página na *Intranet* especificamente para o Comitê Interno de Privacidade, com a composição do grupo, comunicados de privacidade e informações sobre a LGPD;
(ii) Manutenção de mensagem modal nos portais institucionais (Codemge e Codemig) acerca da política de *cookies* e privacidade: Ao acessar os portais, o usuário encontra a seguinte mensagem: “Usamos *cookies* para que possamos melhorar continuamente a experiência do usuário. Ao acessar nosso site, você concorda com o termo de uso de *cookies*.” Junto à

mensagem, há dois botões: “Entendi” e “Mais informações”. Este último leva para a página “Proteção de Dados”, dentro do próprio portal;

(iii) Manutenção da página de Proteção de Dados nos portais institucionais Codemge (codemge.com.br/a-codemge/protecao-de-dados) e Codemig (codemig.com.br/a-codemge/protecao-de-dados). A página contém informações sobre a LGPD e mais de 10 (dez) perguntas e respostas acerca da temática privacidade, incluindo o que são dados pessoais, quais podem ser solicitados pela Companhia, quem é o titular de dados, o que é tratamento e anonimização de dados, qual é o papel da Autoridade Nacional de Proteção de Dados (ANPD), quais são os direitos do titular e as medidas adotadas pela Empresa para proteger os dados pessoais, além do canal de comunicação com a Codemge e da explicação sobre o que são *cookies* e quais são usados no site. O conteúdo foi elaborado pela Gerência de Integridade, Conformidade e Gestão de Riscos (Gicor), com revisão textual pela Gerência de Comunicação (Gerco);

(iv) Publicação de notas na Intranet e no site sobre assuntos relacionados, como Consulta Pública para revisão da Política de Privacidade da Codemge, nova versão desse documento, Dia Internacional da Privacidade, Dia do Arquivo;

(v) Veiculação na Intranet de série de 10 matérias denominada “LGPD e você”, sobre essa lei no contexto da Codemge;

(vi) Veiculação de postagens em redes sociais sobre temas afins, como Dia Internacional da Privacidade e Dia do Arquivo;

(vii) Criação de logomarca do Comitê Interno de Privacidade, com identidade visual para marcar as ações de divulgação do grupo;

(viii) Criação do boletim eletrônico interno PartiCIP, voltado para os empregados da Codemge, com o objetivo de disseminar conceitos, dados e reflexões sobre a importância da privacidade e da LGPD, em especial no âmbito da Companhia;

(ix) Desenvolvimento e lançamento de cartilha eletrônica especialmente desenvolvida para os empregados, intitulada “LGPD na Codemge: a Lei Geral de Proteção de Dados Pessoais e os agentes públicos”, marcando os cinco anos da LGPD, em agosto/2023;

(x) Desenvolvimento e lançamento de cartilha eletrônica sobre LGPD para o público externo, em especial fornecedores da Companhia. O material, denominado “LGPD e Codemge: A Lei Geral de Proteção de Dados Pessoais para entes públicos e privados”, está disponível na seção “Proteção de dados” do site institucional e também foi enviado pelo CIP às gerências, para que os gestores o encaminhassem às empresas contratadas de suas respectivas áreas.

4 – PARTES INTERESSADAS CONSULTADAS

O Comitê Interno de Privacidade (CIP), instituído em julho de 2019, responsável por estudar as exigências e os impactos da Lei Geral de Proteção de Dados Pessoais (LGPD) para a Companhia e propor plano de trabalho para adequação da Empresa, iniciou os trabalhos com a realização de reuniões individualizadas com diretorias, gerências e comissões da empresa, buscando conscientizar sobre a relevância da LGPD e sensibilizar sobre a importância da atuação de todos no contexto de adequação e conformidade da organização.

Em seguida, foram realizados *benchmarkings* com outras estatais de renome para conhecimento

do andamento dos trabalhos de adequação à LGPD nessas instituições, como: Banco de Desenvolvimento de Minas Gerais (BDMG), Companhia Energética de Minas Gerais (Cemig), Companhia de Saneamento de Minas Gerais (Copasa) e Companhia de Saneamento do Paraná (Sanepar).

A partir das reuniões com diretorias, gerências e comissões da empresa, o CIP elaborou um formulário para mapeamento de dados e o encaminhou a esses grupos, para que fosse realizado o levantamento dos processos, atividades, contratos, dentre outros, em que eram coletados e armazenados dados pessoais, com a finalidade de mensurar a amplitude de aplicação da Lei Geral de Proteção a Dados Pessoais dentro da Companhia. Nele, às áreas foi atribuído identificar:

- Processo (em qual contexto/ atividade/contrato da empresa o dado pessoal é coletado);
- Dados pessoais coletados;
- Finalidade da coleta;
- Tempo de guarda;
- Justificativa de guarda;
- Nome do sistema/suporte em que a informação é coletada/armazenada;
- Existência de coleta e/ou armazenamento de documentos físicos com dados pessoais, com especificação em caso positivo;
- Ocorrência de compartilhamento do dado pessoal com outros setores ou terceiros, com especificação em caso positivo;
- Destinação final dos dados pessoais.

Em seguida, com o subsídio de informações de todas as áreas técnicas da Companhia, foi realizado o mapeamento de dados pessoais tratados no desenvolvimento das atividades da Codemge. A partir do mapeamento, definiram-se como prioridades três braços de atuação, considerando a adequação: nos contratos (jurídico); normativos da casa, incluindo a elaboração da política de privacidade (integridade); e sistemas de informação, intranet e *sites* institucionais (tecnologia da informação).

No tocante à integridade, foram realizadas as seguintes ações de consulta:

(i) Consulta ao jurídico com a finalidade de subsidiar os trabalhos, envolvendo a elucidação de questões legais dúbias e sua aplicabilidade à Companhia, como, por exemplo, os limites de atendimento à Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011) frente à LGPD;

(ii) Reuniões com escritórios de advocacia referência no mercado no quesito proteção de dados para apresentação dos serviços por estes oferecidos e solicitação de orçamento para estudo da viabilidade de contratação de consultoria para o projeto de adequação da Codemge;

(iii) Promoção de palestras com a Dra. Patrícia Peck Pinheiro e o com Dr. Luiz Gustavo Miranda

para fomentar a discussão sobre a LGPD e incentivar a conscientização da Empresa.

A Codemge interagiu ainda com a sociedade em geral quando da revisão de seus normativos internos, destacando-se nesse contexto a Política de Privacidade e a Política de Segurança da Informação, tendo sido realizadas consultas públicas sobre o texto proposto, em dezembro e julho de 2022 respectivamente, antes de sua aprovação final.

Nesse sentido, durante a elaboração e execução do Plano de adequação da Codemge à legislação de proteção de dados, foram consultados os gestores e todo o corpo funcional da Companhia, integrantes de equipes de proteção de dados em estatais de renome, membros de escritórios de advocacia referência em LGPD no mercado, além da comunidade como um todo.

5 – DIRETRIZES DE TRATAMENTO DE DADOS PESSOAIS NA CODEMGE

A Codemge, no desenvolvimento de suas atividades, trata dados pessoais desde que amparada por hipóteses legais e autorizativas, considerando o disposto no artigo 7º da Lei 13.709/2018.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para **o cumprimento de obrigação legal ou regulatória** pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a **execução de contrato ou de procedimentos preliminares** relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o **exercício regular de direitos em processo judicial, administrativo ou arbitral**, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> IX - quando necessário para **atender aos interesses legítimos do controlador** ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. **(Grifo nosso)**

A Companhia, via de regra, não utiliza as bases legais descritas nos incisos I, III, IV, VII, VIII e X acima

dispostos. A natureza de suas atividades compatibiliza-se em maior grau com as hipóteses de cumprimento de obrigação legal ou regulatória; execução de contrato ou de procedimentos preliminares; exercício regular de direitos em processo judicial, administrativo ou arbitral, e; atendimento aos interesses legítimos do controlador.

A Política de Privacidade da Codemge traz que, para o uso da base cumprimento de obrigação legal ou regulatória, deve haver uma imposição de ordem para o tratamento de dados pessoais, como o determinado por lei ou ato normativo, não sendo o tratamento, nestas situações, discricionário.

Quanto à execução de contrato ou procedimentos preliminares, o documento elenca que tal "hipótese legal terá lugar quando o tratamento de dados pessoais estiver atrelado à necessidade de cumprimento de obrigações contratuais ou pré-contratuais. Para a utilização desta hipótese, todavia, o titular dos dados pessoais deve ser parte no contrato, ou o tratamento deve ser realizado a seu pedido".

A base legal exercício regular de direitos em processo judicial, administrativo ou arbitral, conforme a Política de Privacidade da Codemge, será utilizada quando necessária "para garantir o exercício da representação e da produção de provas da Companhia em discussões judiciais, administrativas ou arbitrais, sem a possibilidade de obstrução pelo titular de direitos".

O atendimento aos interesses legítimos do controlador, por sua vez, será utilizado residualmente, quando não houver hipótese autorizativa mais adequada. Para o uso, deverá ser aplicado um teste de proporcionalidade (teste do interesse legítimo), nos termos do referido normativo interno, com o intuito de balancear os direitos dos titulares, garantidos pela lei, em face de interesse legítimo da Codemge. Para essa verificação, a Companhia considera as finalidades legítimas, a necessidade, o balanceamento e a presença de salvaguardas, garantindo ainda que haja transparência para o titular sobre como seus dados são tratados e as medidas técnicas para mitigar riscos de exposição dos seus dados.

Ademais, a Companhia divulga em seu *site* institucional as informações sobre privacidade para os titulares dos dados pessoais, o contato do encarregado, o canal de comunicação para solicitações de titulares e esclarecimentos sobre o uso de *cookies* em seus sítios eletrônicos. Por fim, a Codemge não apresenta orientações específicas na Política de Privacidade nem no *site* sobre a realização de transferências internacionais de dados em razão de tal tratamento não configurar parte das atividades usuais da Companhia.

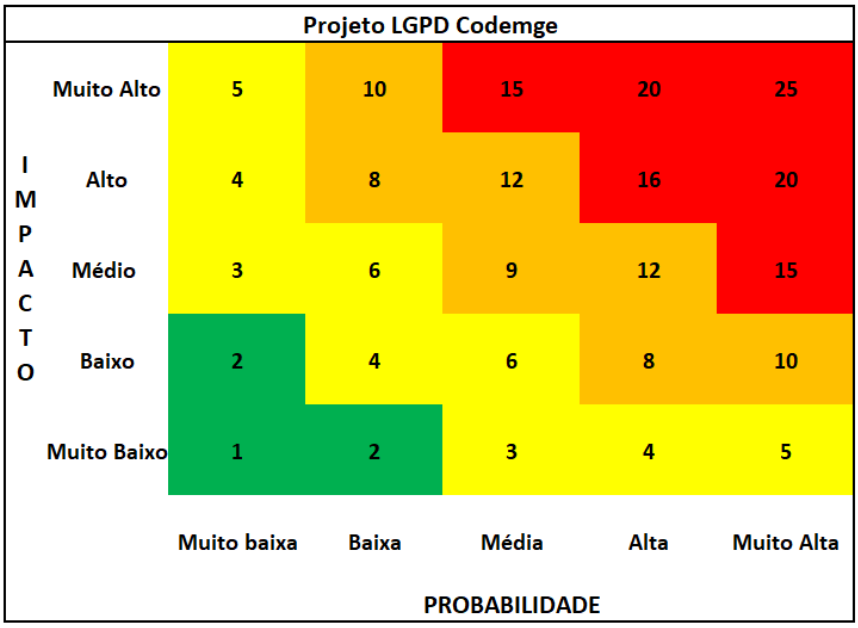
6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Em cumprimento ao art. 5º, XVII da LGPD, foram identificados e avaliados os principais riscos referentes ao tratamento de dados pessoais envolvidos nas atividades desenvolvidas na Companhia.

Classificação	Valor
Baixo	1 e 2

Classificação	Valor
Moderado	3 a 7
Alto	8 a 14
Crítico	15 a 25

Matriz Probabilidade x Impacto



Considerando a matriz de Probabilidade e Impacto, o risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado;
- laranja, configura um risco alto e
- vermelho, indica risco crítico.

Para a classificação dos riscos em razão da probabilidade, foi utilizada a seguinte métrica:

Probabilidade	Frequência	Descrição
1-Muito baixa	< 10%	Evento pode ocorrer apenas em circunstâncias excepcionais
2-Baixa	>=10% <= 30%	Evento **pode** ocorrer em algum momento
3-Média	>30% <= 50%	Evento **deve** ocorrer em algum momento
4-Alta	>50% <= 90%	Evento provavelmente ocorra na maioria das circunstâncias
5-Muito alta	>90%	Evento esperado que ocorra na maioria das circunstâncias

Quanto à classificação dos riscos em razão do impacto, as medidas analisadas foram:

ESACALA DE IMPACTO	LEGENDA QUALITATIVA	LEGENDA QUANTITATIVA	
NÍVEL		AUMENTO NO CUSTO	AUMENTO NO PRAZO
1- MUITO BAIXO	Evento cujo impacto é INSIGNIFICANTE e pode ser absorvido por meio de atividades normais	até 10%	até 5%
2- BAIXO	Evento cujo impacto é POUCO SIGNIFICANTE e pode ser recuperado, absorvido e tratado, mas carecem de esforço da gestão	>10% até 20%	>5% até 10%
3- MÉDIO	Evento cujo impacto é SIGNIFICANTE, com baixa posssibilidade de recuperação, mas pode ser gerenciado em circunstâncias normais	>20% até 20%	>10% até 15%
4- ALTO	Evento crítico com impacto MUITO SIGNIFICANTE, com possibilidade remota de recuperação e, com a devida gestão, pode ser suportado	>30% até 50%	>15% até 20%
5- MUITO ALTO	Evento com impacto MÁXIMO e sem a possibilidade de recuperação	>50%	>20%

Dessa forma, apresenta-se como resultado do estudo a seguinte matriz de riscos e seu respectivo *heatmap*:

Nº de ID do Risco	Objetivo do CIP ou da LGPD impactado pelo risco	Risco	Macroprocesso	Categoria	Descrição do Risco	Causa	Justificativa da Classificação	Probabilidade	Impacto	Nível do Risco
1	Segurança cibernética (item 8.8 da PC 04) (item 8.4 da PC 16)	**Ataque cibernético resultante em vazamento de dados**	Gestão da Tecnologia da Informação	Segurança da informação	Possibilidade de um ataque cibernético que gere roubo de dados em qualquer servidor, sistema ou plataforma em que estejam armazenados dados pessoais controlados ou operados pela Companhia.	1- A implementação inadequada de controle de segurança, como autenticação forte, criptografia de dados e verificação em duas etapas. 2- A engenharia social, como *phishing, pretexting* ou manipulação psicológica, podem ser utilizadas por agentes externos para obter informações de acesso ou credenciais de funcionários da Companhia, permitindo o acesso indevido a dados pessoais.	Quando agentes externos não autorizados têm acesso a dados pessoais da Companhia, eles podem explorar esses dados para fins criminosos, como fraude, roubo de identidade ou extorsão. Além disso, a exposição de dados pessoais pode levar a danos à reputação da Companhia, perda de confiança dos fornecedores, bem como possíveis ações legais e multas por descumprimento das disposições acerca da proteção de dados pessoais.	**4**	**5**	**20**
2	Diretrizes e bases legais (itens 5 e 6.3 da PC 16)	**Dependência de Sistemas geridos por órgãos externos**	Gestão da Tecnologia da Informação	Tecnológico	Controle insuficiente sobre os dados pessoais devido à obrigação de uso de sistema gerido e mantido por um terceiro.	Dificuldades em assegurar que as práticas do terceiro estejam alinhadas com os requisitos específicos da LGPD, especialmente considerando a subordinação da Codemge a diretrizes governamentais que implicam no uso obrigatório de determinados sistemas e plataformas.	Quando a Companhia confia em um terceiro para gerenciar e manter seu sistema eletrônico, ela transfere parte dessa responsabilidade para esse terceiro. No entanto, se o terceiro não adotar as medidas adequadas de segurança e proteção de dados, a Companhia pode ser considerada corresponsável pelas violações da LGPD.	**4**	**4**	**16**

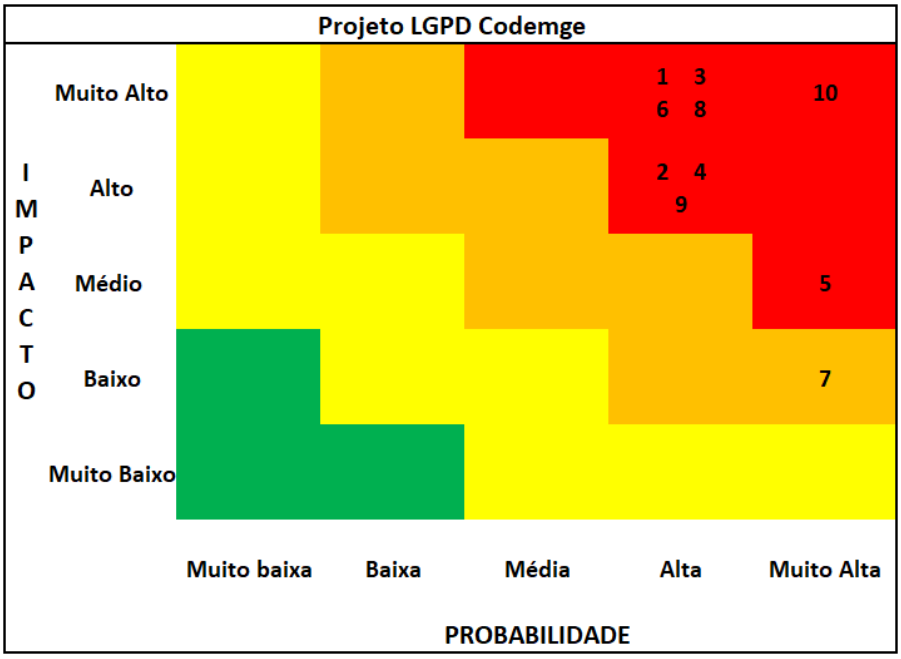
3	Art. 6º, VII, LGPD	**Vazamento de dados por operadores**	Governança, Riscos e Compliance	Operacional	Descumprimento pelo operador das diretrizes fornecidas pela Codemge ou desrespeito à ditames da LGPD.	1 - Erro Humano. 2 - Orientações falhas por parte da Codemge.	A Companhia celebra um grande número de contratos, o que aumenta a possibilidade de descumprimento de diretrizes por parte de algum dos operadores que trata dados pessoais em seu nome.	**4**	**5**	**20**
4	Segurança da Informação (itens 8.5 e 12 da PC 16)	**Fragilidades nos tratamentos de dados pessoais no processo de viagens corporativas**	Gestão organizacional	Operacional	Falhas ou vulnerabilidades no tratamento de dados pessoais nos processos de viagens corporativas considerando o trâmite entre as gerências da Companhia e no compartilhamento com a agência de viagens contratada pela Codemge para aquisição de passagens e hospedagens.	1-O compartilhamento ou trâmite inadequado de informações durante o processo de viagens corporativas, como o envio de dados pessoais por meios inseguros ou para destinatários não autorizados, resultando em falhas de segurança e exposição dos dados a terceiros.	Vulnerabilidades no tratamento de dados aumentam o risco de vazamento de dados pessoais, o que pode resultar em prejuízos financeiros e danos à reputação.	**4**	**4**	**16**

5	Art. 6º, II, LGPD	**Coleta de dados pessoais em quantidade superior ao necessário em procedimentos licitatórios e contratações**	Gestão Organizacional	Operacional	Possibilidade da Companhia coletar uma quantidade de dados pessoais além do necessário para os processos de licitação e contratação.	A falta de conscientização ou treinamento adequado dos responsáveis pela coleta de dados, levando a uma abordagem excessiva na obtenção de informações dos licitantes e contratados.	A Companhia celebra um grande número de contratos e tem a obrigação legal de publicar informações sobre os mesmos, em cumprimento a requisitos de transparência e controle social. Dessa forma, a solicitação excessiva de dados, além de ferir a LGPD, aumenta o risco de exposição e divulgação indevida de dados de licitantes e contratados.	**5**	**3**	**15**
6	Diretrizes (item 5.1.g da PC 16)	**Plano de resposta a incidentes de segurança e violações de dados pessoais inadequados**	Gestão da Tecnologia da Informação	Segurança da informação/ Legal	Ausência de diretrizes claras e procedimentos definidos para lidar de forma eficaz com resposta a incidentes de segurança envolvendo dados pessoais	A incapacidade de atendimento às diretrizes da LGPD, principalmente na observância ao prazo, comunicação devida e medidas adotadas quando em face de incidentes e pedidos de titulares	Os Incidentes de segurança mal gerenciados e pedidos de titulares não atendidos podem ter um impacto financeiro, legal e reputacional para a Companhia.	**4**	**5**	**20**

7	Art. 6º, III, LGPD	**Armazenamento prolongado de dados pessoais sem necessidade**	Governança, Riscos e Compliance	Conformidade/legal	Desrespeito ao ciclo de vida adequado no tratamento de dados pessoais.	Ausência de definição adequada de prazos de armazenamento e falta de verificação dos dados armazenados.	A ausência de prazos de armazenamento e falta de verificação dos dados armazenados é um risco para Codemge, pois a lei determina que os dados pessoais devem ser armazenados por prazos definidos, ou até que sua finalidade seja alcançada.	**5**	**2**	**10**
8	Diretrizes (item 5.1.d da PC 16)	**Acesso indevido a dados pessoais por agentes externos**	Gestão da Tecnologia da Informação	Segurança da informação	Possibilidade de indivíduos externos à Codemge acessarem, sem autorização, dados pessoais sob a guarda da Companhia, em meio digital ou físico.	Falha nos controles internos de verificação prévia quando da autorização de acesso a sistemas, plataformas e arquivos físicos ou digitais da Companhia.	Quando agentes externos não autorizados obtêm autorização de acesso a dados pessoais de gestão da Companhia por controle de acesso inadequado, falhas de segurança ou de verificação de identidade dos titulares, a situação desencadeia a possibilidade de sanção por violação dos ditames da legislação de proteção de dados pessoais pátria, além de sujeitar a Empresa a danos reputacionais.	**4**	**5**	**20**

9	Art. 6º, IV, LGPD	**Restrição de acesso aos titulares quando do pedido para ciência, modificação ou solicitação de exclusão de dados amparados pela LGPD.**	Governança, Riscos e Compliance	Legal	Falha da Companhia no atendimento a direitos dos titulares dos dados elencados no art. 18 da LGPD (acessar, corrigir, excluir os seus dados...)	1 - Falha de comunicação e de recebimento de pedidos de titulares. 2 - Incapacidade técnica da Codemge de atendimento aos pedidos. 3 - Intempestividade no atendimento a solicitações.	A Codemge, como empresa pública, tem a possibilidade de receber pedidos de titulares da sociedade em geral, considerando seus diversos tipos de atuação e sua interação com o público, de forma que deve estar preparada tecnológica e tecnicamente para atender às solicitações, sob pena de incorrer em sanções da legislação de proteção de dados.	**4**	**4**	**16**
10	Plano de ação CIP (Relatório final 1ª fase: item 5.3.4)	**Inadequação contratual à LGPD**	Governança, Riscos e *Compliance*	Legal/Governança	Contratos celebrados não adequados aos requisitos estabelecidos pela LGPD	1- A falta de conhecimento sobre a LGPD durante a elaboração dos contratos pode resultar na omissão de cláusulas essenciais. 2 - Elaboração de cláusulas ofensivas à LGPD por desconhecimento da legislação.	A Companhia possui uma variedade enorme de contratações e modelos de negócios que precisam de cláusulas, no mínimo gerais, de adequação e observância à LGPD como forma de conformidade à legislação de proteção de dados, com caráter educativo e foco na prevenção de tratamentos indevidos.	**5**	**5**	**25**

Heatmap dos riscos mapeados envolvendo o tratamento de dados pessoais na Codemge: sem implementação de controles



7 – MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco [1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	
1 - Ataque cibernético resultante em vazamento de dados	Medida 1: acesso à rede por VPN segura e uso de Firewall Medida 2: uso de autenticação em dois fatores para acesso ao ambiente computacional	Reduzir	3	4	12	Sim
2 - Dependência de Sistemas geridos por órgãos externos	Medida 1: cláusulas contratuais de sigilo e privacidade dos dados. Medida 2: no caso do Sistema SEI, um dos sistemas mais utilizados na Companhia para tramitação e assinatura de documentos, o cadastro de usuários externos possui uma rigorosa validação do cadastro com exigência de comprovação da identidade e documentação do usuário, além dos recursos oferecidos pelo próprio sistema, de concessão de acesso aos documentos para os usuários externos.	Aceitar	3	4	12	Sim
3 - Vazamento de dados por operadores	Medida 1: Adequação de todos os contratos vigentes e em via de celebração da Companhia, com inclusão de cláusulas de	Reduzir	3	4	12	Sim

	proteção de dados. Medida 2: Elaboração de cartilha orientativa com envio a todos os parceiros e fornecedores da Codemge, além de publicação no site da Companhia.					
4 - Fragilidades nos tratamentos de dados pessoais no processo de viagens corporativas	Medida 1: restrição de acesso ao fluxo de viagens a pessoas não envolvidas na viagem ou no fluxo Medida 2:	Reduzir / Compartilhar	3	3	9	Sim
5 - Coleta de dados pessoais em quantidade superior ao necessário em procedimentos licitatórios e contratações	Medida 1: Elaboração da Política de Privacidade da Companhia, com diretrizes para o tratamento de dados. Medida 2: Adequação de todos os normativos internos e formulários utilizados nas atividades desenvolvidas na Companhia à legislação de proteção de dados. Medida 3: Adequação dos contratos e minutas de editais da Companhia com cláusulas de proteção de dados.	Reduzir	3	3	9	Sim
6 - Plano de resposta a incidentes de segurança e violações de dados pessoais inadequados	Medida 1: Elaboração e implementação de Normativo Interno para atendimento a incidentes de privacidade, com desenho do fluxo e definição de responsabilidades e papéis de atuação em situações dessa natureza.	Reduzir	2	4	8	Sim
7 - Armazenamento prolongado de dados pessoais sem necessidade	Medida 1: Elaboração da Política de Privacidade da Companhia, com diretrizes para o tratamento de dados. Medida 2: Adequação de todos os normativos internos e formulários utilizados nas atividades desenvolvidas na Companhia à legislação de proteção de dados. Medida 3: Adequação dos contratos e minutas de editais da Companhia com cláusulas de proteção de dados. Medida 4: Utilização da tabela de temporalidade de arquivos.	Reduzir	4	2	8	Sim
8 - Acesso indevido a dados pessoais por agentes externos	Medida 1: uso de senhas fortes Medida 2: uso de autenticação em dois fatores no acesso ao ambiente computacional	Reduzir	2	3	6	Sim
9 - Restrição de acesso aos titulares quando do pedido para ciência, modificação ou solicitação de exclusão de dados amparados pela LGPD	Medida 1: Elaboração e implementação de Normativo Interno para atendimento a pedidos de titulares, com desenho do fluxo e definição de responsabilidades e papéis de atuação em situações dessa natureza. Medida 2: Disponibilização de canal para envio de solicitações de titulares, com a devida divulgação no site da Companhia. Medida 3: Acompanhamento rotineiro pelo Comitê Interno de Privacidade dos canais de recebimento de pedidos de titulares.	Reduzir	2	3	6	Sim
10 - Inadequação contratual à LGPD	Medida 1: Implementação de aditivos em todos os contratos vigentes da Companhia com cláusulas de proteção de dados.	Reduzir	2	2	4	Sim

	Medida 2: Inclusão de cláusulas de proteção de dados em todas as minutas padrão de contratos e editais da Companhia.					

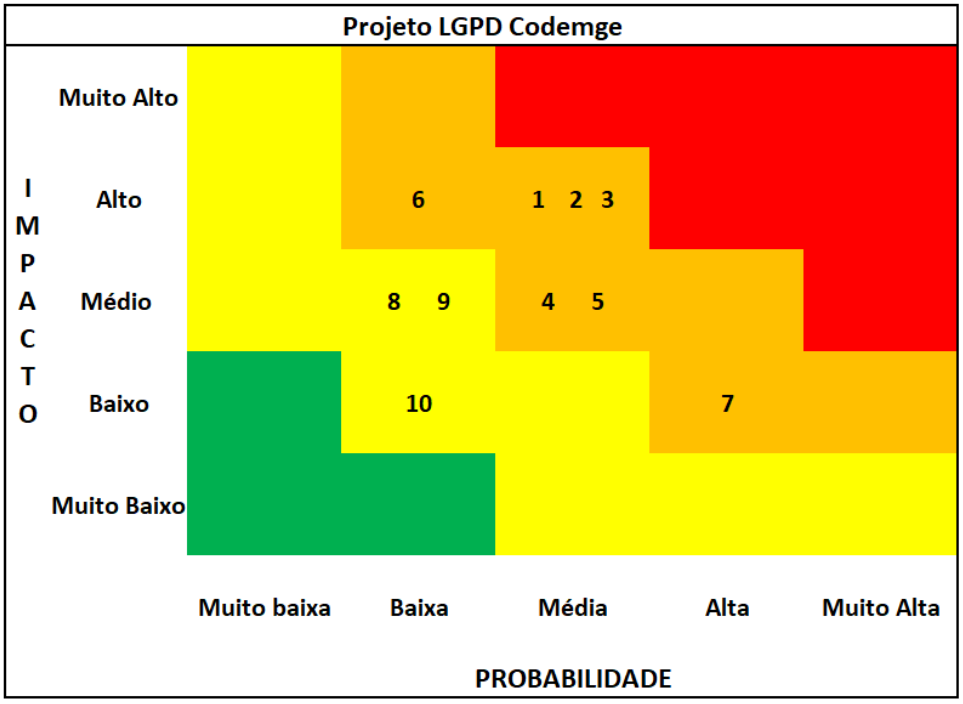
Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

[2] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

[3] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

Heatmap dos riscos mapeados envolvendo o tratamento de dados pessoais na Codemge: após implementação de controles e adoção de medidas de tratamento dos riscos



9 – INCIDENTES RELATADOS

O Comitê Interno de Privacidade mantém os registros de incidentes relatados e providências adotadas, à disposição da Autoridade Nacional de Proteção de Dados (ANPD). Os incidentes verificados até o momento pelo CIP não acarretaram risco ou dano relevante aos titulares de dados.

10 – PRÓXIMAS AÇÕES

Para o próximo exercício o Comitê Interno de Privacidade planejou:

- Elaboração de um plano de ação para 2024/2025;
- Elaboração de um Regimento Interno do Comitê;
- Atualização anual do Relatório de Impacto.

11 – APROVAÇÃO

ENCARREGADO	Coordenadora do Comitê Interno de Privacidade (CIP)
_____ Patrícia Sanglard Fadlallah	_____ Érica Rosália de Jesus Parreiras

Integrante do CIP – Tecnologia e Inteligência de Dados	Integrante do CIP – Jurídico
_____ Cláudia Patrocínio Veloso	_____ Denise Lobato de Almeida

Integrante do CIP – Auditoria Interna	Integrante do CIP – Comunicação
_____ Juliana Lúcia Mascarenhas Gomes Ferreira	_____ Marcello Pereira Machado

Integrante do CIP – Recursos Humanos	Integrante do CIP – Comunicação
_____ Ronaldo José Madureira	_____ Suellen Silva de Almeida

AUTORIDADE REPRESENTANTE DO CONTROLADOR
_____ Thiago Coelho Toscano Diretor-Presidente da Codemge

Belo Horizonte, 15 de janeiro de 2024