AMAZONAS
GOVERNO DO ESTADO

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS.

COMPANHIA DE DESENVOLVIMENTO DO ESTADO DO AMAZONAS – CIAMA.

www.ciama.am.gov.br
facebook.com/ciamaamazonas
instagram.com/ciama_amazonas/

ciama@ciama.am.gov.br
Fone: (92) 2123-9999
Avenida Tefé, 3279, Japiim
Manaus - AM
CEP: 69078-000

Companhia de **Desenvolvimento do Estado do Amazonas**

SUMÁRIO

1 IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO 3

2 NECESSIDADE DE ELABORAR O RELATÓRIO 3

3 DESCRIÇÃO DO TRATAMENTO 4

3.1 Tratamento de Dados 4

3.2 Compartilhamento de Dados 5

3.3. Tratamento de dados que envolvem crianças, adolescentes ou outro grupo vulnerável 6

3.4. Medidas de Segurança 6

3.5. Finalidade do Tratamento 7

4. PARTES INTERESSADAS CONSULTADAS 7

5. NECESSIDADE E PROPORCIONALIDADE 7

6. RISCOS À PROTEÇÃO DE DADOS PESSOAIS 7

6.1. Categorias de riscos 8

6.2. Medidas de Tratamento de Risco 9

7 CONSIDERAÇÕES FINAIS 9

8 APROVAÇÃO 10

1 IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

CONTROLADOR: Companhia de Desenvolvimento do Estado do Amazonas – CIAMA

OPERADOR: Não se aplica.

ENCARREGADO: Danielly Cristinna Macedo Brasil de Sá – Matrícula: 001181, Ato de designação datado de 02 de março de 2023.

Email do encarregado: privacidade.dados@ciama.am.gov.br

Telefone: 92 2123-9950

2 NECESSIDADE DE ELABORAR O RELATÓRIO

De acordo com o art. 38, caput, da Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), a qualquer momento a Autoridade de Proteção de Dados Pessoais (ANPD) pode determinar à Ciama que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis. Surgindo, assim, a necessidade de se elaborar este documento.

A Companhia, realiza o tratamento dos dados pessoais que se relacionam a pessoa natural identificada ou identificável (art. 5°, I, da LGPD). Existem também os dados pessoais sensíveis, que dizem respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (art. 5º, II, da LGPD).

Considerando os fundamentos da proteção de dados pessoais (art. 2º da LGPD), a boa-fé e os demais princípios a serem observados nas atividades de tratamento de dados pessoais (art. 6º da LGPD), a Companhia dispõe de sistemas de

controles internos, que variam de acordo com a natureza do dado pessoal, para mitigar eventuais riscos de falha na proteção de dados pessoais.

Entretanto, apesar da crescente maturidade da gestão de riscos da Companhia, não se pode garantir a eliminação total dos riscos que, em caso de materialização, causariam impacto à privacidade dos dados pessoais existentes na instituição.

3 DESCRIÇÃO DO TRATAMENTO

A Companhia, já instituiu a política de privacidade, e está alinhada às disposições da LGPD e legislação correlata. A política de privacidade, visa orientar as ações necessárias à garantia da segurança da informação, o que resulta na mitigação de riscos aos quais estão sujeitos os ativos de informação e que poderiam comprometer as atividades da Companhia e o cumprimento de sua missão institucional.

A Companhia vem adotando medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação.

O acesso às bases de dados é controlado, e o acesso é limitado a determinados perfis de usuários. Cada área tem acesso aos dados do servidor pertinentes ao seu setor. Há contínua busca por segurança da informação ao se fazer uso de sistemas corporativos, e ao dar cumprimento às disposições contidas nas normas e de acesso aos sistemas de informações.

3.1 Tratamento de Dados

Existem diversas formas de tratamento dos dados pessoais, considerando a definição da LGPD:

Dados Coletados: i)Dados coletados por meio de documentos protocolados por nossos fornecedores; ii)Dados coletados nos formulários dos cursos de

capacitação nos municípios, e serviços que a Companhia oferece; iii) Dados coletados em recrutamento e contratação de empregados e na contratação de serviços de terceiros; iv)Dados cadastrais da empresas e seus representantes, além dos dados nos processos que envolvem convênios e outros instrumentos congêneres utilizados na Companhia.

Dados Retidos: Os dados são mantidos em banco de dados corporativos, em banco de dados departamentais e arquivos físicos.

Dados Usados: São usados quando pertinentes nos processos de trabalho nas unidades (departamentos) internas da Companhia, gerando as demandas e sempre com justificativas de finalidade.

Dados Eliminados: Os dados retidos pela Companhia, são armazenados nos servidores, e anualmente é realizado backup para HD externo, onde ficam armazenados a disposição dos servidores, caso seja necessário. Esse backup fica protegido dentro do cofre antichamas, localizado no setor financeiro. A Companhia, mantém processos físicos arquivados no arquivo central da companhia, onde estão separados por setor/mês/ano, e estão sendo digitalizados para o servidor e futuramente serão descartados.

3.2 Compartilhamento de Dados

O Compartilhamento de dados pessoais, ocorrem na Companhia no momento da entrega de documentos pessoais para contratação/admissão de colaboradores, no preenchimento de fichas de atendimento durante os cursos de capacitação, durante a elaboração de projetos para os Municípios, processos licitatórios e também quando ocorrem Termo de Cooperação Técnica. Os dados coletados são tratados conforme à LGPD.

3.3. Tratamento de dados que envolvem crianças, adolescentes ou outro grupo vulnerável

A Companhia, não trata dados desses grupos em suas funções finalísticas, contudo, há tratamento de dados de dependentes dos colaboradores que envolvem crianças e adolescentes, e que devem ser observados os requisitos de representação legal, no caso de civilmente incapazes.

3.4. Medidas de Segurança

A Ciama implementa controles de segurança técnicos e organizacionais protegendo os dados pessoais contra roubo, perda ou uso indevido. Os dados serão armazenados em um ambiente operacional seguro que não é acessível sem autorização.

A segurança da informação é constantemente revista e aprimorada com novas medidas de segurança. Uma das abordagens em discussão atualmente é garantir que os dados estejam protegidos durante todo o seu tratamento (desde a coleta até a eliminação). Nesse processo, utilizamos firewall e proxy que protegem os dados de ataques externo, e utilizamos ferramentas que permitem a criptografia durante o acesso ao sistema (servidor), por meio de VPN.

O sistema de segurança da Ciama é regido pelos seguintes princípios da segurança da informação: disponibilidade; integridade; confidencialidade; autenticidade; irretratabilidade; privilégio mínimo; necessidade de conhecer; proteção dos dados pessoais; e proteção da privacidade.

A Companhia aplica medidas de mitigação após avaliações periódicas de risco para garantir um nível adequado de proteção de seus dados pessoais.

3.5. Finalidade do Tratamento

O Tratamento de dados da Companhia, é essencial para a prestação dos serviços públicos. A Companhia atende aos requisitos legais estabelecidos pela LGPD, respeitando os interesses legítimos dos nossos parceiros e colaboradores.

4. PARTES INTERESSADAS CONSULTADAS

Para a elaboração do presente Relatório, foram consultadas as áreas responsáveis pelo tratamento de dados, e demais setores da Companhia.

5. NECESSIDADE E PROPORCIONALIDADE

O tratamento de dados é limitado ao mínimo necessário para a realização das finalidades informadas ao titular. Quando necessário, tem abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

O objetivo é assegurar que o operador realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição, todo servidor ou terceirizado deve seguir o Código de Ética, Conduta e Integridade da Ciama. Além disso, os sistemas de informação possuem logs e controles de acesso.

6. RISCOS À PROTEÇÃO DE DADOS PESSOAIS

A Companhia, tem um processo de gestão de risco estabelecido pelo setor de tecnologia da informação, o processo de gestão de riscos abrange as seguintes perspectivas: Organizacional e operacional.

Dentre os tipos de risco organizacional, destacam-se os riscos à proteção de dados e informações armazenadas pela instituição, em especial aos dados pessoais. Esse tipo de risco pode ser descrito como potencial evento que gera impacto sobre o titular de dados pessoais e a Ciama. Os riscos operacionais, contemplam a possibilidade de ocorrência de perdas resultantes de eventos externos ou de falha,

deficiência ou inadequação de processos internos, pessoas ou sistemas. A metodologia da gestão de risco vem sendo discutida em detalhes, e em breve apresentaremos a Política de gestão de risco.

6.1. Categorias de riscos

Em virtude da introdução da temática de proteção dos dados pessoais, a metodologia de gestão de riscos operacionais da Companhia, passamos a elaborar um esboço para implantar a Política de Gestão de Riscos, onde poderemos mensurar e identificar os riscos específicos a esse assunto. 15 Relatório de Impacto à Proteção de Dados Pessoais mensuração dos riscos específicos a esse assunto. No levantamento dos riscos operacionais à proteção de dados pessoais, os eventos potenciais são analisados nas seguintes categorias:

Acesso não autorizado.	**Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.**
Modificação não autorizada	Modificação de dados pessoais sem a anuência do titular; viola o princípio da segurança.
Perda	Destruição ou extravio de dados pessoais; viola os princípios da segurança e da prevenção.
Apropriação	Apropriação ou uso indébito de dados de pessoais; possibilidades de fraude e vazamento intencional de dados; viola os princípios da segurança e da prevenção.
Remoção não autorizada	Retirada de dados pessoais sem autorização do titular.
Tratamento sem consentimento do titular dos dados pessoais	Tratamento dos dados pessoais sem a devida prévia permissão expressa, inequívoca e informada do titular, salvo exceções legais.
Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Compartilhamento dos dados pessoais com outras entidades privadas (fora da administração pública federal) sem a devida permissão do titular.
Retenção prolongada de dados pessoais sem necessidade	Manter os dados pessoais do titular para além do necessário ou do que estava consentido/autorizado; viola o princípio da necessidade.
Falha ou erro de processamento	Processamento dos dados de forma imperfeita ou equivocada. Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc. Viola o princípio da qualidade dos dados.
Reidentificação de dados pseudonimizados	Anonimização insatisfatória de dados pessoais sensíveis possibilitando inferir quem é a pessoa em questão; viola o direito à anonimização.

6.2. Medidas de Tratamento de Risco

A aplicação da metodologia de identificação e avaliação dos riscos permite classificá-los de acordo com critérios de priorização. Assim, após a validação do tratamento, as ações necessárias para mitigar os riscos são formalizadas e apresentadas. Entendemos como necessário a elaboração de um Plano de Mitigação de Riscos - PMR, que avaliará os tratamentos identificando os riscos, e montando um plano de ação. Assim, reduziremos as probabilidades de ocorrência e/ou os impactos dos riscos mapeados. A condução desses planos possui suporte organizacional, em termos de recursos, e apoio da Diretoria.

7 CONSIDERAÇÕES FINAIS

O presente relatório demonstra, em linhas gerais, como os dados pessoais são coletados, tratados, usados, compartilhados, bem como as medidas adotadas para o tratamento dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares desses dados. Além disso, foram apresentadas informações que denotam o estágio atual da implementação da LGPD.

Este Relatório será revisto e atualizado periodicamente ou sempre que a instituição implementar qualquer tipo de mudança que afete o tratamento dos dados pessoais. A Ciama, preocupa-se em avaliar continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

8 APROVAÇÃO

Responsável pela elaboração do Relatório de Impacto	**Encarregada**
Danielly Cristinna Macedo Brasil de Sá Mat.001181 – Ouvidoria/Ciama	Danielly Cristinna Macedo Brasil de Sá Mat.001181 – Ouvidoria/Ciama

Autoridade representante do controlador	**Autoridade representante do operador**
Antonio **Aluizio Barbosa** Ferreira Diretor Presidente	Não se aplica.

Manaus, 30 de junho de 2023