Relatório de Impacto à Proteção de Dados Pessoais – RIPD

EQUIPE TÉCNICA DE ELABORAÇÃO:

Comitê Interno para Gestão de Privacidade e Segurança da Informação
da **TG Logística e Transportes Ltda**, instituido em 25 de agosto de 2021

Paulo Eduardo do Valle representante legal da
Vergon Tecnologia da Informação Eireli, CNPJ 03.422.234/0001-15,
contratada para Prestação de Serviço à apresentação, estudo e
adequação de acordo com a Lei Geral de Proteção de Dados – LGPD

HISTÓRICO DE VERSÕES:

DATA	VERSÃO	DESCRIÇÃO	AUTORES
11/04/2022	1.0	Conclusão da primeira versão do relatório	• Comitê Interno para Gestão de Privacidade e Segurança da Informação da TG • Vergon Tecnologia da Informação Eireli

Relatório de Impacto à Proteção de Dados Pessoais – RIPD

SUMÁRIO:

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 – Lei Geral de Proteção de Dados).*

I – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO DE DADOS

Controlador	**TG Logística e Transportes Ltda** CNPJ 10.839.911/0001-60 Rua Barão de Mauá, 2060 - Distr. Indl. Getúlio Vargas - Mogi Guaçu/SP e todas as demais unidades de negócio. *Referência: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais – Art. 5º, VI da LGPD.*
Operador	Funcionários e/ou colaboradores da **TG Logística e Transportes Ltda** e/ou terceiros com seus respectivos responsáveis legais relacionados na nossa Política de Privacidade e Proteção de Dados Pessoais item "VIII – Com quem compartilhamos seus dados" e no Guia de Boas Práticas LGPD. *Referência: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador – Art. 5º, VII da LGPD.*

II – IDENTIFICAÇÃO DO ENCARREGADO DE DADOS

Data Protection Officer – DPO / Encarregado de dados	**Renato da Silva Mattos** – Gestor de TI, Membro do Comitê Interno para Gestão de Privacidade e Segurança da Informação – LGPD e Encarregado de Dados E-mail: renato.mattos@tglogistica.com.br – Tel. (19) 3818-1749 *Referência: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD – Art. 5º, VIII da LGPD.*

III – NECESSIDADE DE ELABORAR O RIPD

TG também utiliza-se desse RIPD como forma de guiar o próprio desenvolvimento do projeto de gestão de adequação à LGPD e para atender às exigências legais sobre privacidade e proteção de dados (*privacy by design*), sendo:

a. a qualquer momento sob determinação da ANPD – *Referência: Art. 38º da LGPD – 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;

b. sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:
   - uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
   - rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada – *Referência: Art. 12º, § 2º da LGPD*;
   - tratamento de dado pessoal sensível: 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 – *Referência: Art. 5º, II da LGPD*;
   - 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 – *Referência: Art. 20º da LGPD*;
   - tratamento de dados pessoais de crianças e adolescentes – *Referência: Art. 14º da LGPD*;
   - tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento – *Referência: Art. 42º da LGPD*;
   - tratamento no interesse legítimo do controlador – *Referência: Art. 10º, § 3º da LGPD*;
   - alterações nas leis e regulamentos aplicáveis à 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.

IV – DESCRIÇÃO DO TRATAMENTO

TG observa e 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” – *Referência: Art. 5º, X da LGPD*.

TG coleta dados de seus públicos de relacionamento com foco exclusivo em operar seus serviços e/ou produtos em todos os níveis, além de cumprir a legislação aplicável ao nosso modelo de negócio. No que se refere especificamente às informações de caráter pessoal, os sistemas de controle interno implantados na **TG** variam de acordo com o tipo de suporte (físico ou digital), bem como com a natureza da informação (comum ou sensível).

IV (1) – DADOS DIGITAIS

IV (1.1) – NATUREZA DO TRATAMENTO

São adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O acesso às bases de dados é controlado por grupos de rede e acesso limitado a determinados perfis de usuários.

Há contínua busca por segurança da informação ao se fazer uso de sistemas corporativos a **TG** e ao dar cumprimento às disposições contidas na Política de Privacidade e Proteção de Dados Pessoais e no Guia de Boas Práticas - LGPD, especialmente no que se refere ao acesso à informações.

IV (1.2) – TRATAMENTO DE DADOS

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

- Coletados/Enviados

Os dados são coletados principalmente por meio de sistemas de informação e/ou formulários impressos ou eletrônicos/software e cópias de documentos.

- Retidos/Armazenados

Os dados são mantidos das seguintes formas:

  - bancos de dados corporativos (utilizando os sistemas gerenciadores de banco de dados MySQL, PostgreSQL e SQL Server);
  - bancos de dados departamentais (utilizando os sistemas gerenciadores de banco de dados SQL Server);
  - arquivos (por exemplo: planilhas com extensão XLS e documentos com extensão DOC ou PDF).

- Usados

Os dados são usados em processos de trabalho das unidades de negócio da **TG** (também chamadas neste RIPD de Departamentos) de diversas formas. Pode-se citar a utilização de sistemas de informação desenvolvidos pelo Departamento de Tecnologia da Informação, pelas próprias unidades ou adquiridos de terceiros; também poderá ser utilizado ferramentas de análise de dados (por exemplo: BI – Business Inteligent).

- Eliminados

Os dados podem ser eliminados por meio de ações em sistemas de informação, comandos SQL nos bancos de dados e exclusão de arquivos.

IV (1.3) – FONTE DOS DADOS

As formas de coleta de dados na **TG** são:

- captações de informações externas: são enviados arquivos de dados ou documentos em papel com informações pessoais pelo próprio titular;
- sistemas de informação: de acesso interno (por exemplo: Sistema Integrado de Administração de Recursos Humanos e Sistema Integrado de Gestão Empresarial) e de acesso externo (por exemplo: Sistema de Cadastro e Gerenciamento de Clientes e Fornecedores);

Como coletamos os dados?	Fornecidos pelo próprio titular
Formulários impressos ou eletrônicos/software e cópias de documentos	Ao entrar em contato ou se cadastrar em nosso web site ou intranet corporativa. Faremos apenas o uso daqueles efetivamente necessários para que possamos atingir as finalidades.
	Coletados automaticamente
Cookies do web site	Tais como: características do dispositivo de acesso, do navegador, IP (com data e hora), origem do IP, informações sobre cliques, páginas acessadas, termos de procura digitado em nosso web site ou intranet corporativa. Para tal coleta, a **TG** fará uso de algumas tecnologias padrões, como cookies, pixel tags, beacons e local shared objects, que são utilizadas com o propósito de melhorar a experiência de navegação do titular nos serviços, de acordo com seus hábitos e suas preferências.
	Coletados pelas nossas unidades de negócios
Formulários impressos ou eletrônicos/software e cópias de documentos	Em cumprimento às obrigações legais e fornecimento de serviços e/ou produtos, de clientes, colaboradores e/ou funcionários, fornecedores, parceiros de negócios e/ou terceiros.
	Biometria
Software de leitura biométrica	Relógio de ponto eletrônico local com armazenamento local ou em nuvem.
	Atendimentos institucionais
Registro de informações	Presencial, formulário de contato no web site, e-mail, aplicativos de mensagens instantâneas e/ou telefônico.

IV (1.4) – COMPARTILHAMENTO DOS DADOS

O compartilhamento de dados pessoais ocorre com as instituições reguladas, apenas com o consentimento do titular.

Compartilhamento dos dados?	Com fornecedores, parceiros de negócios e/ou terceiros
Dados pessoais e/ou dados pessoais sensíveis	I. Quando houver determinação legal de uma autoridade judicial, administrativa ou governamental; II. Com nossa equipe interna de marketing para divulgação de conteúdos e publicidades; III. Transações e alterações societárias envolvendo a **TG**, hipóteses em que a transferência das informações será necessária para a continuidade dos serviços; IV. Com as unidades de negócios da **TG**, hipóteses em que a transferência das informações será necessária para a continuidade dos serviços; V. Com empresas parceiras e fornecedores, no desenvolvimento dos serviços voltados ao titular; VI. Empresas de tecnologia responsáveis pelos cookies utilizados para análise de uso do nosso web site ou intranet corporativa; VII. Empresas de hospedagem e plataforma de gerenciamento do nosso web site ou intranet corporativa; VIII. Empresas de serviços de operação de dados em nuvem; IX. Aplicações de comunicação via internet; X. Órgãos governamentais federais, estaduais e municipais para cumprimento de determinações legais ou judiciais, caso ocorram; XI. Auditorias internas e externas para conferência e certificação de conformidade; XII. Prestadores de serviços contratados e/ou terceirizados: advogados, auditores, contadores, desenvolvimento de softwares, empresas de limpeza, medicina em saúde do trabalho, segurança e vigilância; XIII. Software para armazenamento externo de contratos e documentação relacionados; XIV. Bancos, para a execução de transações financeiras, como pagamentos, recebimentos e reembolsos; XV. Serviços de proteção ao crédito para avaliação e liberações de crédito; XVI. Farmácias, supermercados entre outras referente a benefícios na aquisição de serviços e/ou produtos.

Quais são os operadores?	Colaboradores e/ou funcionários, parceiros de negócios e/ou terceiros
Dados pessoais e/ou dados pessoais sensíveis	I. Aplicativos de comunicação; II. Departamento Comercial; III. Departamento Contábil; IV. Departamento de Logística; V. Departamento de Recursos Humanos; VI. Departamento de Tecnologia da Informação; VII. Departamento Financeiro VIII. Departamento Fiscal; IX. Empresa terceirizada de armazenamento de dados; X. Empresa terceirizada de auditoria de administração interna; XI. Empresa terceirizada de consulta de antecedentes criminais; XII. Empresa terceirizada de eventos, comemorações e brindes/presentes; XIII. Empresa terceirizada de exames laboratoriais; XIV. Empresa terceirizada de gerenciamento de risco; XV. Empresa terceirizada de hospedagem de domínio, site e e-mails; XVI. Empresa terceirizada de hospedagem de softwares e aplicativos em nuvem; XVII. Empresa terceirizada de locação de veículos; XVIII. Empresa terceirizada de limpeza; XIX. Empresa terceirizada de manutenção de máquinas e veículos;

XX. Empresa terceirizada de manutenção predial;
XXI. Empresa terceirizada de monitoramento por câmeras e alarme;
XXII. Empresa terceirizada de medicina em saúde do trabalho;
XXIII. Empresa terceirizada de recepção e portaria;
XXIV. Empresa terceirizada de refeições, marmitas ou vales;
XXV. Empresa terceirizada de rastreamento de veículos;
XXVI. Empresa terceirizada de RH – contratação ou empregos temporários;
XXVII. Empresa terceirizada de segurança patrinomial;
XXVIII. Empresa terceirizada de segurança do trabalho;
XXIX. Empresa terceirizada de softwares e sistemas de informação;
XXX. Empresa terceirizada de telefonia;
XXXI. Empresa terceirizada de transportes de cargas;
XXXII. Empresa terceirizada de transportes de documentos – Correios ou motoboys;
XXIII. Empresa terceirizada de transportes de pessoas – ônibus, vans e aplicativos;
XXIV. Empresa terceirizada de vale/ticket abastecimento;
XXV. Escritório de Advocacia;
XXVI. Escritório de Contabilidade, Escrita Fiscal e RH;
XVII. Conta salário – Bancos;
XVIII. Convênio com Farmácia – A Popular;
XXIX. Convênio com Supermercados – Ponto Novo e PegMais;
XL. Convênio odontológico;
XLI. Convênio ou seguro saúde;
XLII. Estágios – aprendizes ou graduandos;
XLIII. Hospedagem em Hoteis e Pousadas;
XLIV. Obrigações trabalhistas – Caixa Federal, Ministérios do Trabalho e Saúde;
XLV. Passagem de viagens por avião ou ônibus;
XLVI. Pagamento de pensão alimentícia fixada por juiz;
XLVII. SCPC – Serviço Central de Proteção do Crédito – consulta de clientes;
XLVIII. Seguradoras de colaboradores e funcionários – proteção de vida e funeral;
XLIX. Seguradoras de transporte de cargas e veículos;
L. Sindicatos e associações;

IV (1.5) – MEDIDAS DE SEGURANÇA

As medidas de segurança adotadas pela **TG** têm validade para qualquer tipo de informação. Elas são definidas pela Política de Privacidade e Proteção de Dados Pessoais e no Guia de Boas Práticas - LGPD, as quais contém os Procedimentos Operacionais de Segurança em Tecnologia da Informação. Define-se informação sensível como aquela que necessita de proteção contra revelação não autorizada, e o Departamento de Tecnologia da Informação normatiza o uso desses recursos.

- Transferência de Arquivos

Para a transferência de arquivos eletrônicos, para destinatários internos, com informação sensível, devem ser utilizadas:

- pastas compartilhadas localizadas em servidor de arquivos sigilosos;
- mensagem de e-mail com anexo criptografado, com a senha do arquivo sendo transmitida por outro meio, como telefone, por exemplo.

Para a transferência de arquivos eletrônicos de/para destinatários externos, podem ser utilizados:

- anexos de e-mail, caso não haja necessidade de garantia de entrega. Se a informação for sensível,
- o anexo deve estar criptografado, com a senha do arquivo sendo transmitida por outro meio, como telefone.
- mídias removíveis (pendrive, CD, DVD ou HD externo) podem ser utilizadas para a transferência de arquivos corporativos mediante justificativa e com a anuência da chefia imediata ou o Departamento de Tecnologia da Informação, em especial em caso de impossibilidade de uso dos meios tecnológicos descritos acima. Nesse caso, é obrigatória

a aplicação de criptografia para proteção da informação sempre que viável tecnologicamente.
- Não são considerados meios adequados para a transferência de arquivos eletrônicos: pastas compartilhadas em estações de trabalho (desktops e notebooks), e-mail particular e serviços de terceiros na Internet (exemplo: Dropbox, Google Drive e Onedrive).

- Servidores de arquivos

Os servidores de arquivos possuem áreas de armazenamento reservadas para cada unidade. Os administradores de cada unidade são responsáveis por conceder permissão de acesso às pastas e arquivos, observados os princípios da necessidade de conhecer e do privilégio mínimo.

Para as informações sigilosas, existe um servidor de arquivos sigilosos (com criptografia no tráfego de rede e auditoria completa de acessos). Esse servidor é administrado e acessado exclusivamente pelo Departamento de Tecnologia da Informação.

- Impressão de documentos

Não deverão ser impressos arquivos eletrônicos corporativos com informação sensível fora das dependências da **TG** e demais unidades de negócios.

- Descarte de informações

O descarte de informações corporativas gravadas em qualquer mídia deverá ser feito de maneira a impedir a sua recuperação.

- Monitoramento

O Departamento de Tecnologia da Informação poderá monitorar, para fins de trilhas de auditoria, os acessos e gravações de arquivos e as transferências e impressões de arquivos eletrônicos corporativos.

É de responsabilidade de cada unidade de negócios da **TG** assegurar o uso correto e eficiente da área de armazenamento reservada a ela, verificando periodicamente se:

- apenas arquivos necessários aos processos de trabalho da unidade estão armazenados;
- não existem arquivos que infrinjam direitos autorais ou que apresentem outros riscos jurídicos, como músicas, filmes e livros que não tenham sido adquiridos a **TG**.

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 o descarte). Nesse processo, são utilizados diversos sistemas, tecnologias e ferramentas para permitir a criptografia e o controle de acesso de forma integrada.

Medidas de segurança adotadas	Armazenamento de dados físicos
Dados pessoais e/ou dados pessoais sensíveis	I. Caixas arquivos catalogadas, numeradas e etiquetadas; II. Estantes para arquivos abertas; III. Armários fechados e com fechadura; IV. Sala com porta e acesso restrito ao pessoal do setor/departamento; V. Alarme; VI. Câmera de monitoramento; VII. Sensor de incêndio; VIII. Extintor de incêndio; IX. Prédio em alvenaria com laje de concreto; X. Departamento Comercial arquivados por 5 anos e após incinerados; XI. Departamento Contábil arquivados por tempo indefinido; XII. Departamento de Logística arquivados por 5 anos e após incinerados; XIII. Departamento de Recursos Humanos arquivados por tempo indefinido; XIV. Departamento Financeiro arquivados por 5 anos e após incinerados; XV. Departamento Fiscal arquivados por 5 anos e após incinerados;
Medidas de segurança adotadas	Armazenamento de dados digitais
Dados pessoais e/ou dados pessoais sensíveis e biométricos	I. Em computadores locais com login e senha de acesso;

II. Em servidor de arquivos locais com login, senha de acesso e políticas de segurança com restrições de acesso por grupos ou usuários;
III. Backup diário de dados em armazenamento local – HDs externos, guardados com o pessoal responsável pela TI;
IV. Backup diário de dados em armazenamento em nuvem, com acesso restrito ao pessoal responsável pela TI;
V. Backup com retenção de até 30 dias;
VI. Computadores e servidores locais com firewall ativos, antivírus atualizado e sistemas operacionais atualizados;
VII. Sala com porta e acesso restrito ao pessoal do setor/departamento;
VIII. Alarme;
IX. Câmera de monitoramento;
X. Sensor de incêndio;
XI. Extintor de incêndio;
XII. Prédio em alvenaria com laje de concreto;
XIII. Arquivados digitais retidos por tempo indefinido;
XIV. Dados biométricos armazenados no relógio ponto e mantidos no próprio dispositivo e no sistema de gestão de RH por tempo indefinido ou excluídos quando da demissão do colaborador e/ou funcionário;

V – ESCOPO DE TRATAMENTO

O escopo representa a abrangência do tratamento de dados. As seções seguintes mostram detalhes sobre a extensão do escopo para os dados digitais. Com relação aos dados contidos em documentos físicos, conforme visto anteriormente, recebem o mesmo tratamento dos digitais, pois podem ser digitalizados assim que adentram uma das unidade de negócios da **TG**.

V (1.1) – TIPOS DE DADOS

Consideração dos dados	Tratamento para
Dados pessoais de colaboradores e/ou funcionários	I. Nome completo; II. Data de nascimento; III. Número e imagem da Carteira de Identidade (RG); IV. Número e imagem do Cadastro de Pessoas Físicas (CPF); V. Número e imagem do Título de Eleitor; VI. Número e imagem do Certificado de Reservista; VII. Número e imagem da Carteira Nacional de Habilitação (CNH); VIII. Número e Imagem do cartão de Vale Transporte; IX. Número e imagem do cartão de Alimentação; X. Número e imagem do cartão de Refeição; XI. Número e imagem do Programa de Integração Social (PIS); XII. CTPS física e/ou digital; XIII. Fotografia 3×4; XIV. Imagem da Certidão de Casamento ou Declaração de União Estável; XV. Imagem do Diploma; XVI. Endereço completo; XVII. Números de telefone, WhatsApp e endereços de e-mail; XVIII. Banco, agência e número de contas bancárias; XIX. Sua imagem, considerando sua foto;
Consideração dos dados	Tratamento para
Dados pessoais sensíveis de colaboradores e/ou funcionários	I. Número e imagem do cartão de Plano Médico; II. Número e imagem do cartão de Plano Odontológico; III. Número e imagem do Cartão Sus; IV. Exames e atestados médicos, especialmente admissionais, periódicos, incluídos de retorno por afastamento superior a 30 dias em caso de doença, acidente ou parto, de mudança de função, demissionais e ainda aqueles que atestem doença ou acidente; V. Certidão de nascimento dos filhos menores de 14 anos, Carteira de vacinação dos menores de 7 anos, e atestado de matrícula e frequência escolar semestral dos maiores de 4 anos; VI. Sua biometria;

	VII. Dados de filiação a Sindicato ou associação;
Dados pessoais de clientes, fornecedores e/ou terceiros	I. Nome completo II. CPF III. RG IV. Endereço completo; V. Números de telefone, WhatsApp e endereços de e-mail;

Os dados pessoais tratados pela **TG** têm como finalidade realizar a prestação de serviço ou oferta de produtos, cumprir obrigações legais e regulatória, ampliar nosso relacionamento, informar você sobre novidades, funcionalidades, conteúdos, e-books, vídeos técnicos, notícias e demais eventos que consideramos relevante para você bem como para fins publicitários, como o envio de informações de marcas, produtos e promoções da **TG**, além da divulgação de eventos ou para a realização de pesquisas relacionadas às suas atividades, com gestão de qualidade e excelência no atendimento.

Podemos enviar-lhe notificações por e-mail, SMS ou aplicativos de mensagens, como WhatsApp, relativas ao seu contato, realizado através de nosso web site ou intranet corporativa ou que você solicitou especificamente (como boletins informativos ou notificações). Você pode desativar essa comunicação a qualquer momento.

O tratamento dos dados de menores deverá ser realizado com o consentimento específico e fornecido por pelo menos um dos pais ou pelo responsável legal, observando os procedimentos disponibilizados pela **TG** para tal consentimento.

V (1.2) – VOLUME DE DADOS

O escopo representa a abrangência do tratamento de dados. As seções seguintes mostram detalhes sobre a extensão do escopo para os dados digitais. Com relação aos dados contidos em documentos físicos, conforme visto anteriormente, recebem o mesmo tratamento dos digitais, pois podem ser digitalizados assim que adentram uma das unidade de negócios da **TG**.

Há diversas bases que possuem dados pessoais na **TG**. Uma das mais relevantes é a que pode receber diariamente dados cadastrais de pessoas físicas. Essa base possui aproximadamente 0 milhões de registros. Os dados recebidos são cadastrados de novos colaboradores e/ou funcionários e de novos clientes e fornecedores e/ou terceirizados.

Armazenados em um banco de dados principal (SQL Server), possuem aproximadamente 0 gigabytes. Esses dados podem ser copiados diariamente para as unidade de negócios da **TG** e atender às necessidades dos departamentos.

V (1.3) – FREQUÊNCIA DE TRATAMENTO DE DADOS

TG recebe diariamente atualizações de dados cadastrais de pessoas físicas, seja por demandas de novos registros ou atualizações cadastrais.

V (1.4) – RETENÇÃO DOS DADOS

Os responsáveis de cada departamento em conjunto com o Comitê Interno para Gestão de Privacidade e Segurança da Informação da **TG** podem definir o tempo de retenção e de descarte para cada base de dados, sempre observando aspectos legais quando aplicáveis.

Essas informações dizem respeito a toda a base de dados e não especificamente aos dados pessoais nela contidos.

As informações presentes nas bases de dados e nos outros sistemas de informação do Departamento de Recursos Humanos não são eliminadas.

Todos os dados utilizados para atendimento aos órgãos públicos são armazenados pela **TG** e não são eliminados ou podem ser eliminados quando observados os prazos legais.

V (1.5) – TITULARES AFETADOS PELO TRATAMENTO DE DADOS

Qualquer pessoa física ou jurídica, colaborador e/ou funcionário, cliente ou fornecedor, pode ser afetada pelo tratamento de dados na **TG**.

VI – CONTEXTO DO TRATAMENTO DE DADOS

TG trata os dados pessoais de acordo com os propósitos legítimos e específicos de modo compatível com a sua finalidade, cujo caráter é de interesse privado, e objetiva executar as competências legais ou cumprir as atribuições legais da sua atividade econômica.

VI (1.1) – NATUREZA DO RELACIONAMENTO – **TG** COM OS TITULARES DE DADOS

TG trata os dados pessoais de acordo com os propósitos legítimos e específicos de modo compatível com a sua finalidade, cujo caráter é de interesse privado, e objetiva executar as competências legais ou cumprir as atribuições legais da sua atividade econômica.

VI (1.2) – TRATAMENTO DE DADOS QUE ENVOLVEM CRIANÇAS, ADOLESCENTES OU OUTRO GRUPO VULNERÁVEL

Esses grupos não realizam operações e/ou mantem relacionamento comercial com a **TG**. Contudo, há dados de dependentes de colaboradores e/ou funcionários da **TG** que envolvem crianças e adolescentes, mas são observados todos os requisitos e tratamentos adequados para esses dados e sempre obtendo consentimento expresso do seu representante legal.

VI (1.3) – TRATAMENTO DE DADOS CONFORME DETERMINAÇÃO LEGAL

O tratamento de dados é aquele previsto em regras públicas.

VI (1.4) – EXPERIÊNCIAS ANTERIORES

TG demonstra ter precaução com as informações que coleta e manuseia, tendo em vista não somente a importância desses dados para sua atividade econômica, mas também a natureza sigilosa de boa parte deles. As obrigações previstas na Lei 13.709/2018 (LGPD – Lei Geral de Proteção de Dados), criam um regime de restrição ao acesso não autorizado a muitas das informações pessoais tratadas pela **TG** que se movimenta no cumprimento legal.

VI (1.5) – AVANÇOS EM TECNOLOGIA E SEGURANÇA

As seguintes ferramentas de proteção de dados estão em avaliação:

- Microsoft – permite configurar políticas para classificar, rotular e proteger dados com base em seu nível de confidencialidade. A classificação pode ser totalmente automática, coordenada pelos usuários ou baseada em recomendação. Também é possível definir quem pode acessar dados e o que as pessoas podem fazer com eles – por exemplo, permite a exibição e edição de arquivos, mas não o seu encaminhamento. Os dados são protegidos, estejam eles armazenados em infraestruturas locais ou na nuvem;
- Vergon – sistema de backup automático e encriptografado em nuvem;
- Adoção de solução de firewall para proteção das bordas de acesso à internet.

Questões práticas em relação ao desempenho no uso dos dados e espaço de armazenamento ainda estão sendo avaliadas.

VII – FINALIDADE DO TRATAMENTO

A finalidade do tratamento dos dados pela **TG** relaciona-se ao estrito cumprimento de obrigação legal ou regulatória.

Referência: Art. 10º da LGPD – "O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei."

VIII – 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 tratamento é feito apenas quando é indispensável e com propósito de cumprimento de obrigação legal e regulatória, pesquisa e divulgação de estatísticas para cálculo e divulgação de indicadores agregados (sem consultas individualizadas).

Com o objetivo de assegurar que o operador realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela **TG**, todo colaborador e/ou funcionário e/ou terceirizado deve seguir o Manual de Conduta Interna da **TG**. Além disso, os sistemas de informação possuem logs e controles de acesso.

IX – RISCOS À PROTEÇÃO DE DADOS PESSOAIS

Os riscos podem ser divididos em riscos de origem financeira – risco de mercado, crédito e liquidez – e riscos de origem organizacional – risco operacional e estratégico – e têm diferentes dimensões de impacto – como impacto financeiro, reputacional e de negócio.

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.

Dentre os tipos de risco operacional, destacam-se os riscos à proteção de dados e informações armazenadas pela **TG**, 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 sobre a **TG**. No Guia de Boas Práticas - LGPD, demonstramos a metodologia da gestão de risco na **TG** é discutida em detalhes.

IX (1.1) – CATEGORIAS DE RISCOS

Os riscos podem ser divididos em riscos de origem financeira – risco de mercado, crédito e liquidez – e riscos de origem organizacional – risco operacional e estratégico – e têm diferentes dimensões de impacto – como impacto financeiro, reputacional e de negócio.

Em virtude da introdução da temática de proteção dos dados pessoais, a metodologia de gestão de riscos operacionais da **TG** passou por recente alteração com a inclusão de novas taxonomias para identificação e mensuração dos riscos específicos a esse assunto. No levantamento dos riscos operacionais à proteção de dados pessoais, os eventos potenciais são analisados nas categorias a seguir:

1. Acesso não autorizado	Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.
2. Modificação não autorizada	Modificação de dados pessoais sem a anuência do titular. Viola o princípio da segurança.
3. Perda	Destruição ou extravio de dados pessoais. Viola os princípios da segurança e da prevenção.
4. 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.
5. Remoção não autorizada	Retirada de dados pessoais sem autorização do titular.
6. Coleção excessiva	Extração de mais dados do que o necessário para a realização do trabalho, ou do que é previsto em Lei ou foi autorizado pelo usuário. Viola o princípio da necessidade.
7. Informação insuficiente sobre a finalidade do tratamento	A finalidade declarada para o uso das informações pessoais é insatisfatória, não é específica ou pode suscitar interpretações diversas.
8. 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.
9. 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.

10. 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.
11. Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	Erro ao vincular dados do verdadeiro titular a outro. Viola o princípio da qualidade dos dados.
12. Falha ou erro de processamento	Processamento dos dados de forma imperfeita ou equivocada. Exemplo: 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.
13. Reidentificação de dados pseudonimizados	Anonimização insatisfatória de dados pessoais sensíveis possibilitando inferir quem é a pessoa em questão. Viola o direito à anonimização.

IX (1.2) – IDENTIFICAÇÃO DOS RISCOS

Apresentam-se a seguir exemplos iniciais não exaustivos de riscos identificados e mensurados, de acordo com a metodologia de gerenciamento de riscos operacionais à proteção de dados pessoais:

- vazamento intencional de dados pessoais;
- alteração intencional de dados pessoais;
- permissão indevida para acesso a dados pessoais;
- furto de informações confidenciais;
- divulgação não autorizada de dados pessoais contidos nos documentos e arquivos;
- quebra não autorizada de sigilo bancário;
- invasão de sistemas para coleta de dados pessoais;
- invasão do site da **TG** por hackers.

Uma avaliação completa desse tipo específico de risco está planejada em todos os processos da **TG** que envolvem o armazenamento de dados pessoais.

IX (1.3) – MEDIDAS DE TRATAMENTO DOS RISCOS

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 pela alta administração, as ações necessárias para mitigar os riscos são formalizadas pelos departamentos em Planos de Mitigação de Riscos (PMR). A elaboração desses PMR, quando os planos forem necessários, cabe ao Departamento de Tecnologia da Informação.

Dessa forma, vários planos de mitigação estão em andamento com o objetivo de reduzir a probabilidade de ocorrência e/ou os impactos dos riscos mapeados. A condução desses planos possui suporte organizacional, em termos de recursos, e apoio da alta administração.

X – CONFORMIDADE À LEI GERAL DE PROTEÇÃO DE DADOS

Com a publicação da LGPD, que dispõe sobre tratamento de dados pessoais por pessoa natural ou jurídica de direito público ou privado, surgiu a necessidade da **TG** rever seus processos no intuito de verificar o estágio atual de conformidade à referida norma.

Dessa forma, ao longo desse ano, as unidades de negócio da **TG** realizaram avaliações de conformidade à LGPD. No “Resumo da Metodologia de Gestão de Conformidade”, a metodologia da gestão de conformidade na **TG** é apresentada em detalhes.

Conforme mencionado anteriormente, até o momento, foram realizadas 5 avaliações de conformidade à LGPD pelas unidades de negócio da **TG**. Os principais resultados dessas avaliações podem ser conhecidos nas seções seguintes.

X (1.1) – IMPACTO DA NÃO CONFORMIDADE E URGÊNCIA PARA AÇÃO

De acordo com a Figura X 1.1.1, 35% das possíveis não conformidades gerariam impactos de níveis consideráveis (muito alto e alto) para a instituição. Entretanto, para uma melhor medição do grau de conformidade a uma obrigação, a efetividade dos controles implantados, que é representada pela urgência para ação, também deve ser considerada.

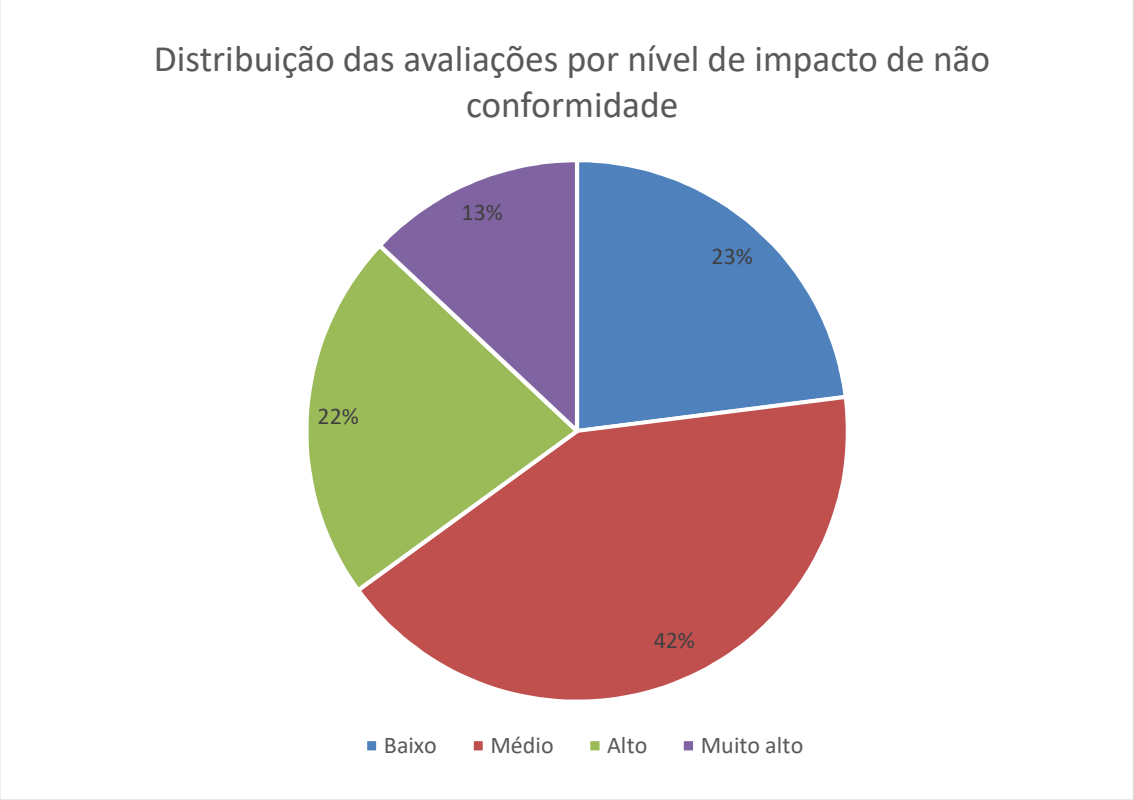

Figura X 1.1.1

Assim, ao analisar o gráfico da Figura X 1.1.2, verifica-se que grande parte das avaliações (90%) foi aferida com grau de urgência para ação média ou baixa, ou seja, na percepção das unidades, os controles implantados são considerados adequados para garantir o razoável cumprimento da LGPD.

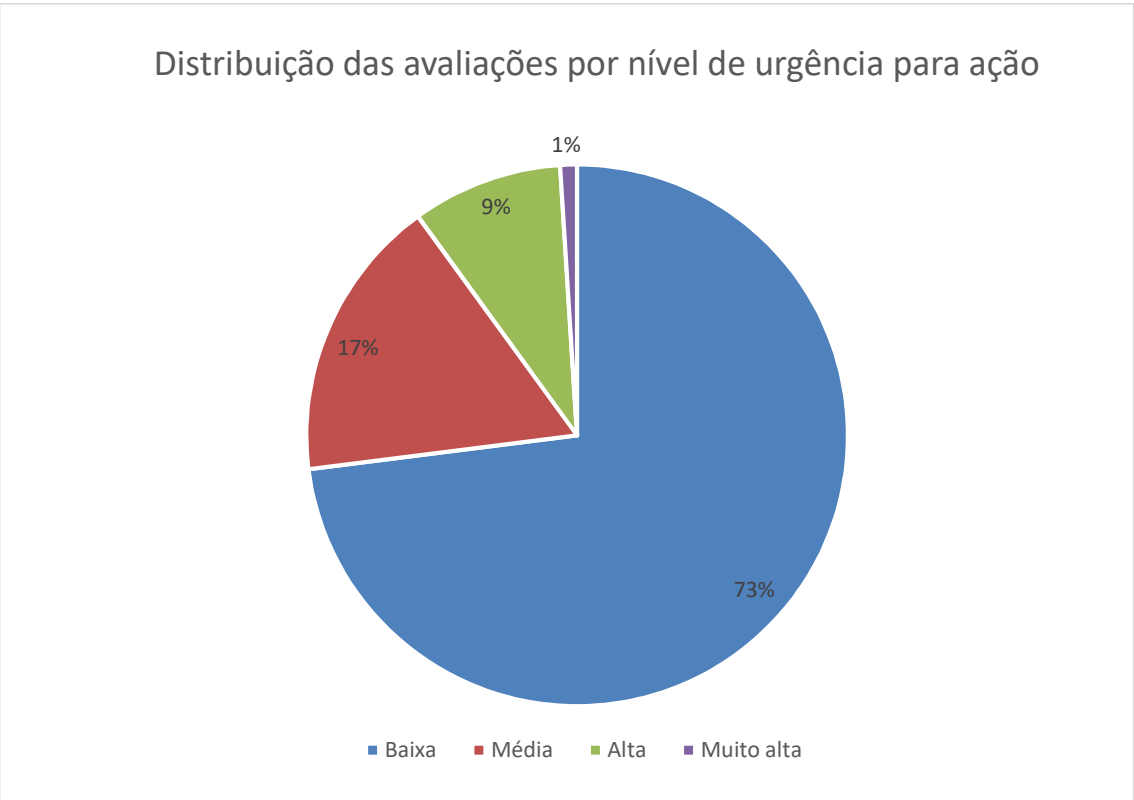

Figura X 1.1.2

X (1.2) – CRITICIDADE

A partir da composição do impacto da não conformidade e da urgência para ação, encontra-se o grau de criticidade da obrigação avaliada. Conforme a Figura X 1.2.1, somente 4% das avaliações podem ser consideradas críticas. Ressalta-se que a **TG** tem implementado ações para reduzir a criticidade dessas avaliações.

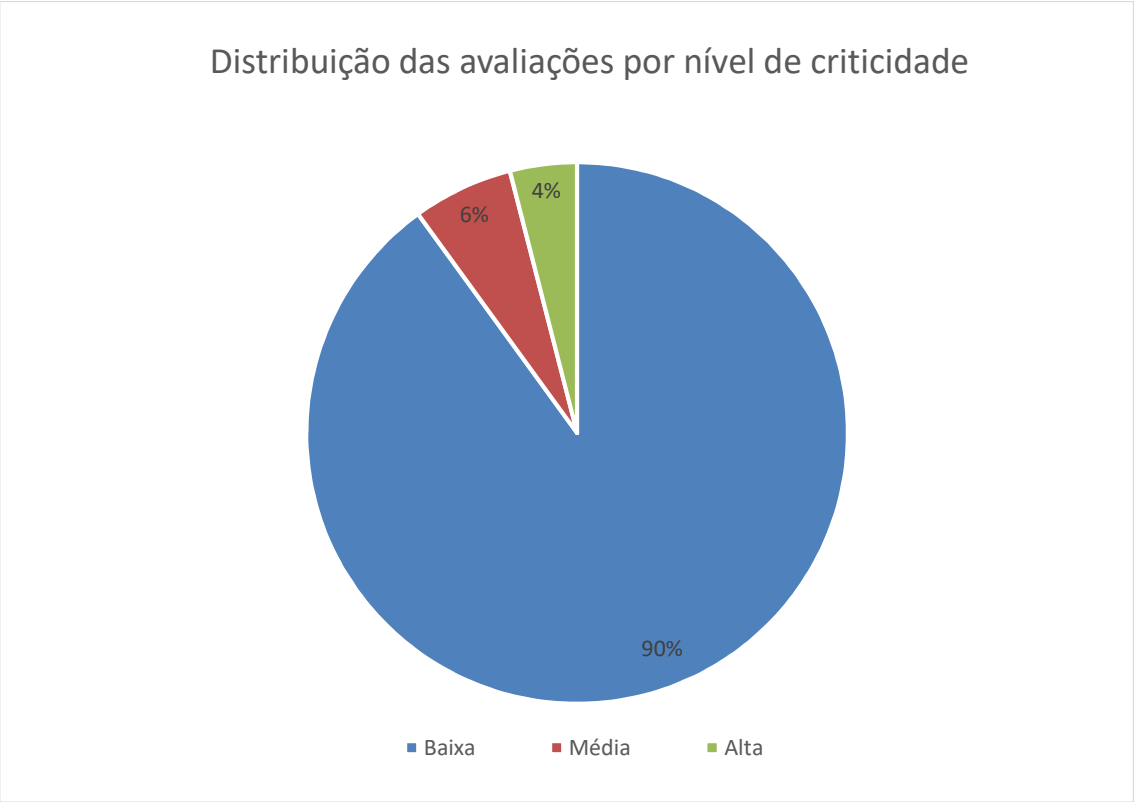

Figura X 1.2.1

X (1.3) – POSSÍVEIS CAUSAS DE NÃO CONFORMIDADE

Outro fator importante para auxiliar o planejamento de ações pelas unidades de negócios da **TG** é a identificação de possíveis causas de não conformidade. Na Figura X 1.3.1 podem ser vistas as distribuições das causas apontadas nas avaliações críticas. Destacam-se, por representarem cerca de 80% das causas identificadas, organização interna da **TG** (não conformidade decorrente de falhas na integração entre unidades e/ou componentes organizacionais), tecnologia da informação (não conformidade decorrente da indisponibilidade de recursos apropriados de TI) e gerenciamento (não conformidade decorrente do gerenciamento no âmbito da própria unidade ou componente organizacional, o qual pode se originar das atividades de planejamento, controle, organização dos recursos, liderança etc).

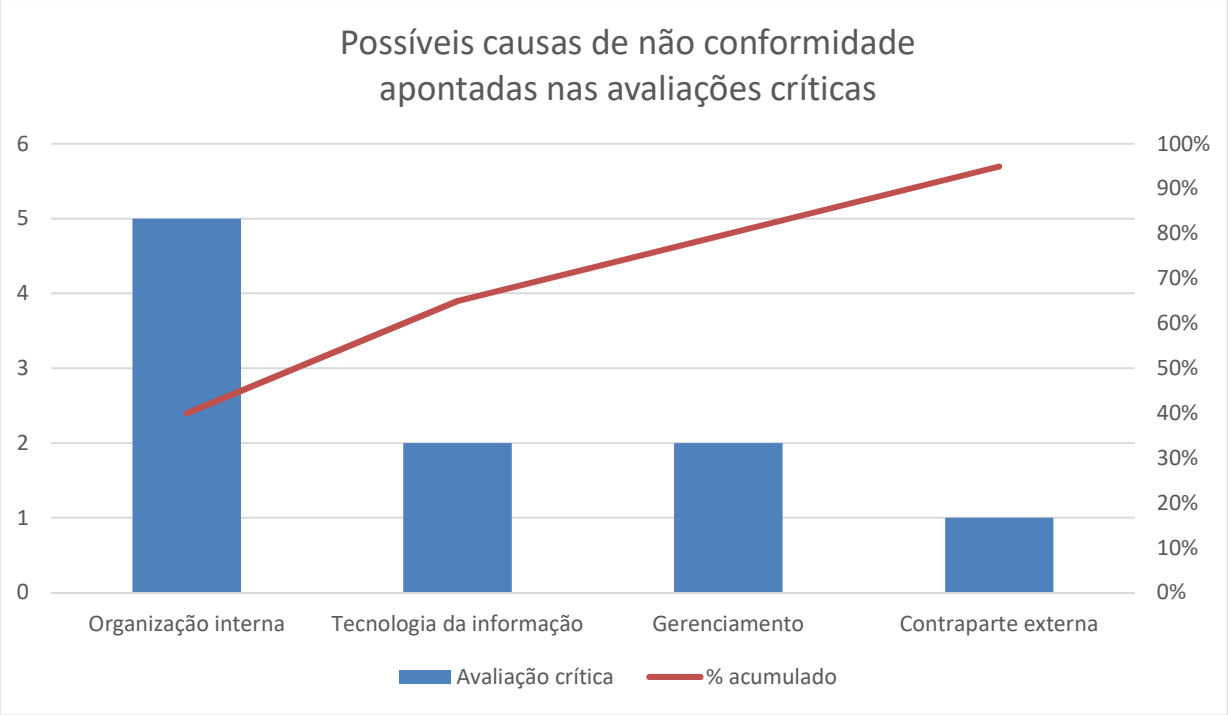

Figura X 1.3.1

A seguir detalhes das possíveis causas de não conformidades indicadas pelas unidades de negócios da **TG** nas avaliações críticas.

Taxonomia de causa	Observações
Organização interna da TG	Está sendo levantada a base de dados pessoais objeto de tratamento pelas áreas da **TG**. Não há informações da **TG** sobre dados tratados de forma automatizada (inteligência artificial, algoritmos, tratamentos sem intervenção humana)
Tecnologia da informação	Deve ser implementada a funcionalidade para distribuição, entre as áreas da **TG**, de dúvidas, pedidos de confirmação de tratamento e acesso a dados, pedidos de retificação de dados.
Gerenciamento	Ainda não definimos os procedimentos para retificações.

Ressalta-se ainda que todas as possíveis causas apontadas nas avaliações críticas já estão sendo tratadas.

X (1.4) – AÇÕES DE CONFORMIDADE

Como resultado das avaliações realizadas, as unidades de negócios da **TG** planejaram 17 ações de conformidade, sendo que 15 (ou 88%) já foram concluídas. Daquele total, 12% referem-se às avaliações críticas, como pode ser visto na Figura X 1.4.1. Destacamos, ainda, que todas as avaliações críticas possuem ações de tratamento em implantação na **TG**.

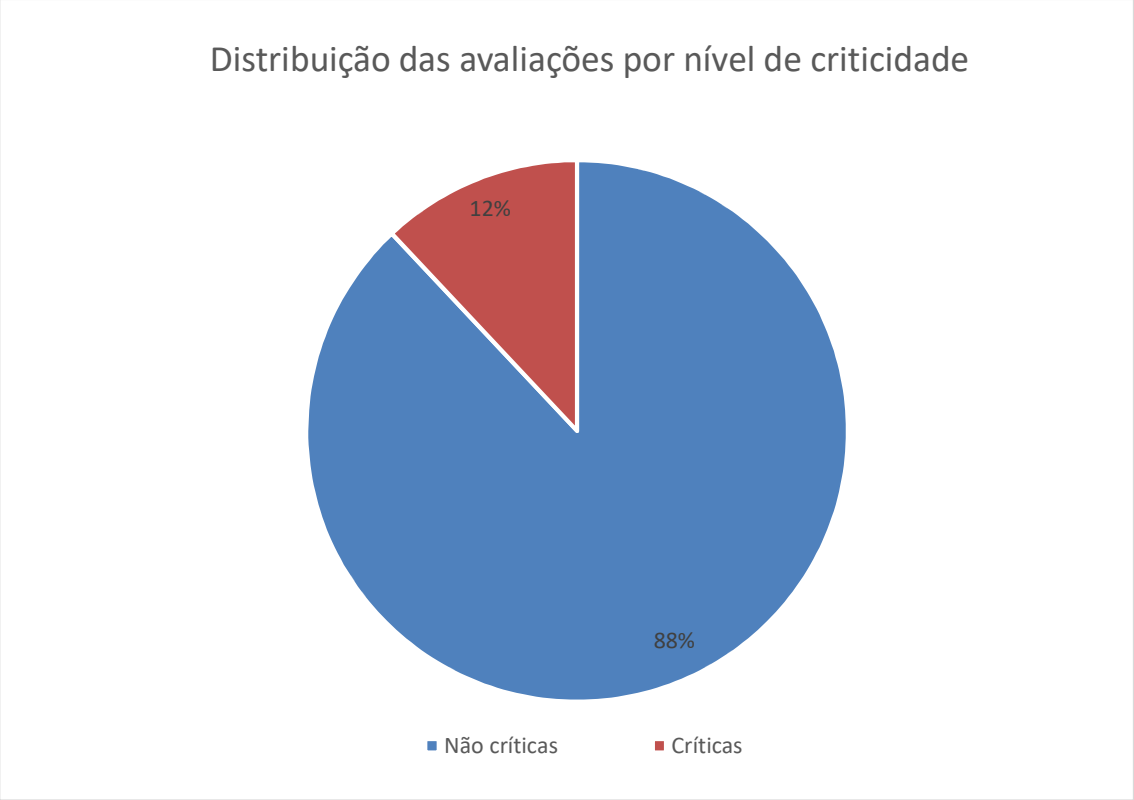

Figura X 1.4.1

XI – CONSIDERAÇÕES FINAIS

Este documento 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 de conformidade da **TG** à LGPD.

Este RIPD será revisto e atualizado anualmente ou sempre que a **TG** implementar qualquer tipo de mudança que afete o tratamento dos dados pessoais. **TG** 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.

XII – APROVAÇÃO

Mogi Guaçu/SP,11 de abril de 2022.

TG Logística e Transportes Ltda
TG (representante do controlador)

DPO (Data Protection Officer)
Encarregado pelo Tratamento de Dados Pessoais