Titulo:

Política de Privacidade e Proteção de Dados Pessoais

Elaborado/Alterado por:

GERÊNCIA DE COMPLIANCE GESTÃO DE RISCOS E CONTROLE INTERNO - GGR

Aprovado por:

Diretoria Colegiada

1. OBJETIVO

Esta Política estabelece as orientações gerais para a proteção de dados pessoais dentro do ambiente corporativo da COMPESA, uma vez que, na execução de suas operações, coleta, manuseia e armazena informações que podem estar relacionadas a pessoas físicas identificadas e/ou identificáveis (“Dados Pessoais”), com vistas a:

- Estar em conformidade com as leis e regulamentações aplicáveis de proteção de Dados Pessoais e seguir as melhores práticas;
- Proteger os direitos dos integrantes, clientes, fornecedores e parceiros contra os riscos de violações de Dados Pessoais;
- Ser transparente com relação aos procedimentos da Companhia no Tratamento de Dados Pessoais; e
- Promover a conscientização em toda a Companhia em relação à proteção de Dados Pessoais e questões de privacidade.

2. APLICAÇÃO

Esta Política é aplicável à Compesa e a todos os parceiros que tenham acesso a quaisquer Dados Pessoais detidos por esta Companhia ou em seu nome. Procedimentos adicionais podem ser criados de acordo com exigência da legislação local.

Qualquer legislação aplicável deve prevalecer caso esteja ou venha a estar em conflito com esta Política.

3. DEFINIÇÕES

3.1 Anonimização: Processo e técnica por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Dado anonimizado não é considerado Dado Pessoal.

3.2 Consentimento: Manifestação livre, informada e inequívoca pela qual o Titular concorda com o Tratamento de seus Dados Pessoais para uma finalidade determinada.

3.3 Controlador: Pessoa jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.

3.4 Dado(s) Pessoal(ais): Qualquer informação relativa a uma pessoa singular identificada ou identificável, que pode ser identificada, direta ou indiretamente, por referência a um identificador como nome, número de identificação, dados de localização, identificador *on-line* ou a um ou mais fatores específicos a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

3.5 Dado(s) Pessoal(ais) Sensível(eis): Todo Dado Pessoal que pode gerar qualquer tipo de discriminação como, por exemplo, os dados 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.

3.6 Encarregado de Proteção de Dados ou *Data Protection Officer* (DPO): O profissional designado como encarregado formal/oficial de proteção de dados, conforme previsto nas leis de proteção de dados, tais como GDPR e LGPD, para um determinado território. O DPO pode ser um colaborador ou uma pessoa terceirizada.

3.7 GDPR: Regulamento (UE) 2016/679 do Parlamento Europeu de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao Tratamento de Dados Pessoais e à livre circulação desses dados e que revoga a Diretiva 95 / 46 / CE (Regulamento Geral de Proteção de Dados).

3.8 LGPD: Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de Tratamento de Dados Pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

3.9 Política de Segurança da Informação: Diretrizes corporativas globais da Compesa sobre Segurança da Informação, conforme normativo GTI-POL-001/Compesa , que podem ser alteradas periodicamente.

3.10 Dado pessoal de criança e adolescente: Dado relativo a pessoas menores de 18 anos.

4. RESPONSABILIDADES

4.1 Gerência de Compliance, Gestão de Riscos e Controle Interno

Manter atualizado a norma conforme definido pela Lei nº 13.709 (Lei Geral de Proteção de Dados) de 14/08/2018 e suas atualizações;

Verificar o atendimento às definições constantes nesta norma;

4.2 Demais unidades organizacionais da Compesa

Atender às determinações inscritas neste documento.

5. DETALHAMENTO

5.1 PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

Esta seção descreve os princípios que devem ser observados na coleta, manuseio, armazenamento, divulgação e Tratamento de Dados Pessoais pela Compesa para atender aos padrões de proteção de dados no âmbito corporativo e estar em conformidade com a legislação e regulamentação aplicáveis onde tiver operação ou atividade comercial.

5.1.1 Legalidade, Transparência e Não Discriminação

I - A Compesa trata os Dados Pessoais de forma justa, transparente e em conformidade com legislação e regulamentação aplicáveis.

II - A Compesa somente trata Dados Pessoais quando o propósito/finalidade do tratamento se enquadra em uma das hipóteses legais permitidas, abaixo elencadas, sendo certo que os Titulares de Dados devem ser informados sobre a razão e a forma pela qual seus Dados Pessoais estão sendo tratados antes ou durante a coleta:

a) necessidade para a execução de um contrato do qual o Titular dos Dados é parte;

b) exigência decorrente de lei ou regulamento ao qual a Compesa está sujeita;

c) interesse legítimo pelo Tratamento, hipótese na qual tal interesse legítimo será comunicado previamente; e

d) necessidade de prover ao Titular dos Dados o exercício regular de direito em processo judicial, administrativo ou arbitral.

III - Quando o Tratamento de Dados Pessoais não se enquadrar nas hipóteses acima, a Compesa deve obter o Consentimento dos Titulares dos Dados para o Tratamento de seus Dados Pessoais e assegurar que este Consentimento seja obtido de forma específica, livre, inequívoca e informada. A COMPESA deve coletar, armazenar e gerenciar todas as respostas de Consentimento de maneira organizada e acessível para que a comprovação de Consentimento possa ser fornecida quando necessário.

IV - Da mesma forma, o Titular de Dados deve ter a possibilidade de retirar o seu Consentimento a qualquer momento com a mesma facilidade que foi fornecido.

V - Em algumas circunstâncias, a Compesa também pode ser obrigada a tratar Dados Pessoais Sensíveis, envolvendo, mas não se limitando, a:

a) dados relacionados à saúde ou à vida sexual;

b) dados genéticos ou biométricos vinculados a uma pessoa física;

c) dados sobre orientação sexual;

d) dados sobre condenações ou ofensas criminais;

e) dados que evidenciem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas; e

f) dados referentes à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

VI - O Tratamento de Dados Pessoais Sensíveis é proibido, exceto nos casos específicos descritos abaixo, nos quais deverão ser observados padrões de segurança mais robustos do que os empregados aos demais Dados Pessoais:

a) quando for necessário para o cumprimento de obrigação legal ou regulatória;

b) quando for necessário para o exercício regular de direitos a exemplo da defesa ou proposição de ações judiciais, administrativas ou arbitrais;

c) quando for necessário para o cumprimento de obrigações e o exercício de direitos em matéria de emprego, previdência social e proteção social;

d) para proteção à vida ou à incolumidade física do Titular do Dado incluindo dados médicos com fins preventivos e/ou ocupacionais;

e) para fins de promoção ou manutenção de igualdade de oportunidades entre pessoas de origem racial ou étnica diferente; e

f) quando o Titular dos Dados tiver dado o seu Consentimento explícito, de acordo com a legislação e regulamentação aplicáveis.

5.1.2 Limitação e Adequação da Finalidade

O Tratamento de Dados Pessoais deve ser realizado de maneira compatível com a finalidade original para a qual os Dados Pessoais foram coletados, não podendo ser coletados com um propósito e utilizados para outro. Quaisquer outras finalidades devem ser compatíveis com a razão original para qual os Dados Pessoais foram coletados.

5.1.3 Princípio da Necessidade (Minimização dos Dados)

A Compesa somente pode tratar Dados Pessoais na medida em que seja necessário para atingir um propósito específico. O compartilhamento de Dados Pessoais com outra área ou outra empresa deve considerar este princípio, só podendo ser compartilhados quando tenham um amparo legal adequado.

5.1.4 Exatidão (Qualidade dos Dados)

A Compesa deve adotar medidas razoáveis para assegurar que quaisquer Dados Pessoais em sua posse sejam mantidos precisos e atualizados em relação às finalidades para as quais foram coletados, sendo certo que deve ser possibilitado ao Titular do Dado Pessoal a possibilidade de requerer a exclusão ou a correção de dados imprecisos ou desatualizados.

5.1.5 Retenção e Limitação do Armazenamento de Dados

A Compesa deve ter conhecimento de suas atividades de Tratamento, dos períodos de retenção estabelecidos e dos processos de revisão periódica, não podendo manter os Dados Pessoais por prazo superior ao necessário para atender as finalidades pretendidas.

5.1.6 Integridade e Confidencialidade (Livre Acesso, Prevenção e Segurança)

A Compesa deve assegurar que medidas técnicas e administrativas apropriadas sejam aplicadas aos Dados Pessoais para protegê-los contra o Tratamento não autorizado ou ilegal, bem como contra a perda acidental, destruição ou danos. O Tratamento de Dados Pessoais também deve garantir a devida confidencialidade. Dentre as medidas técnicas mais comuns, podem ser descritas:

I - Anonimização: os Dados Pessoais são tornados anônimos de tal forma que não mais se referem a uma pessoa direta ou indiretamente identificável. O anonimato tem que ser irreversível;

II - Pseudoanonimização: os Dados Pessoais não mais se relacionam diretamente com uma pessoa identificável (por exemplo, mencionando seu nome), mas não é anônimo porque ainda é possível, com informações adicionais, que são mantidas separadamente, identificar uma pessoa.

5.1.7 Responsabilização e Prestação de Contas

A Compesa é responsável e deve demonstrar o cumprimento desta Política, assegurando a implementação de diversas medidas que incluem, mas que não estão limitadas a:

I - Garantia de que os Titulares dos Dados Pessoais possam exercer os seus direitos;

II - Registro de Dados Pessoais, incluindo:

a) registros de atividades de Tratamento de Dados Pessoais com a descrição dos propósitos/finalidades desse Tratamento, os destinatários do compartilhamento dos Dados Pessoais e os prazos pelos quais a Compesa deve retê-los; e

b) registro de incidentes de Dados Pessoais e violações de Dados Pessoais;

III - Garantia de que os Terceiros que sejam Processadores de Dados Pessoais também estejam agindo de acordo com esta Política e com a legislação e regulamentação aplicáveis;

IV - Garantia de que a Compesa, quando requerido, registre junto à Autoridade Supervisora aplicável um Encarregado de Dados ou DPO; e

V - Garantia de que a Compesa esteja cumprindo todas as exigências e solicitações de qualquer Autoridade de Supervisão à qual esteja sujeita.

5.2 PADRÕES DE SEGURANÇA

5.2.1 Importância da Proteção de Dados Pessoais

A Compesa está comprometida com a implementação dos padrões de Segurança da Informação e com a proteção de Dados Pessoais com vistas a garantir o direito fundamental do indivíduo à autodeterminação da informação.

5.2.2 Garantir a Segurança dos Dados Pessoais

A confidencialidade, integridade e disponibilidade, bem como autenticidade, responsabilidade e não-repúdio são objetivos a serem perseguidos para a segurança dos Dados Pessoais.

5.2.3 Obrigação do Sigilo de Dados Pessoais

Todos os Integrantes com acesso a Dados Pessoais estão obrigados aos deveres de confidencialidade dos Dados Pessoais mediante a anuência ao Código de Conduta e Integridade, quando do ingresso na Compesa e periodicamente, nos termos da Lei nº 13.303/2016.

5.2.4 Privacidade de Dados Pessoais por Concepção e por Padrão

Ao implementar novos processos, procedimentos ou sistemas que envolvam o Tratamento de Dados Pessoais, a Compesa deve adotar medidas para garantir que as regras de Privacidade e Proteção de Dados sejam adotadas desde a fase de concepção até o lançamento/implantação destes projetos.

5.3 DIREITOS DOS TITULARES DE DADOS PESSOAIS

A Compesa está comprometida com os direitos dos Titulares de Dados Pessoais, os quais incluem:

I - Informação, no momento em que os Dados Pessoais são fornecidos, sobre como seus Dados Pessoais serão tratados;

II - Informação sobre o Tratamento de seus Dados Pessoais e o acesso aos Dados Pessoais que a Compesa detenha sobre eles;

III - Correção de seus Dados Pessoais se estiverem imprecisos, incorretos ou incompletos;

IV - Exclusão, bloqueio e/ou anonimização de seus Dados Pessoais em determinadas circunstâncias (“direito de ser esquecido”). Isso pode incluir, mas não se limita a, circunstâncias em que não é mais necessário que a Compesa retenha seus Dados Pessoais para os propósitos para os quais foram coletados;

V - Restrição do Tratamento de seus Dados Pessoais em determinadas circunstâncias;

VI - Opor-se ao Tratamento, se não estiver baseado em legítimo interesse;

VII - Retirar o Consentimento a qualquer momento, se o Tratamento dos Dados Pessoais se basear no Consentimento do indivíduo para um propósito específico;

VIII - Portabilidade dos Dados Pessoais a outro fornecedor de serviço ou produto mediante requisição expressa em determinadas circunstâncias;

IX - Revisão das decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais; e

X - Apresentação de queixa à Compesa ou à Autoridade de Proteção de Dados aplicável, se o Titular dos Dados Pessoais tiver motivos para supor que qualquer um de seus direitos de proteção de Dados Pessoais tenha sido violado.

5.4 TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

O tratamento dos dados pessoais de crianças e adolescentes deve se dar no melhor interesse de seus titulares.

I - Os dados de crianças (menores de 12 anos) normalmente são tratados com o consentimento de, ao menos, um de seus responsáveis legais, com exceção das situações legais em que o consentimento não é exigido, como, por exemplo, na execução de serviço público;

II - A informação sobre o tratamento de dados pessoais sensíveis ou referentes a crianças ou adolescentes estará disponível em linguagem clara e simples, com concisão, transparência, inteligibilidade e acessibilidade, na forma da lei e de acordo com as regras do regime de tramitação sob segredo de Justiça.

5.5 PRESTADORES DE SERVIÇOS TERCEIRIZADOS

Os prestadores de serviços terceirizados que tratem Dados Pessoais sob as instruções da Compesa estão sujeitos às obrigações impostas aos Processadores de acordo com a legislação e regulamentação de proteção de Dados Pessoais aplicáveis. A Compesa deve assegurar que no contrato de prestação de serviço sejam contempladas as cláusulas de privacidade que exijam que o Processador de Dados terceirizado implemente medidas de segurança, bem como controles técnicos e administrativos apropriados para garantir a confidencialidade e segurança dos Dados Pessoais e especifiquem que o Processador está autorizado a tratar Dados Pessoais apenas quando seja formalmente solicitado pela Compesa .

5.6 GERENCIAMENTO DE VIOLAÇÃO DE DADOS

I - Todos os incidentes e potenciais violações de dados devem ser reportadas à **Gerência de Compliance, Gestão de Riscos e Controle Interno (GGR)** da Compesa. Todos os colaboradores devem estar cientes de sua responsabilidade pessoal de encaminhar e escalonar possíveis problemas, bem como de denunciar violações ou suspeitas de violações de Dados Pessoais assim que as identificarem. No momento em que um incidente ou violação real for descoberto, é essencial que os incidentes sejam informados e formalizados de forma tempestiva.

II - Violações de dados incluem, mas não se limitam a, qualquer perda, exclusão, roubo ou acesso não autorizado de dados pessoais controlados ou tratados pela Compesa.

III - O registro e o tratamento de incidentes de segurança da informação que envolvam violação de dados pessoais devem se tratados conforme Plano de Resposta à Incidentes de Dados, anexo I.

IV - A avaliação dos riscos inerentes ao tratamento de dados pessoais bem como as medidas para mitigação dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares dos dados estão descritos em documento próprio intitulado Relatório de Impacto à Proteção dos Dados Pessoais (RIPD), anexo II.

5.7 AUDITORIAS DE PROTEÇÃO DE DADOS

I - A Compesa deve garantir que existam revisões periódicas a fim de confirmar que as iniciativas de Privacidade, seu sistema, medidas, processos, precauções e outras atividades, incluindo o gerenciamento de proteção de Dados Pessoais, são efetivamente implementados e mantidos e estão em conformidade com a legislação e regulamentação aplicáveis.

II - Adicionalmente e, conforme previsto no Normativo AUD-NI-001/Compesa, o tema deve ser avaliado com a devida periodicidade e de acordo com os riscos existentes. Caso os riscos sejam relevantes, a Auditoria Interna (AUD) da Compesa deverá incluir revisão específica independente no plano anual de auditoria interna.

6. INSTRUMENTOS NORMATIVOS RELACIONADOS

- GGR-POL-008: Política de Gestão de Riscos
- GTI-POL-001: Política de Segurança da Informação
- GGR-NI-003: Norma Interna de Gestão de Riscos
- AUD-NI-001: Norma de Auditoria Interna
- Código de Conduta e Integridade COMPESA

7. REFERÊNCIAS

- Constituição da República Federativa do Brasil de 1988;
- Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 13.303, de 30 de junho de 2016: Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;
- Regulamento Geral sobre a Proteção de Dados 2016/679 (GDPR).

8. HISTÓRICO DE ALTERAÇÕES

Nº da Versão	Data	Natureza da Revisão e/ou Alteração	RD vinculada
1	27/01/2021	Emissão inicial	RD 026/2020
2	25/10/2023	Atualização	RD 015/2023

ANEXOS

ANEXO 1 - Anexo I - Plano de Resposta a Incidentes de Segurança e Privacidade
Plano de Resposta revisado e atualizado em abril/2023

ANEXO 2 - Anexo II - Relatório de Impacto à Proteção de Dados - RIPD
Relatório com os riscos revisado em abril/2023

Plano de Resposta a Incidentes de Segurança e Privacidade

LGPD – COMPESA

Sumário

1 Introdução

Este documento define o Plano de Resposta a Incidentes de Segurança e Privacidade [1] da Compesa [2]. O plano descreve a forma como a Compesa vai responder aos incidentes de vazamento de dados pessoais, classificando-os pelo grau de severidade e criticidade. A resposta deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que podem ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência.

1.1 Abrangência

Este plano abrange todos os recursos computacionais pertencentes, operados, mantidos e controlados pela Compesa.

1.2 Glossário

Para o completo entendimento do processo descrito neste plano, é necessário compreender alguns termos técnicos referente a área de segurança da informação. São estes os termos:

- **ANPD**: Autoridade Nacional de Proteção de Dados [3].
- **Backup**: é uma cópia de segurança dos dados (informações) de um dispositivo de armazenamento ou sistema para outro ambiente para que esses mesmos dados possam ser restaurados em caso de perda dos dados originais ou que ocorra um acidente [4].
- **BPMN**: Business Process Model and Notation – é uma representação gráfica feita a partir de ícones que simbolizam o fluxo de processo [5].
- **DevOps**: metodologia que descreve meios que auxiliam a agilizar os processos para levar uma demanda da área de desenvolvimento de software à implantação em um ambiente de produção. Essas demandas podem ser, por exemplo, um novo recurso de software, uma solicitação de aprimoramento ou uma correção de bug [6].
- **DLP**: Data Loss Prevention – é um conjunto de práticas e ferramentas que auxiliam no controle dos dados confidenciais de uma organização para que permaneçam disponíveis para os usuários autorizados e não sejam compartilhados ou disponibilizados para usuários não autorizados [7].
- **DPO**: Data Protection Officer – Encarregado por estabelecer e gerir a comunicação entre a empresa, a ANPD e o titular (dono dos dados pessoais) [8].
- **LGPD**: Lei de Proteção Geral de Dados [9].
- **IP**: Internet Protocol – é o principal protocolo (conjunto de regras) de comunicação da Internet, responsável por endereçar e encaminhar os pacotes de dados que trafegam pela rede mundial de computadores [10].
- **Máquina Virtual:** também conhecido como processo de virtualização, é um programa que simula um ambiente computacional, capaz de executar sistemas operacionais e aplicativos como se fosse uma máquina física [11].
- **Sistema Operacional**: é um software cuja função é administrar e gerenciar os recursos de um sistema estabelecendo a interface entre o computador e o usuário [12].

- **Snapshot**: é o estado de um sistema em um ponto específico no tempo [13].
- **Triagem**: Ato de selecionar registros a fim de dar um tratamento intensivo e rápido para o incidente [14].

2 Definição dos Incidentes

No artigo 5º da LGPD [9] define que o dado pessoal é uma informação relacionada a pessoa natural identificada ou identificável. E, dado pessoal sensível é o dado 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. Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade [15]. Assim, um Incidente com Dados Pessoais é um evento que leva à segurança a destruição, perda, alteração, divulgação ou acesso não autorizados, de forma acidental ou ilícita, a dados pessoais transmitidos, armazenados ou processados pela empresa que possui esses dados armazenados [16].

3 Definição do Fluxo de Tratamento dos Incidentes

Este capítulo define o fluxo de tratamento aos incidentes de segurança e privacidade na Compesa através da especificação dos processos e pessoas envolvidas.

3.1 Atores

Os atores são pessoas que desempenham uma função importante no processo de resposta a incidentes de segurança e privacidade. São esses os atores:

- **Notificador** - pessoa ou sistema de monitoração que notifica incidente.
- **Centro de Operações de Incidentes** – equipe que monitora 24h por dia o registro de incidentes e tem o papel de classificar esses registros pela severidade e categoria (privacidade ou de segurança) bem como realizar a triagem dos incidentes que serão repassados ao Time de Resposta a Incidentes Críticos.
- **Comitê LGPD** – analisa registros de incidentes, interage com diversos atores e coordena a operação de tratamento.
- **Responsável pelo Sistema** – pessoa que responde pelo sistema que está envolvido no incidente.
- **Encarregado pelo Tratamento de Dados Pessoais (DPO)** - responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais.
- **Time DevOps** – profissionais das áreas de desenvolvimento e operações que atuam em equipe no desenvolvimento e instalação de soluções.

3.2 Processos

Um processo é um conjunto de atividades e comportamentos executados por humanos ou sistemas computacionais para alcançar um ou mais resultados [17]. Os processos possuem atividades que agregam valor para os clientes ou apoiam ou gerenciam outros processos. Na figura 1, há um diagrama BPMN que se refere aos processos necessários para resposta aos incidentes de segurança relativo a problemas com dados pessoais.

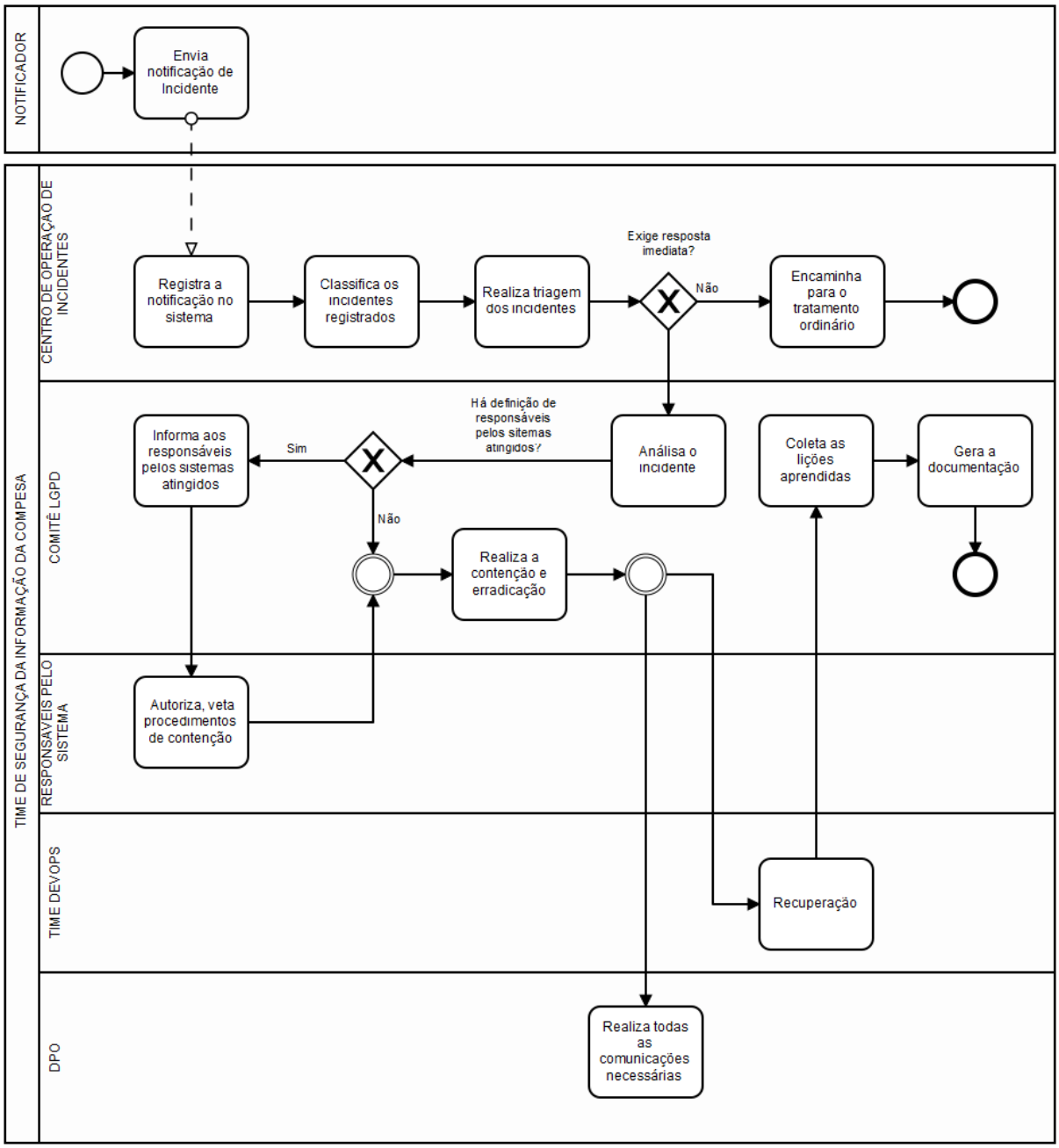


FIGURA 1 DIAGRAMA BPMN DO PROCESSO DE RESPOSTA A INCIDENTES.

3.2.1 Inicio

Um registro de incidente pode ser realizado por uma pessoa, interna ou externa a Compesa, ou de forma automática através de um Sistema computacional de Prevenção a Vazamento de Dados (DLP). Quando o registro de incidente é realizado, a notificação é recebida pela equipe do Centro de Operação de Incidentes.

3.2.2 Triagem

O Centro de Operação de Incidentes deve fazer uma classificação preliminar da severidade e categoria do incidente. Posteriormente, uma triagem deverá ser realizada a fim de selecionar quais são os incidentes que necessitam de resposta imediata. Esses registros são então repassados para o Comitê LGPD para que seja realizado o tratamento devido.

3.2.3 Análise

Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases. Nesse momento, deve-se engajar especialistas dos sistemas afetados para colaborar com a análise.

Nessa fase, o Comitê Gestor de Dados Pessoais deve avaliar e decidir sobre comunicar o incidente para a Autoridade Nacional de Proteção de Dados Pessoais – ANPD bem como aos titulares dos dados. Essa decisão deve ser pautada na matriz de riscos constante no Relatório de Impacto à Proteção de Dados Pessoais – RIPD (Anexo 1) e sob a ótica do Art. 48 da LGPD. Para fins de referência, todos os eventos enquadrados no nível de impacto extremo dessa matriz devem ser comunicados à ANPD. A comunicação deve ser realizada conforme item 3.2.8.

3.2.4 Contenção e Erradicação

O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas computacionais afetados a fim de evitar mais danos. Conforme a necessidade e a autorização obtida, serão realizados o desligamento dos sistemas ou de funcionalidades especificas e a publicação de avisos de indisponibilidade para manutenção. Todas ações devem ser realizadas tomando os cuidados possíveis para não comprometer as evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança. Durante o processo de contenção e erradicação, devem ser acionados os responsáveis pelos sistemas impactados, conforme indicado em documentação, que irão orientar e se manifestar sobre os procedimentos de contenção e erradicação. Serão realizados backup (*snapshots*) dos sistemas computacionais para a análise posterior.

3.2.5 Recuperação

A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema. Caso exista Plano de Continuidade de Negócio dos sistemas impactados, eles devem ser iniciados, conforme especificado. O Comitê LGPD tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação. Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas. Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

3.2.6 Lições Aprendidas

Consiste em se avaliar o processo de tratamento do incidente e verificar a eficácia das soluções adotadas. Deve-se relacionar e documentar no chamado do incidente as falhas e os recursos inexistentes ou insuficientes, para que sejam providenciados em futuras ocasiões. A partir da mitigação do incidente e sua resolução, deve ser conduzido o apanhado de lições aprendidas com outros atores se necessário. As lições aprendidas têm como objetivo de discutir erros e dificuldades encontradas na mitigação do evento ocorrido, propor melhoria na infraestrutura computacional e para os processos de resposta a incidentes. A área afetada deve ser comunicada das decisões tomadas para prevenção de incidentes da mesma natureza, caso se tenha consenso de implementar melhorias na infraestrutura de segurança.

3.2.7 Documentação

O Time de Resposta a Incidentes Críticos deve documentar o incidente em uma base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

3.2.8 Comunicações

Assim que possível, no caso de incidente com dados pessoais e após avaliação do Comitê da LGPD, o Encarregado de Tratamento de Dados (DPO) deverá realizar as comunicações obrigatórias por Lei, bem como informar e subsidiar os Encarregados de Tratamento de Dados dos controladores do sistema.

A comunicação para ANPD deve utilizar formulário próprio disponibilizado por aquela autoridade e enviado por meio do canal específico para peticionamento. Outras comunicações direcionadas aos titulares dos dados também podem ser consideradas, nesse caso, o evento será analisado sob a ótica do Art. 48 da LGPD.

4 Conclusão

Este Plano de Resposta a Incidentes visa atender os preceitos estabelecidos na Lei 13.709/2018 - LGPD bem como dar uma resposta rápida e confiável aos incidentes identificados por esta Companhia. A

Compesa se compromete a manter este documento sempre atualizado para acompanhar as mudanças na área tecnológica e de processos da empresa.

5 Referências

1. ALLEASY. Plano de respostas a incidentes: quais são as suas fases?, 2020. Disponivel em: <https://www.alleasy.com.br/2020/02/10/plano-de-respostas-a-incidentes-fases/>. Acesso em: 22 out. 2021.

2. COMPESA. História e Perfil. Disponivel em: <https://servicos.compesa.com.br/historia-e-perfil/>. Acesso em: 22 out. 2021.

3. GOV.BR. Autoridade Nacional de Proteção de Dados. **ANPPD - Português**. Disponivel em: <https://www.gov.br/anpd/pt-br>. Acesso em: 22 out. 2021.

4. COSSETTI, M. C. O que é backup? [E como fazer]. **tecnoblog.net**. Disponivel em: <https://tecnoblog.net/285077/o-que-e-backup/>. Acesso em: 22 out. 2021.

5. TOTVS. Como funciona e quais as vantagens da notação BPMN? **TOTVS**, 2020. Disponivel em: <https://www.totvs.com/blog/gestao-industrial/bpmn/>. Acesso em: 22 out. 2021.

6. RED HAT, INC. Mas o que é DevOps mesmo? **Tópicos Sobre TI da Red Hat**. Disponivel em: <https://www.redhat.com/pt-br/topics/devops>. Acesso em: 22 out. 2021.

7. LEADCOMM. O QUE É DLP - DATA LOSS PREVENTION e como posso proteger minha empresa. **Leadcomm - Trusted Digital Security**. Disponivel em: <https://leadcomm.com.br/2020/09/16/o-que-e-data-loss-prevention-dlp-e-como-posso-proteger-minha-empresa/>. Acesso em: 22 out. 2021.

8. ALGAR TECH S.A. O que é Data Protection Officer e o que tem a ver com a LGPD? **Algar Tech Blog**. Disponivel em: <https://algartech.com/pt/blog/o-que-e-o-data-protection-officer/>. Acesso em: 22 out. 2021.

9. GOV.BR. Lei Geral de Proteção de Dados Pessoais (LGPD). **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 22 out. 2021.

10. PISA, P. O que é IP? **techtudo**. Disponivel em: <https://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html>. Acesso em: 22 out. 2021.

11. GOGONI, R. O que é uma máquina virtual? **tecnoblog.net**. Disponivel em: <https://tecnoblog.net/302438/o-que-e-uma-maquina-virtual/>. Acesso em: 22 out. 2021.

12. GOGONI, R. O que é um sistema operacional? **tecnoblog.net**. Disponivel em: <https://tecnoblog.net/303055/o-que-e-um-sistema-operacional/>. Acesso em: 22 out. 2021.

13. RENNER, S. Backup e storage snapshots: Como funcionam juntos para a corporação em operação constante. **Veeam Blog**. Disponivel em: <https://www.veeam.com/blog/pt-br/how-snapshots-backups-work-together.html>. Acesso em: 22 out. 2021.

14. TIFLUX. Porque fazer a triagem das solicitações é importante. **Tiflux Blog**, 2019. Disponivel em: <https://tiflux.com/blog/triagem-das-solicitacoes/>. Acesso em: 22 out. 2021.

15. UFRJ.BR. Incidentes de Segurança da Informação. **Diretoria de Segurança da Informação**. Disponivel em: <https://www.security.ufrj.br/denuncie-um-incidente/>. Acesso em: 22 out. 2021.

16. LGPD BRASIL. Ocorreu um incidente de segurança com dados pessoais. E agora? **lgpdbrasil.com.br**, 2021. Disponivel em: <https://www.lgpdbrasil.com.br/ocorreu-um-incidente-de-seguranca-com-dados-pessoais-e-agora/>. Acesso em: 22 out. 2021.

17. ZEEV. Guia completo sobre o que é BPM e BPMS e o que isso tem a ver com Gestão por Processos. **Zeev Blog**. Disponivel em: <https://blog.zeev.it/saiba-o-que-e-bpm-e-bpms-e-o-que-isso-tem-a-ver-com-gestao-de-processos/>. Acesso em: 22 out. 2021.

6 Histórico de Revisões

Data	Versão	Descrição	Autor
Agosto/2021	1.0	Versão inicial do Plano de Respostas	Alixandro Pereira de Jesus - AUD
Abril/23	1.1	Revisão, sem alteração. Inclusão como anexo na Política de Privacidade e Proteção de Dados Pessoais.	Luciana Rebouças Campelo - GGR

RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

(RIPD)

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	
Companhia Pernambucana de Saneamento - Compesa	
Operador	
Companhia Pernambucana de Saneamento - Compesa	
Encarregado - DPO	
Anderson Santos Quadros	
Autoridade Representante do Controlador	
Romildo Bezerra Porto	Presidente
E-mail Encarregado	**Telefone Encarregado**
lgpd@compesa.com.br	(81) 3412-9206

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Segundo o inciso XVII do art. 5º da LGPD, o RIPD é uma documentação que deve ser mantida pelo Controlador dos dados pessoais, conforme segue:

> *Art. 5º Para os fins desta Lei, considera-se:*
>
> *...*
>
> *XVII - relatório de impacto à proteção de dados pessoais: 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;*

O presente RIPD foi elaborado, oportunamente, considerando a hipótese prevista no Art. 38 da Lei 13.709/2018 – LGPD:

> *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.***

Este documento foi elaborado em via única em virtude de outros documentos internos, já construídos no âmbito da adequação à LGPD, possuírem informações complementares acerca do fluxo e tratamento de dados pessoais nos diversos

setores da empresa.

Para tanto, a construção do RIPD perpassou pelas seguintes etapas:

Figura 1 – Etapas construção do RIPD.

3 – DESCRIÇÃO DO TRATAMENTO

O art. 5º, X da LGPD 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”.

Na Compesa são tratados dados de três grupos de usuários sendo:

a) clientes;

b) colaboradores e

c) fornecedores.

A análise específica sobre o tratamento em cada grupo está descrita no mapeamento do fluxo de dados com foco nos processos de negócio da empresa.

3.1 – NATUREZA DO TRATAMENTO

A natureza representa como a instituição trata os dados pessoais, para melhor entendimento esse item vai ser dividido em tópicos, de acordo com cada grupo: clientes, colaboradores e fornecedores.

Clientes – os dados dos clientes são coletados diretamente desses, ou seja, a fonte é o próprio titular dos dados, através dos canais de atendimento da empresa sendo:

a) lojas de atendimento;

b) canal 0800;

c) e-mails;

d) loja virtual;

e) aplicativo Compesa Mobile; e

f) entre outros canais.

Esses dados são armazenados em banco de dados e utilizados nos sistemas corporativos internos, principalmente no Sistema Integrado de Gestão de Serviço de Saneamento (GSAN). Os dados são operados principalmente pelas gerências fins, com a finalidade da operacionalização dos serviços contratados, e pelas unidades de atendimento, cadastro, faturamento e cobrança. São compartilhados dados estritamente necessários para consecução do contrato firmado entre as partes e, por fim, são eliminados seguindo os critérios da tabela de temporalidade disponível no portal de privacidade da empresa.

Colaboradores – os dados dos colaboradores são coletados quando da contratação destes, inicialmente armazenados em meio físico, posteriormente transcritos e digitalizados para os servidores da Compesa. Os dados são tratados e operados principalmente pela área de Recursos Humanos, Gerência de Gestão de Pessoas (GGP) e, em alguns casos, pelas Unidades de Negócios (gerências descentralizadas). Além daqueles compartilhamentos de cunho obrigatórios pela legislação trabalhista, são compartilhados dados com empresas de seguro, instituições financeiras, empresas de vale transporte, vale alimentação, operadoras

de planos de saúde e previdência social privada, sempre à pedido e com o consentimento dos titulares dos dados, já a eliminação ocorre seguindo a tabela de temporalidade.

Fornecedores - neste grupo são coletados dados dos representantes legais para elaboração dos contratos e dos empregados com cessão de mão de obra, para evidências de prestação de serviços. São armazenados nos servidores da Compesa e utilizados nos sistemas corporativos. De forma geral, não há compartilhamento de dados do agrupamento fornecedores, a exceção daqueles previstos na Lei de Acesso a Informação. Os dados são operados pelas unidades de contratos, fiscal e financeira. Já a eliminação, assim como os dois grupos anteriores, segue a tabela de temporalidade.

Mais detalhes sobre forma de coleta, operadores, tratamento e eliminação estão disponíveis no inventário de dados e nos mapeamentos do fluxo de dados pessoais.

3.2 – ESCOPO DO TRATAMENTO

Conforme destacado no item anterior, o escopo do tratamento de dados ocorre dentro dos três agrupamentos: **clientes, fornecedores e colaboradores**, com escopos distintos tanto do ponto de vista geográfico quanto em volume de dados.

Nesse contexto, o quadro 1, a seguir, estratifica o grupo “clientes” de acordo com os dados cadastrais dos sistemas corporativos da Compesa.

Quadro 1 – estratificação dos clientes da Compesa.

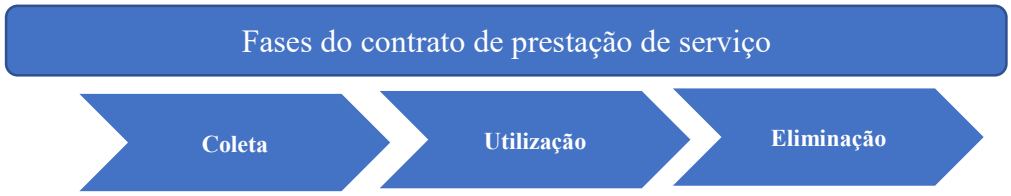
Ordem	Perfil Imóvel	Categoria Principal	Qt. Imóveis	Qt. Economia	Qt. Moradores
1	CORPORATIVO	COMERCIAL	207	4.882	71.683
2	CORPORATIVO	INDUSTRIAL	71	72	6.554
3	CORPORATIVO	PUBLICO	179	269	74.979
4	CORPORATIVO	RESIDENCIAL	799	99.420	188.627
5	GRANDE	COMERCIAL	1.007	11.138	121.113
6	GRANDE	INDUSTRIAL	154	201	5.800
7	GRANDE	PUBLICO	953	1.235	186.240
8	GRANDE	RESIDENCIAL	4.987	130.219	349.965
9	NORMAL	COMERCIAL	125.181	144.953	777.126
10	NORMAL	INDUSTRIAL	5.648	5.726	53.005
11	NORMAL	PUBLICO	15.222	15.943	557.904
12	NORMAL	RESIDENCIAL	2.278.936	2.532.030	6.379.112
13	TARIFA SOCIAL	RESIDENCIAL	71.818	72.007	191.755
Total			2.505.162	3.018.095	8.963.863

Fonte: GSAN em 18/04/2023.

A LGPD estabeleceu o regramento para a proteção de dados de pessoas naturais, portanto, o presente trabalho tem foco nos itens 12 e 13 já em destaque no quadro acima. Ressalta-se que são solicitados apenas os dados do titular do contrato. Até a data de elaboração deste documento, a Compesa presta serviço no estado de Pernambuco, portanto possui abrangência estadual.

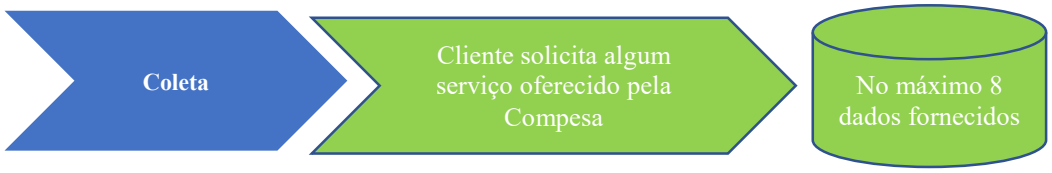
De forma geral, os dados pessoais coletados dos clientes são aqueles suficientes para operacionalização do contrato de prestação de serviço, não sendo possível tal atividade sem o tratamento dos referidos dados. Dessa forma, o ciclo tem início a pedido do próprio titular dos dados pessoais, conforme demonstrado na Imagem 1, a seguir.

Imagem 1: Fases do Contrato de Prestação de Serviço



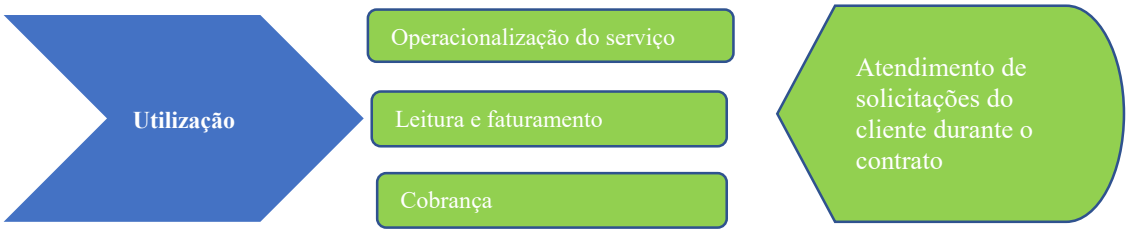
A Compesa é uma concessionária de serviço público e o instrumento contratual padrão é o contrato de adesão, assim o cliente aceita os termos desse instrumento quando da contratação dos serviços e nesse momento é necessário fornecer os dados pessoais, conforme demonstrado na Imagem 2, a seguir:

Imagem 2: Coleta de Dados dos Clientes



De forma quantitativa, são solicitados 8 (oito) dados pessoais de clientes, sendo: a) nome; b) endereço; c) telefone; d) e-mail; e) sexo; f) RG; g) CPF; h) dados bancários. Após o fornecimento dos dados pessoais, as informações são inseridas no sistema GSAN e posteriormente seguem para a próxima fase de tratamento, conforme evidenciado na Imagem 3, a seguir:

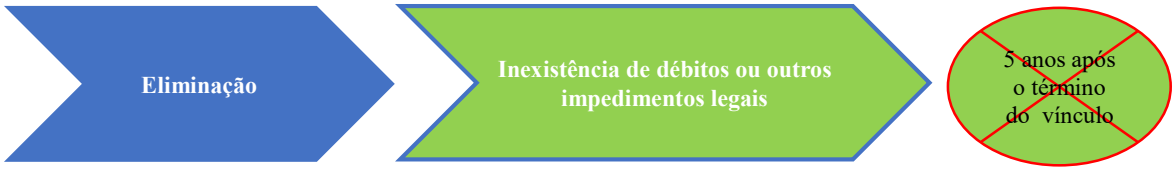
Imagem 3: Operacionalização dos Dados dos Clientes



A utilização é uma fase interna de tratamento de dados e normalmente a mais extensa, ela existirá enquanto o cliente mantiver o contrato com a empresa. Conforme pode se depreender da ilustração acima, o tratamento ocorre por operadores distintos, seja do ponto de vista operacional (quando da instalação de uma ligação de água) seja na fase de cobrança, nessa etapa são necessários compartilhamentos de informações com empresas parceiras, que realizam os serviços terceirizados mediante contrato e com responsabilidade sobre o uso dos dados pessoais compartilhados exclusivamente para operacionalização dos serviços, inclusive com cláusulas específicas referente à LGPD nos contratos.

A próxima fase de tratamento de dados é a eliminação, conforme apresentado na imagem 4, a seguir. Essa etapa segue alguns condicionantes para que ocorra de forma automática, a primeira é a inexistência/encerramento de relação contratual durante um dado período de tempo, para o caso de clientes 5 (cinco) anos, após esse período é necessário que não exista pendências entre as partes, para que os dados sejam efetivamente eliminados do banco de dados.

Imagem 4: Eliminação dos Dados dos Clientes



Cabe destacar que a eliminação dos dados segue os parâmetros definidos na tabela de temporalidade, salvo por determinação judicial diferente.

Já no agrupamento de colaboradores, a abrangência é estadual em virtude dos contratos mantidos com os diversos municípios pernambucanos consequentemente são contratados colaboradores para diferentes locais do estado. Os dados coletados, para empregados próprios, são aqueles necessários

para contratação via Consolidação das Leis do Trabalho (CLT), além daqueles requeridos para contratação por meio de concurso público. No caso de empregados terceirizados, são solicitados dados para confirmação da prestação do serviço, para acesso aos sistemas corporativos da Companhia e/ou para controle interno.

De forma quantitativa, são solicitados 7 (sete) dados pessoais de colaboradores terceirizados sendo: a) nome; b) cadastro de pessoas físicas (CPF); c) registro geral (RG); d) data de nascimento; e) sexo; f) endereço de e-mail; e g) número do telefone. Para os empregados próprios e os empregados em comissão (ad nutum)[1] são coletados 16 (dezesseis) dados pessoais: a) nome; b) sexo; c) registro geral (RG); d) cadastro de pessoas físicas (CPF); e) endereço residencial; f) número do telefone; g) endereço de e-mail; h) profissão; i) filiação; j) estado civil; l) dados bancários; m) título eleitoral; n) certificado de reservista; o) foto; e p) certidões negativas criminais estaduais e federais. Os colaboradores terceirizados e próprios são distribuídos nos quantitativos, demonstrados no Quadro 2, a seguir:

Quadro 2 – quantidade de colaboradores ativos da Compesa

Quadro de colaboradores	
Empregados próprio	3.053
Empregados terceirizados	3.212
Total	6.265

Fonte: Humanus/SIC em 12/04/2023

Além do quantitativo listado acima, a Compesa mantém dados de colaboradores que já não fazem parte do seu quadro funcional, conforme disposta na tabela de temporalidade, essas informações precisam ser armazenadas por 5 anos. Nessa conjuntura, estão armazenados dados de 671 empregados próprios e 41 empregados em comissão.

Já as fases de tratamento se assemelham àquelas relacionadas aos clientes, onde a necessidade de coleta ocorre por força de instrumento contratual e a eliminação se dá após um período de tempo definido na tabela de temporalidade, conforme demonstrado na imagem 5, a seguir.

[1] Os Empregos em Comissão, ad nutum, são aqueles de livre nomeação e exoneração, podendo ser ocupados por qualquer pessoa, servidor público ou não (Regimento Interno da Compesa 2021, Art. 13 § 2º).

Imagem 5 – Fluxo da coleta, armazenamento e eliminação dos dados

Inicialmente, os dados são coletados via formulários próprios e posteriormente inseridos em banco de dados da empresa. São compartilhados com órgãos públicos como, Receita Federal do Brasil; Ministério do Trabalho e Emprego; Instituto Nacional do Seguro Social; Caixa Econômica Federal, entre outros, por força da legislação trabalhista brasileira e com outros atores a pedido do próprio empregado como instituições financeiras, operadoras de planos de saúde, entre outros. Nesse agrupamento, os dados ficam disponíveis na escala 24x7 (24 horas e 7 dias por semana), porém são tratados no horário comercial. Já a eliminação segue os parâmetros da tabela de temporalidade.

Por fim, no agrupamento fornecedores são coletados dados pessoais dos representantes legais das empresas contratadas, nesse caso, a abrangência geográfica pode ser nacional de acordo com a origem do contratado. As informações são coletadas junto aos titulares dos dados na fase da contratação e são armazenadas na rede interna da Companhia. Alguns dados são publicizados, conforme preconiza a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso a Informação). Em casos específicos (cessão de mão de obra) são solicitados comprovantes de pagamentos salariais e guias de tributos a fim de mitigar o risco de ações trabalhistas subsidiárias contra a Compesa.

De forma quantitativa, são solicitados no máximo 9 (nove) dados pessoais (nome, endereço, RG, CPF, telefone, estado civil, profissão, sexo e, quando o fornecedor é pessoa física, dados bancários).

Atualmente existem 497 (quatrocentos e noventa e sete) contratos ativos na Compesa e mais 1.764 (um mil, setecentos e sessenta e quatro) encerrados nos últimos 5 anos. Sendo assim, considerando que cada contratado possui ao menos um representante legal, então existem informações de ao menos 2.261 (duas mil, duzentos e sessenta e uma) pessoas.

3.4 – FINALIDADE DO TRATAMENTO

O principal motivo para tratamento de dados ocorre em função da execução de instrumentos contratuais, onde a parte interessada (titular de dados) fornece as informações necessárias ao Controlador para que este venha a prestar-lhes serviços. No caso dos agrupamentos colaboradores e fornecedores o motivo é o mesmo, alterando-se a ordem de interesses. Portanto, conforme preconiza o inciso V, Art. 7º da LGPD, tal hipótese não carece de consentimento do titular dos dados. Outra finalidade existente é aquela prevista no inciso III, também do Art. 7º da LGPD, que trata da instrumentalização de políticas públicas, principalmente para a população em maior vulnerabilidade social, a exemplo da oferta da tarifa social para aqueles que fazem parte dos extratos sociais de baixa renda, ou seja, população hipossuficiente.

O retorno esperado para as partes interessadas é o alcance do objeto contratual, isto é, a materialização do ato jurídico perfeito, o que para os clientes representa o recebimento do serviço prestado, para os colaboradores operacionalização dos contratos de trabalho e para os fornecedores a prestação do serviço e/ou venda de alguma mercadoria.

4 – PARTES INTERESSADAS CONSULTADAS

A Companhia optou por realizar as adequações à LGPD por meio de uma comissão multidisciplinar formada por membros das principais áreas impactadas pelos efeitos da Lei em tela, sendo: a) Tecnologia da Informação; b) Recursos Humanos; c) Comercial; d) Jurídico; e) Compliance e f) Governança. Através dessa comissão foram consultadas diversas gerências (muitas dessas operadoras de dados no âmbito interno), para confirmar a necessidade dos dados coletados, a viabilidade de implantação de controles, a descontinuação do uso de dados.

A comissão citada acima tornou-se o Comitê Gestor de Proteção de Dados Pessoais, órgão colegiado e permanente na estrutura da Companhia, presidido pelo *Data Protection Officer* (DPO) e com atribuições previstas em regimento interno próprio. A principal responsabilidade é deliberar sobre ações que tenham impacto em toda a empresa.

No âmbito externo, a Secretaria da Controladoria Geral do Estado de Pernambuco (SCGE/PE) foi consultada para dirimir eventuais dúvidas tais como acúmulo de funções do DPO, formas de monitoramento externo, entre outras.

5 – NECESSIDADE E PROPORCIONALIDADE

De forma geral, o tratamento de dados realizado pela Compesa encontra guarida no Art. 7º, inciso V da LGPD:

> *Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
>
> *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;*

Dessa forma, todos os dados coletados são necessários para execução das atividades estabelecidas nos respectivos instrumentos contratuais. Assim, os dados são tratados de acordo com os agrupamentos já citados nos itens anteriores (clientes, colaboradores e fornecedores), onde para atender aos clientes são coletados dados residenciais (para instalação de redes e ramais), nome e Cadastro de Pessoa Física (com a finalidade de realização de cobrança), telefone e endereço de e-mail (para o contato e atendimento).

Já para os colaboradores, conforme disponibilizado no inventário de dados, são coletadas informações pessoais para cumprimento da legislação fiscal e trabalhista (nome, endereço, cadastro de pessoa física, cadastro nacional de informações sociais - CNIS, carteira de trabalho e previdência social - CTPS, remuneração, entre outros) e outras relacionadas ao Direito (certidões criminais, eleitorais, entre outros). No caso de fornecedores, são coletados dados de identificação dos representantes legais e para comprovação do cumprimento das responsabilidades trabalhistas por parte das empresas contratadas, ambos os casos (colaboradores e fornecedores) também são regidos por instrumentos contratuais.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

a) Identificação dos riscos

O ponto de partida inicial para identificação dos riscos foi o trabalho de mapeamento dos processos realizado através do projeto “aprimoramento dos macroprocessos e conformidade da gestão da Compesa” que foi finalizado no ano de 2019, através desse projeto foram identificados e mapeados 25 (vinte e cinco) processos de negócios envolvidos nas atividades da empresa. Nesse trabalho foram identificadas as principais atividades das unidades que compõem o processo. Esse projeto foi revisitado em 2022/2023 e suas premissas reaplicadas, inclusive com revisão e inclusão de 5 novos riscos e entre eles, o risco de vazamento de dados - LGPD. Dessa forma, além do mapeamento das informações pessoais, foi possível identificar fragilidades existentes na execução das atividades, com ênfase na LGPD, bem como seus riscos inerentes.

A metodologia de captura de informações foi a mesma utilizada para mapear os processos de negócio, sendo entrevistas com colaboradores chave e análise documental. Tal método mostrou-se o mais aderente tendo em vista que já se sabia quais atividades eram desenvolvidas nas áreas entrevistadas, cabendo apenas o detalhamento dessas atividades com enfoque no fluxo de dados pessoais.

O mapeamento de processos possibilita a identificação dos problemas nos processos e dos riscos a estes relacionados, visando a sua associação futura a atividades de controle que mitiguem o potencial de materialização dos riscos levantados, criando ações preventivas e/ou corretivas para melhor funcionamento dos processos da organização. Adicionalmente, dentro de um contexto empresarial de que a atividade será executada e explorada, é importante ressaltar que um risco não pode ser eliminado, sempre irá existir, podendo ser transferido, reduzido ou aceito, mediante efetivo gerenciamento.

Desta forma, com a identificação, a análise e o endereçamento dos riscos relacionados, cabe aos responsáveis dos processos gerenciá-los e/ou mitigá-los para evitar uma materialização indesejada e seus impactos nos processos a que se relacionam. Nesse contexto, o mapeamento foi realizado com enfoque nos fluxos dos dados, consequentemente os riscos identificados também tiveram ênfase nas adversidades ligadas aos dados pessoais.

A seleção das unidades a serem entrevistadas ocorreu após a elaboração de um formulário on-line, o qual foi distribuído para todas as gerências da Companhia, o intuito principal da pesquisa foi identificar quais unidades realizavam tratamento de dados pessoais, quais dados eram capturados e como eram armazenados. Apesar da limitação inicial em decorrência do tema ser ainda abstrato para a maioria, os resultados foram excelentes e serviram como uma das diretrizes para este mapeamento.

b) Avaliação dos riscos

No que concerne a avaliação dos riscos, atualmente já existe, dentro da Companhia, um programa de gestão de riscos implantado, ele conta com políticas, normas, papéis e responsabilidades já institucionalizados. Dessa forma, o gerenciamento dos riscos que envolvem o tratamento de dados pessoais foi trabalhado na mesma metodologia e sistemática já desenvolvida na Compesa de forma que haja simetria e sinergia entre os trabalhos realizados.

Assim, na metodologia de gerenciamento de riscos adotada pela Compesa são considerados dois critérios para avaliação dos riscos: o impacto e a vulnerabilidade, mais detalhados adiante.

Já os parâmetros escalares adotados na Política de Gestão de Riscos para enquadramento nos critérios de impacto e vulnerabilidade são divididos em quatro níveis: a) baixo; b) médio; c) alto e d) extremo. Também foram atribuídos quantificadores para ilustração do grau de exposição ao risco em termos quantitativos conforme demonstrado no quadro 3, a seguir:

Quadro 3 – Quantificadores para disposição do nível do risco

Classificação	Valor
Baixo	5
Médio	10
Alto	15
Extremo	20

Fonte: Análise Geral de Riscos Compesa 2019 (adaptada).

Para fins de mensuração dos eventos de riscos que envolvem a proteção de dados

pessoais, a dimensão “impacto” foi avaliada de acordo com o volume de dados a qual o evento está atrelado. Ou seja, quanto maior o volume de dados tratados maior foi a classificação dada na escala. Além disso, o tratamento de dados considerados sensíveis recebeu a classificação de impacto extremo em virtude do potencial de dano à empresa e ao próprio titular do dado, conforme apresentado no quadro 4, a seguir.

Quadro 4 – Critérios para definição do nível de impacto

Impacto	Critérios para avaliação do impacto
Extremo	Tratamento ou possibilidade de tratamento de todo banco de dados da empresa e/ou acesso a dados sensíveis coletados pelo controlador.
Alto	Tratamento ou possibilidade de tratamento de parte limitada dos dados contidos no banco de dados do controlador (ex. dados pessoais de uma determinada localidade).
Médio	Tratamento de dados de forma individual e/ou compartilhamento com outras áreas.
Baixo	Tratamento de dados de forma individual.

Fonte: Análise Geral de Riscos Compesa 2019 (adaptada).

Já para avaliação da vulnerabilidade foram utilizados critérios que levam em consideração a existência e a efetividade dos controles para mitigação dos eventos de riscos mapeados. Os controles identificados foram também avaliados quanto ao desenho (se foram corretamente pensados e estruturados para mitigação das fragilidades) e quanto à operação (se estão implementados e em operação). O quadro 5, a seguir, resume o enquadramento nas quatro faixas de vulnerabilidade:

Quadro 5 – critérios para definição do nível de vulnerabilidade

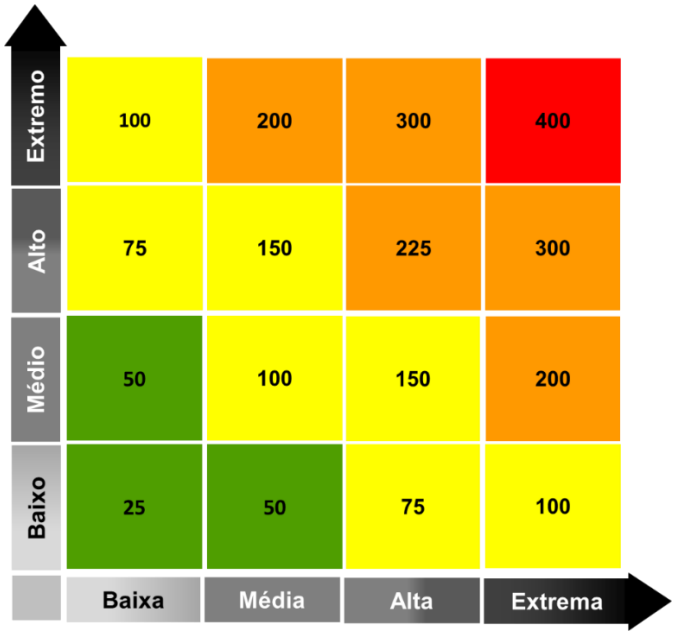
Vulnerabilidade	Critérios para avaliação da vulnerabilidade
Extrema	As linhas de defesa da Organização **são insuficientes para minimizar o risco, em função da ausência de controles chave ou recorrência de problemas.**
Alto	As linhas de defesa da Organização são insuficientes para minimizar o risco, em função da ineficácia de controles existentes, ou recorrência de problemas.
Médio	Os **controles existentes não operam de forma padronizada** ou são ineficientes e podem não minimizar o risco.
Baixo	Os controles existentes **minimizam o risco.**

Fonte: Análise Geral de Riscos Compesa 2019 (adaptada).

A combinação desses critérios (impacto e vulnerabilidade) resulta no nível de exposição de um determinado evento de risco. Os quantificadores (i x v) também

podem ser utilizados para definir a disposição dos eventos de riscos no gráfico de calor, conforme pode ser observado, na imagem 6, a seguir:

Imagem 6: Mapa de calor para disposição dos riscos



Realizada as considerações acerca da metodologia de classificação dos eventos de risco, bem como a definição de nível de criticidade de tais eventos (exposição), além da compilação de todos eventos de riscos identificados nos mapeamentos, então passou-se a dispor essas informações em uma matriz de impacto x vulnerabilidade conforme pode ser observado no quadro 6, a seguir. Os eventos de riscos estão elencados por tema, isto, foram agrupamento de acordo com os processos que estão inseridos.

Quadro 6 – Matriz de impacto x vulnerabilidade

Id	Risco referente ao tratamento de dados pessoais	I	V	Exposição (I x V)
R01	Risco de compartilhamento indevido de bases extraídas de sistemas corporativos (GISCOMP, BI, GSAN, HUMANUS etc);	20	20	400
R02	Risco de perda acidental de dados dos sistemas corporativos (GISCOMP, BI, GSAN, HUMANUS etc);	20	15	300
R03	Risco de sequestro de dados dos clientes (interno e externos) da Companhia	20	15	300

Id	Risco referente ao tratamento de dados pessoais	I	V	Exposição (I x V)
R04	Risco de invasão à base de dados da Companhia.	20	15	300
R05	Risco de armazenamento indevido de dados pessoais, bases com grande volume de informações dos clientes, em computadores e/ou e-mails;	20	20	400
R06	Risco de perda de rastreabilidades das informações extraídas e/ou consultadas no Giscomp.	20	20	400
R07	Risco de acesso indevido a dados sensíveis de clientes (tarifa social) anexados no GSAN;	20	20	400
R08	Risco de vazamento e/ou compartilhamento de dados sensíveis de clientes enquadrados na tarifa social armazenados em modo digital;	20	20	400
R09	Risco de tratamento indevido (acesso e/ou compartilhamento) em virtude de acesso aos dados por empregados terceirizados (0800, loja de atendimento, apoio administrativo etc).	20	15	300
R10	Risco de vazamento de dados compartilhados com empresas de leitura, telecobrança e/ou cobrança por sms;	15	15	225
R11	Risco de alteração de dados indevida pela equipe de cadastramento, atendentes de loja ou qualquer outro colaborador;	15	20	300
R12	Risco de vazamento e/ou compartilhamento de dados pessoais comuns e/ou sensíveis (dados de saúde, financeiro etc.) armazenados em modo digital;	20	20	400
R13	Risco de perda acidental de dados sensíveis armazenados em formato físico;	20	20	400
R14	Risco de perda intencional de dados sensíveis armazenados fisicamente;	20	20	400
R15	Risco de vazamento de dados sensíveis de colaboradores (dados de saúde, financeiro etc.) armazenados em físico;	20	20	400
R16	Risco de perda e/ou compartilhamento indevido dos dados dos clientes em virtude da reutilização de Ordens de Serviços, com informações pessoais, como rascunho.	10	15	150
R17	Risco de divulgação de dados pessoais equivocadas através da publicização dos contratos firmados com clientes corporativos;	15	10	150
R18	Risco de perda e/ou acesso indevido de dados pessoais pela tramitação de documentação física dos clientes;	10	15	150
R19	Risco de acesso não autorizado às informações existentes em faturas dos clientes individualizados.	10	15	150
R20	Risco de compartilhamento ou distribuição de dados pessoais com terceiros sem o consentimento do titular dos dados pessoais;	20	15	300
R21	Risco de perda e/ou compartilhamento de dados armazenados em meio físico;	10	20	200
R22	Risco de exposição de documentos no SEI por eventual falha na Classificação do nível de acesso;	10	10	100
R23	Risco de vazamento de dados na tramitação de faturas impressas.	10	10	100

Id	Risco referente ao tratamento de dados pessoais	I	V	Exposição (I x V)
R24	Risco de perda e/ou interceptação de arquivos com dados pessoais quando da tramitação para empresas de cobrança.	15	10	150
R25	Retenção prolongada de dados pessoais além das definições da tabela de temporalidade;	15	15	225
R26	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	15	15	225
R27	Risco de acesso não autorizado aos dados de clientes através de armazenamento vulnerável de cópias nos dispositivos (tablets) dos cadastradores;	10	5	50
R28	Risco de exposição dos dados dos clientes impressos nas faturas quando da entrega pelo leiturista;	10	10	100
R29	Risco de acesso indevido aos dados de clientes inseridos no contrato de atendimento;	10	20	200
R30	Risco de destruição de dados acidental pela utilização de dispositivos móveis;	10	5	50

Legenda: I – Impacto; V – Vulnerabilidade.

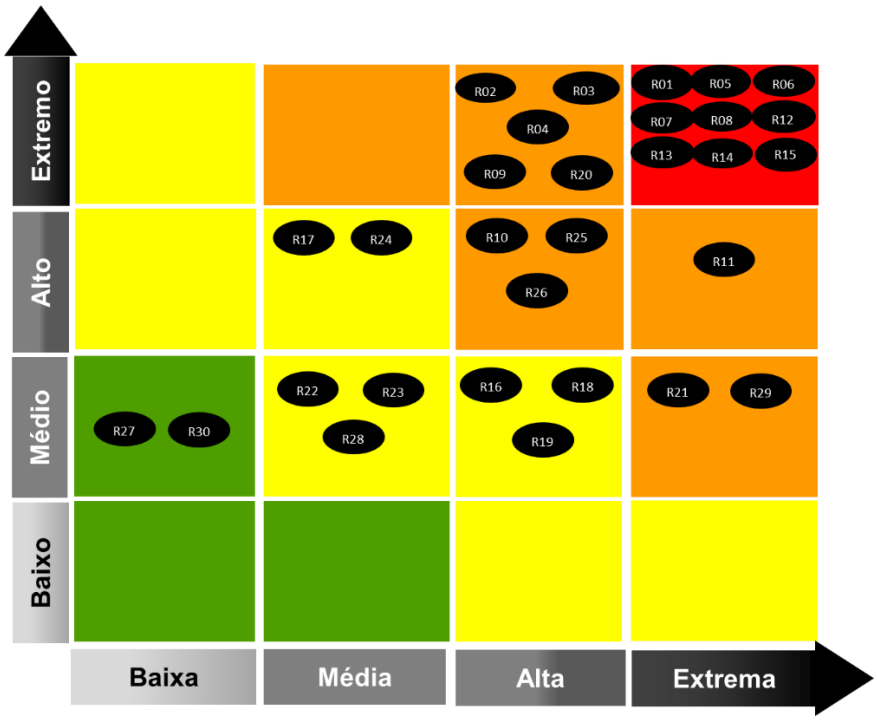
[1] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[2] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[3] Exposição: é o nível de risco, a magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas vulnerabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

No que diz respeito ao gráfico de calor, os eventos de risco estão dispostos de acordo com a imagem 7, a seguir, os números representam o ID dos riscos:

Imagem 7: Mapa da Exposição de Riscos



7 – MEDIDAS PARA TRATAR OS RISCOS

Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).

Desta forma, o processo de mapeamento identificou os riscos inerentes aos processos de negócio, bem como identificou os controles existentes para mitigação desses riscos. Eles foram mensurados utilizando a metodologia já existente na Companhia e já mencionada no item a) do tópico 6 deste relatório. Ademais, para os casos dos riscos classificados como extremos, foram propostos novos controles ou melhoria daqueles já existentes a fim de reduzir o nível de exposição ao nível de tolerância aos riscos definida pela administração. O quadro 7, a seguir correlaciona as medidas de controle com os eventos de riscos mapeados, assim como o tratamento adotado na empresa:

Quadro 7 – Medidas de controle para gerenciamento dos riscos

Id	Risco	Risco Inerente	Medidas	Risco Residual	Efeito sobre o Risco	Medidas Aprovadas
R01	Risco de compartilhamento indevido de bases extraídas de sistemas corporativos (GISCOMP, BI, GSAN, HUMANUS etc);	Extremo	8 - Controle de acesso aos sistemas por meio de usuário e senha.	Extremo	Reduzir	Sim
R02	Risco de perda acidental de dados dos sistemas corporativos (GISCOMP, BI, GSAN, HUMANUS etc);	Extremo	19 - Controle de acesso complementar para manipulação da base de dados. 22 - Realização de backups dos dados de acordo com a política de segurança da informação.	Alto	Aceitar	Sim
R03	Risco de sequestro de dados dos clientes (interno e externos) da Companhia	Extremo	24 - Uso de tecnologias como Antivirus, antispam, antiphishing, etc. 8 - Controle de acesso aos sistemas por meio de usuário e senha.	Alto	Aceitar	Sim
R04	Risco de invasão à base de dados da Companhia.	Extremo	25 - Utilização de firewall entre a internet e servidores. 9 - Controle de acesso complementar para manipulação dos dados da base.	Alto	Aceitar	Sim
R05	Risco de armazenamento indevido de dados pessoais, bases com grande volume de informações dos clientes, em computadores e/ou e-mails;	Extremo	-	Extremo	Reduzir	Sim
R06	Risco de perda de rastreabilidades das informações extraídas e/ou consultadas no Giscomp.	Extremo	-	Extremo	Reduzir	Sim
R07	Risco de acesso indevido a dados sensíveis de clientes (tarifa social) anexados no GSAN;	Extremo	8 - Controle de acesso aos sistemas por meio de usuário e senha.	Extremo	Reduzir	Sim
R08	Risco de vazamento e/ou compartilhamento de dados sensíveis de clientes enquadrados na tarifa social armazenados em modo digital;	Extremo	8 - Controle de acesso aos sistemas por meio de usuário e senha.	Extremo	Reduzir	Sim
R09	Risco de tratamento indevido (acesso e/ou compartilhamento) em virtude de acesso aos dados por empregados terceirizados (0800, loja de atendimento, apoio administrativo etc).	Extremo	11 - Controle de cessão de acesso para empregados terceirizados. 7 - Compartilhamento de responsabilidades sobre a proteção de dados com previsão em contrato.	Alto	Reduzir	Sim

Id	Risco	Risco Inerente	Medidas	Risco Residual	Efeito sobre o Risco	Medidas Aprovadas
R10	Risco de vazamento de dados compartilhados com empresas de leitura, telecobrança e/ou cobrança por sms;	Extremo	11 - Controle de cessão de acesso para empregados terceirizados. 7 - Compartilhamento de responsabilidades sobre a proteção de dados com previsão em contrato.	Extremo	Reduzir	Sim
R11	Risco de alteração de dados indevida pela equipe de cadastramento, atendentes de loja ou qualquer outro colaborador;	Extremo	9 - Controle de acesso complementar para manipulação dos dados da base. 12 - Controle de Rastreabilidade de alteração de dados de cadastro.	Alto	Aceitar	Sim
R12	Risco de vazamento e/ou compartilhamento de dados pessoais comuns e/ou sensíveis (dados de saúde, financeiro etc.) armazenados em modo digital;	Extremo	8 - Controle de acesso aos sistemas por meio de usuário e senha.	Extremo	Reduzir	Sim
R13	Risco de perda acidental de dados sensíveis armazenados em formato físico;	Extremo	10 - Controle de acesso físico aos depósitos.	Extremo	Reduzir	Sim
R14	Risco de perda intencional de dados sensíveis armazenados fisicamente;	Extremo	10 - Controle de acesso físico aos depósitos.	Extremo	Reduzir	Sim
R15	Risco de vazamento de dados sensíveis de colaboradores (dados de saúde, financeiro etc.) armazenados em físico;	Extremo	10 - Controle de acesso físico aos depósitos.	Extremo	Reduzir	Sim
R16	Risco de perda e/ou compartilhamento indevido dos dados dos clientes em virtude da reutilização de Ordens de Serviços, com informações pessoais, como rascunho.	Alto	15 - Diretriz institucional de não reutilizar rascunho que contenham dados pessoais.	Alto	Aceitar	Sim
R17	Risco de divulgação de dados pessoais equivocadas através da publicização dos contratos firmados com clientes corporativos;	Extremo	17 - Dupla checagem do arquivo a ser publicizado no portal da Lei de Acesso a Informação. 20 - Monitoramento pela equipe de compliance dos arquivos divulgados.	Médio	Aceitar	Sim
R18	Risco de perda e/ou acesso indevido de dados pessoais pela tramitação de documentação física dos clientes;	Alto	2 - A tramitação ocorre por malote através de empresas especializadas.	Médio	Aceitar	Sim
R19	Risco de acesso não autorizado às informações existentes em faturas dos clientes individualizados.	Alto	23 - Rotina de entrega das faturas com selo de privacidade.	Alto	Aceitar	Sim

Id	Risco	Risco Inerente	Medidas	Risco Residual	Efeito sobre o Risco	Medidas Aprovadas
R20	Risco de compartilhamento ou distribuição de dados pessoais com terceiros sem o consentimento do titular dos dados pessoais;	Alto	4 - Capacitação dos colaboradores sobre a LGPD, incluindo as hipóteses de compartilhamento.	Alto	Reduzir	Sim
R21	Risco de perda e/ou compartilhamento de dados armazenados em meio físico;	Extremo	10 - Controle de acesso físico aos depósitos.	Extremo	Reduzir	Sim
R22	Risco de exposição de documentos no SEI por eventual falha na Classificação do nível de acesso;	Extremo	5 - Capacitação dos colaboradores sobre o uso do SEI na tramitação de informações. 13 - Definição de colaborador chave (em cada gerência) para dirimir eventuais dúvidas sobre o uso do SEI.	Médio	Aceitar	Sim
R23	Risco de vazamento de dados na tramitação de faturas impressas.	Alto	18 - Envio de arquivo em formato txt com layout específico definido entre as partes. 7 - Compartilhamento de responsabilidades sobre a proteção de dados com previsão em contrato. 14 - Devolução das faturas em caixas lacradas.	Baixo	Aceitar	Sim
R24	Risco de perda e/ou interceptação de arquivos com dados pessoais quando da tramitação para empresas de cobrança.	Extremo	26 - Utilização de protocolo FTP para compartilhamento de arquivo especificamente com a empresa que realiza a telecobrança. 7 - Compartilhamento de responsabilidades sobre a proteção de dados com previsão em contrato.	Médio	Aceitar	Sim
R25	Retenção prolongada de dados pessoais além das definições da tabela de temporalidade;	Alto	1 -	Alto	Reduzir	Sim
R26	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	Alto	12 - Controle de Rastreabilidade de alteração de dados de cadastro.	Alto	Aceitar	Sim
R27	Risco de acesso não autorizado aos dados de clientes através de armazenamento vulnerável de cópias nos dispositivos (tablets) dos cadastradores;	Alto	21 - Os dispositivos são acessados com senha vinculadas especificamente	Baixo	Aceitar	Sim

Id	Risco	Risco Inerente	Medidas	Risco Residual	Efeito sobre o Risco	Medidas Aprovadas
			aos CPFs dos cadastradores. 16 - Dispositivos funcionam offline.			
R28	Risco de exposição dos dados dos clientes impressos nas faturas quando da entrega pelo leiturista;	Alto	23 - Rotina de entrega das faturas com selo de privacidade. 7 - Compartilhamento de responsabilidades sobre a proteção de dados com previsão em contrato.	Médio	Aceitar	Sim
R29	Risco de acesso indevido aos dados de clientes inseridos no contrato de atendimento;	Extremo	3 - Acesso ao contrato ocorre após o preenchimento de outros dados pessoais.	Extremo	Reduzir	Sim
R30	Risco de destruição de dados acidental pela utilização de dispositivos móveis;	Médio	16 - Dispositivos funcionam offline. 6 - Compartilhamento de responsabilidades com a empresa contratada prevendo incidentes na matriz de riscos anexa ao contrato.	Baixo	Aceitar	Sim

Histórico de Revisões

Data	Versão	Descrição	Autor
13/07/2021	1.0	Conclusão da primeira versão do relatório	Alixandro Pereira de Jesus - AUD
Abril/23	1.1	Revisão com atualização do DPO e dados corporativos. Inclusão como anexo na Política de Privacidade e Proteção de Dados Pessoais.	Luciana Rebouças Campelo - GGR