RELATÓRIO GLOBAL DE ANÁLISE DE PROTEÇÃO DE DADOS (RGAPD)

Cimentos Itambé

*Documento gerado em 11 de Abril de 2025*.

*Análise realizada por: Cimentos Itambé*

*Encarregado de Dados: Emerson Passos*

A Lei n. 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais – LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Os esforços afins à adequação requerida foram orientados, preliminarmente, pela identificação de áreas e atividades organizacionais demandantes de atenção quanto à proteção de dados pessoais, possibilitando:

a) O melhor entendimento quanto a condição atual da organização frente ao tratamento e proteção de dados pessoais;

b) A definição, com fundamentação metodológica, do nível de maturidade da organização para a proteção de dados pessoais;

c) A identificação, análise e avaliação de riscos à proteção de dados pessoais, potencialmente capazes de impactar negativamente a organização;

d) A proposição de ações de aprimoramento de indicadores e/ou condições discrepantes associadas à proteção de dados pessoais; e

e) O desenvolvimento de documentos comprobatórios que orientem melhores práticas no tratamento de dados pessoais.

Atenciosamente,

## 1. RESUMO EXECUTIVO

### 1.1. Contexto Analisado

| Razão Social | | |
|---|---|---|
| Cimentos Itambé | | |
| CEP | Endereço | CNPJ |
| | | |

### 1.2. Responsáveis Organizacionais

| Encarregado de Dados | Email |
|---|---|
| Emerson Passos | encarregado.lgpd@cimentoitambe.com.br |
| Comitê de Adequação | Email |
| | |

### 1.3. Informações Globais

| Início do Projeto | Término do Projeto | Processos mapeados |
|---|---|---|
| 17.03.2025 | | 17 |

### 1.4. Time Consultivo

| Responsáveis pela Adequação | Email |
|---|---|
| Carolina Maciel | carolina.maciel@martinellilabs.com.br |
| Paloma Hellmann | paloma.hellmann@martinellilabs.com.br |

### 1.5. Nível de Proteção de Dados




Tomando como referência os critérios estabelecidos para a mensuração do atual nível de proteção de dados, em uma escala de 0 (zero) a 100 (cem) pontos, onde 0 (zero) pontos corresponde ao completo desacordo com a LGPD e 100 (cem) pontos corresponde a respectiva adequação, observou-se um desempenho de 68 pontos.

O nível de proteção de dados, ora evidenciado, decorreu da análise de informações associadas aos registros de operações de tratamento de dados pessoais; as condições existentes de segurança de informações; as condições de proteção de dados pessoais de fornecedores e/ou parceiros institucionais e, por fim, as condições de governança existentes.

Foram mapeados e analisados 17 processos associados aos Registros de Operações de Tratamento de Dados Pessoais; 2 fornecedores e/ou parceiros institucionais; e as condições de segurança de informações existentes.

### 1.6. Análise de Criticidade de Processos

#### 1.6.1. Registros de Operações de Tratamento de Dados Pessoais

Os processos mapeados, associados aos Registros de Operações de Tratamento de Dados Pessoais (ROPA), foram analisados a partir de 30 (trinta) pontos de atenção, organizados sob 05 (cinco) perspectivas, a saber: (1) identificação do processo; (2) titulares e tipo de dados; (3) finalidade e base legal; (4) compartilhamento e transferência; e (5) coletas de dados.

Cada processo mapeado, de forma específica, foi submetido a uma análise de criticidade.

A análise de criticidade é consolidada pela atribuição, por parte do consultor designado, de critérios de probabilidade e impacto. Como resultado, os processos são classificados e organizados como de riscos toleráveis, significativos, sérios ou intoleráveis.

Na sequência, são apresentadas a síntese das análises de criticidades dos processos do ROPA.

| Área / Setor | Processo | Pontuação | Criticidade |
|---|---|---|---|
| Dir Financeira – DF | ROPA DEMONSTRAÇÃO | | |
| Dep. Gestão de Pessoas – DGP | Recrutamento e Seleção de Colaboradores para o Grupo SIRAMA | 2.4 | Leve |
| Dep. Financeiro – DFIN | Análise de Crédito | 2 | Leve |
| Dir Adm e Jurídica - DAJ | DJUR \| Defesa em Processos Judiciais e Administrativos | 3.4 | Leve |
| Dir Adm e Jurídica - DAJ | DJUR \| Elaboração de Contratos | 2 | Leve |
| Dir Adm e Jurídica - DAJ | DJUR \| Societário | 2.29 | Leve |
| Dir Adm e Jurídica - DAJ | DJUR \| Solicitação de Pareceres | 2 | Leve |
| Dep. Suprimentos – DSUP | Cadastro de Fornecedores | 2.4 | Leve |
| Dep. Tecnologia da Informação – DTI | Cadastro de Colaboradores no AD (Microsoft Active Directory) | 2 | Leve |
| Dep. Controladoria – DCON | Apuração de Dividendos | 2.25 | Leve |
| Dep. Gestão de Pessoas – DGP | Relações com a Justiça do Trabalho | 3 | Leve |
| Dep. Gestão de Pessoas – DGP | Relações Sindicais | 5.4 | Moderado |
| Dep. Gestão de Pessoas – DGP | Saúde do Trabalho | 3 | Leve |
| Dep. Gestão de Pessoas – DGP | Segurança do Trabalho | 3 | Leve |
| Dep. Gestão de Pessoas – DGP | Contratação de Colaboradores do Grupo SIRAMA | 3.17 | Leve |
| Dep. Gestão de Pessoas – DGP | Extinção do Contrato de Trabalho | 3 | Leve |
| Dep. Gestão de Pessoas – DGP | Treinamento de Colaboradores do Grupo SIRAMA | 3.17 | Leve |

#### 1.6.2. Segurança de Informações

As condições existentes de segurança de informações foram analisadas a partir de 37 (trinta e sete) critérios de avaliação. Como resultado, as condições existentes evidenciaram que a exposição à riscos à segurança de informações são classificadas como: Leve

### 1.6.3. Fornecedores e/ou Parceiros Institucionais

Foram analisadas as condições de proteção de dados pessoais de 2 fornecedores e/ou parceiros institucionais. No mesmo sentido, que os formulários do ROPA e de segurança de informações, os fornecedores e/ou parceiros institucionais foram analisados a partir de 33 (trinta e três) critérios de avaliação. Como resultado, os fornecedores e/ou parceiros institucionais foram classificados e organizados como de riscos toleráveis, significativos, sérios ou intoleráveis.

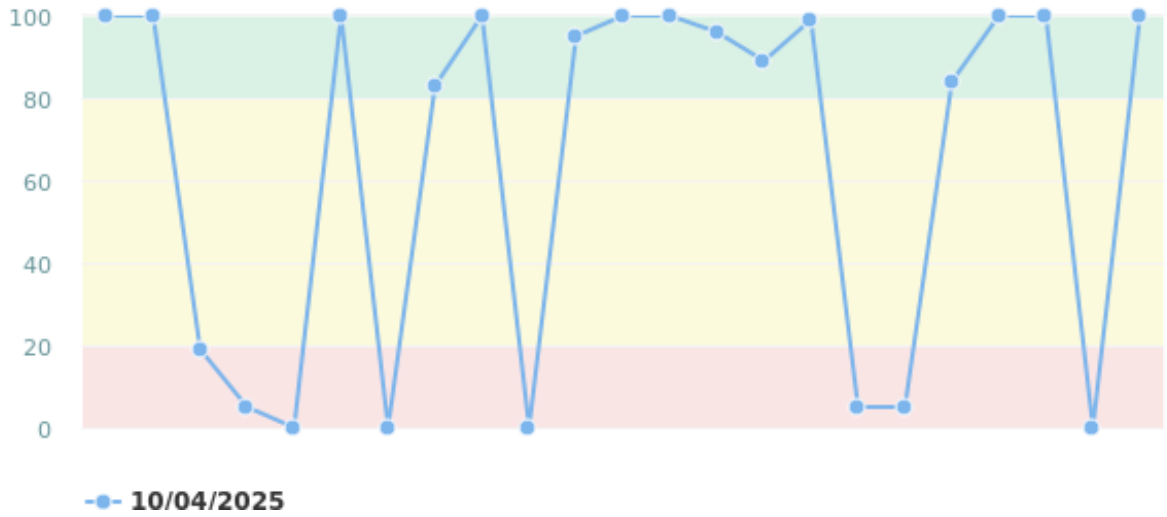
| Pessoa Jurídica | Tipo | Pontuação | Criticidade |
|---|---|---|---|
| ICTS \| Canal de Denúncias | Fornecedor | 0.88 | Leve |
| Microsoft | Fornecedor | | |

### 1.7. Perfil de Desempenho

Os processos de tratamento de dados, mapeados e sintetizados na subseção 1.6, foram submetidos a um modelo avaliação de desempenho, consolidado pela Metodologia de Multicritério em Apoio à Decisão – Construtivista (MCDA-C), com o objetivo de evidenciar o Nível Global de Proteção de Dados do contexto analisado e suas oportunidades de aprimoramentos.

As informações inseridas nos formulários de inventários de dados (ROPA, Segurança de Informações e Fornecedores e/ou Parceiros Institucionais), foram organizadas em 04 (quatro) áreas de atenção, a saber: (1) governança de dados; (2) áreas e processos; (3) segurança de informações; e (4) avaliação de fornecedores. Ao todo, foram identificados, organizados e mensurados 20 (vinte) indicadores que explicitam o desempenho do contexto analisado frente a proteção de dados pessoais.

Os resultados da avaliação de desempenho são apresentados forma de 03 (três) gráficos, o primeiro já destacado no item 1.5. Nível de Proteção de Dados. O segundo, denominado de perfil de desempenho.

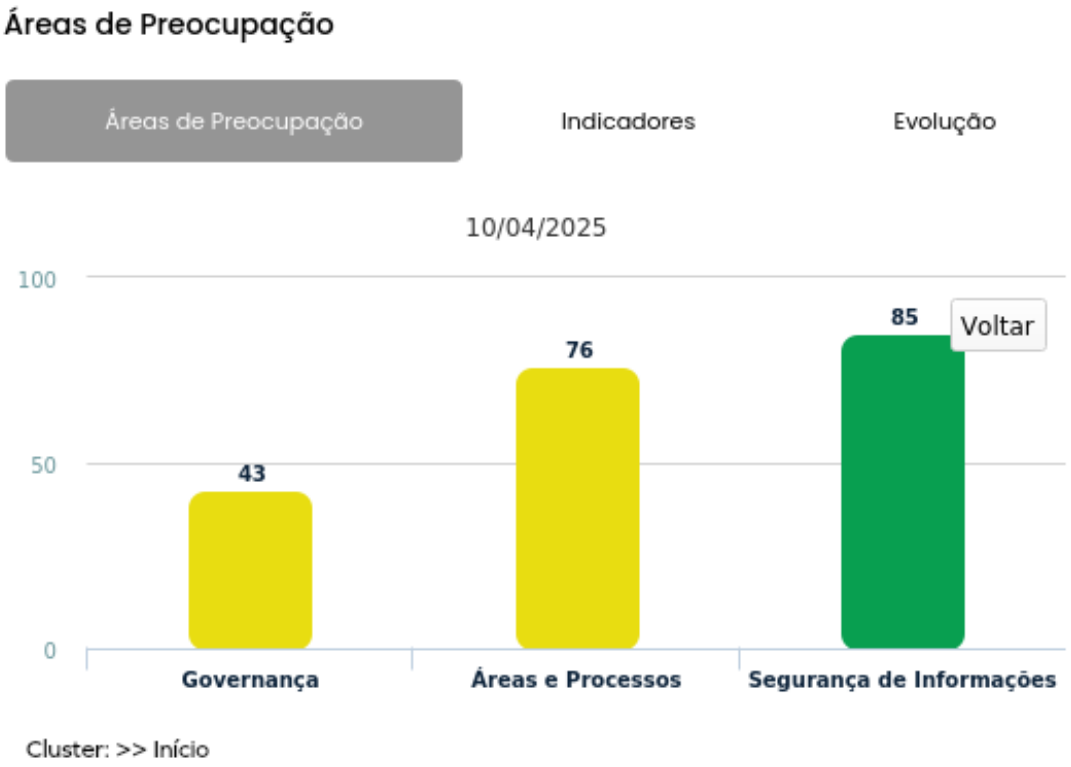



O gráfico “Perfil de Desempenho” possui 03 (três) faixas de desempenho. Uma faixa na cor “verde”, destacando, em conformidade com a MCDA-C, indicadores em nível de excelência; uma faixa na cor “amarela”, destacando indicadores em nível de mercado e/ou competitividade; e, uma faixa na cor “vermelho”, destacando indicadores em nível de comprometimento.

No mesmo sentido, destaca todos os indicadores que mensuram, de forma global, o nível de proteção de dados do contexto analisado.

Percebe-se, então, que a organização: Cimentos Itambé, possui: 15 indicadores em nível de excelência; 0 indicadores em nível de competitividade; e 8 indicadores em nível de comprometimento.

Com o objetivo, de aprimorar a análise do nível de proteção de dados, destacamos o terceiro gráfico




**1.8. Análise de Riscos à Proteção de Dados**

O conceito atribuído ao termo “risco” apresenta-se como universal, sendo definido como um evento capaz de impactar, positiva ou negativamente, qualquer atividade que tenha como objetivo a disponibilização de produtos, bens ou serviços.

O risco quando observado sob o foco da proteção de dados pessoas está relacionado a probabilidade de concretização de eventos que impactem negativamente organizações e seus atores, estimulando-os a gerar conhecimentos como forma de minimizar suas perdas reais ou potenciais.

Observamos e incorporamos os pressupostos preconizados pela Norma ISO 31.000 para os processos de identificação, análise e avaliação de riscos.

**Riscos associados à proteção de dados pessoais**

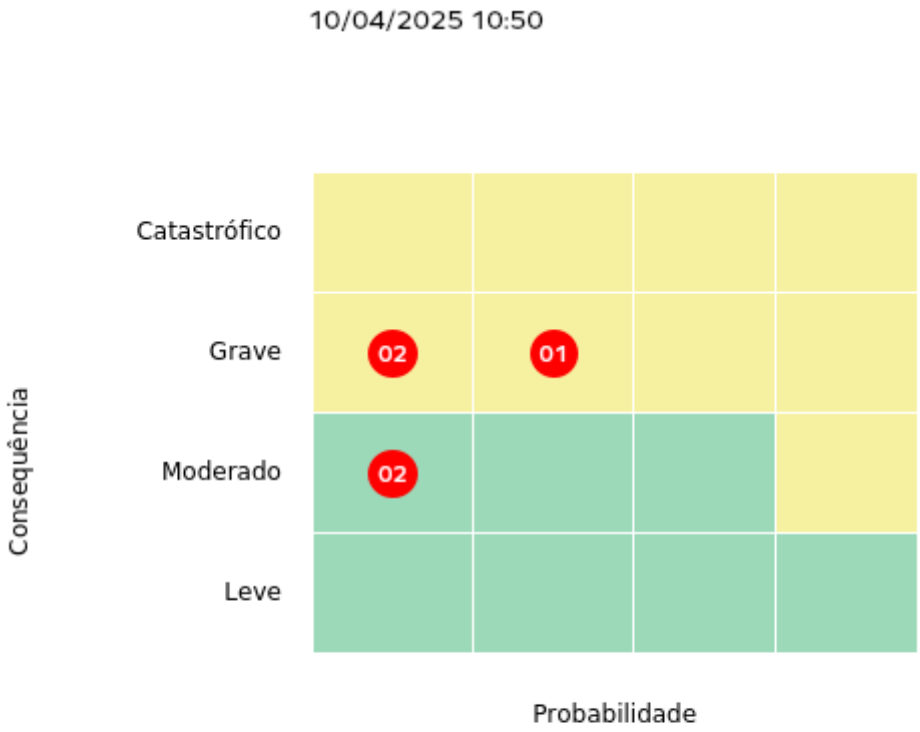
Foram identificados cinco(5) riscos associados à proteção de dados, sendo eles:

R1 - Sanções judiciais e/ou administrativas;
R2 - Crimes cibernéticos;
R3 - Dano reputacional;
R4 - Perdas de parceiros institucionais / comerciais;
R5 - Rescisões contratuais;

Cada risco identificado foi submetido a um processo estruturado de análise e avaliação (Anexo 10) sendo

possível estimar suas consequências e a probabilidade de concretização.

Como resultado, construiu-se uma matriz de riscos à proteção de dados pessoais com o objetivo de evidenciar suas criticidades e demandas por tratamento.



10/04/2025 10:50

| Risco | Consequência | Probabilidade | TS | Pontuação | |
|---|---|---|---|---|---|
| R1 - Sanções judiciais e/ou administrativas | Grave | 27% | 30% | 23 pts | análise |
| R2 - Crimes cibernéticos | Grave | 18% | 20% | 15 pts | análise |
| R3 - Dano reputacional | Moderado | 22% | 20% | 11 pts | análise |
| R4 - Perdas de parceiros institucionais / comerciais | Moderado | 23% | 15% | 12 pts | análise |
| R5 - Rescisões contratuais | Grave | 23% | 15% | 19 pts | análise |

## 2. ANÁLISE REGULATÓRIA

Parte integrante deste documento, destacam-se os dispositivos legais associados ao tratamento de dados pessoais do contexto analisado.

-

## 3. PARECERES

**Parecer #1**

**Análise Técnica do Mapeamento da Lei Geral de Proteção de Dados – Grupo Sirama**

---

O núcleo Law Tech realizou a análise dos documentos encaminhados pela empresa Grupo Sirama, referentes ao seu mapeamento de conformidade com a Lei Geral de Proteção de Dados (LGPD).

Todos os Registros de Operações de Tratamento de Dados Pessoais (ROPA) enviados pela empresa foram integralmente replicados na plataforma Privia, sem qualquer alteração nas respostas fornecidas. Como resultado, o nível de proteção de dados atingiu a pontuação de 68, sendo que testes, 51 pontos se referem a indicadores de Governança e ROPA e 17 pontos são resultados da avalição realizada no setor responsável pela Segurança da Informação.

Apesar de esse índice poder ser considerado satisfatório em termos gerais, é importante destacar que a equipe responsável pela análise **não realizou ajustes nas respostas dos ROPAs**. Durante a revisão, foram identificadas diversas inconsistências que, caso corrigidas, certamente impactariam de forma significativa o nível de proteção de dados da empresa Grupo Sirama.

A seguir, apresentamos alguns exemplos dessas inconsistências:

**1 - Ausência da definição do agente de tratamento**
Em nenhum dos processos descritos foi identificada a indicação da posição ocupada pelo agente de tratamento. A LGPD estabelece diferentes níveis de responsabilidade conforme o tipo de agente envolvido, sendo eles:

- Controlador
- Controlador conjunto
- Operador
- Suboperador

Essa omissão compromete a correta atribuição de responsabilidades e pode gerar impactos na governança e na responsabilização em caso de incidentes de dados.

**2 - Inconsistência quanto ao tratamento de dados sensíveis**
Outro ponto que merece atenção diz respeito à categorização dos dados pessoais tratados, especialmente os dados sensíveis. A maioria dos ROPAs do Grupo Simara informa que não há tratamento de dados sensíveis nos processos analisados. No entanto, foram observadas contradições em algumas dessas afirmações. Exemplos:

- **Processo:** Relações Sindicais

Apesar de o registro indicar que não há dados sensíveis, consta entre os dados tratados o “nome” e o “valor da mensalidade” paga ao sindicato.

De acordo com o artigo 5º, inciso II, da LGPD:

*“II - 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.”*

Portanto, a menção à filiação sindical torna o dado pessoal tratado sensível por definição legal, o que exige medidas específicas de proteção, além de hipóteses legais de tratamento mais restritivas.

**Processo:** Recrutamento e Seleção de Colaboradores para o Grupo Sirama

No processo citado, é indicada a coleta de “Foto (dado biométrico)”, sendo atribuída a esse tratamento a base legal do “exercício regular de direitos”.

Contudo, essa justificativa exige uma análise mais criteriosa. De maneira geral, a base legal mencionada não se mostra a mais adequada para embasar o tratamento de dados biométricos em processos seletivos. A utilização da imagem do candidato, sem a devida justificativa e sem a demonstração de sua estrita necessidade, levanta preocupações quanto à legalidade e à proporcionalidade da coleta.

Caso a empresa esteja coletando fotos exclusivamente para fins de documentação em processos administrativos formais, poder-se-ia cogitar a aplicação do “exercício regular de direitos”. Entretanto, no contexto específico de recrutamento e seleção, essa base legal pode ser considerada inadequada ou forçada, especialmente na ausência de uma justificativa clara da necessidade dessa coleta.

Dada a natureza sensível do dado (imagem, enquanto dado biométrico), e considerando o princípio da minimização previsto na LGPD, a base legal mais apropriada parece ser o consentimento do titular, desde que colhido de forma livre, informada e inequívoca. Ressaltamos, contudo, que a adoção dessa base legal exigirá adequações no processo, como a implementação de mecanismos para coleta, registro e eventual revogação do consentimento.

**Tratamento de dados de crianças, adolescentes e idosos**

Por fim, outro ponto que requer reavaliação diz respeito ao tratamento de dados pessoais de crianças, adolescentes e idosos, os quais são considerados, de forma pacificada pela Agência Nacional de Proteção de Dados (ANPD), como dados sensíveis, independentemente da sua natureza específica.

A LGPD impõe cuidados redobrados no tratamento desses dados, exigindo bases legais específicas, além de medidas de segurança e transparência mais rigorosas.

Em processos como análise de crédito, por exemplo, é necessário questionar: a empresa pode afirmar, com segurança, que não há clientes com 60 anos ou mais em sua base? No caso de jovens aprendizes contratados, todos possuem efetivamente 18 anos ou mais no momento da coleta dos dados? Além disso, ao coletar informações de cônjuges de colaboradores, há garantia de que não estão sendo tratados dados de pessoas idosas?

Como um exemplo, é possível mencionar o processo "Extinção de contrato de trabalho" no qual se manifesta da seguinte forma:

**9. DADOS SENSÍVEIS**: NÃO
**10. DADOS PESSOAIS** DE CRIANÇAS E ADOLESCENTES: SIM- filhos de colaboradores.

Uma vez que há dados pessoais de crianças e adolescente, há dados sensíveis no processo como um todo.

Diante desses pontos, recomenda-se uma reavaliação criteriosa dos processos que podem envolver o tratamento de dados de menores de idade e idosos, com a devida adequação das bases legais e salvaguardas exigidas pela legislação.

**3 - Do compartilhamento e transferência internacional dos dados**

Em diversos processos analisados, foi possível identificar indícios de compartilhamento ou até mesmo transferência internacional de dados pessoais. No entanto, essa realidade **não está refletida nas respostas fornecidas à pergunta** “Compartilhamento de dados”, que, em grande parte dos casos, está preenchida como “não”.

Um exemplo ilustrativo:

- **PROCESSO** Elaboração de Contratos
- **DESCRIÇÃO DO PROCESSO:** a Área Requisitante (Departamento responsável pela contratação e gestão do bem ou serviço) solicita ao DJUR a formalização de instrumento contratual. Para elaboração do contrato é necessária a qualificação civil da fornecedora e de seus representantes legais.
- **FORMA DE OBTENÇÃO DOS DADOS:** os dados são fornecidos pelo titular dos dados à Área Requisitante do contrato (setor da empresa responsável pela contratação) e compartilhados com o Departamento Jurídico;
- **COMPARTILHAMENTO DOS DADOS**: não há compartilhamento dos dados. O produto do processo é o contrato.

Essa resposta contradiz o próprio fluxo descrito no processo, uma vez que há, de fato, **compartilhamento interno** entre setores da organização.

É importante esclarecer que o **compartilhamento de dados** pode ocorrer de diferentes formas e deve ser corretamente identificado e classificado:
1 - **Compartilhamento interno**: Refere-se à circulação de dados pessoais entre setores distintos dentro da mesma empresa ou entre empresas que compõem um mesmo grupo econômico. Ressalta-se que, no caso de grupos econômicos, é necessário que haja normas corporativas globais válidas e devidamente documentadas, para que esse compartilhamento seja considerado regular e seguro. Essas normas precisam estar validadas pela ANPD.

2 - **Compartilhamento externo (nacional):** Acontece quando os dados são transferidos para agentes externos à empresa ou ao grupo econômico, seja de forma física ou digital. Quando digital, deve-se atentar para o local de armazenamento dos dados, que devem permanecer em servidores localizados no Brasil para que não se configure uma transferência internacional.

A ausência de identificação precisa sobre o compartilhamento pode comprometer a transparência exigida pela LGPD e prejudicar a adoção de medidas adequadas de segurança e responsabilidade. Recomenda-se, portanto, uma revisão atenta dos processos que envolvam múltiplas áreas, prestadores de serviço ou sistemas em nuvem, para garantir a correta classificação e documentação desses fluxos de dados.

**Transferência internacional de dados**

Embora os processos revisados indiquem, de forma recorrente, que **não há transferência internacional de dados**, a consultoria ressalta que essa afirmação é, na maioria dos casos, pouco provável. Mesmo quando a empresa dispõe de servidores físicos próprios, como é o caso do Grupo Sirama.

A justificativa para essa ressalva é o uso recorrente de sistemas de terceiros na operação de diversos processos internos. Esses sistemas, por sua vez, frequentemente utilizam servidores localizados fora do território nacional, o que configura transferência internacional de dados nos termos da LGPD.

Um exemplo concreto é o uso do Sistema Sênior. Em avaliação interna, a consultoria identificou que essa plataforma realiza transferência internacional de dados. Dessa forma, **todos os processos realizados por meio desse sistema também estarão sujeitos a esse tipo de transferência.**

Outro exemplo relevante está relacionado aos benefícios corporativos, como os planos de saúde, que normalmente fazem uso de plataformas que armazenam dados em servidores internacionais. Ademais, sistemas amplamente utilizados na rotina empresarial como Microsoft Excel (quando utilizado com sincronização via nuvem), serviços de e-mail e outros softwares baseados em cloud computing, também podem incorrer em transferência internacional, **caso não haja garantia de que seus servidores estão localizados no Brasil.**

Além disso, foi identificado que o backup de dados da empresa é realizado por meio da solução "Barracuda Backup", **a qual armazena a maior parte de suas informações em servidores internacionais.**

É fundamental que essas transferências sejam corretamente identificadas e documentadas, especialmente após a entrada em vigor da Resolução CD/ANPD nº 19/2024, que estabelece requisitos específicos para a transferência internacional de dados pessoais.

Vale ressaltar que a transferência internacional, por si só, não representa uma infração à LGPD ou desabona o tratamento de dados da empresa. No entanto, ela impõe **obrigações adicionais**, como a verificação do grau de proteção do país destinatário, a existência de cláusulas contratuais específicas, e, em alguns casos, a necessidade de autorização da ANPD.

Portanto, a ausência de identificação desses fluxos de dados pode comprometer a conformidade da empresa com a legislação vigente. Recomenda-se, assim, uma revisão técnica detalhada de todos os sistemas utilizados nos processos da organização, a fim de garantir a correta aplicação das disposições legais relativas à transferência internacional de dados.

Diante das constatações anteriores, torna-se imprescindível que a empresa passe a identificar, de forma explícita, os sistemas e ferramentas utilizados na execução dos processos, e não apenas os setores envolvidos no fluxo de dados.

A descrição genérica do tipo “os dados são compartilhados entre a área requisitante e o departamento jurídico” **não é suficiente** para garantir a rastreabilidade, a segurança e a correta identificação de eventuais compartilhamentos ou transferências internacionais. O que certamente refletirá no nível de proteção de dados.

É necessário que as descrições operacionais dos processos sejam mais contextualizadas, identificando claramente os meios pelos quais os dados transitam. Um exemplo mais adequado seria:

*“O titular dos dados fornecerá à área requisitante do contrato (setor da empresa responsável pela contratação) a documentação necessária via e-mail (Outlook). Após o recebimento desses dados, a área requisitante encaminhará os mesmos também via e-mail (Outlook) para o Departamento Jurídico. Com os dados em mãos, o Departamento Jurídico iniciará a elaboração do contrato utilizando a plataforma Microsoft Word e, posteriormente, a plataforma DocuSign para a assinatura do contrato. O documento assinado é devolvido à área requisitante via e-mail, que o encaminhará ao titular.”*

Esse tipo de descrição permite mapear com clareza os pontos de tratamento e circulação de dados pessoais, inclusive identificando quais sistemas estão envolvidos e se existe potencial para compartilhamento externo ou transferência internacional.

Além de estar em conformidade com os princípios da transparência e da prestação de contas (accountability), exigidos pela LGPD, esse nível de detalhamento facilita a aplicação de medidas de segurança da informação e a definição de bases legais apropriadas para cada etapa do tratamento uma vez que a Resolução mencionada anteriormente, limita as bases legais que podem ser utilizados em processos que contenham transferência intercional de dados.

Portanto, recomenda-se que todos os processos descritos nos ROPAs sejam revistos e atualizados, com a devida inserção das ferramentas, sistemas e plataformas utilizadas em cada fase do tratamento de dados pessoais.

**4 - Do descarte de dados**

No que se refere ao descarte de dados pessoais, a empresa informa, em diversos processos, que há um procedimento instituído. Contudo, a descrição apresentada nos ROPAs é genérica, limitada à expressão *"conforme prazos prescricionais"*, sem fornecer detalhes sobre **como, quando e por quais meios esse descarte é efetivamente realizado.**

A ausência dessas informações levanta uma série de questionamentos importantes que precisam ser abordados para garantir a conformidade com os princípios da transparência, da limitação da finalidade e da segurança previstos na LGPD. Dentre as questões que devem ser esclarecidas, destacam-se:

- Qual é o prazo prescricional adotado para cada tipo de dado? Esse prazo é expressamente previsto em contrato, em norma interna ou fundamentado em obrigação legal ou regulatória?
- O prazo é padronizado para todos os dados tratados, ou varia conforme o tipo de dado, a finalidade ou a categoria do titular?
- Como ocorre o descarte de dados físicos? Os documentos são rasgados, triturados, incinerados ou apenas descartados em lixo comum? Envolvem uma empresa terceira responsável pelo descarte? Se sim, qual empresa e o nível de segurança acordado?
- No caso de dados digitais, qual é o procedimento adotado para garantir a eliminação segura? O descarte ocorre em todos os sistemas utilizados, ou apenas em sistemas internos?
- Há registro (log) desses descartes digitais? Existe rastreabilidade e possibilidade de auditoria desses eventos?
- Os prestadores de serviço que eventualmente tratem dados pessoais em nome da empresa seguem o mesmo padrão? Eles são auditados quanto à eliminação adequada dos dados?

A resposta a essas perguntas é fundamental para a construção de uma política de descarte clara, segura e documentada, conforme exige o artigo 6º, inciso I (finalidade) e inciso X (responsabilização e prestação de contas) da LGPD.

Recomenda-se, portanto, a revisão dos ROPAs para inserção dessas informações com maior detalhamento, bem como a elaboração ou atualização de uma Política de Retenção e Descarte de Dados Pessoais, contendo prazos definidos, métodos de descarte físico e digital, e procedimentos de controle e rastreabilidade.

**5 - Ausência de informações relevantes**

Conforme mencionado anteriormente, é essencial que os processos contenham descrições mais detalhadas, bem como respostas mais completas às perguntas do mapeamento. A identificação dos dados tratados nesses processos também requer atenção especial.

Como exemplo, destacamos os ROPAs relacionados a processos jurídicos, que não mencionam a existência de assinatura entre os dados tratados, informação comumente presente nesse tipo de contexto. Outro caso é o do processo de admissão, cuja descrição sugere que nem todos os documentos legalmente exigidos para a contratação de um colaborador foram listados.

---

Os pontos relatados acima representam as falhas mais críticas identificadas nos ROPAs analisados e indicam que a pontuação obtida pela empresa (68 pontos), no que se refere ao Nível de Proteção de Dados do Grupo Simara, **possivelmente não reflete a realidade.**

Recomenda-se, portanto, que todos os ROPAs, não apenas os citados nesta análise, passem por uma revisão minuciosa, com especial atenção à completude, coerência e correção das informações fornecidas, garantindo maior conformidade com os princípios e exigências da LGPD.

**Parecer #2**

A área de Segurança da Informação tem como foco principal a identificação e a análise de quatro tipos específicos de controles:
1. Controles Operacionais;
2. Controles de Pessoas;
3. Controles Físicos;
4. Controles Tecnológicos.

No que se refere ao Grupo Sirama, é importante destacar que os documentos comprobatórios fornecidos à consultoria evidenciam ações concretas e eficazes por parte do setor responsável pela Segurança da Informação, resultando em uma análise geral bastante positiva.

Entretanto, vale ressaltar que, para a validação completa dos 48 controles da ISO 27001, seria indispensável a realização de uma conversa direta com o setor responsável, a fim de esclarecer pontos específicos e obter informações complementares. A ausência desse contato impossibilita a confirmação de algumas respostas, seja por falta de documentação adicional, seja por eventuais responsabilidades atribuídas a outros setores.

---

**Condição Identificada**

**1. No escopo dos controles operacionais, responsável pela análise dos critérios:**

(a) Políticas de Segurança da Informação;
(b) Papeis e Responsábilidades;
(c) Segregação de Funções;
(d) Responsabilidade da Diretoria;
(e) Inteligência de Ameaças;
(f) Inventário de Informações;
(g) Uso Aceitável de Informações;
(h) Devolução de Ativos;
(j) Classificação de Informações;
(k) Transferência de Informações;
(l) Controle de Acessos;
(m) Gestão de Identidades;
(n) Informações de Autenticação;
(o) Direitos de Acesso;
(p) Segurança de Informação nas Relações com Fornecedores;
(q) Segurança da Informação para o Uso de Serviços em Nuvem;
(r) Planejamento e Preparação da Gestão de Incidentes de Segurança da Informação;
(s) Avaliação e Decisão Sobre Eventos de Segurança da Informação;
(t) Prontidão de TIC para Continuidade de Negócios;
(u) Requisitos Legais, Estatutários, Regulamentáres e Contratuais.

**Dos controles listados acima:**

**06** foram classificados como risco leve
**01** foi classificado como risco moderado
**01** foi classificado como fisco grave (é possível que esse grau de criticidade só tenha sido atribuído em decorrência

da ausência de informações que precisariam ser sanadas em uma conversa junto ao setor).
**00** foram classificados como risco crítico

***Alguns controles não foram respondidos devido à ausência de informações concretas, sendo necessário alinhar com o setor responsável para prosseguir.***

**2. No escopo do controle de pessoas, é realizada a análise dos seguintes critérios:**

(a) Seleção
(b) Termos e Condições de Contratação;
(c) Conscientização, Educação e Treinamento em Segurança da Informação;
(d) Acordos de Confidencialidade ou não Divulgação;
(e) Trabalho Remoto;
(f) Relato de Eventos de Segurança da Informação;

Dos controles listados acima:

**01** foi classificados como risco leve
**00** foram classificados como risco moderado
**00** foram classificados como fisco grave
**01** foi classificados como risco crítico (é possível que esse grau de criticidade só tenha sido atribuído em decorrência da ausência de informações que precisariam ser sanadas em uma conversa junto ao setor).

***Alguns controles não foram respondidos devido à ausência de informações concretas, sendo necessário alinhar com o setor responsável para prosseguir.***

**3. No âmbito dos Controles Físicos, foram análisados os critérios:**

(a) Perimetros de Segurança Física;
(b) Entrada Física;
(c) Segurança de Escritórios, Salas e Instalações;
(d) Monitoramento de Segurança Física;
(e) Segurança de Ativos fora das Instalações da Organização;

**Dos controles listados acima:**

00 foram classificados como risco leve
00 foram classificados como risco moderado
00 foram classificados como fisco grave
00 foram classificados como risco crítico

***As perguntas relacionadas ao controle físico da empresa exigem uma abordagem diferenciada, envolvendo outros setores, como os responsáveis pela segurança patrimonial, portaria etc. É necessário realizar uma conversa com a empresa para determinar o nível de criticidade de cada controle.***

**4. Por fim, no âmbito dos Controles Tecnológicos, foram análisados os critérios:**

(a) Dispositivos de Endpoint do Usuário;
(b) Direitos de Acessos Privilegiados;
(c) Restrição de Acesso à Informação;
(d)Autenticação Segura;
(e) Prevenção contra Malwere;
(f) Gestão de Vulnerabilidades Técnicas;
(g) Exclusão de Informações;

(h) Mascaramento de Dados;
(i) Prevenção de Vazamentos de Dados;
(j) Backup de Informações;
(k) Redundância de Recursos para Tratamento de Informações;
(l) Log;
(m) Atividades de Monitoramento.

**Dos controles listados acima:**

**04** foram classificados como risco leve
**00** foram classificados como risco moderado
**00** foram classificados como fisco grave
01 foi classificado como risco crítico (é possível que esse grau de criticidade só tenha sido atribuído em decorrência da ausência de informações que precisariam ser sanadas em uma conversa junto ao setor).
De forma geral, é evidente a aplicação de boas práticas relacionadas à Segurança da Informação no Grupo Sirama. A documentação comprobatória fornecida é coesa e apresenta, de maneira clara, objetiva e eficaz as melhores práticas adotadas, refletindo o bom nível técnico dos profissionais envolvidos.

No entanto, recomenda-se a realização de uma conversa com o setor responsável, a fim de esclarecer algumas dúvidas e viabilizar respostas completas para todas as questões avaliadas neste escopo, algumas das quais só podem ser plenamente compreendidas mediante esse alinhamento.

Recomenda-se também que os processos documentados (como TIC, Backup, entre outros) passem por revisões periódicas e por testes simulados regulares, de forma a garantir que os procedimentos teóricos possam ser efetivamente aplicados na prática e que os responsáveis possuem total conhecimento sobre como e quando agir.

Este é o parecer.

## 4. RECOMENDAÇÕES

## 5. PLANOS DE AÇÃO