1. RESUMO EXECUTIVO

O Resumo Executivo do Relatório de Impacto à Proteção de Dados (RIPD) apresenta uma visão concisa e abrangente das principais informações e conclusões referentes à adequação da empresa **Tombini e Cia Ltda** às exigências da Lei Geral de Proteção de Dados (LGPD).

1.1 Contexto analisado

- **Razão social:** Tombini e Cia Ltda
- **CEP:** 89.887-000
- **Endereço:** Avenida Brasil, 433, Centro - Palmitos/SC
- **CNPJ:** 82.809.088/0001-51

1.2 Responsáveis organizacionais

Encarregado de Dados	E-mail
Krinom Tecnologia e Desenvolvimento Ltda	dpo@grupotombini.com.br

Comitê gestor	E-mail
Adriane Fadani	contabilidade@grupotombini.com.br
Karolina Tombini	karolina@grupotombini.com.br
Pablo Luis Schena Reinheimer	pablo@grupotombini.com.br
Krinom Tecnologia e Desenvolvimento Ltda	carolina@krinom.com.br

O Encarregado de Dados atua como o principal vetor de conformidade da organização, constituindo o canal oficial de comunicação entre o

Controlador (a instituição), os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD), nos termos do artigo 41 da

LGPD.

Suas atribuições compreendem:

a. Receber reclamações, solicitações e comunicações dos titulares de dados, prestar os esclarecimentos devidos e adotar as providências necessárias para a garantia de seus direitos;

b. Receber as notificações e comunicações da ANPD, prestando esclarecimentos e coordenando a resposta institucional da organização;

c. Orientar de forma contínua os colaboradores, contratados e terceiros a respeito das melhores práticas operacionais e de segurança da informação;

d. Executar as demais atribuições delegadas pela Alta Administração ou determinadas pelas regulamentações e normas complementares da ANPD.

O Comitê Gestor é um órgão colegiado, multidisciplinar e deliberativo, responsável por governar, aprovar e superintender as estratégias de privacidade e proteção de dados no âmbito institucional. Reunindo lideranças de áreas críticas (como Jurídico, Tecnologia da Informação, Recursos Humanos e Operações), o Comitê assegura que a conformidade com a LGPD seja implementada de forma transversal. Suas principais responsabilidades incluem:

a. Analisar, deliberar e aprovar as políticas internas, normas e procedimentos de privacidade e segurança da informação;

b. Validar o cronograma de remediação, supervisionar a mitigação de riscos e garantir o aporte de recursos necessários ao programa;

c. Prestar suporte estratégico ao Encarregado de Dados nas decisões de alto impacto;

d. Apoiar na avaliação de eventuais incidentes de segurança, chancelando planos de contingência e mitigação de danos;

e. Avaliar periodicamente os indicadores de maturidade do programa e promover ações de conscientização corporativa.

1.3 Informações globais

- **Início do Projeto:** 20.04.2024
- **Término do Projeto:** 20.09.2024
- **Processos mapeados:** 87
- **Condição (fase) atual da programação de adequação à LGPD:** Fase coleta de informações

Condições de programação de adequação à LGPD

Para assegurar a conformidade integral com a Lei Geral de Proteção de Dados Pessoais, o programa é estruturado em cinco condições e etapas interdependentes, conforme detalhado a seguir:

- **Fase coleta de informações**: Representa o estágio inicial de diagnóstico e mapeamento de dados *(data mapping)*. Nesta fase, realiza-se o levantamento minucioso de todos os processos institucionais que envolvem o tratamento de dados pessoais. O objetivo é inventariar quais dados são tratados, por quais áreas, quais as finalidades que justificam a coleta, onde são armazenados e com quem são compartilhados, criando uma visão holística e realista do fluxo de informações na organização.
- **Fase de análise de informações e riscos:** Consiste na avaliação crítica e analítica dos dados coletados face às exigências da LGPD

(gap analysis). Nesta etapa, confrontam-se as práticas atuais da instituição com os preceitos legais e regulatórios, identificando vulnerabilidades jurídicas, fragilidades nos contratos com terceiros e brechas na segurança da informação. A partir daí, mensuram-se os riscos associados e os impactos potenciais à privacidade dos titulares.

- **Fase de recomendações:** É o momento de desenho estratégico e proposição das soluções de conformidade. Com base nos riscos e inconformidades mapeados na fase anterior, são elaborados relatórios técnicos e pareceres que indicam os caminhos necessários para mitigação de riscos. Isso inclui a recomendação de novas políticas internas, adequações contratuais, criação de avisos de privacidade e indicação de salvaguardas tecnológicas a serem adotadas.
- **Fase de implantação:** Refere-se à execução prática e operacionalização de todas as diretrizes validadas na fase de recomendações. É o momento em que o programa ganha vida: os novos contratos e termos são formalizados, as ferramentas de segurança da informação são configuradas, as políticas institucionais são publicadas e são realizados os treinamentos de conscientização com os colaboradores para consolidar a cultura de privacidade.
- **Fase de monitoramento:** Etapa contínua voltada à governança, sustentabilidade e maturidade do programa a longo prazo. Como os processos institucionais e o fluxo de dados são dinâmicos, esta fase estabelece auditorias periódicas, rotinas de verificação de conformidade e canais de atualização frente a novas normativas da ANPD, garantindo que a instituição permaneça protegida e em conformidade perene.

1.4 Time consultivo

Finalmente, são listados os membros do time consultivo responsável por guiar e assessorar a empresa Tombini e Cia Ltda em suas iniciativas de adequação à LGPD, fornecendo seus nomes e e-mails de contato para facilitar a comunicação

Responsáveis pela adequação	E-mail
Carolina Maciel	carolina.maciel@martinellilabs.com.br

1.5 Nível de proteção de dados

Com o propósito de fundamentar a estrutura metodológica e operacional adotada, a seção a seguir detalha os critérios e fluxos analíticos que guiaram a execução deste programa. Esta abordagem visa conferir total transparência, rastreabilidade e segurança às ações propostas, servindo como referencial técnico para o entendimento das conclusões apresentadas no parágrafo subsequente:



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 87 pontos.

O nível de proteção de dados, apresentado neste relatório, foi obtido por meio da análise de diversas informações relacionadas aos registros de operações de tratamento de dados pessoais, as condições atuais de segurança da informação, o status da proteção de dados pessoais dos fornecedores e/ou parceiros institucionais, e, por último, a avaliação das práticas de governança existentes.

No decorrer do processo de diagnóstico, mapeou-se e examinou-se um total de 105 processos vinculados aos Registros de Operações de Tratamento de Dados Pessoais (ROPA). Adicionalmente, foram avaliados 38 operadores de dados, juntamente com as diretrizes e salvaguardas de segurança da informação já estabelecidas.

1.6 Análise de criticidade de processos

São examinados os processos associados aos Registros de Operações de Tratamento de Dados Pessoais (ROPA) e os classificamos com base em sua importância e impacto na proteção de dados. **Cada processo é analisado em relação a 30 pontos críticos**, agrupados em cinco perspectivas-chave. São atribuídos critérios de probabilidade e impacto, categorizando os processos como de riscos toleráveis a intoleráveis. **Apresentaremos uma síntese das análises, destacando os principais pontos de atenção e recomendações para mitigar os riscos.**

1.6.1 Registros de operações de tratamento de dados pessoais

Durante a análise dos processos associados aos Registros de Operações de Tratamento de Dados Pessoais (ROPA), **foram considerados 30 pontos cruciais, agrupados em 05 perspectivas fundamentais:**

- Identificação do processo
- Titulares e tipos de dados

- Finalidade e base legal
- Compartilhamento e transferência
- Coleta de dados

Cada processo foi minuciosamente examinado quanto à sua criticidade, atribuindo-se critérios de probabilidade e impacto pelo consultor responsável. **Essa abordagem permitiu classificar os processos em riscos toleráveis, significativos, sérios ou intoleráveis, oferecendo uma visão clara sobre os potenciais impactos na proteção de dados.**

A partir dessas análises, **será apresentada uma síntese abrangente**, destacando os principais pontos críticos identificados e oferecendo recomendações estratégicas para fortalecer a segurança e a conformidade dos processos de tratamento de dados do ROPA.

Área / Setor	Processo	Pontuação	Criticidade
Recursos Humanos	Recrutamento e seleção	4.17	**Leve**
Recursos Humanos	Processo admissional	4.35	**Leve**
Recursos Humanos	Envio de dados ao E-social	3.71	**Leve**
Recursos Humanos	Fechamento | Folha de pagamento e 13°	4.35	**Leve**
Recursos Humanos	Férias	4.35	**Leve**
Recursos Humanos	Licença maternidade	3.76	**Leve**
Recursos Humanos	Licença paternidade	3.76	**Leve**

Recursos Humanos	Auxílio doença	4.18	**Leve**
Recursos Humanos	Processo demissional	4.35	**Leve**
Recursos Humanos	Cartão ponto	3.76	**Leve**
Recursos Humanos	Benefícios | Plano odontológico Bradesco	4.59	**Leve**
Recursos Humanos	Benefícios | Plano de saúde	4.59	**Leve**
Recursos Humanos	Benefício | Alimentação PicPay	5	**Moderado**
Recursos Humanos	Vale transporte	3.71	**Leve**
Recursos Humanos	Integração | Treinamento	4.41	**Leve**
Recursos Humanos	Advertência	3.94	**Leve**
Segurança do Trabalho	Exames ocupacionais	6.53	**Moderado**
Segurança do Trabalho	Planilha de controle - Saúde, Segurança e Meio Ambiente (SSMA)	6.06	**Moderado**
Segurança do Trabalho	Planilha de controle - Atestado de Saúde Ocupacional (ASO)	6.06	**Moderado**
Segurança do Trabalho	Controle de colaboradores - Sistema Avior	6.59	**Moderado**
Segurança do Trabalho	Controle e acompanhamento de treinamentos - Conecta Tombini	6.47	**Moderado**

Segurança do Trabalho	Ficha de Equipamento de Proteção Individual (EPI)	6.33	**Moderado**
Segurança do Trabalho	Carta de preposto - Sistema de gestão e produtos perigosos da empresa	6.82	**Moderado**
Segurança do Trabalho	Registro SESMT	5.24	**Moderado**
Segurança do Trabalho	Abertura de CAT	6.18	**Moderado**
Segurança do Trabalho	CIPA	5.11	**Moderado**
Segurança do Trabalho	Investigação de acidente de trabalho	5.39	**Moderado**
Fiscal | Contábil	Lançamento fiscal | Fretes	6.06	**Moderado**
Fiscal | Contábil	Lançamento fiscal - Folha de pagamento	6.06	**Moderado**
Fiscal | Contábil	Declaração de imposto de renda | Sócios da empresa	6.18	**Moderado**
Fiscal | Contábil	Cadastro de clientes e fornecedores | Documentação dos sócios	7.59	**Moderado**
Fiscal | Contábil	Balanço patrimonial	6.76	**Moderado**
Fiscal | Contábil	Relatórios de faturamento | Anual e trimestral	5.12	**Moderado**
Fiscal | Contábil	Registros e alterações de contratos socias - Junta Comercial	6.82	**Moderado**
Financeiro	Contas a receber | Títulos	6.47	**Moderado**
Financeiro	Contas a receber | Fretes	6.47	**Moderado**

Faturamento	Emissão de documentos | Transporte de Carga	5	**Moderado**
Faturamento	Contratos de terceiros	4.5	**Leve**
Administrativo	Acesso aos cadastros dos colaboradores e motoristas	4.94	**Leve**
Administrativo	Cadastro de motoristas nos sistemas dos clientes | Ordem de coleta	4.94	**Leve**
Administrativo	Acesso ao Ponto Eletrônico | Monitoramento da jornada do departamento	5.12	**Moderado**
Administrativo	Contratação de prestador de serviço | Chapa	4.47	**Leve**
Júridico	Apoio aos escritórios externos | Documentação demandas judiciais	4.11	**Leve**
Júridico	Prepostos | Audiências	4.28	**Leve**
Júridico	Análise de contrato	5.12	**Moderado**
Júridico	Elaboração de contrato	5.5	**Moderado**
Recursos Humanos	Controle | Planilha de advertências	5	**Moderado**
Recursos Humanos	Controle | Planilha de colaboradores desligados	5	**Moderado**
Recursos Humanos	Controle | Planilha de pagamentos dos colaboradores	5.53	**Moderado**
Recursos Humanos	Termo de LGPD	3.59	**Leve**

Recursos Humanos	Termo de uso de imagem	3.59	**Leve**
Recursos Humanos	Abertura de conta salário | Caixa Econômica Federal	4.71	**Leve**
Recursos Humanos	Controle | Planilha de controle da jornada dos motoristas	5.12	**Moderado**
Recursos Humanos	Declaração de imposto de renda | Colaboradores	3.59	**Leve**
Recursos Humanos	Empréstimos consignados | Avaliação	5.12	**Moderado**
Recursos Humanos	Envio de documentação dos colaboradores para os clientes	5.41	**Moderado**
Financeiro	Contas a pagar | Colaboradores	4.35	**Leve**
Financeiro	Contas a pagar | Prestadores de serviço	3.94	**Leve**
Financeiro	Vendas de veículos | Análise do contrato e preenchimento do CRV	4.35	**Leve**
Financeiro	Vendas de veículos | Emissão de boletos para pagamento	4.35	**Leve**
Financeiro	Vendas de veículos | Alienação e Reserva de domínio.	4.35	**Leve**
Relacionamento com Cliente | Vendas	Prospecção de clientes	4.33	**Leve**
Relacionamento com Cliente | Vendas	Licitação nacionais privadas	5	**Moderado**
Relacionamento com Cliente | Vendas	Envio de documentação | Licitação nacionais privadas	4.12	**Leve**

Relacionamento com Cliente | Vendas	Envio de documentação para clientes	4.71	**Leve**
Expedição e Logística	Emissão de documentos fiscais | Transporte de cargas	4.35	**Leve**
Expedição e Logística	Acompanhamento da viagem	4.59	**Leve**
Gestão de Frotas	Apoio aos motoristas	3.94	**Leve**
Gestão de Frotas	Ordem de abastecimento	4.44	**Leve**
Manutenção | Oficina	Atendimento das solicitações de manutenção | Motoristas	4.18	**Leve**
Manutenção | Oficina	Ordem de serviço | Externa	4.29	**Leve**
Manutenção | Oficina	Ordem de serviço | Interna	4.06	**Leve**
Manutenção | Oficina	Ordem de serviço | Acidentes	4.29	**Leve**
Compras | Suprimentos	Negociação de compras | Orçamentos	3.59	**Leve**
Compras | Suprimentos	Solicitação de compras	4.18	**Leve**
Compras | Suprimentos	Ordem de compra	4.29	**Leve**
Almoxarifado	Lançamento de peças, materiais e suprimentos	3.59	**Leve**
Monitoramento de Motoristas	Monitoramento da Frota	4.11	**Leve**
Monitoramento de Motoristas	Monitoramento de Entrega	4.11	**Leve**

Núcleo de Conformidade	Controle de Integração e Treinamento	4.17	**Leve**
Núcleo de Conformidade	Controle Termo de LGPD	3.39	**Leve**
Núcleo de Conformidade	Controle Termo de Uso de Imagem	3.39	**Leve**
Núcleo de Conformidade	Canal de Denúncias	3.39	**Leve**
Núcleo de Conformidade	Apoia à Auditorias | Fornecimento de Documentos	3.39	**Leve**
Núcleo de Conformidade	Campanha Zero Acidentes	4.17	**Leve**
Núcleo de Conformidade	Controle de Apoio ao RH	4.17	**Leve**
Relacionamento com Cliente | Pós Vendas	Satisfação do Cliente | Atendimento	4.33	**Leve**

1.6. 2 LIA

À luz da LGPD, Artigo 7º, IX, o legítimo interesse figura como uma das bases legais mais flexíveis e complexas para o tratamento de dados pessoais, exigindo, em contrapartida, um rigoroso juízo de proporcionalidade por parte do controlador. O LIA é o instrumento documental indispensável para demonstrar e fundamentar a licitude desse tratamento, estruturando-se sob o princípio da responsabilização *(accountability)*. Sua análise é composta por um teste de quatro fases:

a. Verificação de que o interesse do controlador é lícito, concreto e atende a finalidades legítimas;

b. Confirmação de que o tratamento é estritamente necessário para atingir o objetivo, não havendo meio menos intrusivo;

c. Ponderação que garante que os direitos e liberdades fundamentais

do titular não prevaleçam sobre o interesse econômico ou institucional da organização;

d. Implementação de medidas de transparência (como o direito de oposição/opt-out) e segurança para mitigar os impactos aos titulares.

Organograma	Inventário de Dados
Recursos Humanos	Recrutamento e seleção

1.Finalidade legítima (Art. 10, caput e inciso I da LGPD)

ID	Questionamentos/Orientações	Resposta
1	**Qual é a finalidade do tratamento de dados pessoais?** Detalhar qual o objetivo que se pretende atingir com o tratamento dos dados pessoais.	Realizar a avaliação e seleção dos candidados que enviaram currículo para as vagas de trabalho em aberto da Tombini.
2	**O tratamento é necessário para atender um ou mais objetivos organizacionais?** Se o tratamento é necessário para atingir um objetivo comercial legal, é provável que seja legítimo.	Sim , selecionar os candidados aptos para recrutar e preencher as vagas de trabalho da empresa.
3	**Situação concreta** Detalhe o contexto em que se dará o tratamento de dados.	As vagas disponíveis são divulgadas através do site e nas redes sociais em nome da empresa. Os currículos podem ser enviados através do e-mail institucional (recrutamento@grupotombini.com.br), WhatsApp Corporativo, anexados no site da empresa ou entregues pessoalmente.
4	**O tratamento é necessário para atender um ou mais objetivos específicos de terceiros?** Embora você possa apenas identificar as finalidades de tratamento para aplicar o legítimo interesse, recomendamos que liste os demais agentes de tratamento interessados na atividade de tratamento pretendido. Por exemplo: parceiros de negócio.	Sim, em alguns casos, ás vagas preenchidas pelos candidatos serão para atuar de forma direta com os clientes da empresa. Inclusive, para a seleção dos candidatos é avaliado requisitos exigidos por esses clientes.
5	**Existe alguma referência legal ou normativa que está atrelada ao tratamento pretendido?** Por exemplo: o tratamento precisa ser realizado para suportar uma atividade obrigatória.	Não.

2.Necessidade (Art. 10, §1º da LGPD)

ID	Questionamentos/Orientações	Resposta
6	**Porque o tratamento pretendido é importante para a empresa?** O tratamento é opcional ou crítico para os negócios da empresa.	É importante para preencher os postos de trabalhos e dar contuinidade nos negócios da empresa.
7	**O tratamento é importante para terceiros?** Considere se os interesses estão relacionados a um direito fundamental, um interesse público ou outro tipo de interesse.	Sim, em alguns casos, ás vagas preenchidas pelos candidatos serão para atuar de forma direta com os clientes da empresa. Além de beneficiar, de forma indireta, a sociedade em geral, pois esse processo visa gerar emprego e renda.
8	**Existe outra maneira de alcançar o objetivo?** Se não houver, é claro que o processamento é necessário; ou Se houver outra maneira, mais exigiria esforço desproporcional, o tratamento ainda é necessário; ou Se houver várias maneiras de atingir o objetivo, uma avaliação de impacto na privacidade poderá identificar meios menos invasivos de realizar o tratamento dos dados que seriam necessários; ou Se o tratamento não for necessário, os interesses legítimos não poderão ser considerados como uma base legal para esse tratamento.	Não.
9	**Minimização (Principio da necessidade, uso de dados pessoais menos intrusivos)** Apenas os dados pessoais estritamente necessários para atingir a finalidade pretendida estão sendo processados, evitando, assim, o uso de dados em excesso, não compatíveis e adequados.	Estão sendo processados apenas dados estritamente necessários para atingir a finalidade pretendida.
10	**Outras bases legais** Existe alguma outra base legal, como consentimento, execução do contrato ou obrigação legal, ou outra prevista no rol do Art. 7º?	Sim, poderia utilizar a base legal do consentimento. Entretanto, para possibilitar a utilização dessa base é necessário rever o processo, implementando a formalização, possibilidade de gestão e revogação do consentimento.

3.Balanceamento de direitos (Art. 6°, I; Art.7°, IX e Art.10, II da LGPD)

ID	Questionamentos/Orientações	Resposta
11	**O titular espera que este tratamento de dados ocorra?** Se os titulares esperam que o tratamento ocorra, é provável que o impacto à privacidade já tenha sido considerado por eles e aceito. se eles não tem expectativa, o impacto é maior e ganha mais peso no teste de balanceamento.	Sim. Para esse processo, de forma indireta, há o consentimento dos candidatos devido a leitura da descrição da vaga e o seu consentimento em enviar o seu currículo com os dados pessoais. O títular de dados conhece a finalidade e aceita o tratamento de dados com o envio do currículo.
12	**O tratamento pretendido agrega valor a um produto ou serviço que ele utiliza?**	Não.

13	**É provável que o tratamento tenha um impacto negativo nos direitos do titular?**	Improvável, porque a finalidade do tratamento de dados é estritamente à seleção dos candidados mais aptos para preencher os postos de trabalho. Inclusive, existe o procesos de descarte dos currículos físicos não selecionados, após o período de 1 (um) ano do envio do currículo.
14	**É provável que o tratamento resulte em dano injustificado ou prejuízo ao titular?**	Improvável, porque a finalidade do tratamento de dados é estritamente à seleção dos candidados mais aptos para preencher os postos de trabalho. Inclusive, existe o procesos de descarte dos currículos físicos não selecionados, após o período de 1 (um) ano do envio do currículo.
15	**Pode ocorrer um prejuízo para a empresa caso o tratamento não ocorra?**	Sim, sem o processo de seleção e avaliação dos candidatos a empresa não conseguirá selecionar os candidatos aptos para ás vagas de trabalhos. Impactaria de forma negativa, possibilitando selecionar candidados que não atendem as exigências mínimas das vagas.
16	**Pode ocorrer um prejuízo para terceiros caso o tratamento não ocorra?**	Sim, sem o processo de seleção e avaliação dos candidatos a empresa não conseguirá selecionar os candidatos aptos para ás vagas de trabalhos. Impactaria de forma negativa, possibilitando selecionar candidados que não atendem as exigências mínimas das vagas. Inclusive, alguns clientes tem exigências quanto aos requisitos que devam ser avaliados para contratar empregados que vão atuar de forma direta com esses clientes.
17	**O tratamento é do interesse do titular cujos dados pessoais estão relacionados?**	Sim, pois o tratamento de dados possibilita a contratação do candidato, que por livre interesse, encaminhou seu currículo com os dados pessoais para avaliação.
18	**Os interesses legítimos do titular estão alinhados com a parte dos interesses legítimos para o tratamento pela empresa?** Quais são os benefícios para o titular ou a sociedade?	Sim, tendo em vista que a empresa tem o interesse de selecionar empregados para ocupar os postos de trabalhos, e o titular tem o interesse de ser contratados pela empresa. Além disso, impacta a sociedade gerando benefícios como geração de emprego e renda.
19	**Qual é a conexão entre o titular e a empresa?** Por exemplo: cliente existente; ex-cliente; empregado ou contratado; prospect; fornecedor; outros.	Avaliação dos dados pessoais dos candidatos, enviados através do currículo, para preencher postos de trabalhos.
20	**O processamento limita direitos dos titularse** Se o tratamento prejudicar ou frustrar a capacidade de exercer direitos no futuro que podem afetar o equilíbrio.	O processo não limita, prejudica ou frustra a capacidade do titular exercer direitos.

21	**Os dados pessoais serão obtidos diretamente do titular ou indiretamente?**	Os dados pessoais são obtidos de forma direta pelo títular dos dados, através do envio do seu currículo.
22	**O tratamento pode ser considerado intrusivo ou inadequado pelo titular?**	É pouco provável que o tratamento seja considerado intrusivo ou inadequado pelo titular.
23	**Será ou é fornecido um aviso sobre este tratamento ao titular? Em caso afirmativo, como ele será feito?**	Nos casos dos candidatos aprovados é avisado sobre sua aprovação através de e-mail isntitucional e/ou WhatsApp Corporativo. Entretanto, é possível implementar um retorno a todos os títulares de dados em relação ao preenchimento das vagas que se candidatou.
24	**O titular pode se opor a este tratamento? Se não, explique.**	Sim, poderá se opor, entretanto, será impedido de ser avaliado e concorrer ás vagas de emprego ofertadas pela empresa.
25	**O escopo de tratamento pode ser modificado para reduzir/mitigar riscos ou danos à privacidade?**	É possível sim, implementados formas de formalização, gestão e revogação do consentimento, aviso e retorno sobre o andamento dos processos seletivos e estruturação de processo de descarte dos currículos físicos em período menor que 1 (um) ano. Bem como a estruturação de processo de descarte dos currículos digitais.

4.Salvaguardas e Controles de Riscos (Art. 10, § 2° e § 3° da LGPD)

ID	Questionamentos/Orientações	Resposta
26	**Quais são as medidas e instrumentos empregados para assegurar os direitos dos titulares dos dados pessoais e evitar que os dados sejam eventualmente tratados de modo indevido?**	Os dados são utilizados somente para a finalidade para a qual se destinam, e compartilhadas somente com os colaboradores responsáveis pela realização das entrevistas e demais tramites relacionados ao processo de recrutamento e seleção.
27	**Mitigação de Riscos** Medidas possíveis. Por exemplo: anonimização, pseudoanonimização, segmentação das bases de dados, controle de acesso aos dados.	É possível aplicar processo de anonimização em alguns dados utilizados neste processo, para ter maior proteção.
28	**Transparência** Explicação sobre quais dados são coletados, como eles são utilizados e permitir ao titular acesso a uma cópia dos seus dados pessoais.	Os dados tratados nesse processo são enviados pelo próprio título de dados através de seu currículo. Dessa forma, ele já possuí cópia do seus dados pessoais e transparência de quais dados pessoais estão sendo tratados. Não obstante, caso o candidado tenha condições de aprovação no processo seletivo poderá ser solicitado outros dados pessoais, cabendo ao candidato enviar ou não enviar.

29	**Mecanismos de oposição (opt-out)** Forma como o titular dos dados pode se opor ao tratamento dos seus dados, caso não concorde com este ou o tratamento estiver em desconformidade com a legislação.	Ainda não desenvolvido. É possível elaborar um canal para que o titular entre em contato solicitando a exclusão de seus dados.

5.Avaliação

ID	Questionamentos/Orientações	Resposta
30	**Resultado da avaliação**	Favorável
31	**Considerações** Com base nas respostas acima, formalize se você acredita que pode aplicar o legítimo interesse para o tratamento de dados pessoais pretendido. Por favor, explique, talvez usando tópicos por que você acredita que seja possível ou não aplicar o legítimo interesse. Você deve basear-se nas respostas acima.	É viável a aplicação da base legal legitimo interesse tendo em vista que o tratamento de dados visa realizar o recrutamento e seleção de novos colaboradores, o que traz benefícios a empresa e aos candidatos. Além de existir trasnparência em relação a finalidade do tratamento de dados e de forma indireta o consentimento do título de dados ao enviar seus dados pessoais para avaliação.
32	**Área de Negócio**	Recursos Humanos.
33	**Data da Avaliação**	24/06/2024
34	**Nome do Avaliador**	Gabriel Alberto Ferrari.

6.Avaliação do encarregado pelo tratamento de dados pessoais

ID	Questionamentos/Orientações	Resposta
35	**Resultado da avaliação**	
36	**Considerações** Formalize se você acredita que pode aplicar o legítimo interesse para o tratamento de dados pessoais pretendido.	
37	**Data da avaliação**	
38	**Nome do encarregado**	

1.6. 3 RIPD

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD), em conformidade com o artigo 5º, inciso XVII, da LGPD, constitui a documentação técnica do controlador que descreve pormenorizadamente os processos de tratamento de dados pessoais passíveis de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Este relatório detalha as medidas, salvaguardas e mecanismos de mitigação de riscos adotados pela organização. Trata-se

de uma peça obrigatória para operações que envolvam tratamentos de alto risco, dados sensíveis ou decisões automatizadas, servindo como ferramenta essencial de transparência preventiva *(privacy by design)* e de prestação de contas perante a ANPD.

1.6. 4 Segurança de informações

A segurança da informação como pilar fundamental para o sucesso do programa de adequação à Lei Geral de Proteção de Dados, haja vista a crescente dependência de sistemas de gestão e de dados dentro das organizações.

Nesse contexto, as normas ISO 27001 e 27002 emergem como referências globais para a implementação de Sistemas de Gestão da Segurança da Informação (SGSI) robustos e eficazes. Ambas as normas fornecem um conjunto de diretrizes e controles de segurança que visam proteger os ativos de informação das organizações, garantindo a sua confidencialidade, integridade e disponibilidade.

- **ISO 27001:** Essa norma estabelece os requisitos para a implementação, manutenção e melhoria contínua de um SGSI. Ela define o ciclo de vida do sistema, desde o planejamento e a implementação até a avaliação e a melhoria. A ISO 27001 é certificável, ou seja, as empresas podem obter uma certificação que atesta o cumprimento dos requisitos da norma.

- **ISO 27002:** Complementa a ISO 27001, fornecendo um catálogo detalhado de controles de segurança que podem ser adotados pelas organizações. Esses controles abrangem uma ampla gama de áreas, como gestão de ativos, gestão de acesso, criptografia, gestão de incidentes de segurança e muito mais. A ISO 27002 oferece flexibilidade para que as empresas selecionem os controles mais adequados ao seu contexto específico.

A adoção das normas ISO 27001 e 27002 traz diversos benefícios para as empresas, tais como:

- **Redução de riscos:** Os controles de segurança implementados ajudam a identificar e mitigar as vulnerabilidades, reduzindo o risco de incidentes de segurança.

- **Melhoria da reputação:** A certificação ISO 27001 demonstra o compromisso da empresa com a segurança da informação, fortalecendo a confiança dos clientes, parceiros e stakeholders.

- **Conformidade legal e regulatória:** As normas ISO 27001 e 27002 podem auxiliar as empresas a cumprirem as exigências legais e regulatórias relacionadas à proteção de dados.

- **Otimização de processos:** A implementação de um SGSI pode levar à otimização dos processos de negócios, aumentando a eficiência e a produtividade.

- **Melhoria da tomada de decisões:** Um SGSI fornece informações valiosas para a tomada de decisões estratégicas relacionadas à segurança da informação.

Em vista disso e da crescente complexidade e ameaças cibernéticas, a segurança da informação é um ativo estratégico para as empresas a PRIVIA, aplicou como diretrizes de análise, as normas ISO 27001 e 27002 que oferecem um framework robusto e abrangente para a implementação de um SGSI eficaz. Ao adotar essas normas, as organizações podem proteger seus ativos de informação, garantir a continuidade dos negócios e fortalecer a sua posição no mercado.

Como parâmetros de análises utilizados pela equipe técnica da PRIVIA, são elencados 45 controles de critérios de avaliação. Como resultado, as condições existentes evidenciaram que a exposição à riscos a Segurança da Informação foram classificados como:

PVE	Processo	Execução	Criticidade
Controles Operacionais	SI - CO - Políticas de segurança da informação	Sim	Leve
Controles Operacionais	SI - CO - Papéis e responsabilidades	Sim	Leve
Controles Operacionais	SI - CO - Segregação de funções	Sim	Leve
Controles Operacionais	SI - CO - Responsabilidade da direção	Sim	Leve
Controles Operacionais	SI - CO - Contato com grupos de interesse especial	Sim	Leve
Controles Operacionais	SI - CO - Inteligência de ameaças	Sim	Leve
Controles Operacionais	SI - CO - Inventário de informações	Sim	Leve
Controles Operacionais	SI - CO - Uso aceitável de informações	Sim	Leve
Controles Operacionais	SI - CO - Devolução de ativos	Sim	Leve
Controles Operacionais	SI - CO - Classificação de informações	Sim	Leve
Controles Operacionais	SI - CO - Transferência de informações	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	Moderado
Controles Operacionais	SI - CO - Controle de acessos	Sim	Leve
Controles Operacionais	SI - CO - Gestão de identidade	Sim	Leve

Controles Operacionais	SI - CO - Informações de autenticação	Sim	Leve
Controles Operacionais	SI - CO - Direitos de acesso	Sim	Leve
Controles Operacionais	SI - CO - Segurança de informações nas relações com fornecedores	Sim	Leve
Controles Operacionais	SI - CO - Segurança da informação para uso de serviços em nuvem	Sim	Leve
Controles Operacionais	SI - CO - Planejamento e preparação da gestão de incidentes de segurança da informação	Sim	Leve
Controles Operacionais	SI - CO - Avaliação e decisão sobre eventos de segurança da informação	Sim	Leve
Controles Operacionais	SI - CO - Prontidão de TIC para continuidade de negócios	Sim	Leve
Controles Operacionais	SI - CO - Requisitos legais, estatutários, regulamentares e contratuais	Sim	Leve
Controles de Pessoas	SI - CP - Termos e condições de contratação	Sim	Leve
Controles de Pessoas	SI - CP - Conscientização, educação e treinamento em segurança da informação	Sim	Leve
Controles de Pessoas	SI - CP - Processo disciplinar	Sim	Leve
Controles de Pessoas	SI - CP - Responsabilidades após encerramento ou mudança da contratação	Sim	Leve
Controles de Pessoas	SI - CP - Acordos de confidencialidade ou não divulgação	Sim	Leve

Controles de Pessoas	SI - CP - Trabalho remoto	Sim	**Leve**
Controles de Pessoas	SI - CP - Relato de eventos de segurança da informação	Sim	**Leve**
Controles Físicos	SI - CF - Perímetros de segurança física	Sim	**Leve**
Controles Físicos	SI - CF - Entrada física	Sim	**Leve**
Controles Físicos	SI - CF - Segurança de escritórios, salas e instalações	Sim	**Leve**
Controles Físicos	SI - CF - Monitoramento de segurança física	Sim	**Leve**
Controles Físicos	SI - CF - Segurança de ativos fora das instalações da organização	Sim	**Leve**
Controles Tecnológicos	SI - CT - Direitos de acessos privilegiados	Sim	**Leve**
Controles Tecnológicos	SI - CT - Restrição de acesso à informação	Sim	**Leve**
Controles Tecnológicos	SI - CT - Autenticação segura	Sim	**Leve**
Controles Tecnológicos	SI - CT - Proteção contra malware	Sim	**Leve**
Controles Tecnológicos	SI - CT - Gestão de vulnerabilidades técnicas	Sim	**Leve**
Controles Tecnológicos	SI - CT - Exclusão de informações	Sim	**Leve**
Controles Tecnológicos	SI - CT - Mascaramento de dados	Parcialmente alinhado	**Grave**
Controles Tecnológicos	SI - CT - Prevenção de vazamentos de dados	Sim	**Leve**

Controles Tecnológicos	SI - CT - Backup de informações	Sim	**Leve**
Controles Tecnológicos	SI - CT - Redundância de recursos para tratamento de informações	Sim	**Leve**
Controles Tecnológicos	SI - CT - Log	Sim	**Leve**
Controles Tecnológicos	SI - CT - Atividades de monitoramento	Sim	**Leve**

1.6.5 Operadores de dados

A avaliação criteriosa dos operadores de dados pessoais constitui um pilar indispensável para a segurança jurídica e a mitigação de riscos institucionais. Sob a égide da LGPD, o controlador e o operador respondem de forma solidária por eventuais danos patrimoniais, morais, individuais ou coletivos decorrentes de violações de dados, caso o operador descumpra as obrigações da lei ou as instruções lícitas fornecidas pelo controlador (Artigo 42 da LGPD). Portanto, avaliar e homologar os operadores sob a ótica da proteção de dados não é apenas uma boa prática operacional, mas um dever de diligência (due diligence) essencial para garantir a integridade de toda a cadeia de tratamento e resguardar a organização contra passivos reputacionais e sancionatórios.

Foram analisadas as condições de proteção de dados pessoais de **37 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
Codema Comercial e Importadora Ltda	Fornecedor	0.38	Grave
Trucks Comércio e Tecnologia de Rastreadores e Comunicações Ltda	Fornecedor	0.63	Grave
Trucks Control - Serviços de Logística Ltda	Fornecedor	0.63	Grave
Truck Simione Eireli	Fornecedor	0.13	Crítico
Massotti e Zeni Ltda	Fornecedor	0.13	Crítico
Inovar Soluções em Implementos Rodoviários Ltda	Fornecedor	0.13	Crítico
T4S Tecnologia S.A.	Fornecedor	0.63	Grave
Nox Gerenciamento e Monitoramento de Risco Ltda	Fornecedor	0.88	Leve
Dell Computadores do Brasil Ltda	Fornecedor	0.63	Grave
Gilva Rosa de Macedo	Fornecedor	0.13	Crítico
Camsis Tecnologia Ltda	Fornecedor	0.13	Crítico
Innova32 Ltda	Fornecedor	0.38	Grave
Ambipar Response S/A	Fornecedor	0.63	Grave
Paulimed Medicina e Segurança do Trabalho Ltda	Fornecedor	0.13	Crítico

Gestão de Terceirização em Serviços Seleção e Agenciamento de Mão de Obra Ltda	Fornecedor	0.13	**Crítico**
Maxx Brasil Soluções	Fornecedor	0.13	**Crítico**
Segmento Comércio de Equipamentos de Segurança Ltda	Fornecedor	0.13	**Crítico**
Latina Parts And Solutions Ltda	Fornecedor	0.63	**Grave**
Guincho Jundiai Ltda Me	Fornecedor	0.25	**Crítico**
Whatsapp Corporativo	Fornecedor	1	**Leve**
Google	Fornecedor	1	**Leve**
Sistema Questor	Fornecedor	1	**Leve**
Sistema Avior	Fornecedor	1	**Leve**
Ponto Secullum	Fornecedor	1	**Leve**
Sistema Ponto Mais	Fornecedor	1	**Leve**
Sistema Promax	Parceiro institucional	0.63	**Grave**
PicPay	Fornecedor	1	**Leve**
Mednet	Fornecedor		-
Sistemas TMS	Fornecedor	0.38	**Grave**

Bradesco Plano Odontológico	Fornecedor	1	**Leve**
Banco Bradesco S/A	Fornecedor	1	**Leve**
Caixa Econômica Federal	Fornecedor	1	**Leve**
Microsoft	Fornecedor	1	**Leve**
Detran SC	Fornecedor	1	**Leve**
Detran SP	Fornecedor	1	**Leve**
Sistema OnixSat	Fornecedor	1	**Leve**
Sistema Squelo	-		-

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 03 (três) áreas de atenção, a saber:

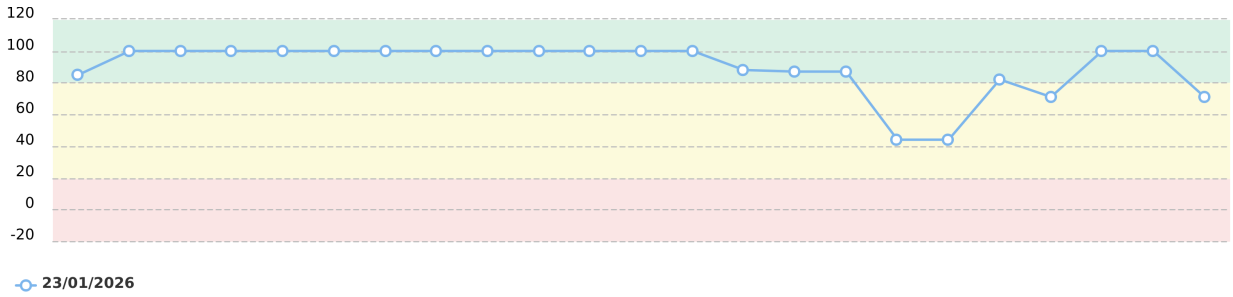
- Governança
- Áreas e Processos

- Segurança de Informações

Ao todo, foram identificados, organizados e mensurados 23 (vinte e três) 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.

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.

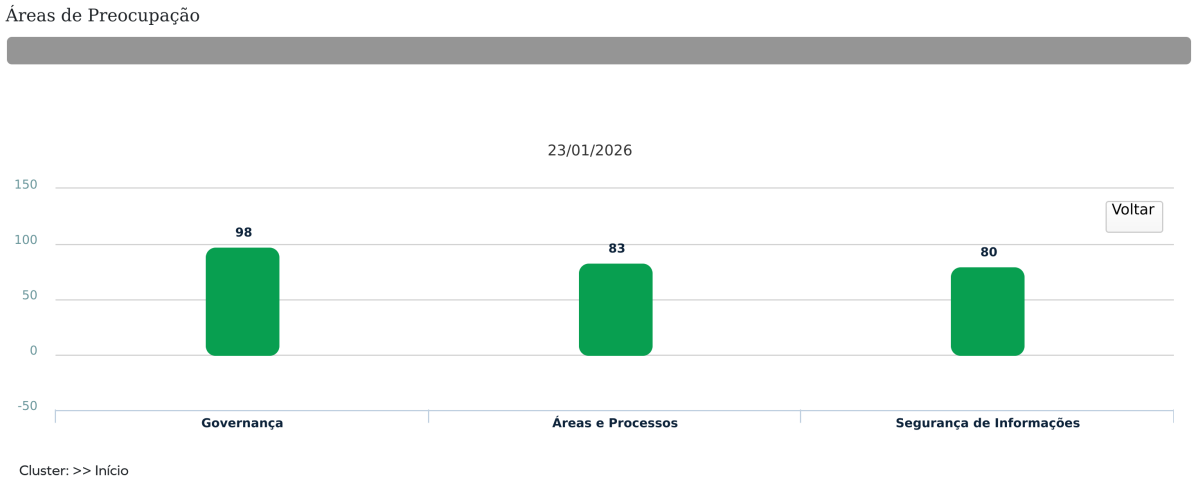
Uma faixa na cor "amarela", destacando indicadores em nível de mercado e/ou competitividade. E, uma faixa na cor "vermelho", destacando indicadores em nível de comprometimento.

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 Tombini e Cia Ltda , possui:

- 19 indicadores em nível de excelência
- 4 indicadores em nível de competitividade
- 0 indicadores em nível de comprometimento

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

Áreas de preocupação



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:

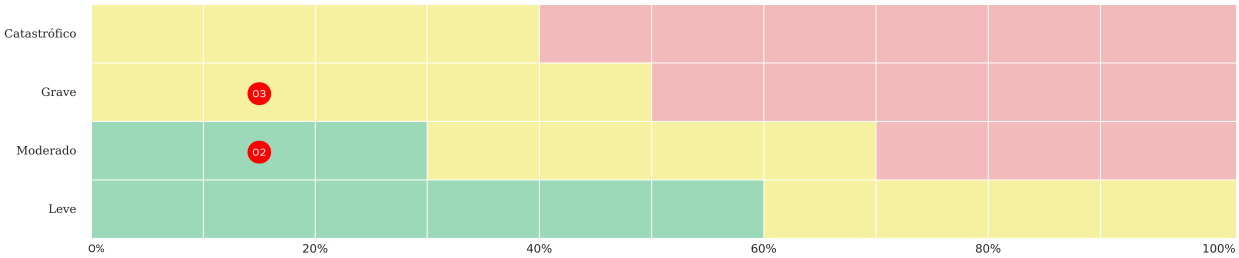
Foram identificados 5 (cinco) riscos associados à proteção de dados, sendo eles:

- **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.

Quadrante



Análise de risco

Risco	Consequência	Prob.	TS	Pts
R1 - Sanções judiciais e/ou administrativas	**Moderado**	16%	30%	9

R2 - Crimes cibernéticos	**Grave**	17%	20%	14
R3 - Dano reputacional	**Grave**	16%	20%	13
R4 - Perdas de parceiros institucionais / comerciais	**Moderado**	15%	15%	8
R5 - Rescisões contratuais	**Grave**	12%	15%	10