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 **Colégio Harmonia Ltda** às exigências da Lei Geral de Proteção de Dados (LGPD).

1.1 Contexto analisado

- **Razão social:** Colégio Harmonia Ltda
- **CEP:** 79.020-101
- **Endereço:** Rua Goias, 930, Jardim dos Estados, Campo Grande/MS
- **CNPJ:** 04.247.695/0001-61

1.2 Responsáveis organizacionais

Encarregado de Dados	E-mail

Comitê gestor	E-mail

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:** 23/06/2026
- **Término do Projeto:**
- **Processos mapeados:** 54

- **Condição (fase) atual da programação de adequação à LGPD:** Fase de análise de informações e riscos

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 Colégio Harmonia 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
Jenifer Tainara da Silva Cardoso	jenifer.cardoso@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 43 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 66 processos vinculados aos Registros de Operações de Tratamento de Dados Pessoais (ROPA). Adicionalmente, foram avaliados 15 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
Secretaria	Contratos | Alunos	3	**Leve**
Secretaria	Matrícula | Aluno - Cadastro Sistema	4.05	**Leve**
Secretaria	Rematrícula | Aluno	4.05	**Leve**
Secretaria	Comunicação | Pais	4.05	**Leve**
Secretaria	Arquivo | Alunos Inativos	3.84	**Leve**
Secretaria	Arquivo | Alunos Ativos	2.89	**Leve**
Departamento Financeiro	Contas a receber | Mensalidades	2.89	**Leve**
Departamento Financeiro	Contas a receber | Controle Inadimplência	3.79	**Leve**
Departamento Financeiro	Contas a pagar | Recebimento de boletos	3.89	**Leve**
Departamento Financeiro	Contas a pagar | Notas Fiscais	3.89	**Leve**

Departamento Financeiro	Contas a pagar | Reembolso colaborador	4.79	**Leve**
Departamento Financeiro	Contas a pagar | Reembolso Alunos (responsáveis)	3.16	**Leve**
Departamento Financeiro	Compras | Fornecedores	3.89	**Leve**
Recursos Humanos	Contratação | Processo seletivo	4.42	**Leve**
Recursos Humanos	Admissão | Recebimento de documentos	3.84	**Leve**
Recursos Humanos	Admissão | Exames	3.47	**Leve**
Recursos Humanos	Abertura de Conta Salário	3.47	**Leve**
Recursos Humanos	Arquivo | Armazenamento de documentos (ativos e inativos)	3.47	**Leve**
Recursos Humanos	Admissão | Jovem Aprendiz	3.84	**Leve**
Recursos Humanos	Admissão | Estagiários	3.84	**Leve**
Recursos Humanos	Folha de Pagamento	3.89	**Leve**
Recursos Humanos	Controle de Jornada	3.26	**Leve**
Recursos Humanos	Gestão de Benefícios | Plano de Saúde (Unimed)	3.32	**Leve**
Recursos Humanos	Gestão de Benefícios | Plano Odontológico (Uniodonto)	3.32	**Leve**
Recursos Humanos	Gestão de Benefícios | Santa Casa Saúde	3.84	**Leve**

Recursos Humanos	Licenças e Afastamentos	4.11	**Leve**
Recursos Humanos	Processo Demissional	3.84	**Leve**
Recursos Humanos	Auditoria Mensal	3.42	**Leve**
Recursos Humanos	Jurídico | Demandas Trabalhistas	3.47	**Leve**
Coordenação Pedagógica	Solicitação de informações administrativas	2.89	**Leve**
Coordenação Pedagógica	Gestão | Professores Horários	3.79	**Leve**
Coordenação Pedagógica	Gestão | Professores Formação	3.26	**Leve**
Coordenação Pedagógica	Relatório Pedagógico | Alunos	3.53	**Leve**
Coordenação Pedagógica	Reuniões Pedagógicas	2.89	**Leve**
Coordenação Pedagógica	Passeios Escolares | Tratativa Alunos	3.58	**Leve**
Coordenação Pedagógica	Passeios Escolares | Tratativa Local Visita	3.79	**Leve**
Assistentes educacionais	Acesso ao cadastro | Aluno	1.89	**Leve**
Assistentes educacionais	Atendimento | Novas Famílias	3.89	**Leve**
Assistentes educacionais	Lançamento de faltas	3.37	**Leve**
Assistentes educacionais	Controle | Alunos com deficiência	1.89	**Leve**

Portaria	Controle de acesso | Ensino Fundamental	1.42	**Leve**
Portaria	Controle | Pessoas autorizadas para buscar	1.53	**Leve**
Portaria	Controle | Monitoramento de Câmeras	2	**Leve**
Portaria	Controle de Acesso | Prestador de serviço	1.42	**Leve**
Direção	Gestão Financeira | Autorização de pagamentos	1.47	**Leve**
Orientação Educacional	Atendimento Famílias	2	**Leve**
Orientação Educacional	Relatório | Alunos com necessidades educacionais de aprendizagem	3	**Leve**
Orientação Educacional	Comunicação | Profissionais Externos	2.95	**Leve**
Orientação Educacional	Relatório | Profissionais Externos	3.79	**Leve**
Orientação Educacional	Controle | Ocorrências	2.89	**Leve**
Orientação Educacional	Acesso | Sistema Cadastro TOTVS	1.47	**Leve**
Orientação Educacional	Boletim escolar | Conselho de Classe	2.05	**Leve**
Secretaria	Transferência Escolar	2.89	**Leve**
Portaria	Controle de acesso | Reconhecimento Facial	1.95	**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	Contratação | Processo seletivo

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 processos seletivos para recrutamento, avaliação e seleção de candidatos para preenchimento de vagas disponíveis na instituição, incluindo análise de currículos, contato com candidatos, realização de entrevistas e demais etapas necessárias à avaliação de perfil e compatibilidade com a vaga.

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. O tratamento é necessário para viabilizar a identificação, avaliação e seleção de candidatos aptos a ocupar vagas disponíveis, permitindo à instituição formar seu quadro de colaboradores de acordo com suas necessidades organizacionais. O tratamento possibilita a análise das informações profissionais e de contato fornecidas pelos candidatos durante o processo seletivo.
3	**Situação concreta** Detalhe o contexto em que se dará o tratamento de dados.	A instituição recebe e analisa dados pessoais de candidatos interessados em oportunidades de trabalho, provenientes de currículos, formulários de candidatura e/ou diretamente dos próprios candidatos. Os dados são utilizados durante as etapas do processo seletivo, incluindo triagem curricular, contato, entrevistas e avaliação de compatibilidade com os requisitos da vaga. Ao final, os dados poderão ser utilizados para formalização da contratação do candidato selecionado ou, quando aplicável, mantidos pelo período definido pela instituição para eventual contato em futuras oportunidades.
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. O tratamento pode envolver terceiros contratados pela instituição para apoiar o processo de recrutamento e seleção, especialmente nos casos de contratação de estagiários e jovens aprendizes. Esses terceiros realizam atividades de divulgação de oportunidades, recebimento, triagem e encaminhamento de candidatos, conforme as condições estabelecidas com a instituição. A participação desses terceiros tem como finalidade viabilizar e apoiar o processo seletivo, não havendo, em princípio, finalidade própria incompatível com a finalidade definida pela instituição.
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.	Sim. O tratamento deve observar a Lei nº 13.709/2018 (LGPD), especialmente os princípios previstos no art. 6º e as hipóteses legais aplicáveis ao tratamento de dados pessoais. Quando adotado o legítimo interesse, deverão ser observados os requisitos previstos nos arts. 7º, IX, e 10 da LGPD, considerando a finalidade concreta, a necessidade do tratamento, as legítimas expectativas do titular e a proteção de seus direitos e liberdades fundamentais. Também deverão ser observadas as normas trabalhistas aplicáveis ao processo de admissão e contratação, quando pertinentes.

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.	O tratamento é essencial para a instituição, pois possibilita a realização de processos de recrutamento e seleção e a identificação de candidatos compatíveis com as vagas disponíveis. O tratamento dos dados permite avaliar qualificações, experiência, perfil e informações necessárias à seleção, contribuindo para a composição e manutenção adequada do quadro de colaboradores, estagiários e jovens aprendizes.
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.	O tratamento também pode atender aos interesses dos próprios candidatos, na medida em que possibilita sua participação em processos seletivos e o acesso a oportunidades de emprego, estágio e aprendizagem. Nos casos de estágio e jovem aprendiz, os terceiros que apoiam o processo seletivo também possuem interesse relacionado à viabilização e encaminhamento dos candidatos às oportunidades disponíveis, dentro das finalidades estabelecidas para o processo.
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.	Embora existam diferentes formas de conduzir o recrutamento e a seleção, alguma forma de tratamento de dados pessoais é necessária para avaliar os candidatos e selecionar aqueles que apresentam maior compatibilidade com os requisitos da vaga. A instituição poderá utilizar meios menos intrusivos, priorizando os dados fornecidos pelo próprio candidato e limitando a coleta às informações pertinentes à vaga. Nos casos em que houver participação de terceiros, seu acesso deverá ser limitado aos dados necessários para a execução das atividades de recrutamento e seleção.
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.	Sim. O tratamento deve ser limitado aos dados pessoais necessários para a realização do processo seletivo.
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?	A depender da atividade específica e da natureza dos dados tratados, poderão ser aplicadas outras bases legais previstas no art. 7º da LGPD.

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. É razoável que o titular espere o tratamento de seus dados para participação em processo seletivo ao fornecer voluntariamente currículo e demais informações para candidatura.
12	**O tratamento pretendido agrega valor a um produto ou serviço que ele utiliza?**	Não se aplica. O tratamento não está relacionado à oferta de produto ou serviço ao titular.
13	**É provável que o tratamento tenha um impacto negativo nos direitos do titular?**	Não. O tratamento é destinado à seleção de candidatos e, quando limitado à finalidade informada, não tende a causar impacto negativo relevante aos direitos do titular.
14	**É provável que o tratamento resulte em dano injustificado ou prejuízo ao titular?**	Não, desde que os dados sejam utilizados exclusivamente para a finalidade do processo seletivo e tratados de forma adequada e segura.
15	**Pode ocorrer um prejuízo para a empresa caso o tratamento não ocorra?**	Sim. A ausência do tratamento pode dificultar ou inviabilizar a realização dos processos seletivos e o preenchimento adequado das vagas.
16	**Pode ocorrer um prejuízo para terceiros caso o tratamento não ocorra?**	A não realização do tratamento pode reduzir o acesso de candidatos às oportunidades de emprego, estágio e aprendizagem.
17	**O tratamento é do interesse do titular cujos dados pessoais estão relacionados?**	Sim. O tratamento também atende ao interesse do titular em participar do processo seletivo e concorrer à oportunidade disponível.
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. Os interesses estão alinhados, pois a instituição busca preencher suas vagas e o titular busca participar do processo seletivo e obter uma oportunidade de trabalho, estágio ou aprendizagem.
19	**Qual é a conexão entre o titular e a empresa?** Por exemplo: cliente existente; ex-cliente; empregado ou contratado; prospect; fornecedor; outros.	O titular possui relação com a instituição em razão de sua candidatura a uma oportunidade de emprego, estágio ou aprendizagem.
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.	Não. O tratamento, quando limitado à finalidade de recrutamento e seleção, não impede o exercício dos direitos do titular previstos na LGPD.
21	**Os dados pessoais serão obtidos diretamente do titular ou indiretamente?**	Diretamente e indiretamente. Os dados podem ser fornecidos diretamente pelo candidato ou recebidos por meio de terceiros responsáveis pela divulgação, triagem e encaminhamento de candidatos.

22	**O tratamento pode ser considerado intrusivo ou inadequado pelo titular?**	Não, em regra. O tratamento está relacionado a uma finalidade esperada pelo candidato e deve se limitar aos dados necessários ao processo seletivo.
23	**Será ou é fornecido um aviso sobre este tratamento ao titular? Em caso afirmativo, como ele será feito?**	Sim. O titular deverá ser informado por meio dos canais e documentos utilizados no processo seletivo, como formulário de candidatura, aviso de privacidade, política de privacidade ou informações disponibilizadas na plataforma utilizada para a candidatura.
24	**O titular pode se opor a este tratamento? Se não, explique.**	Sim. O titular poderá exercer os direitos previstos na LGPD e, quando cabível, manifestar oposição ao tratamento baseado em legítimo interesse.
25	**O escopo de tratamento pode ser modificado para reduzir/mitigar riscos ou danos à privacidade?**	Sim. Os riscos podem ser mitigados mediante limitação dos dados coletados, restrição de acesso, definição de prazos de retenção, utilização dos dados exclusivamente para as finalidades informadas e controle dos terceiros envolvidos no processo seletivo.

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?**	Controle de acesso aos dados, utilização dos dados apenas para a finalidade do processo seletivo, armazenamento seguro, definição de prazo de retenção e possibilidade de exercício dos direitos previstos na LGPD.
27	**Mitigação de Riscos** Medidas possíveis. Por exemplo: anonimização, pseudoanonimização, segmentação das bases de dados, controle de acesso aos dados.	Controle de acesso, limitação dos dados coletados ao mínimo necessário, restrição de compartilhamento com terceiros, armazenamento seguro e definição de prazo para eliminação dos dados.
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 candidatos devem ser informados sobre a coleta, finalidade e utilização de seus dados pessoais, bem como sobre seus direitos previstos na LGPD e os canais disponíveis para exercê-los
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.	O titular poderá solicitar informações sobre o tratamento e exercer os direitos previstos na LGPD pelos canais disponibilizados pela instituição, inclusive manifestar oposição ao tratamento baseado em legítimo interesse, quando aplicável.

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.	O legítimo interesse pode ser aplicado, pois o tratamento é necessário para a realização do processo seletivo, está dentro da expectativa razoável dos candidatos e é limitado aos dados necessários para recrutamento e seleção, com medidas de segurança e proteção aos titulares.
32	**Área de Negócio**	Recursos Humanos (RH)
33	**Data da Avaliação**	06/10/2026
34	**Nome do Avaliador**	Jenifer Cardoso

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 48 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	Não	**Grave**
Controles Operacionais	SI - CO - Papéis e responsabilidades	Parcialmente alinhado	**Moderado**

Controles Operacionais	SI - CO - Segregação de funções	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Grave**
Controles Operacionais	SI - CO - Responsabilidade da direção	Não	**Grave**
Controles Operacionais	SI - CO - Contato com autoridades	Não	**Grave**
Controles Operacionais	SI - CO - Contato com grupos de interesse especial	Não	**Grave**
Controles Operacionais	SI - CO - Inteligência de ameaças	Não	**Grave**
Controles Operacionais	SI - CO - Inventário de informações	Parcialmente alinhado	**Moderado**
Controles Operacionais	SI - CO - Uso aceitável de informações	Não	**Grave**
Controles Operacionais	SI - CO - Devolução de ativos	Sim	**Leve**
Controles Operacionais	SI - CO - Classificação de informações	Não	**Grave**
Controles Operacionais	SI - CO - Transferência de informações	Parcialmente alinhado	**Moderado**
Controles Operacionais	SI - CO - Controle de acessos	Parcialmente alinhado	**Crítico**
Controles Operacionais	SI - CO - Gestão de identidade	Parcialmente alinhado	**Grave**
Controles Operacionais	SI - CO - Informações de autenticação	Parcialmente alinhado	**Grave**

Controles Operacionais	SI - CO - Direitos de acesso	Parcialmente alinhado	**Grave**
Controles Operacionais	SI - CO - Segurança de informações nas relações com fornecedores	Parcialmente alinhado	**Crítico**
Controles Operacionais	SI - CO - Segurança da informação para uso de serviços em nuvem	Não	**Grave**
Controles Operacionais	SI - CO - Planejamento e preparação da gestão de incidentes de segurança da informação	Não	**Grave**
Controles Operacionais	SI - CO - Avaliação e decisão sobre eventos de segurança da informação	Não	**Grave**
Controles Operacionais	SI - CO - Prontidão de TIC para continuidade de negócios	Não	**Grave**
Controles Operacionais	SI - CO - Requisitos legais, estatutários, regulamentares e contratuais	Não	**Grave**
Controles de Pessoas	SI - CP - Seleção	Sim	**Grave**
Controles de Pessoas	SI - CP - Termos e condições de contratação	Não	**Grave**
Controles de Pessoas	SI - CP - Conscientização, educação e treinamento em segurança da informação	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Crítico**
Controles de Pessoas	SI - CP - Processo disciplinar	Não	**Grave**
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	Não	**Grave**
Controles de Pessoas	SI - CP - Trabalho remoto	Sim	**Leve**
Controles de Pessoas	SI - CP - Relato de eventos de segurança da informação	Parcialmente alinhado	**Grave**
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	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Grave**
Controles Físicos	SI - CF - Segurança de ativos fora das instalações da organização	Parcialmente alinhado	**Crítico**
Controles Tecnológicos	SI - CT - Dispositivos de endpoint do usuário	Não	**Grave**
Controles Tecnológicos	SI - CT - Direitos de acessos privilegiados	Sim	**Leve**
Controles Tecnológicos	SI - CT - Restrição de acesso à informação	Parcialmente alinhado	**Grave**
Controles Tecnológicos	SI - CT - Autenticação segura	Não	**Grave**
Controles Tecnológicos	SI - CT - Proteção contra malware	Não	**Grave**

Controles Tecnológicos	SI - CT - Gestão de vulnerabilidades técnicas	Não	**Grave**
Controles Tecnológicos	SI - CT - Exclusão de informações	Não	**Grave**
Controles Tecnológicos	SI - CT - Mascaramento de dados	Não	**Grave**
Controles Tecnológicos	SI - CT - Prevenção de vazamentos de dados	Não	**Grave**
Controles Tecnológicos	SI - CT - Backup de informações	Não	**Grave**
Controles Tecnológicos	SI - CT - Redundância de recursos para tratamento de informações	Não	**Moderado**
Controles Tecnológicos	SI - CT - Log	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Moderado**
Controles Tecnológicos	SI - CT - Atividades de monitoramento	Parcialmente alinhado	**Grave**

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 **15 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
Skill Consultoria e recursos humanos LTDA	Prestador de serviços	0	**Crítico**
CIEE – Centro de Integração Empresa Escola	Parceiro institucional	0.63	**Grave**
Bhecca - Bezerra e Henrique Contabilidade e auditoria Sociedade Simples	Prestador de serviços	0	**Crítico**
Secullum Softwares Ltda	Fornecedor	0.63	**Grave**
Unimed Campo Grande MS Cooperativa de Trabalho Médico	Prestador de serviços	0.38	**Grave**
Uniodonto Mato Grosso do Sul	Prestador de serviços	0.63	**Grave**
Operadora de planos privados de saúde - SANTA CASA SAUDE LTDA	Prestador de serviços	0.38	**Grave**
Triagem Organização LTDA ME	Prestador de serviços	0.63	**Grave**
Sistema em Nuvem - Trify	Fornecedor	0.63	**Grave**

Assistance Consultoria Medicina e Segurança do Trabalho S/S LTDA	Prestador de serviços	0	Crítico
Escritório de advocacia externo - Dra. MARIELLE CEREZINI ANDRADE MARTINS	Prestador de serviços	0	Crítico
TOTVS S.A	Fornecedor	1	Leve
SAE+C Mhund - SAEINFO Informática LTDA	Fornecedor	0.38	Grave
Classapp Sistemas LTDA	Fornecedor	0.63	Grave
FB Processamento de dados S/S LTDA - Corus	Prestador de serviços	0	Crítico

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.

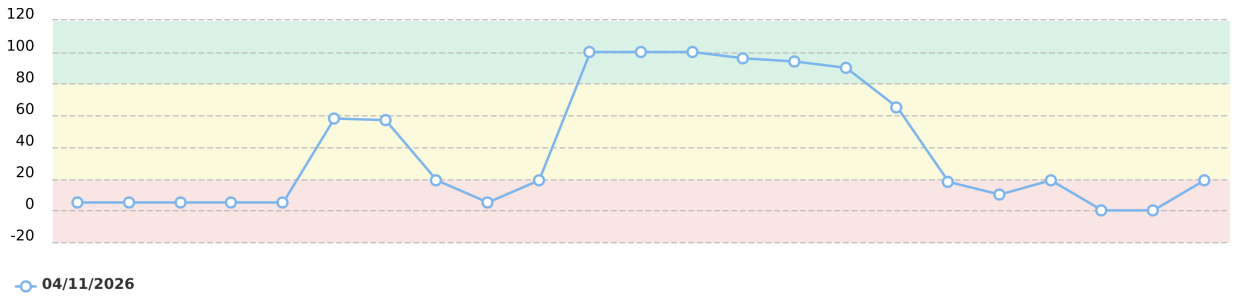
As informações inseridas nos formulários de inventários de dados (ROPA, Segurança de Informações e Fornecedores e/ou Parceiros Institucionais), foram organizadas em 03 (três) áreas de atenção, a saber:

- 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.

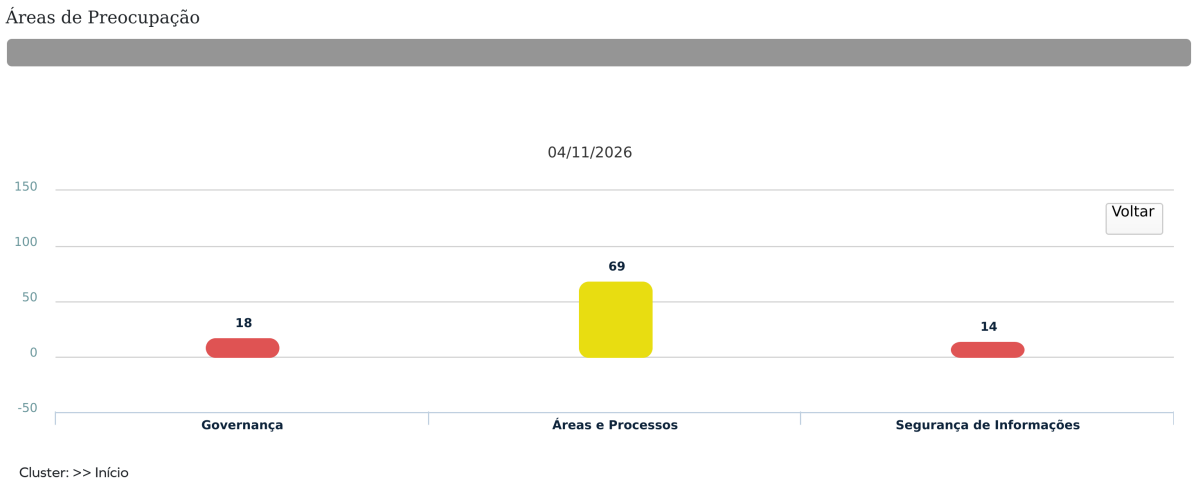
No mesmo sentido, destaca todos os indicadores que mensuram, de forma global, o nível de proteção de dados do contexto analisado. Percebe-se, então, que a organização Colégio Harmonia Ltda, possui:

- 6 indicadores em nível de excelência
- 3 indicadores em nível de competitividade
- 14 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,

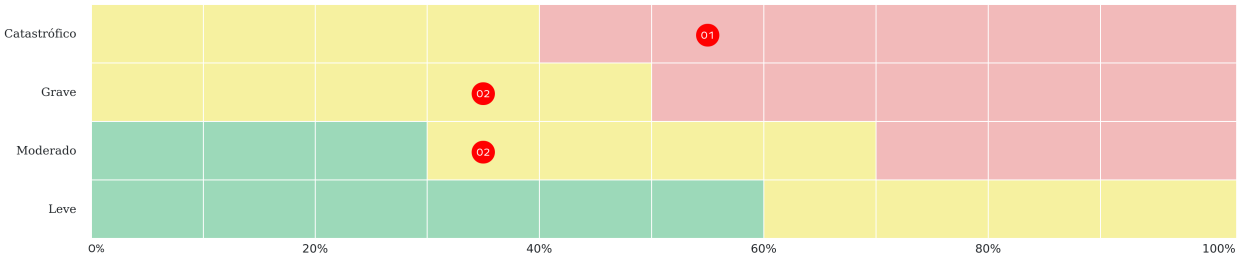
sendo eles:

- **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	**Grave**	36%	30%	31
R2 - Crimes cibernéticos	**Catastrófico**	55%	20%	55

R3 - Dano reputacional	**Grave**	36%	20%	30
R4 - Perdas de parceiros institucionais / comerciais	**Moderado**	35%	15%	18
R5 - Rescisões contratuais	**Moderado**	35%	15%	18