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 **GICON Contabilidade S/S Ltda** às exigências da Lei Geral de Proteção de Dados (LGPD).

1.1 Contexto analisado

- **Razão social:** GICON Contabilidade S/S Ltda
- **CEP:** 88.101-200
- **Endereço:** Avenida Josué Di Bernardi, 239, Campinas - São José/SC
- **CNPJ:** 78.980.737/0001-05

1.2 Responsáveis organizacionais

Encarregado de Dados	E-mail
Martinelli Tecnologia e Inovação Ltda	dpo@gicon.cnt.br

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:**

- **Término do Projeto:**
- **Processos mapeados:** 54
- **Condição (fase) atual da programação de adequação à LGPD:** Fase de implantação / investimentos

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 GICON Contabilidade S/S 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 82 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 60 processos vinculados aos Registros de Operações de Tratamento de Dados Pessoais (ROPA). Adicionalmente, foram avaliados 9 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
Departamento Societário	Abertura de Empresas	4.17	**Leve**
Departamento Societário	Baixa de Empresas	4.17	**Leve**
Departamento Societário	Alterações de Empresas	4.17	**Leve**
Departamento Societário	Cadastro de Vale Alimentação	3.61	**Leve**
Departamento Societário	Cadastro de Vale Transporte	3.94	**Leve**
Benefícios Internos | GICON	Cadastro de Planos de Saúde	4.89	**Leve**
Benefícios Internos | GICON	Cadastro de Plano Odontológico	4.89	**Leve**
Departamento Legal	Cadastro dos Sócios | Clientes	3.56	**Leve**
Departamento Fiscal	Cadastro dos Contadores | PF - Setor legal?	3.56	**Leve**

Departamento Fiscal	Cadastro dos Clientes | Clientes | Setor legal?	5.11	**Moderado**
Departamento Fiscal	Envio de Declarações	3.5	**Leve**
Departamento Fiscal	Apuração Notas Fiscais | Entrada	3.61	**Leve**
Departamento Fiscal	Apuração Notas Fiscais | Saída	3.61	**Leve**
Departamento Pessoal | GICON	Admissão	4.89	**Leve**
Departamento Pessoal | GICON	Demissão	3.78	**Leve**
Departamento Pessoal | GICON	Folha de Pagamento	3	**Leve**
Departamento Pessoal | GICON	Férias	3	**Leve**
Departamento Pessoal | GICON	13º Salário	3	**Leve**
Departamento Pessoal | GICON	Licença Maternidade	3.56	**Leve**
Departamento Pessoal | GICON	Auxilio Doença	3.56	**Leve**
Departamento Pessoal | GICON	Aposentadoria | Procedimento Padrão	3.56	**Leve**
Departamento Pessoal | GICON	Aposentadoria | Especial	3.56	**Leve**
Departamento Pessoal | GICON	Aposentadoria | Invalidez	3.56	**Leve**
Departamento Pessoal | GICON	Fundo de Garantia | FGTS	3.56	**Leve**

Departamento Pessoal | CLIENTES	Cadastro dos Sócios | Clientes	2.44	**Leve**
Departamento Pessoal | CLIENTES	Admissão	3	**Leve**
Departamento Pessoal | CLIENTES	Demissão	2.44	**Leve**
Departamento Pessoal | CLIENTES	Folha de Pagamento	2.44	**Leve**
Departamento Pessoal | CLIENTES	Férias	2.44	**Leve**
Departamento Pessoal | CLIENTES	13º Salário	2.39	**Leve**
Departamento Pessoal | CLIENTES	Licença Maternidade	2.44	**Leve**
Departamento Pessoal | CLIENTES	Auxilio Doença	2.44	**Leve**
Departamento Pessoal | CLIENTES	Aposentadoria | Procedimento Padrão	2.44	**Leve**
Departamento Pessoal | CLIENTES	Aposentadoria | Especial	2.44	**Leve**
Departamento Pessoal | CLIENTES	Aposentadoria | Invalidez	2.44	**Leve**
Departamento Pessoal | CLIENTES	Fundo de Garantia | FGTS	2.22	**Leve**
Departamento Contábil	Triagem de Documentação | Departamentos	4	**Leve**
Departamento Contábil	Controle de Folha de Pagamento | Importação/Integração	3.22	**Leve**
Departamento Contábil	Lançamento de Receitas e Despesas	4	**Leve**

Financeiro | GICON	Abertura de Conta Salário	3.44	**Leve**
Financeiro | GICON	Folha de Pagamento	3.56	**Leve**
Financeiro | GICON	Emissão de Notas Fiscais	5.11	**Moderado**
Financeiro | GICON	Cobranças	5.06	**Moderado**
Financeiro | GICON	Pagamento | Fornecedores	5.5	**Moderado**
Financeiro | GICON	Pagamento | Autônomos	5.5	**Moderado**
Financeiro | GICON	Seguro de Vida	3.56	**Leve**
Financeiro | WILL	Abertura de Conta Salário	3.44	**Leve**
Financeiro | WILL	Folha de Pagamento	3.56	**Leve**
Financeiro | WILL	Emissão de Notas Fiscais	5.11	**Moderado**
Financeiro | WILL	Cobranças	5.06	**Moderado**
Financeiro | WILL	Pagamento | Fornecedores	5.5	**Moderado**
Financeiro | WILL	Pagamento | Autônomos	5.5	**Moderado**
Financeiro | WILL	Seguro de Vida	3.56	**Leve**
Declaração de Imposto de Renda	Declaração Imposto de Renda | PF	2.94	**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.

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	Parcialmente alinhado	**Grave**

Controles Operacionais	SI - CO - Segregação de funções	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Grave**
Controles Operacionais	SI - CO - Inteligência de ameaças	Não	**Grave**
Controles Operacionais	SI - CO - Inventário de informações	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Moderado**
Controles Operacionais	SI - CO - Uso aceitável de informações	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Crítico**
Controles Operacionais	SI - CO - Devolução de ativos	Sim	**Leve**
Controles Operacionais	SI - CO - Classificação de informações	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Crítico**
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	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Grave**
Controles Operacionais	SI - CO - Gestão de identidade	Sim	**Moderado**

Controles Operacionais	SI - CO - Informações de autenticação	Parcialmente alinhado	**Grave**
Controles Operacionais	SI - CO - Direitos de acesso	Parcialmente alinhado	**Moderado**
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	-	-
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	-	-
Controles Operacionais	SI - CO - Prontidão de TIC para continuidade de negócios	Não	**Grave**
Controles Operacionais	SI - CO - Requisitos legais, estatutários, regulamentares e contratuais	Sim	**Leve**
Controles de Pessoas	SI - CP - Seleção	-	-
Controles de Pessoas	SI - CP - Termos e condições de contratação	-	-
Controles de Pessoas	SI - CP - Conscientização, educação e treinamento em segurança da informação	Sim	**Leve**
Controles de Pessoas	SI - CP - Processo disciplinar	-	-
Controles de Pessoas	SI - CP - Responsabilidades após encerramento ou mudança da contratação	-	-

Controles de Pessoas	SI - CP - Acordos de confidencialidade ou não divulgação	Sim	**Leve**
Controles de Pessoas	SI - CP - Trabalho remoto	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Crítico**
Controles de Pessoas	SI - CP - Relato de eventos de segurança da informação	-	-
Controles Físicos	SI - CF - Perímetros de segurança física	-	-
Controles Físicos	SI - CF - Entrada física	-	-
Controles Físicos	SI - CF - Segurança de escritórios, salas e instalações	-	-
Controles Físicos	SI - CF - Monitoramento de segurança física	-	-
Controles Físicos	SI - CF - Segurança de ativos fora das instalações da organização	-	-
Controles Tecnológicos	SI - CT - Dispositivos de endpoint do usuário	-	-
Controles Tecnológicos	SI - CT - Direitos de acessos privilegiados	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Crítico**
Controles Tecnológicos	SI - CT - Restrição de acesso à informação	-	-
Controles Tecnológicos	SI - CT - Autenticação segura	-	-

Controles Tecnológicos	SI - CT - Proteção contra malware	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Grave**
Controles Tecnológicos	SI - CT - Gestão de vulnerabilidades técnicas	-	-
Controles Tecnológicos	SI - CT - Exclusão de informações	-	-
Controles Tecnológicos	SI - CT - Mascaramento de dados	-	-
Controles Tecnológicos	SI - CT - Prevenção de vazamentos de dados	-	-
Controles Tecnológicos	SI - CT - Backup de informações	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Grave**
Controles Tecnológicos	SI - CT - Redundância de recursos para tratamento de informações	Parcialmente alinhado	**Grave**
Controles Tecnológicos	SI - CT - Log	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**Crítico**
Controles Tecnológicos	SI - CT - Atividades de monitoramento	Informado a aderência, contudo, não houve a disponibilização de conteúdo comprobatório	**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 **9 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
OMIE | Software	Fornecedor	0.5	**Grave**
TaskDO | Software	Fornecedor	0	**Crítico**
Banco do Brasil S.A	Fornecedor	1	**Leve**
Caixa Econômica Federal	Fornecedor	1	**Leve**
Unicred Cooperativa de Crédito	Fornecedor	1	**Leve**
Questor	Fornecedor	1	**Leve**

Wk Sistemas	Fornecedor	1	**Leve**
Ottimizza	Fornecedor	0	**Crítico**
Rubi | Senior	Fornecedor	1	**Leve**

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.

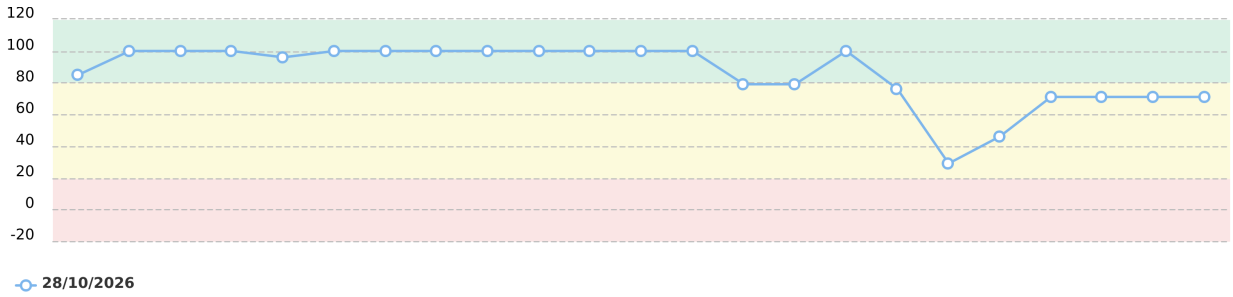
As informações inseridas nos formulários de inventários de dados (ROPA, Segurança de Informações e Fornecedores e/ou Parceiros Institucionais), foram organizadas em 03 (três) áreas de atenção, a saber:

- 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.

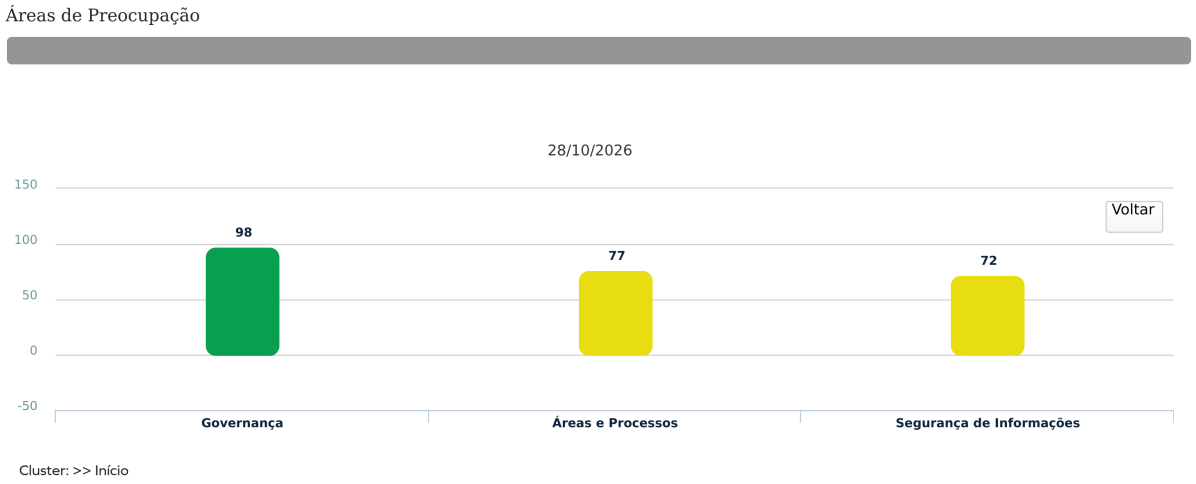
Uma faixa na cor "amarela", destacando indicadores em nível de mercado e/ou competitividade. E, uma faixa na cor "vermelho", destacando indicadores em nível de comprometimento.

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 GICON Contabilidade S/S Ltda, possui:

- 14 indicadores em nível de excelência
- 9 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:

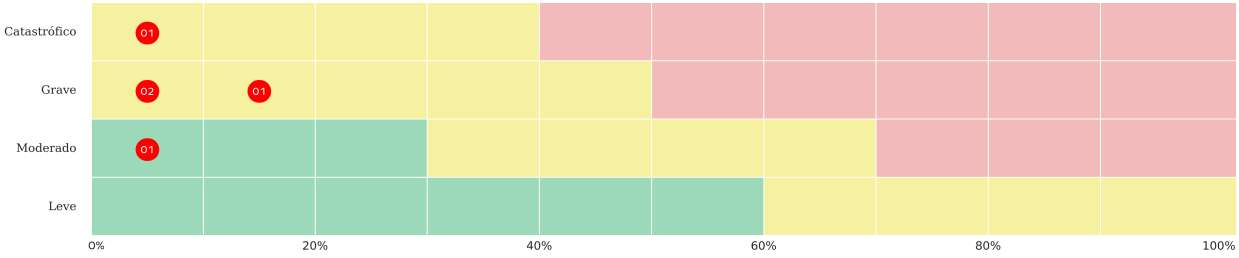
- **R1** - Sanções judiciais e/ou administrativas;

- **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	**Catastrófico**	9%	30%	9
R2 - Crimes cibernéticos	**Grave**	14%	20%	12
R3 - Dano reputacional	**Grave**	9%	20%	7

R4 - Perdas de parceiros institucionais / comerciais	**Moderado**	9%	15%	5
R5 - Rescisões contratuais	**Grave**	9%	15%	7