4. RECOMENDAÇÕES

Neste capítulo, estão elencadas as recomendações técnicas elaboradas pela equipe técnica profissional e capacitada, com o objetivo de orientar a execução de tarefas, processos ou a tomada de decisões. Essas recomendações são fundamentadas em conhecimentos técnicos, pesquisas e experiências práticas, visando garantir a eficiência, do programa de adequação da organização.

Recomendações

As recomendações técnicas apresentadas neste Relatório de Impacto à Proteção de Dados (RIPD) são fundamentadas em uma análise detalhada dos processos e práticas de tratamento de dados pessoais. O objetivo é fornecer diretrizes claras e ações específicas que visam mitigar riscos, fortalecer a conformidade com a Lei Geral de Proteção de Dados (LGPD), e assegurar a proteção dos dados pessoais de forma eficaz e contínua.

Baseado nas estatísticas apresentadas pelo sistema, o consultor indicou os seguintes pareceres técnicos:

Importante | Formalização e divulgação do Encarregado (DPO) e do Comitê Gestor de Proteção de Dados

Importante | Conclusão da documentação da Política de Segurança da Informação

Importante | Aprimoramento da segurança patrimonial e dos backups

Importante | Política de retenção e tabela de temporalidade

Importante | Procedimento de descarte

Importante | Retenção e armazenamento de dados por obrigação legal e regulatória

Importante | Programa de capacitação

Importante | Segurança da Informação e TI

Recomendável | Conclusão do programa de capacitação

Recomendável | Correção e portabilidade de dados

Recomendável | Análise de fornecedores

A seguir, serão detalhados as recomendações técnicas, divididas por áreas estratégicas, oferecendo uma visão abrangente e prática para orientar a empresa na adoção de melhorias contínuas em suas operações de tratamento de dados pessoais.

Formalização e divulgação do Encarregado (DPO) e do Comitê Gestor de Proteção de Dados

Importante

Área de Preocupação:
Governança

Ponto de atenção:

Conforme verificado, a organização atribuiu a responsabilidade de Encarregado de Dados mas ainda não houve a divulgação ao público externo. A empresa também já constituiu a Comissão de Proteção de Dados Pessoais mas ainda não há um registro formal da nomeação do Cômite e das reuniões periódicas.

Recomendação:

Desse modo, recomenda-se à organização formalizar e manter os registros relacionados à atuação do Encarregado de Dados e do Comitê Gestor de Proteção de Dados, incluindo a formalização da nomeação dos respectivos responsáveis e a documentação das reuniões e deliberações realizadas pelo Comitê.

Recomenda-se, ainda, a divulgação do Encarregado de Dados e de suas informações de contato ao público externo, de modo a assegurar a adequada disponibilização do canal de comunicação com os titulares de dados pessoais e com a ANPD.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:16

Conclusão da documentação da Política de Segurança da Informação

Importante

Área de Preocupação:
Segurança de Informações

Ponto de atenção:

Conforme analisado, a Política de Segurança da Informação ainda está em desenvolvimento.

Recomendação:

Recomenda-se à organização concluir a elaboração e formalização da Política de Segurança da Informação, assegurando sua aprovação, implementação e disponibilização aos públicos internos pertinentes, de modo a consolidar as diretrizes e medidas aplicáveis à proteção dos dados pessoais tratados pela organização.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:19



Aprimoramento da segurança patrimonial e dos backups

Importante

Área de Preocupação:
Segurança de Informações

Ponto de atenção:

Conforme analisado, a estrutura de segurança patrimonial e backup está em nível baixo e precisa ser aprimorada e documentada.

Recomendação:

Desse modo, recomenda-se à organização aprimorar as medidas de segurança relacionadas à proteção dos dados pessoais, especialmente quanto à segurança patrimonial e aos procedimentos de backup, assegurando que as medidas de mitigação de riscos adotadas sejam formalmente documentadas e aplicadas de maneira consistente nos processos pertinentes.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Crimes cibernéticos
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:26

Política de retenção e tabela de temporalidade

Importante

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

Conforme analisado, os dados ficam, em sua maioria, armazenados por tempo indeterminado e não existe política/tabela de temporalidade, ficando a definição sob responsabilidade de cada departamento.

Recomendação:

Desse modo, recomenda-se à organização estabelecer e formalizar uma política de retenção de dados pessoais, contemplando tabela de temporalidade aplicável aos processos e procedimentos identificados, com definição dos respectivos prazos de guarda e critérios para sua manutenção.

Recomenda-se, ainda, que os períodos de retenção sejam definidos de forma centralizada e observem as obrigações legais e regulatórias aplicáveis, evitando a manutenção de dados pessoais por prazo indeterminado sem justificativa.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Crimes cibernéticos

- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:29

Procedimento de descarte

Importante

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

Conforme verificou-se não há processos definidos de descarte na organização.

Recomendação:

Recomenda-se à organização elaborar e implementar procedimento formal de descarte de dados pessoais, contemplando critérios, responsabilidades, métodos e registros aplicáveis ao descarte de documentos e informações em meios físicos e digitais. O procedimento deverá estar alinhado aos prazos de retenção definidos pela organização e assegurar que o descarte ocorra de forma segura, especialmente quanto aos documentos físicos que contenham dados pessoais, evitando sua destinação ao lixo comum.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:30

Retenção e armazenamento de dados por obrigação legal e regulatória

Importante

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

Foi verificado que os processos mapeados possuem necessidade de retenção e armazenamento de dados pessoais em decorrência de obrigações legais e regulatórias, bem como de compartilhamento ou transferência dessas informações a terceiros para o cumprimento dessas obrigações. Nesse contexto, identificou-se a necessidade de manter evidências documentais que demonstrem as obrigações aplicáveis e os respectivos prazos de retenção, vinculando-as aos processos correspondentes e ao RIPD.

Recomendação:

Recomenda-se à organização identificar, documentar e manter evidências das obrigações legais e regulatórias que fundamentam os prazos de retenção, armazenamento e eventual compartilhamento ou transferência de dados pessoais, especialmente nos processos relacionados às áreas fiscal, tributária, trabalhista e previdenciária.

Recomenda-se, ainda, que tais evidências sejam vinculadas aos respectivos processos e anexadas ao RIPD, de modo a demonstrar a justificativa para os períodos de retenção e para os compartilhamentos realizados em cumprimento de obrigação legal ou regulatória.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:38

Programa de capacitação

Importante

Área de Preocupação:

Áreas e Processos

Ponto de atenção:

Foi verificado, durante as entrevistas realizadas, que os colaboradores da Tombini, de modo geral, não possuíam familiaridade com a Lei Geral de Proteção de Dados Pessoais, evidenciando a necessidade de fortalecimento da conscientização e capacitação interna quanto à proteção de dados pessoais e às responsabilidades relacionadas aos processos de tratamento realizados pela organização.

Recomendação:

Recomenda-se à organização estruturar e implementar um programa contínuo de capacitação e conscientização em proteção de dados pessoais, contemplando os colaboradores de acordo com suas funções e responsabilidades nos processos de tratamento de dados. O programa deverá abordar, de forma prática e compatível com a realidade da organização, os principais aspectos da LGPD, boas práticas de proteção de dados, segurança da informação, responsabilidades dos colaboradores e procedimentos internos aplicáveis.

Recomenda-se, ainda, que sejam mantidos registros das capacitações realizadas, incluindo participantes, conteúdos abordados e respectivas datas, possibilitando o acompanhamento da efetividade do programa e a comprovação das ações de conscientização promovidas pela organização.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:45

Segurança da Informação e TI

Importante

Área de Preocupação:

Segurança de Informações

Ponto de atenção:

Foi verificado que os controles de Segurança da Informação avaliados apresentam diferentes níveis de risco, com concentração relevante de classificações nos níveis grave e crítico, evidenciando a necessidade de priorização e tratamento dos riscos identificados, especialmente daqueles classificados nos níveis mais elevados.

Recomendação:

Recomenda-se à organização estabelecer e implementar um plano de tratamento dos riscos identificados na avaliação dos controles de Segurança da Informação, priorizando os controles classificados como risco crítico e grave. O plano deverá contemplar a definição das medidas de adequação aplicáveis, respectivos responsáveis e prazos para implementação, bem como o acompanhamento periódico da evolução das ações.

Recomenda-se, ainda, que as medidas implementadas sejam devidamente documentadas, permitindo evidenciar o tratamento dos riscos identificados e o aprimoramento contínuo dos controles de segurança da informação da organização.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Crimes cibernéticos
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:53

Conclusão do programa de capacitação

Recomendável

Área de Preocupação:
Governança

Ponto de atenção:

O programa de capacitação dos colaboradores está em desenvolvimento.

Recomendação:

Recomenda-se à organização concluir e implementar o programa de capacitação dos colaboradores em proteção de dados pessoais, contemplando conteúdos relacionados à LGPD, às responsabilidades dos colaboradores no tratamento de dados pessoais e às boas práticas de segurança e proteção de dados.

Recomenda-se, ainda, manter registros que evidenciem a realização das capacitações, de forma a possibilitar o acompanhamento e a comprovação das ações realizadas.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Crimes cibernéticos
- Dano reputacional

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:22

Correção e portabilidade de dados

Recomendável

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

Foi verificado que a organização possui mecanismos parciais para correção dos dados pessoais e que, em determinados processos, existem limitações quanto à possibilidade de portabilidade dos dados, tendo sido identificada a necessidade de análises complementares para avaliar a adequação desses procedimentos às exigências da LGPD.

Recomendação:

Portanto, recomenda-se à organização avaliar e, quando tecnicamente e juridicamente aplicável, aprimorar os procedimentos relacionados ao exercício dos direitos de correção e portabilidade dos dados pessoais, especialmente nos processos em que foram identificadas limitações.

Recomenda-se que as análises complementares já indicadas sejam realizadas e, quando aplicável, sejam estabelecidos mecanismos que possibilitem o atendimento adequado às solicitações dos titulares.

Riscos associados:

- Sanções judiciais e/ou administrativas

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:32

Análise de fornecedores

Recomendável

Área de Preocupação:
Áreas e Processos

Ponto de atenção:

Conforme analisado os fornecedores.

Recomendação:

Recomenda-se à organização implementar ações de aprimoramento e adequação à LGPD junto aos fornecedores e parceiros classificados como de risco crítico ou grave, especialmente quanto à obtenção e formalização de informações relacionadas às práticas de privacidade e proteção de dados adotadas por esses terceiros.

Recomenda-se, ainda, manter registros das avaliações realizadas, das ações de adequação solicitadas e dos respectivos acompanhamentos, de modo a evidenciar o monitoramento dos operadores e parceiros que representam maior risco ao tratamento de dados pessoais.

Riscos associados:

- Sanções judiciais e/ou administrativas
- Dano reputacional
- Perdas de parceiros institucionais / comerciais
- Rescisões contratuais

Autor: Jenifer Tainara da Silva Cardoso em 07/10/2026 11:41