YTECH
SOLUÇÕES

Relatório de Impacto à Proteção de Dados Pessoais

Solution 3

CyberSul
Softwares de Gestão

adx

Abril 2026

Sumário

Histórico de Revisões

Data	Versão	Descrição	Autor
20/04/2025	1.0	Conclusão da primeira versão do relatório	Grupo ADX

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador
YTECH Soluções
Operador
CyberSul – Softwares e Gestão
DPO
Grupo ADX
E-mail DPO
dpo@ytechsolucoes.com

2. OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais realizados pela empresa YTECH Soluções no sistema Solution3 desenvolvido pela CyberSul, que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

3. O SISTEMA SOLUTION3

O Solution3 presente na YTECH Soluções, é uma solução de ERP robusto e personalizável voltado a empresas de pequeno e médio porte, desenvolvida pela CyberSul – Softwares de Gestão, empresa brasileira com atuação em diversos estados, especializada no

desenvolvimento de soluções em sistemas de gestão integrada para empresas. No Solution 3, a integração dos sistemas de contas a receber, contas a pagar, assistência técnica, gerência de produção, controle de estoques e materiais, faturamento, gestão de clientes e fornecedores, controle de compras, livros fiscais, contabilidade e controle patrimonial, formam um conjunto de ferramentas que centralizam as informações da organização. O sistema é possui customização dinâmica, assim seus clientes conseguem adaptar os recursos da solução conforme suas necessidades, flexibilizando a ferramenta para atender aos processos internos.

4. NECESSIDADE DE ELABORAR O RELATÓRIO

A elaboração deste relatório justifica-se pela operação do sistema ERP solution3 da CyberSul na YTECH Soluções, cujo ambiente centraliza o tratamento de dados pessoais de clientes (responsáveis legais) e de colaboradores, abrangendo coleta, armazenamento, compartilhamento e eventual classificação como inativos.

Os seguintes fatores tornam necessária a elaboração ou atualização do RIPDP:

- Conformidade à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e regulamentações emanadas pela Autoridade Nacional de Proteção de Dados - ANPD;
- Orientação e direcionamento dos colaboradores da YTECH Soluções com relação ao tratamento dos dados pessoais de colaboradores e clientes que, por razões contratuais, legais e fiscais, são coletadas em seus processos formais;
- Definição de políticas internas de garantia da segurança e governança dos dados pessoais coletados;

- Garantia de proteção e mitigação de riscos eventualmente envolvidos evitando: (i) ameaças ou riscos à privacidade; à segurança; à integridade e/ou à confidencialidade; (ii) destruição acidental ou ilícita; perda; alteração; divulgação ou acesso não autorizado; (iii) quaisquer outras formas ilegais de tratamento; e (iv) incidentes de segurança ou privacidade.

- Adoção de uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;

- tratamento de dado pessoal sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (LGPD, art. 5º, II);

- processamento de dados pessoais usados para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);

- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);

- alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados etc.

5. PARTES INTERESSADAS CONSULTADAS

Para elaboração deste Relatório de Impacto, foram consultadas as seguintes partes com objetivo de identificação de riscos e de possíveis tratamentos indevidos de dados pessoais e dados pessoais sensíveis no uso do sistema Solution3 da CyberSul:

Parte Consultada	Papel / Função	Observações Relevantes
Gerente Administrativo	Responsável pelo cadastro e gestão de dados no ERP	Identificação dos dados coletados, fluxos de compartilhamento e práticas atuais de tratamento
Analista de Suporte Sênior	Auxilia a gerente do administrativo em questões técnicas de infraestrutura na empresa.	Não realiza o tratamento ou qualquer operação sobre o sistema.
CyberSul – Softwares e Gestão	Operador / Desenvolvedor do ERP Solution3	Fornecimento do sistema, responsável pela criação de usuários e suporte técnico. Possui Política de Privacidade publicada em seu site. Detém permissão administrativa exclusiva no sistema e banco de dados. Questões sobre segurança do sistema, fluxo de dados e versões de sistema e banco de dados não foram respondidas e devem ser formalizadas neste documento.

Tabela 1 - Partes interessadas consultadas

6. DESCRIÇÃO DO TRATAMENTO

6.1. NATUREZA DO TRATAMENTO

As operações realizadas no sistema Solution3 utilizam dados pessoais de clientes e colaboradores da YTECH. Não são registrados dados pessoais sensíveis no sistema.

Foram identificados **2 operadores de dados**: EVEO e a CyberSul. A infraestrutura é composta por uma máquina virtual em nuvem, gerenciada pela empresa EVEO. O acesso ao sistema pelos usuários da YTECH é realizado via VPN (Virtual Private Network). Atualizações do sistema são realizadas de forma silenciosa pela CyberSul, com notificação por e-mail aos usuários. Em caso de necessidade de suporte, a CyberSul acessa remotamente a mesma máquina virtual.

A coleta dos dados pessoais dos titulares se dá de forma manual, principalmente por e-mail ou mensagem via WhatsApp, e manipulados no sistema pelos colaboradores responsáveis (Gerente Administrativo/Financeiro ou Coordenadora Financeira). Dados de clientes são utilizados para elaboração e execução de contratos. Dados de colaboradores são utilizados para permitir o acesso destes ao sistema.

A Gerente do Administrativo e a Coordenadora Financeira são os principais atores que manipulam o sistema. Para estes são disponibilizadas uma série de funcionalidades que permitem a operacionalização dos dados pessoais coletados para fins administrativos e financeiros do controlador.

As operações de tratamento contemplam: coleta, registro, armazenamento, classificação, acesso e utilização dos dados pessoais, estando alinhadas com as obrigações legais aplicáveis. Os dados dos titulares estão descritos na **Tabela 1**.

Após geração do contrato os dados pessoais dos titulares de dados não são deletados do Whatsapp ou do e-mail. As contas de e-mails, números de telefone e dispositivos onde o Whatsapp está instalado são todos corporativos.

As concessões ou revogações de acesso e atribuições de perfis de acesso ao sistema, para os colaboradores da YTECH, são realizadas mediante abertura de chamado com a CyberSul, com envio das credenciais por e-mail. Não há credenciais compartilhadas. O acesso ao Solution3 é individual mediante usuário e senha.

O acesso ao sistema por parte dos colaboradores é individual e intransferível. O sistema conta com controle de acesso por perfis/níveis, e a redefinição de senha pode ser realizada pelo próprio colaborador. Contudo, não há requisitos mínimos de complexidade de senha nem autenticação multifator (MFA).

Não há processos de expurgo ou política de exclusão de dados pessoais do sistema Solution3. Após encerramento de contrato com cliente, ou desligamento de colaborador, os dados são apenas classificados como inativos. Todas as informações são mantidas no sistema por tempo indeterminado.

Não há ambiente de homologação separado para testes de atualização, e o sistema não possui versão mobile.

No sistema Soution3 não há dados de titulares pertencentes a qualquer grupo vulnerável (crianças, adolescentes ou pessoa incapaz).

Foram identificados **2 operadores de dados**: EVEO e a CyberSul. A desenvolvedor CyberSul é responsável pelo suporte ao Solution3. A máquina onde o sistema encontra-se instalado, e sua respectiva base de dados, estão hospedados na infraestrutura da EVEO, provedor de Infraestrutura como Serviço (IaaS). O acesso a esta máquina é realizado através de software VPN provido pela própria EVEO.

Não é realizado nenhum tipo de compartilhamento de dados com os operadores nem com terceiros, seja por exportação ou integração. Ocasionalmente dados podem ser visualizados pela equipe de suporte da CyverSul.

As obrigações dos operadores de dados devem ser reguladas por contrato, estabelecendo a duração, escopo, finalidade, instruções de processamento documentadas,

fornecimento de qualquer documentação que apresente evidências de conformidade com a LGPD, notificação imediata de qualquer violação de dados etc. Conforme alinhamento com as partes interessadas consultadas, há, entre os contratos firmados com os terceirizados, parágrafo que cite compromisso em manter sigilo sobre as informações acessadas, termo de confidencialidade ou qualquer termo de adequação a LGPD.

Rotinas de backup de toda a infraestrutura do Solution3 (máquina e bancos de dados) está sob responsabilidade da CyberSul.

O diagrama a seguir descreve as interações dos principais atores com o ciclo de vida dos dados pessoais e dados pessoais sensíveis tratados pelo sistema.

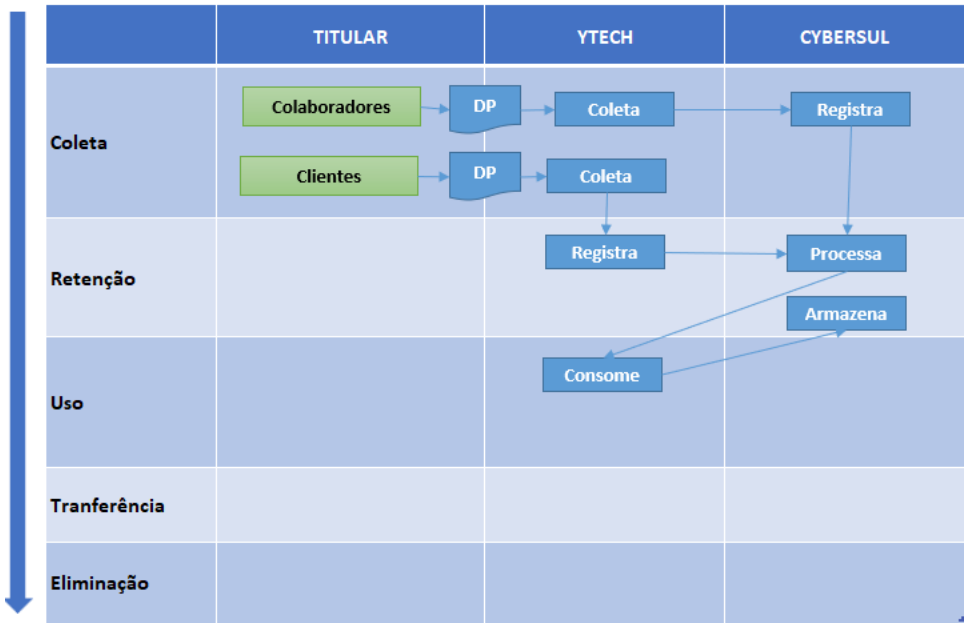

Figura 1 – Fluxo de Dados

Legenda da Figura 1:

DP - Dados Pessoais
DPS – Dados Pessoais Sensíveis
Operadores - pessoa ou empresa que trata os dados pessoais em nome do MARATÁ
Titular - pessoa física a quem se referem os dados pessoais que são objeto de tratamento

Não foram identificadas medidas formais de segurança implementadas pelo controlador até o momento da realização deste diagnóstico, sendo recomendada a adoção urgente de registro de logs, política de senhas e plano de contingência.

6.2. ESCOPO DO TRATAMENTO

Os dados tratados pelo sistema abrangem aproximadamente **11 titulares de dados,** entre cadastros de clientes e colaboradores.

Em geral, o sistema utiliza, nas suas operações de negócio, **4 dados pessoais** e **0 dados pessoais sensíveis**. Listamos na **Tabela 1** os dados pessoais dos titulares tratados na execução das rotinas operacionais do sistema.

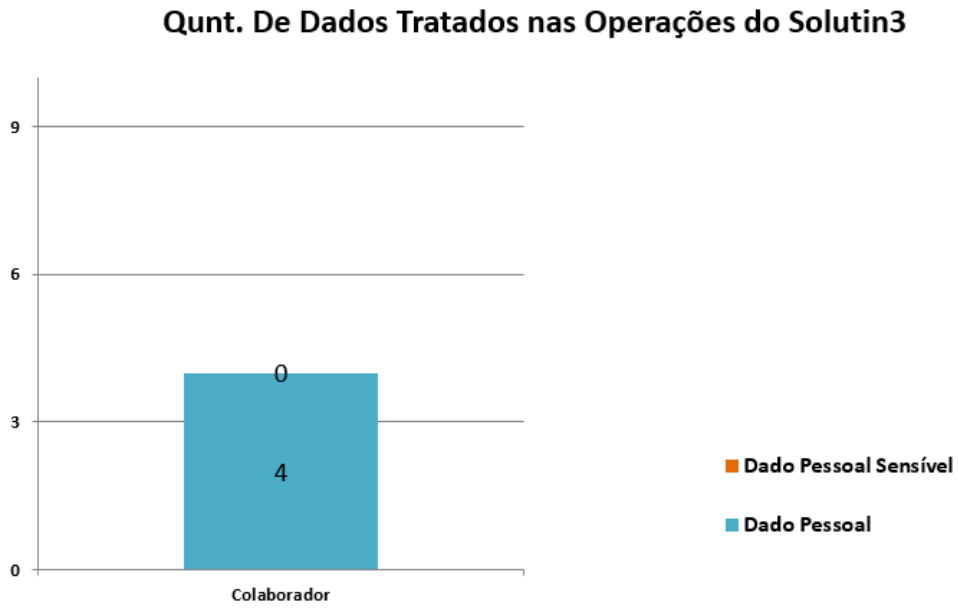

Figura 2 - Quantidade de dados tratados no sistema

Clientes		Colaboradores	
Dado Pessoal	**Dado Pessoal Sensível**	**Dado Pessoal**	**Dado Pessoal Sensível**
Nome completo		Nome completo	
Número do CPF		E-mail	
E-mail			
Telefone			

Tabela 2 - Dados pessoais por titular tratados no Solution3

Frequência do tratamento: contínua, conforme necessidade operacional e admissional.

Período de retenção: enquanto houver vínculo empresarial com o titular e, após o encerramento do vínculo, pelo prazo legal exigido pela legislação aplicável. Os registros não são eliminados, sendo apenas classificados como inativos no sistema.

Abrangência geográfica: nacional, com dados coletados e armazenados em território brasileiro.

6.3. FINALIDADE DO TRATAMENTO

O tratamento de dados pessoais no ERP Solution3 pela YTECH possui as seguintes finalidades:

- Execução de contrato: tratamento de dados de clientes (responsáveis legais) para elaboração, formalização e execução de contratos comerciais – base legal: art. 7º, V, LGPD;
- Proteção do crédito e prevenção à fraude: uso de dados cadastrais de clientes para fins de cobrança e relacionamento comercial – base legal: art. 7º, X, LGPD;
- Interesse legítimo do controlador: gestão interna e operacional da empresa (controle financeiro, fiscal e contábil) – base legal: art. 7º, IX c/c art. 10, LGPD.

7. PROPORCIONALIDADE E NECESSIDADE

7.1. Fundamentação Legal

O tratamento de dados pessoais realizado pela YTECH por meio do ERP Solution3 fundamenta-se nas seguintes hipóteses legais previstas no art. 7º da LGPD:

- Inciso V – Execução de contrato: dados de clientes utilizados para elaboração e gestão de contratos comerciais;

- Inciso IX c/c art. 10 – Legítimo interesse do controlador: gestão operacional, financeira e fiscal da empresa.

- Inciso X – Proteção de crédito: dados dos clientes utilizados para fins de cobrança e relacionamento comercial.

7.2. Minimização e Qualidade dos dados

Conforme informado pelo controlador, todos os dados coletados e armazenados possuem finalidade definida e são efetivamente utilizados para os fins declarados. No entanto, identificam-se as seguintes necessidades de melhoria:

- Implementar processo formal de revisão periódica dos dados armazenados para garantir sua atualização e exatidão;

- Eliminar ou anonimizar dados de titulares cujo vínculo tenha sido encerrado e cujo prazo legal de retenção já tenha expirado, em vez de apenas classificá-los como inativos. Conforme a LGPD, a definição do prazo deve ser realizada de acordo com o objetivo do tratamento desses dados. Uma vez que o objetivo é alcançado, os dados devem ser arquivados, eliminados ou anonimizados;

- Formalizar a coleta de dados por meio de formulários padronizados, substituindo o envio informal por e-mail e WhatsApp.

7.3. Medidas para garantia dos direitos dos titulares (Art. 18)

Não há transferências internacionais de dados identificadas no contexto do ERP Solution3, razão pela qual não se aplicam as salvaguardas previstas no Capítulo V da LGPD.

As solicitações devem ser avaliadas pelo DPO ou comitê estabelecido e monitorado quanto ao cumprimento dentro do prazo estabelecido pela ANPD.

Como forma de garantir que os titulares sejam informados sobre o tratamento dos seus dados, indicamos as seguintes oportunidades de melhoria organizacional:

- A YTECH deverá implementar canal formal para atendimento às solicitações dos titulares de dados, garantindo o exercício dos seguintes direitos previstos no art. 18 da LGPD:
  - Confirmação da existência de tratamento e acesso aos dados;
  - Correção de dados incompletos, inexatos ou desatualizados;
  - Anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade;
  - Portabilidade dos dados a outro fornecedor de serviço;
  - Eliminação dos dados pessoais tratados com base no consentimento;
  - Informação sobre entidades com as quais os dados foram compartilhados;
  - Revogação do consentimento.
- Implementar termo de consentimento quando forem solicitados dados pessoais ou dados pessoais sensíveis de titulares dados para fins de cadastro no sistema. O termo pode ser assinado digitalmente, deve possuir data e horário e pode ser armazenado no sistema Solution3.
- Implementar rotina para informar ao usuário do sistema e solicitar a sua ciência, quando da alteração na Política de Privacidade Interna e Termos de Uso.
- Recomendamos também que os colaboradores sejam treinados (especialmente aqueles que lidam diretamente com a coleta de dados) para que conheçam os direitos dos titulares, saibam responder os principais questionamentos que possam surgir e manipular corretamente os dados coletados.

7.4. Medidas para assegurar conformidade dos Operadores

Para garantir a conformidade dos operadores as seguintes ações devem ser realizadas:

- Os contratos com Operadores devem ser ajustados, estabelecendo duração, escopo, finalidade, instruções de processamento documentadas, fornecimento de qualquer documentação que forneça evidências de conformidade com a LGPD, notificação imediata de qualquer violação de dados etc.

- Regularmente o DPO deverá conduzir auditoria nos processos de negócio à vista da LGPD, esta avaliação inclui o sistema Solution3 e os dados pessoais nele presentes.

- O DPO, juntamente com o comitê, são responsáveis por deliberarem quaisquer modificações operacionais e de negócios que impactem a privacidade e a proteção dos dados e os mecanismos de garantia a adequação à LGPD.

A priori, é importante salientar que no tocante à adequação a Lei 13.709/18 (Lei Geral de Proteção de Dados), não se limita aos dados do titular utilizados na elaboração dos diversos contratos, mas também aos que serão necessários para a execução de contrato ou de procedimentos preliminares relacionados aos contratos dos quais seja parte o titular.

É imprescindível a observância dos contratos para que as empresas contratadas cumpram a Lei Geral de Proteção de Dados, pois, além de ser dever delas, também é da YTECH Soluções resguardar os dados dos titulares a fim de evitar responsabilizações de natureza administrativas, em razão de órgãos como a exemplo do Procon e da Autoridade Nacional de Proteção de Dados – ANPD, ou judiciais de natureza cível.

8. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Abaixo, a **Figura 3** apresenta o peso definido para cada nível de probabilidade e impacto e, na **Figura 4**, temos a matriz de exposição ao risco.

Probabilidade	Valor
Baixa	1
Média	2
Alta	3

Impacto	Valor
Baixo	1
Médio	2
Alto	3

Figura 3 – Valores Probabilidade e Impacto

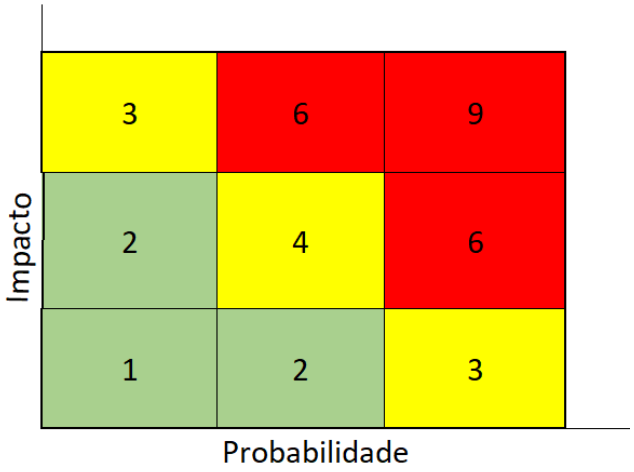

Figura 4 – Diagrama Probabilidade e Impacto

A **Tabela 3** mostra o resultado da avaliação dos riscos mais comuns associados a sistemas da informação e privacidade, no contexto do Solution3.

ID	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R01	Acesso não autorizado ao ERP por ausência de política formal de controle de acesso e senha.	1	3	**3**
R02	Modificação não autorizada de dados cadastrais de clientes e funcionários no ERP.	2	3	**6**
R03	Perda de dados por falha na infraestrutura hospedada via VPN, sem plano de contingência documentado.	3	3	**9**
R04	Roubo ou vazamento de dados transmitidos via WhatsApp durante a coleta.	2	3	**6**
R05	Remoção não autorizada (colaborador não tem a permissão para retirar ou copiar dados pessoais para outro local).	2	3	**6**
R06	Ausência de logs do sistema, impossibilitando rastreamento de alterações e incidentes.	3	3	**9**
R07	Coleta excessiva ou sem finalidade definida de dados pessoais de clientes.	1	2	**2**
R08	Informação insuficiente aos titulares sobre a finalidade e o tratamento dos seus dados pessoais.	3	3	**9**
R09	Ausência de termo de consentimento ou qualquer outro mecanismo formal de bases legais documentadas.	2	3	**6**
R10	Falha em garantir os direitos dos titulares (acesso, correção, eliminação) por ausência de canal formal.	3	2	**6**
R11	Retenção prolongada de dados pessoais após o fim do vínculo, sem política de expurgo definida.	3	2	**6**
R12	Vinculação/ associação indevida, direta ou indireta, dos dados pessoais ao titular.	1	2	**2**
R13	Não há procedimento padrão estabelecido para o descarte dos dados após o atingimento da finalidade.	3	2	**6**
R14	Ausência de autenticação multifator (MFA) no acesso ao ERP.	2	2	**4**
R15	Vazamento por intermédio do funcionário.	2	3	**6**
R16	Infraestrutura sem certificação de segurança ou política de privacidade formalizada pelo desenvolvedor (CyberSul).	1	3	**3**
R17	Transferência ou processamento por meio de terceiros	1	3	**3**

R18	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.).	2	3	**6**
R19	Coleta informal de dados via WhatsApp e e-mail, sem registro auditável e sem criptografia garantida.	2	3	**6**

Tabela 3 - Riscos relacionados ao tratamento

Legenda da Tabela 3:

1 -P = Probabilidade
2 - I = Impacto
3 – (P x I) = Probabilidade x Impacto

9. MEDIDAS PARA TRATAR OS RISCOS

As medidas de tratamento funcionam como respostas aos riscos identificados. A principal meta é evitar ou mitigar os efeitos da materialização dos riscos. A **Tabela 4** mostra a relação entre cada risco e cada medida.

Risco	Medida(s)	Efeito sobre o Risco[1]	Medida(s)[2] Implantadas(s)?
R01 - Acesso não autorizado	Implementar política formal de controle de acesso por perfil/nível no Solution3.	Mitigar	Não
	Aprimoramento do controle de acesso com adição de mecanismo MFA no sistema.	Mitigar	Não
	Definir requisitos mínimos de complexidade de senhas.	Mitigar	Não
	Proibir contas compartilhadas.	Mitigar	Sim

R02 - Modificação não autorizada	Habilitar logs de auditoria no Solution3.	Mitigar	Não
	Realizar backups periódicos com validação de integridade.	Mitigar	Não
	Restringir permissões de edição por perfil de acesso.	Mitigar	Não
R03 – Perda de dados	Implementar rotina formal de backup com retenção mínima de 90 dias.	Mitigar	Não
	Elaborar Plano de Continuidade e Contingência (PCN).	Mitigar	Não
	Verificar com CyberSul a disponibilidade de backup automático no Solution3.	Mitigar	Não
R04 – Roubo/ Vazamento na coleta	Substituir coleta via WhatsApp por formulários seguros ou portal do cliente.	Mitigar	Não
	Adotar criptografia nas comunicações.	Mitigar	Não
	Proibir conexões simultâneas com o mesmo identificador de usuário ou conta.	Mitigar	Não
	Treinar colaboradores sobre práticas seguras de coleta.	Mitigar	Não
R05 - Remoção não autorizada	Definir perfis e grupos de acesso aos dados e funcionalidades.	Mitigar	Não
R06 – Ausência de Logs	Solicitar à CyberSul a habilitação de logs de acesso e alteração no Solution3.	Mitigar	Não
	Definir responsável pelo monitoramento periódico dos logs.	Mitigar	Não
	Registrar e arquivar logs por no mínimo 6 meses.	Mitigar	Não
R07 - Coleção excessiva ou sem finalidade	Todas as modificações de cadastro que tenham impacto na privacidade precisam ser avaliadas pelo DPO.	Mitigar	Não
	Remoção ou bloqueio dos campos inutilizados nos formulários de cadastro no Solution3.	Mitigar	Não
R08 - Falta de informação ao titular	Elaborar e disponibilizar Política de Privacidade ao titular.	Mitigar	Sim
	Incluir cláusula de privacidade nos contratos com clientes.	Mitigar	Não

R09 - Ausência de bases legais documentadas	Modificar os processos internos a fim de coletar o consentimento dos titulares quando pertinente.	Mitigar	Não
	Mapear e documentar formalmente as bases legais para cada operação de tratamento.	Mitigar	Não
	Incluir termo de ciência nos contratos de trabalho e comerciais.	Mitigar	Não
R10 - Direitos dos titulares	Criar canal formal para atendimento a solicitações dos titulares.	Mitigar	Sim
	Definir SLA de resposta (máx. 15 dias conforme LGPD).	Mitigar	Sim
	Treinar equipe para atendimento a solicitações de titulares.	Mitigar	Sim
R11- Retenção prolongada	Implantar procedimento para descarte ou separação dos dados pessoais mais antigos e desnecessários no sistema Solution3.	Mitigar	Não
	Definir e documentar política de retenção e expurgo de dados pessoais.	Mitigar	Não
	Estabelecer rotina de revisão anual dos cadastros inativos.	Mitigar	Não
	Eliminar ou anonimizar dados após o prazo legal de retenção.	Mitigar	Não
R12 - Vinculação/ associação indevida dos dados pessoais ao titular	Implementar programa de treinamento dos colaboradores que manipulam o Solution3 em relação à Segurança da Informação e Privacidade, bem como reforçar sobre o uso correto de dados pessoais no sistema.	Mitigar	Não
R13 - Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Implementar rotina ou processo de descarte de dados após atingir a finalidade de tratamento.	Mitigar	Não
	Revisar com DPO ou comitê da privacidade quais dados podem ser excluídos e quais não podem sob nenhuma circunstância. Não sendo possível a exclusão, limitar o acesso ou anonimizar as informações.	Mitigar	Não

R14 - Ausência de MFA	Implementar autenticação multifator no acesso à VPN.	Mitigar	Não
	Avaliar disponibilidade de MFA no Solution3 junto à CyberSul.	Mitigar	Não
	Exigir renovação periódica de senhas (mínimo a cada 90 dias).	Mitigar	Não
R15 - Vazamento por intermédio do funcionário	Revisar termo de sigilo e coletar assinatura do funcionário após realização de treinamento em Segurança da Informação e Privacidade.	Mitigar	Não
	Evitar o armazenamento de qualquer formulário ou documento com dados pessoais em dispositivos pessoais dos usuários.	Mitigar	Sim
R16 - Infraestrutura sem política de privacidade	Solicitar à CyberSul documento formal de Política de Privacidade e comprovante de conformidade com a LGPD;	Mitigar	Não
	Incluir cláusula de responsabilidade LGPD no contrato com a CyberSul.	Mitigar	Não
	Verificar se o contrato prevê notificação de incidentes de segurança.	Mitigar	Não
R17 - Transferência ou processamento por meio de terceiros	Realizar auditorias regulares nos processos de negócio que incluem o Solution3 e os operadores de dados.	Mitigar	Não
R18 - Falha ou erro de processamento	Homologar o acesso às informações após aplicação de atualizações no sistema Solution3.	Mitigar	Não
	Manter o sistema atualizado com versão mais estável e homologada.	Mitigar	Não
R19 - Coleta informal sem auditabilidade	Padronizar a coleta por meio de formulários digitais com registro de recebimento.	Mitigar	Não
	Armazenar comprovantes de coleta com data e identificação do titular.	Mitigar	Não
	Implementar processo de validação e conferência dos dados recebidos.	Mitigar	Não

Tabela 4 - Relação Risco X Medida

Legenda da Tabela 4:

1 - Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Mitigar, Evitar, Compartilhar e Aceitar.
2 - Medida implantada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

10. PLANOS DE AÇÕES

Para facilitar o trabalho de alocação dos responsáveis, os controles foram agrupados em **43** planos de ações. A ADX fez uma sugestão a ser aprovada pelo cliente na **Figura 5 e Tabela 5.**

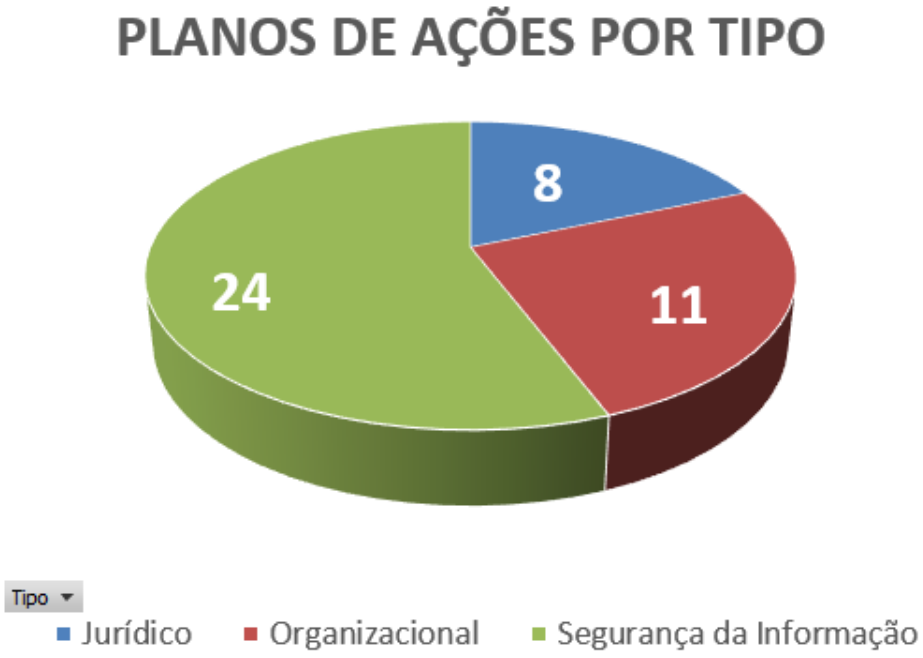

Figura 5 – Dashboard planos de ações

Nº	Medidas	Risco Associado	Tipo	Responsável
1	Implementar política formal de controle de acesso por perfil/nível no Solution3.	R01 - Acesso não autorizado.	Jurídico	YTECH
2	Aprimoramento do controle de acesso com adição de mecanismo MFA no sistema.	R01 - Acesso não autorizado.	Segurança da Informação	YTECH
3	Definir requisitos mínimos de complexidade de senhas.	R01 - Acesso não autorizado.	Segurança da Informação	YTECH
4	Habilitar logs de auditoria no Solution3 (confirmar disponibilidade com CyberSul).	R02 - Modificação não autorizada.	Segurança da Informação	YTECH
5	Realizar backups periódicos com validação de integridade.	R02 - Modificação não autorizada.	Segurança da Informação	YTECH
6	Restringir permissões de edição por perfil de acesso.	R02 - Modificação não autorizada.	Segurança da Informação	YTECH
7	Implementar rotina formal de backup com retenção mínima de 90 dias.	R03 – Perda de dados.	Segurança da Informação	YTECH
8	Elaborar Plano de Continuidade e Contingência (PCN).	R03 – Perda de dados.	Segurança da Informação	ADX
9	Verificar com CyberSul a disponibilidade de backup automático no Solution3.	R03 – Perda de dados.	Segurança da Informação	YTECH
10	Substituir coleta via WhatsApp por formulários seguros ou portal do cliente.	R04 – Roubo/ Vazamento na coleta.	Segurança da Informação	YTECH
11	Adotar criptografia nas comunicações.	R04 – Roubo/ Vazamento na coleta.	Segurança da Informação	YTECH
12	Proibir conexões simultâneas com o mesmo identificador de usuário ou conta.	R04 – Roubo/ Vazamento na coleta.	Segurança da Informação	YTECH
13	Treinar colaboradores sobre práticas seguras de coleta.	R04 – Roubo/ Vazamento na coleta.	Organizacional	YTECH

14	Definir perfis e grupos de acesso aos dados e funcionalidades.	R05 - Remoção não autorizada.	Segurança da Informação	YTECH
15	Solicitar à CyberSul a habilitação de logs de acesso e alteração no Solution3.	R06 – Ausência de Logs.	Segurança da Informação	YTECH
16	Definir responsável pelo monitoramento periódico dos logs.	R06 – Ausência de Logs.	Segurança da Informação	YTECH
17	Registrar e arquivar logs por no mínimo 6 meses.	R06 – Ausência de Logs.	Segurança da Informação	YTECH
18	Todas as modificações de cadastro que tenham impacto na privacidade precisam ser avaliadas pelo DPO.	R07 - Coleção excessiva ou sem finalidade.	Segurança da Informação	YTECH
19	Remoção ou bloqueio dos campos inutilizados nos formulários de cadastro no Solution3.	R07 - Coleção excessiva ou sem finalidade.	Segurança da Informação	YTECH
20	Incluir cláusula de privacidade nos contratos com clientes.	R08 - Falta de informação ao titular.	Jurídico	YTECH
21	Modificar os processos internos a fim de coletar o consentimento dos titulares quando pertinente.	R09 - Ausência de bases legais documentadas.	Organizacional	YTECH
22	Mapear e documentar formalmente as bases legais para cada operação de tratamento.	R09 - Ausência de bases legais documentadas.	Organizacional	ADX
23	Incluir termo de ciência nos contratos comerciais.	R09 - Ausência de bases legais documentadas.	Jurídico	YTECH
24	Implantar procedimento para descarte ou separação dos dados pessoais mais antigos e desnecessários no sistema Solution3.	R11- Retenção prolongada.	Segurança da Informação	YTECH
25	Definir e documentar política de retenção e expurgo de dados pessoais.	R11- Retenção prolongada.	Segurança da Informação	YTECH

26	Estabelecer rotina de revisão anual dos cadastros inativos.	R11- Retenção prolongada.	Organizacional	YTECH
27	Eliminar ou anonimizar dados após o prazo legal de retenção.	R11- Retenção prolongada.	Organizacional	YTECH
28	Implementar programa de treinamento dos colaboradores que manipulam o Solution3 em relação à Segurança da Informação e Privacidade, bem como reforçar sobre o uso correto de dados pessoais no sistema.	R12 - Vinculação/ associação indevida dos dados pessoais ao titular.	Organizacional	YTECH
29	Implementar rotina ou processo de descarte de dados após atingir a finalidade de tratamento.	R13 - Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade.	Organizacional	YTECH
30	Revisar com DPO ou comitê da privacidade quais dados podem ser excluídos e quais não podem sob nenhuma circunstância. Não sendo possível a exclusão, limitar o acesso ou anonimizar as informações.	R13 - Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade.	Jurídico	YTECH
31	Implementar autenticação multifator no acesso à VPN.	R14 - Ausência de MFA.	Segurança da Informação	YTECH
32	Avaliar disponibilidade de MFA no Solution3 junto à CyberSul.	R14 - Ausência de MFA.	Segurança da Informação	YTECH
33	Exigir renovação periódica de senhas (mínimo a cada 90 dias).	R14 - Ausência de MFA.	Segurança da Informação	YTECH
34	Revisar termo de sigilo e coletar assinatura do funcionário após realização de treinamento em Segurança da Informação e Privacidade.	R15 - Vazamento por intermédio do funcionário.	Organizacional	YTECH
35	Solicitar à CyberSul documento formal de Política de Privacidade e comprovante de conformidade com a LGPD.	R16 - Infraestrutura sem política de privacidade.	Jurídico	YTECH
36	Incluir cláusula de responsabilidade LGPD no contrato com a CyberSul.	R16 - Infraestrutura sem política de privacidade.	Jurídico	YTECH

37	Verificar se o contrato prevê notificação de incidentes de segurança.	R16 - Infraestrutura sem política de privacidade.	Jurídico	YTECH
38	Realizar auditorias regulares nos processos de negócio que incluem o Solution3 e os operadores de dados.	R17 - Transferência ou processamento por meio de terceiros.	Jurídico	YTECH
39	Homologar o acesso às informações após aplicação de atualizações no sistema Solution3.	R18 - Falha ou erro de processamento.	Segurança da Informação	YTECH
40	Manter o sistema atualizado com versão mais estável e homologada.	R18 - Falha ou erro de processamento.	Segurança da Informação	YTECH
41	Padronizar a coleta por meio de formulários digitais com registro de recebimento.	R19 - Coleta informal sem auditabilidade.	Organizacional	YTECH
42	Armazenar comprovantes de coleta com data e identificação do titular.	R19 - Coleta informal sem auditabilidade.	Organizacional	YTECH
43	Implementar processo de validação e conferência dos dados recebidos.	R19 - Coleta informal sem auditabilidade.	Organizacional	YTECH

Tabela 5 - Planos de Ações

11. APROVAÇÃO

A assinatura deste documento atesta que o Grupo ADX elaborou o Relatório de Impacto à Proteção de Dados Pessoais do sistema Solution3 da CyberSul sem nenhuma pendência.

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	GESTOR YTECH
_____ **Grupo ADX** Aracaju, 10 de maio de 2026	_____ **YTECH** Aracaju, 10 de maio de 2026

ENCARREGADO DE DADOS PESSOAIS (DPO)
_____ Aracaju, 10 de maio de 2026