YTECH
SOLUÇÕES

# RELATÓRIO DO DIAGNÓSTICO PARA ADEQUAÇÃO À LGPD

# Comitê Gestor de Privacidade da YTECH

| Nome | Setor | E-mail |
|---|---|---|
| Jairo Soirefmann | Diretoria | jairo@ytechsolucoes.com.br |
| Lorena Bandeira | Administrativo | lorena@ytechsolucoes.com.br |
| Carla Mendes | Financeiro | carla@ytechsolucoes.com.br |
| Matheus Santana | Área Técnica | matheus@ytechsolucoes.com.br |

# Equipe Técnica do Grupo ADX

| | |
|---|---|
| **Adriano Lima**<br>DPO e Diretor de Operações | **Laís Gomes**<br>Gerente de Projetos |
| **Hendrick Arcanjo**<br>Consultor de Tecnologia | **Saulo Santos**<br>Advogado |

| Histórico de revisões | | | |
|---|---|---|---|
| **Versão** | **Data** | **Autor** | **Descrição** |
| 1.0 | 14/04/2026 | Grupo ADX | Elaboração do documento |

# Sumário

## ÍNDICE DE FIGURAS

# 1 - Termo de Confidencialidade

O relatório final do diagnóstico LGPD da Ytech é um documento confidencial e deverá ser utilizado somente por membros do comitê de privacidade. A revelação direta ou indireta de qualquer parte deste documento, para pessoas não autorizadas, dará a Ytech direito de tomar as ações legais cabíveis a este tipo de conduta. Para ter acesso ao documento na sua íntegra, o colaborador deverá ter assinado o termo de confidencialidade.

# 2 – Resumo Executivo

Com o objetivo de proteger a privacidade da população brasileira, foi sancionada, em agosto de 2018, a Lei Geral de Proteção de Dados (LGPD). Inspirada na legislação europeia, - GDPR (General Data Protection Regulation) - a regulamentação local tem como objetivo aumentar o controle do fluxo de informações pessoais nas organizações e fiscalizar a forma como elas são utilizadas.

É de extrema importância o completo entendimento do ciclo de vida da informação dentro da empresa, visando a implantação de todos os controles jurídicos e de segurança da informação para adequação à lei. A figura a seguir descreve as fases desse ciclo de acordo com a LGPD.


*Figura 1 - Ciclo de vida da informação.*

Já se sabe que a LGPD alterará significativamente as regras para a coleta, armazenamento e utilização de informações dentro das empresas. O que poucos líderes de TI e negócios já perceberam é que seguir as novas condições não é apenas uma questão de se evitar sanções. Na verdade, a LGPD pode ser uma grande oportunidade para que as empresas brasileiras entrem de vez na transformação digital, obtendo grandes vantagens comerciais.

Cientes dos benefícios que a adequação à Lei Geral de Proteção de Dados pode trazer para a governança dos dados da organização, a Ytech assumiu o compromisso de elaborar um diagnóstico detalhado para levantamento de todos os ajustes necessários pela lei.

Como as informações transitam pelos setores da empresa assim como o nosso sangue transita pelos nossos órgãos, foi necessário analisar as diversas fontes de dados existentes. A imagem a segui mostra um exemplo de alguns locais importantes que foram auditados.


*Figura 2 - Fontes de informações.*

O diagnóstico apresenta, como resultado das análises frente às diversas documentações apresentadas e das inspeções realizadas nos principais setores da empresa, uma visão profunda do momento em que a empresa se encontra perante aos requisitos processuais, jurídicos e de segurança da informação. O documento final do diagnóstico norteará todas as ações e projetos a serem implantados, tendo sempre como base o alinhamento com a estratégia da corporação, através do plano estratégico corporativo.

# 3 – A YTECH

A YTECH Soluções é uma empresa brasileira especializada na integração de tecnologias voltadas à mobilidade corporativa e automação de processos. Atuando há mais de uma década no mercado, a organização se destaca por fornecer soluções completas de captura automática de dados e infraestrutura tecnológica, apoiando empresas na transformação digital de suas operações.

Seu portfólio contempla a implementação de sistemas e dispositivos como coletores de dados, leitores de código de barras, impressoras industriais, etiquetas eletrônicas de prateleira (ESL) e redes sem fio, permitindo maior eficiência, rastreabilidade e controle das informações nos processos organizacionais.

A YTECH atende diversos segmentos, incluindo varejo, indústria, logística e saúde, oferecendo soluções que conectam operações em tempo real, aumentam a produtividade e melhoram a experiência do cliente. Além disso, a empresa atua no desenvolvimento de soluções personalizadas para toda a cadeia de suprimentos, promovendo maior integração entre sistemas, pessoas e dados.

Com foco em inovação e desempenho operacional, a YTECH tem como missão apoiar seus clientes na adaptação às demandas do mercado, por meio da utilização de tecnologias avançadas que otimizam processos, reduzem erros e fortalecem a tomada de decisão baseada em dados

# 4 – Organogramas

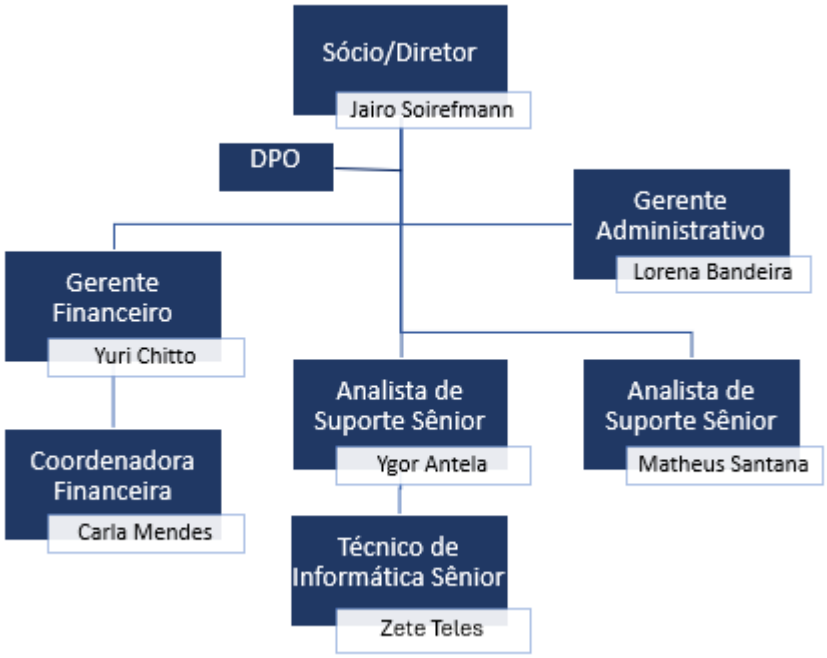



*Figura 3 - Organograma da Ytech.*

# 5 – Canvas da Engenharia do Negócio

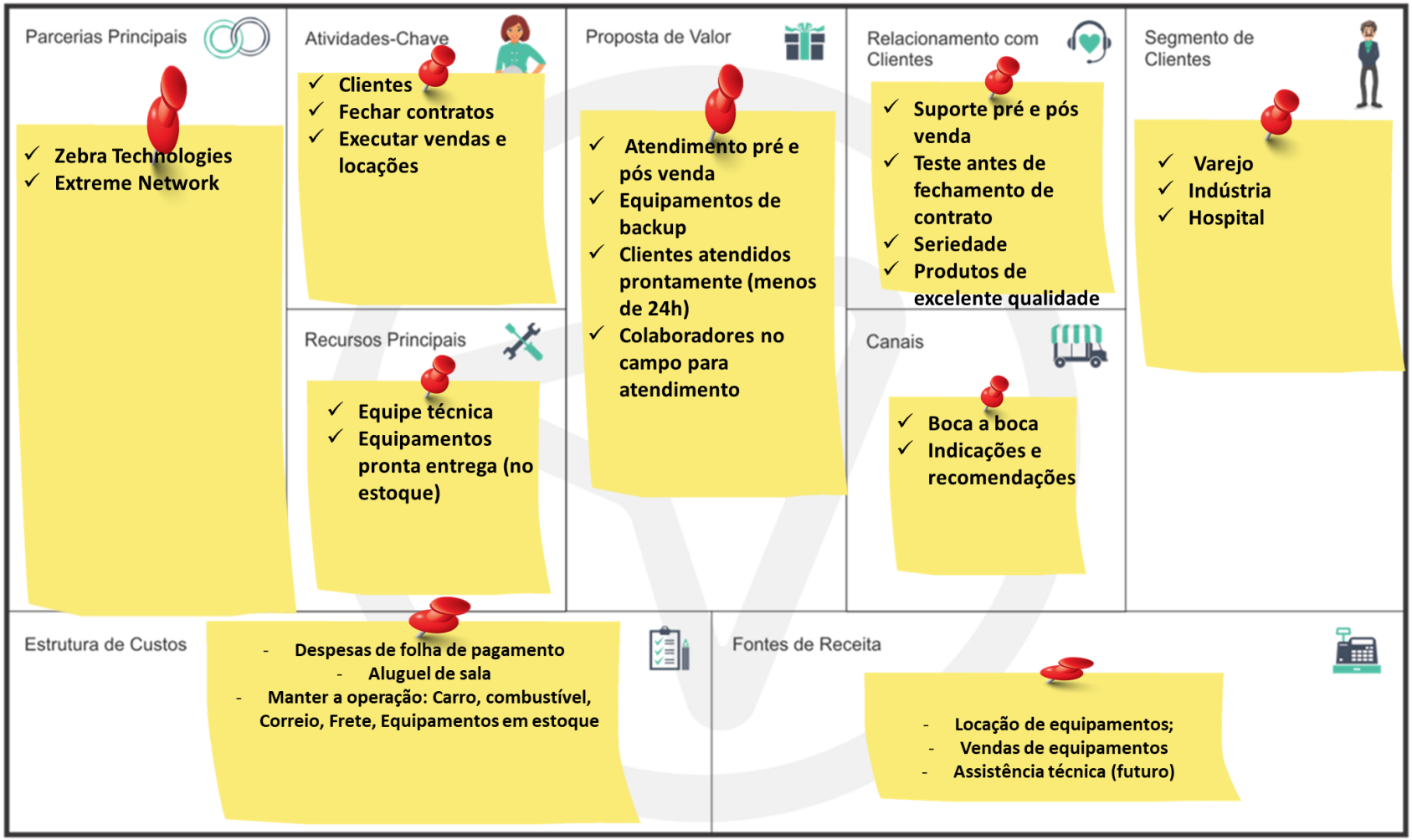



*Figura 4 - Canvas BMG da Ytech*

# 6 – Macroprocesso

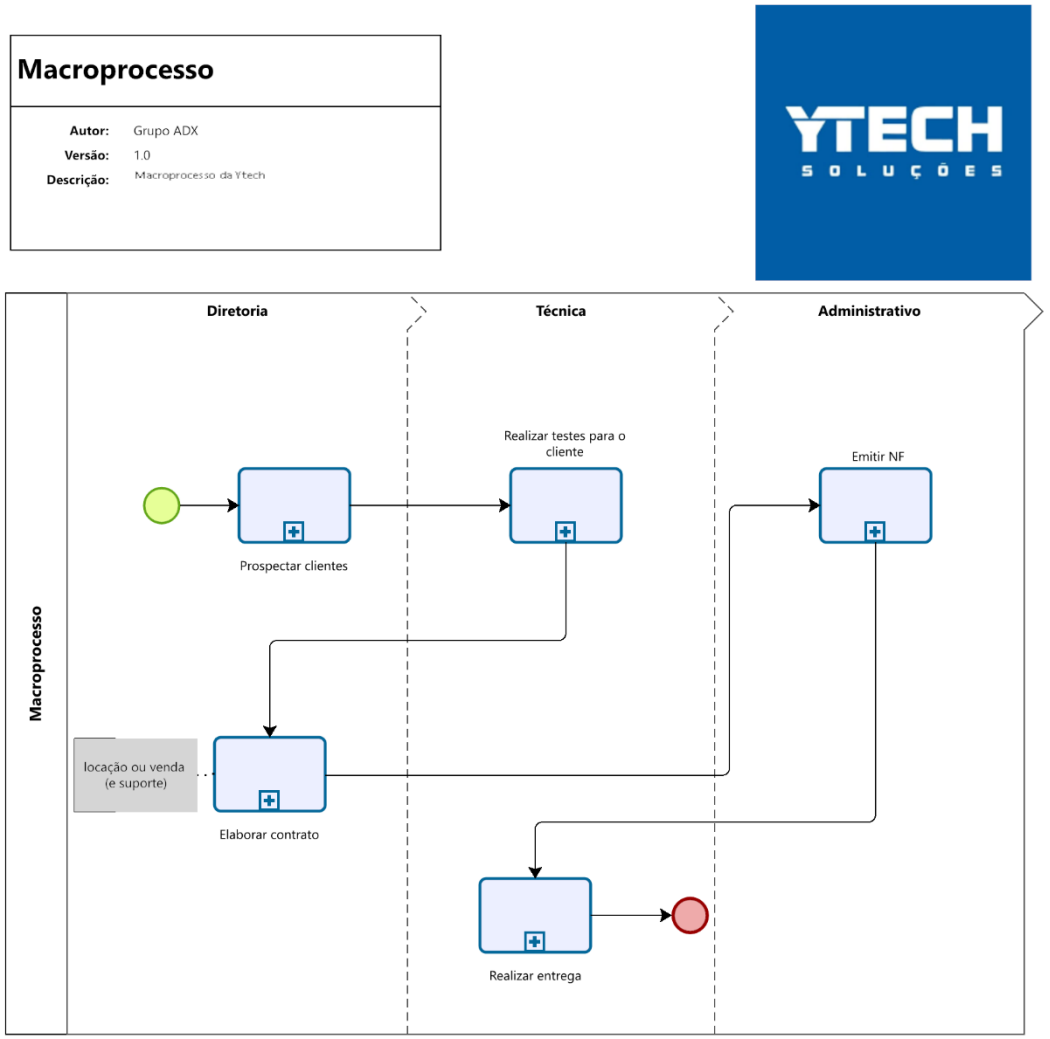



*Figura 5 - Macroprocesso da Ytech*

# 7 – Contratos, políticas e procedimentos analisados

A análise dos contratos, políticas e procedimentos da Ytech foi dividida em duas etapas:

- **I** – Análise dos contratos com fornecedores e colaboradores da Ytech à luz da LGPD;
- **II** – Elaboração de aditivo contratual para os contratos com fornecedores, incluindo cláusulas referentes ao tratamento de dados pessoais e revisão e inclusão de cláusulas nos contratos de colaboradores referentes ao tratamento de dados pessoais dos colaboradores.

# 8 – Mapeamento de dados pessoais

Para facilitar o levantamento de dados pessoais, realizou-se um Workshop onde foi realizado um treinamento sobre os principais conceitos relacionados a LGPD e onde foram levantados os principais fluxos de dados pessoais entre os setores, fornecedores e parceiros, através do Canvas desenvolvido pelo Grupo ADX. Todo o trabalho foi feito com o Canvas LGPD da ADX, demostrado na **Figura 9**.

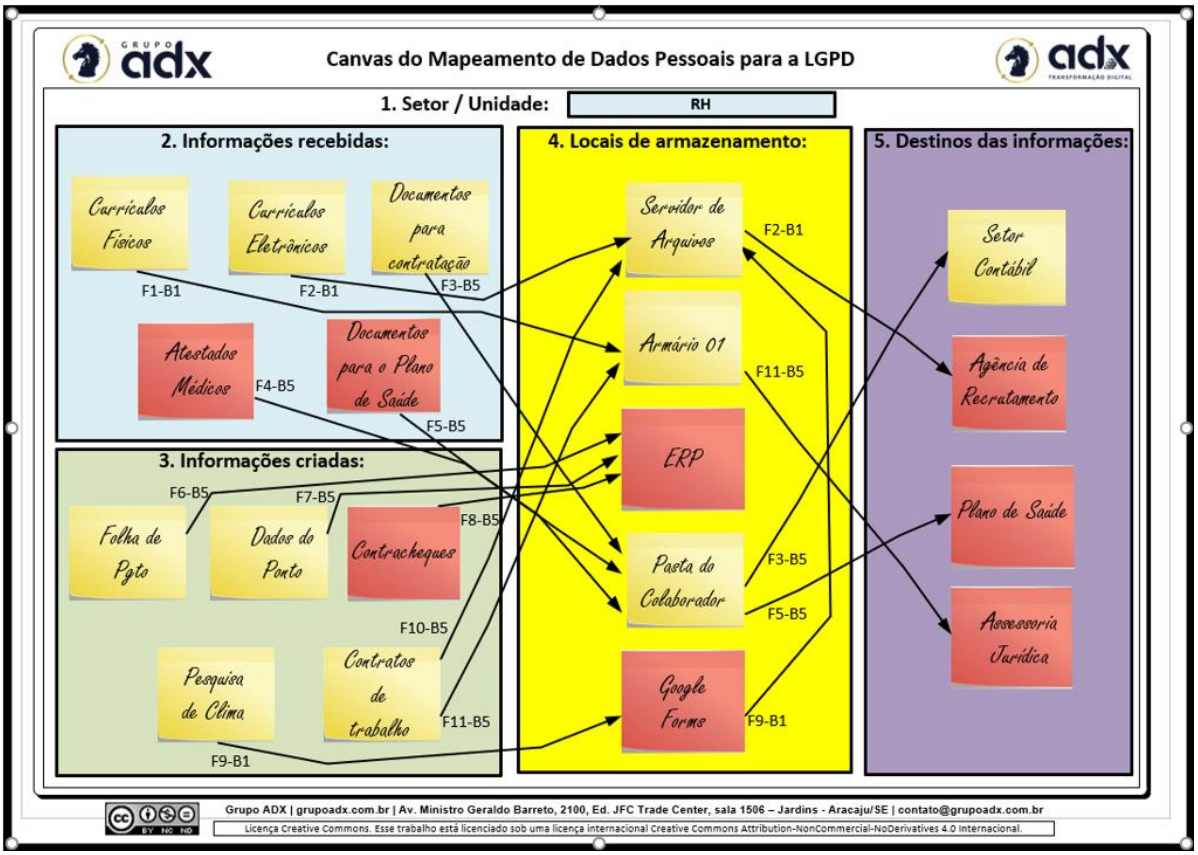



*Figura 6 - Canvas do Mapeamento de Dados para a LGPD.*

Todo o material produzido serviu como ponto de entrada do trabalho de mapeamento de dados pessoais dentro da Ytech. Os Canvas produzidos para cada setor podem ser vistos nas imagens a seguir.


*Figura 7 - Canvas LGPD do setor Administrativo*


*Figura 8 - Canvas LGPD do setor financeiro*

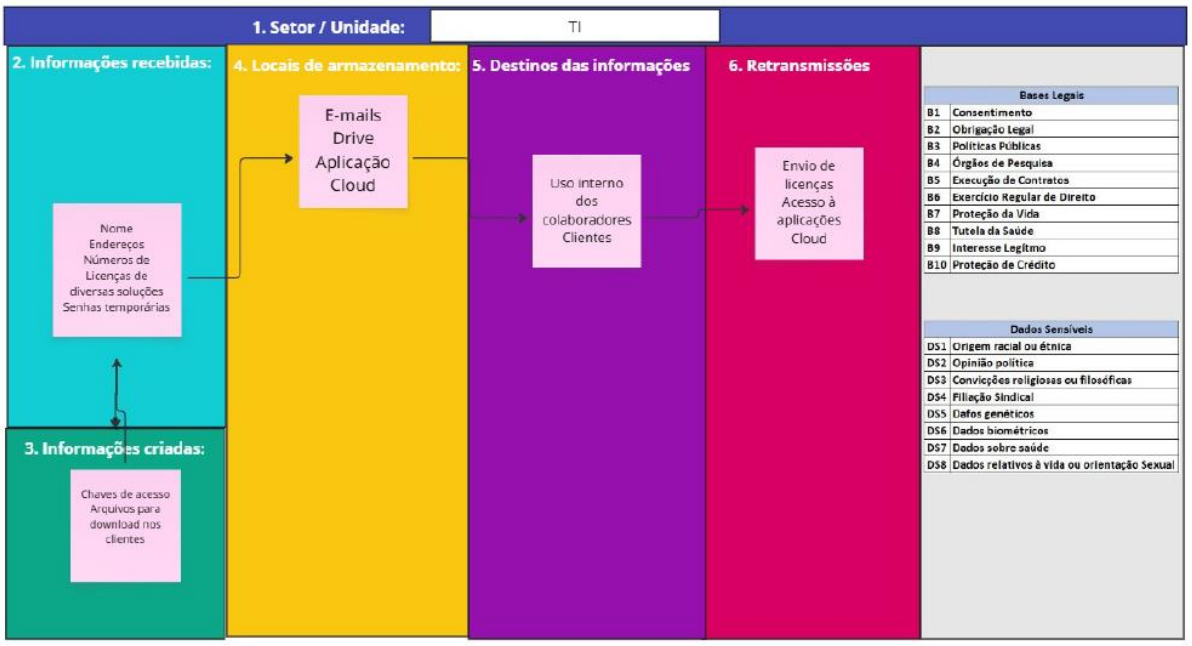



*Figura 9 – Área técnica*

Os fluxos identificados nesse Workshop serviram de ponto de partida para o detalhamento das informações pessoais tratadas por cada setor da empresa, realizado através de entrevistas individuais com cada participante.

Com as informações coletadas nas entrevistas, os fluxos de dados foram desenhados na ferramenta Bizagi, descrevendo detalhadamente todos os processos que tratam dados pessoais. Cada processo foi minuciosamente validado com os responsáveis, através de vídeo conferências.

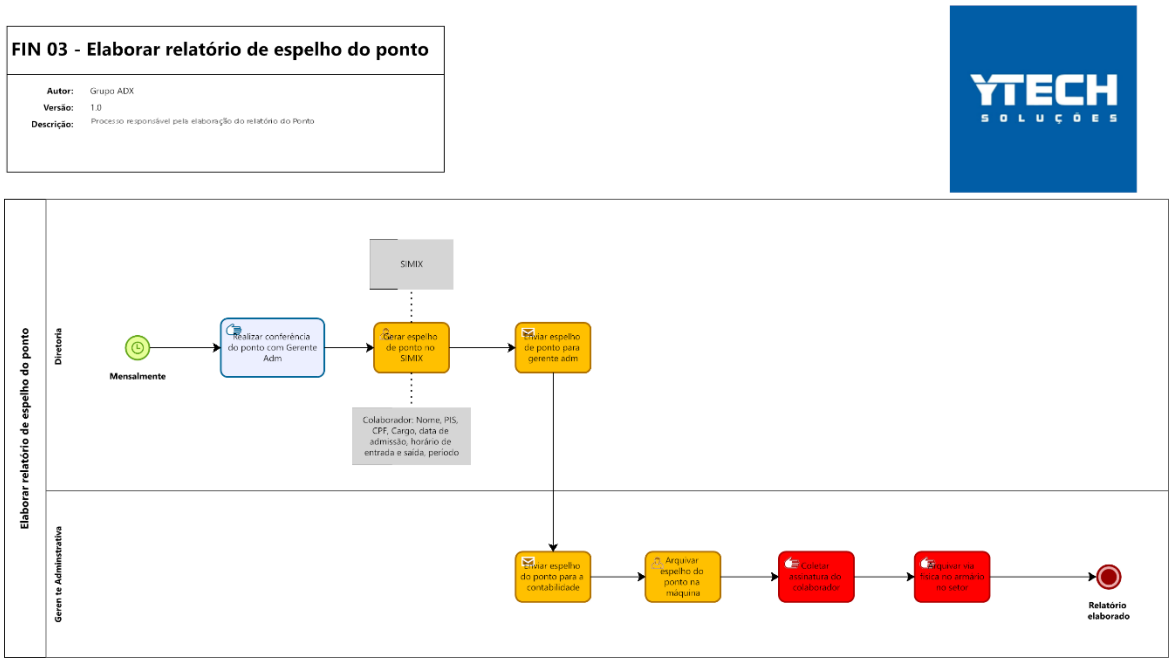
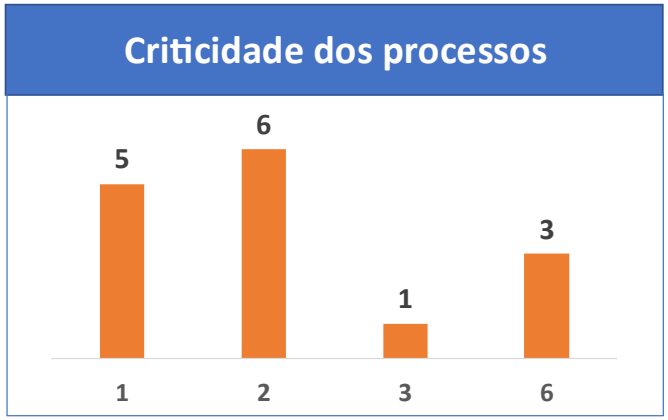


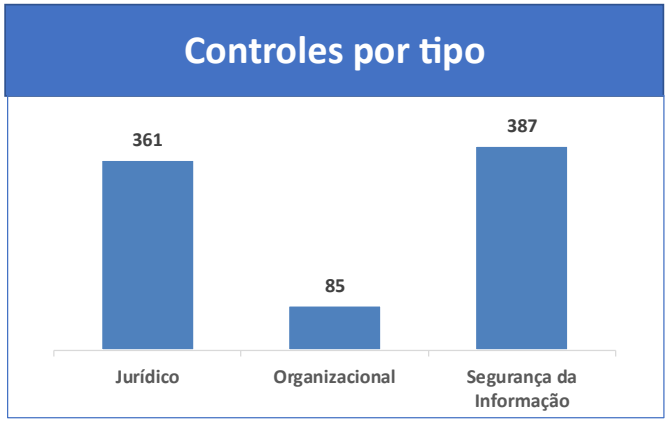

*Figure 1 - Exemplo de processo mapeado.*

Após o completo entendimento de cada processo, foi feita uma análise sobre os riscos existentes em relação aos requisitos para adequação à LGPD. A figura a seguir mostra um resumo do trabalho feito com **4** setores, **15** processos de negócio que tratam dados pessoais, resultando em um total de **92** riscos. Para tratamento desses riscos, foram propostos **123** controles (Jurídicos, organizacionais ou de segurança da informação).

YTECH SOLUÇÕES

| | |
|---|---|
| 15 | Quantidade de processos |
| 92 | Quantidade de riscos mapeados |
| 123 | Qtd. de controles mapeados |
| 47% | Percentual de processos que tratam dados pessoais sensíveis |
| 14 | Processos que fazem internacionalização de dados |
| 01 | Processos que tratam dados de crianças e adolescentes |
| 17 | Nº de operadores externos |



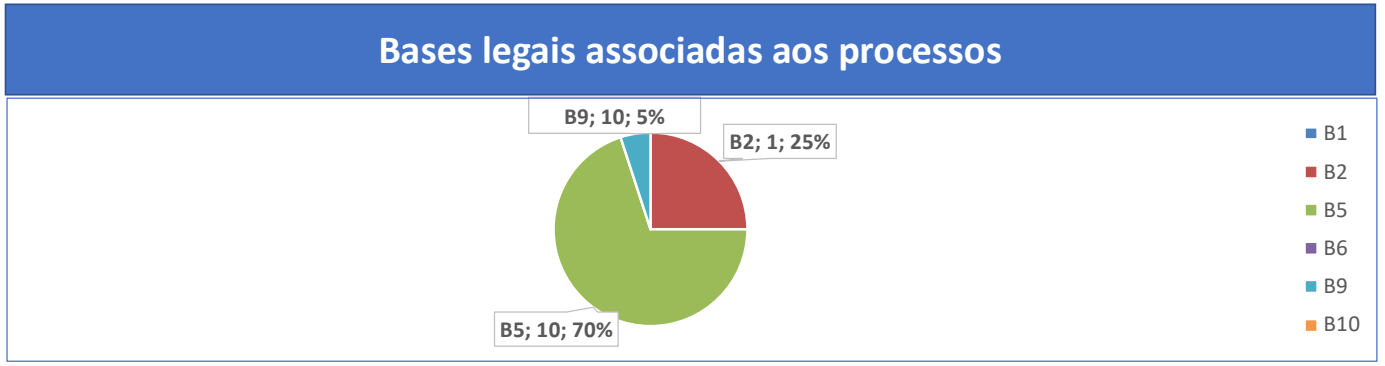




*Figure 2 - Dashboard resumo dos processos mapeados.*

# 9 – Análise de segurança

Essa sessão descreverá todas as análises realizadas em relação à segurança da informação do ambiente da Ytech.

## 9.1 – Conhecimento do ambiente

A análise de segurança iniciou com o conhecimento do ambiente de tecnologia da Ytech. Sendo uma empresa de pequeno porte, e por hospedar todos os serviços e arquivos críticos na nuvem, o escritório da Ytech não possui, em seu ambiente interno, infraestrutura de servidores, serviços de rede ou solução para gestão de identidades, autenticação e gerenciamento de ativos.

Não há domínio em sua rede privada.

O mapa de rede completo pode ser visto na imagem a seguir.

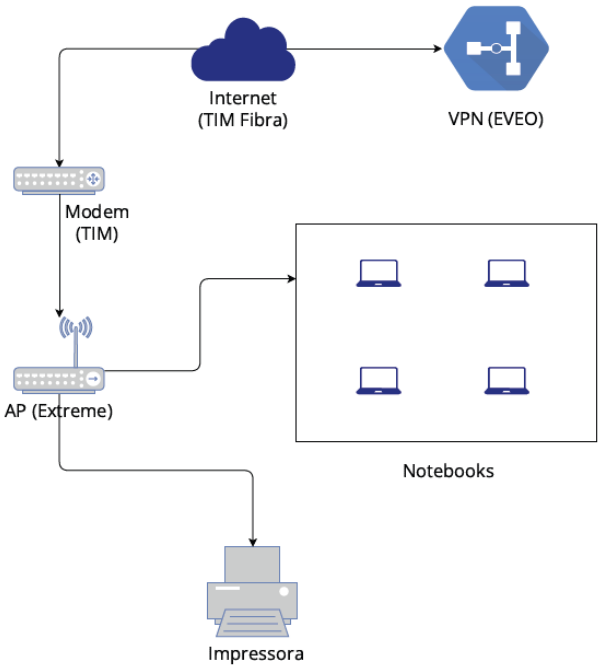



*Figura 10 - Mapa de rede.*

9.2 – Equipamentos

Os seguintes equipamentos fazer parte do ambiente interno da Ytech.

| Tipo | Modelo | Número de Série |
|---|---|---|
| Notebook | HP Latitude 3550 | 35762440144 |
| Notebook | HP Latitude 3550 | 29111160784 |
| Notebook | Lenovo Ideapad 3 | PEOBBH87 |
| Notebook | Lenovo Ideapad 1 | PEOBCL4X |
| Smartphone | Motorola Edge 60 Fusion | 89562818 |
| Smartphone | Motorola Edge 60 Fusion | 89564586 |
| Smartphone | Motorola Edge 60 Fusion | ZF5259XW7B |
| Smartphone | Motorola Edge 60 Fusion | ZF528PG8B |
| Impressora | HP LaserJet MFP | BRDSSCC01V |
| Ponto de Acesso | Extreme Networks AP5010 | |

*Figure 3 -Equipamentos do ambiente interno*

9.3 – Sistemas utilizados

A tabela a seguir apresenta a relação de sistemas e software usados pela Ytech.

| Nome | Descrição | Localização |
|---|---|---|
| Solution3 - CyberSul | ERP | Provedor de hospedagem da EVEO |
| AUVO | Software para gestão de tickets e monitoramento de equipes externas. | Nuvem |
| Extreme Cloud IQ | Plataforma para gerenciamento de ativos de rede. | Nuvem |
| Extreme Platform One | Plataforma de gerenciamento de redes que integra segurança e IA. | Nuvem |
| Urmobo MDM | Ferramenta para gerenciamento de dispositivos móveis corporativos. | Nuvem |
| Google Workspace | Suíte da Google para produtividade e colaboração. | Nuvem |
| Ekahau | Software para design, análise e validação de redes Wi-Fi de alto desempenho. | Máquina do técnico |
| StageNow | Software para configuração de dispositivos Zebra Technologies. | Máquina do técnico |

*Figure 4 -Sistemas e softwares utilizados pela empresa*

9.4 – Análise de segurança do site

Essa seção mostra os resultados das análises de segurança realizadas no ambiente.

9.4.1 – Itens críticos de segurança

A ADX realizou uma análise de segurança para mapear as áreas onde a Ytech precisa ter maior atenção em relação a confidencialidade, integridade e disponibilidade das informações. O resultado dessa análise pode ser visto na tabela a seguir com a seguinte legenda:

- Requisito de segurança implementado completamente;
- Requisito de segurança necessitando de melhorias;
- Requisito de segurança não implementado;
- Requisito de segurança inexistente.

| **Infraestrutura** | | |
|---|---|---|
| **Defesa de perímetro** | | **OBS** |
| Solução de Firewalls | | Não se aplica. |
| Regras e filtros de firewall | | Não se aplica. |
| Antivírus - Estação de trabalho | | Utilizam soluções gratuitas, além do antivírus nativo da Microsoft. Não há sistema gerenciador. |
| Antivírus - Servidores | | Não se aplica. |
| Acesso remoto | | VPN utilizada para acessar a VM do ERP localizado em um provedor IaaS. Necessita melhorar mecanismo de autenticação. |
| Servidores DNS | | Não possuem. Serviço de DNS do provedor de internet ou público. |
| Filtro de conteúdo | | Não definido. |
| Sistemas de prevenção de intrusão | | Não detectado. |
| **Segmentação** | | **OBS** |
| VLANs | | Não definido. |
| Rede sem fio | | Precisa melhorar método de autenticação. |
| DMZ | | Não se aplica. |
| Listas de controle de acesso | | Não possuem. |

| Autenticação | | OBS |
|---|---|---|
| Usuários administrativos |  | Não há serviços para gestão de identidades e ativos. |
| Contas de serviços |  | Não há serviços de rede. |
| Usuários de acesso remoto |  | OK. |
| Política de senhas |  | Precisa criar a política de senhas. |
| Contas inativas |  | Não se aplica. |
| **Gerenciamento e monitoramento** | | **OBS** |
| Denúncia e resposta a incidentes |  | Precisa ser definido para atender a LGPD. |
| Segurança física |  | Acesso ao escritório através de porta com fechadura comum. Estoque sem controle de acesso. |
| Monitoramento dos ativos de rede |  | Há somente um AP e uma impressora no local. |
| Monitoramento dos links |  | Não é realizado. Possuem somente um provedor de internet. |
| Monitoramento dos servidores |  | Não há servidores no ambiente. |

## Pessoal

| Requisitos e avaliações | | OBS |
|---|---|---|
| Requisitos de segurança |  | Necessidade de capacitação em segurança. |
| Avaliações periódicas de segurança |  | Não foram detectadas auditorias de segurança. |
| **Políticas e procedimentos** | | **OBS** |
| Políticas de RH |  | Precisa criar procedimentos da TI para contratação e desligamento de colaboradores. |
| Treinamento e conscientização |  | Precisa criar agenda de treinamentos. |
| Termo de uso dos recursos |  | Não detectado. |
| **Autorização e controle de acesso** | | **OBS** |
| Conscientização em segurança |  | Precisa criar eventos recorrentes. |
| Treinamento em segurança |  | Não possuem. |

## Aplicações

| Implantação e uso | | OBS |
|---|---|---|
| Virtualização |  | Não implementado em ambiente interno. VM com ERP monitorado pelo desenvolvedor. |
| Uso de cluster |  | Não implementado. |
| Recuperação de dados |  | Precisa escrever uma política de backup. |
| Eliminação de vulnerabilidades |  | Windows Update com configuração automática. Não há solução para AV. |

| Projeto de aplicativos | | OBS |
|---|---|---|
| Autenticação |  | Precisa criar a política de senhas. |
| Política de senhas |  | Precisa criar a política de senhas. |
| Autorização e controle de acesso |  | OK |
| Registro em logs |  | Não possuem. |
| Homologação das alterações |  | Não foi detectado procedimento. |
| Metodologia de desenvolvimento |  | Não desenvolvem software. |
| **Operações** | | |
| **Política de segurança** | | **OBS** |
| Classificação de dados |  | Precisa criar a política de classificação. |
| Descarte de dados |  | Não há procedimentos. |
| Segurança dos serviços |  | Não há procedimentos. |
| Gerenciamento de contas de usuários |  | OK. |
| Workflow e gerenciamento de documentos |  | Não foi detectado. |
| Metodologia de gerenciamento de projetos |  | Não foi detectada. |
| **Gerenciamento da rede** | | **OBS** |
| Documentação da rede |  | Necessita ser atualizada. |
| Homologação de paths |  | Não foi detectado. |
| Monitoramento de ativos |  | Há somente um AP e uma impressora no local. |
| **Backup e restauração** | | **OBS** |
| Arquivos e logs |  | Não foi detectado solução de backup. Backup do ERP de responsabilidade do desenvolvedor. |
| Recuperação contra desastres |  | Precisa documentar a política de Backup. Backup do ERP de responsabilidade do desenvolvedor. |
| Política de backup |  | Precisa documentar a política de Backup. |
| Software de Backup |  | Não foi detectado solução de backup. Backup do ERP de responsabilidade do desenvolvedor. |
| Testes de restore |  | Não foi detectado solução de backup. |

*Tabela 6 – Análise de segurança.*

O gráfico a seguir demonstra uma comparação entre o valor atual e o valor ideal de cada área de segurança avaliada. A diferença entre a linha verde e a linha vermelha destaca a lacuna de segurança ainda existente no ambiente da Ytech.

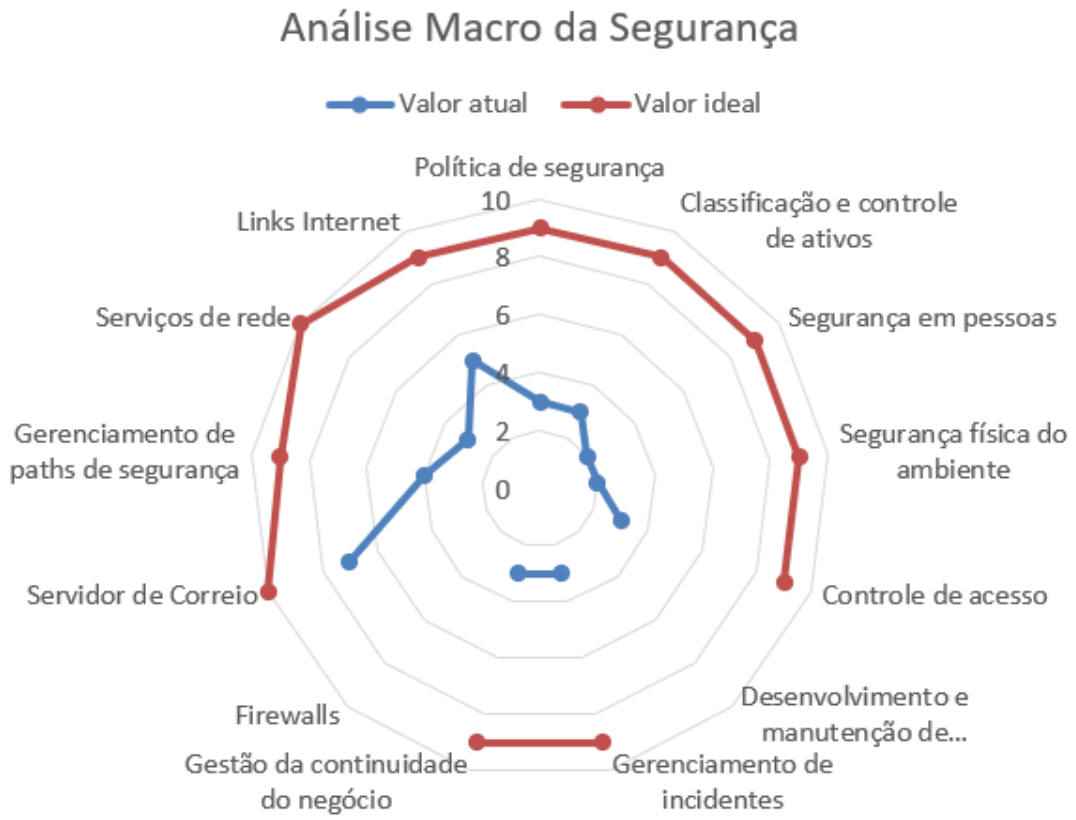



*Figura 11 - Resumo do status dos controles de segurança.*

9.5 – Análise dos requisitos da ISO 27001

A ISO 27001 é uma norma internacional publicada pela Internacional Standardization Organization (ISO) e descreve como gerenciar a segurança da informação em uma organização. A versão mais recente desta norma foi publicada em 2013, e seu título completo agora é ISO/IEC 27001:2013. A primeira versão desta norma foi publicada em 2005, e foi desenvolvida com base na Norma Britânica BS 7799-2.

A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequena ou grande. Ela é escrita pelos melhores especialistas mundiais no campo de segurança da informação e provê metodologia para a implementação da gestão da segurança da informação em uma organização. Ela também possibilita que organizações obtenham certificação, o que significa que um organismo certificador independente confirmou

que uma organização implementou a segurança da informação em conformidade com a ISO 27001.

Foi realizado um diagnóstico em relação aos controles da norma ISO 27001. O diagnóstico usou o modelo proposto por Marcos Sêmola, onde cada item avaliado recebe uma nota e a soma de todas as avaliações é comparada com a tabela a seguir:

| Conformidade ISO 27001 | |
|---|---|
| **Pontuação** | **Nível de Conformidade** |
| 80-54 | Bom |
| 53-27 | Médio |
| 26- 0 | Ruim |

*Tabela 7 – Níveis de conformidade ISO 27001.*

Nas tabelas a seguir, estão os resultados de cada área avaliada da norma.

| 1. POLÍTICA DE SEGURANÇA | Avaliação | OBS |
|---|---|---|
| Política de segurança? | 0 - Não | Não detectada. |
| Algum responsável pela gestão da política de segurança? | 0 - Não | Não detectado. |
| **Resultado** | **0** | |

*Tabela 8 – Análise da PSI.*

| 2. SEGURANÇA ORGANIZACIONAL | Avaliação | OBS |
|---|---|---|
| Infraestrutura de segurança da informação para gerenciar as ações corporativas? | 0 - Não | Não detectado. Será implementado para a LGPD. |
| Fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas? | 0 - Não | Não detectado. Será implementado para a LGPD. |
| Definição clara das atribuições de responsabilidade associadas à segurança da informação? | 0 - Não | Não definido. |
| Identificação dos riscos no acesso de prestadores de serviço? | 0 - Não | Não foi detectada uma política específica para os fornecedores. |
| Controle de acesso específico para os prestadores de serviço? | 0 - Não | Não foi detectada uma política específica para os fornecedores. |
| Requisitos de segurança dos contratos de terceirização? | 0 - Não | Não foi detectada uma política específica para os fornecedores. |
| **Resultado** | **0** | |

*Tabela 9 – Análise da Segurança Organizacional.*

| 3. CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO | Avaliação | OBS |
|---|---|---|
| Inventário dos ativos físicos, tecnológicos e humanos? | 1 - Parcialmente | Necessário atualização. |
| Critérios de classificação da informação? | 0 - Não | Não foi detectada uma política de classificação. |
| **Resultado** | **1** | |

*Tabela 10 – Análise dos Ativos.*

| 4. SEGURANÇA EM PESSOAS | Avaliação | OBS |
|---|---|---|
| Critérios de seleção e política de pessoal? | 0 - Não | Não foi detectado. |
| Acordo de confidencialidade, termos e condições de trabalho? | 0 - Não | Não foi detectado. |
| Processos para capacitação e treinamento de usuários? | 0 - Não | Não existe programação para capacitação em segurança. |
| Estrutura para notificar e responder aos incidentes e falhas de segurança? | 0 - Não | Não existe formalmente. |
| **Resultado** | **0** | |

*Tabela 11 – Análise do RH*

| 5. SEGURANÇA FÍSICA E DE AMBIENTE | Avaliação | OBS |
|---|---|---|
| Definição de perímetros e controle de acesso físico aos ambientes? | 1 - Parcialmente | |
| Recursos para segurança e manutenção dos equipamentos? | 0 - Não | Não há controles ou ferramentas. |
| Estrutura para fornecimento adequado de energia? | 0 - Não | |
| Segurança de cabeamento? | 0 - Não | Não há requisitos mínimos de infraestrutura. |
| **Resultado** | **1** | |

*Tabela 12 – Análise da Segurança Física.*

| 6. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES | Avaliação | OBS |
|---|---|---|
| Procedimentos e responsabilidades operacionais? | 0 - Não | Não foram detectados procedimentos na área de TI. |
| Controle de mudanças operacionais? | 0 - Não | Não foram detectados procedimentos na área de TI |
| Segregação de funções e ambientes? | 0 - Não | Não há segmentação. |
| Planejamento e aceitação de sistemas? | 1 – Parcialmente | |
| Procedimentos para cópias de segurança? | 0 - Não | Precisa escrever uma política de Backup. |
| Controles e gerenciamento de Rede? | 0 - Não | Não há solução. |
| Mecanismos de segurança e tratamentos de mídias? | 0 - Não | Precisa definir procedimentos. |
| Procedimentos para documentação de sistemas? | 1 - Parcialmente | Precisa atualizar procedimentos. |
| Mecanismos de segurança do correio eletrônico? | 2 - Sim | OK. |
| **Resultado** | **4** | |

*Tabela 13 – Análise das operações e comunicações.*

| 7. CONTROLE DE ACESSO | Avaliação | OBS |
|---|---|---|
| Requisitos do negócio para controle de acesso? | 1 - Parcialmente | Precisa revisar permissões em sistemas. |
| Gerenciamento de acessos do usuário? | 1 - Parcialmente | Precisa revisar acesso em sistemas. |
| Controle de acesso à rede? | 0 - Não | |
| Controle de acesso ao sistema operacional? | 0 - Não | Não se aplica. |
| Controle de acesso às aplicações? | 1 - Parcialmente | Precisa melhorar mecanismo de autenticação. |
| Monitoração do uso e acesso ao sistema? | 0 - Não | Não foram detectados procedimentos. |
| Critérios para computação móvel e trabalho remoto? | 0 - Não | Não foram detectados procedimentos. |
| **Resultado** | **3** | |

*Tabela 14 – Análise do Controle de Acesso.*

| 8. DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS | Avaliação | OBS |
|---|---|---|
| Requisitos de segurança de sistemas? | 0 - Não | Não se aplica. |
| Controles de criptografia? | 0 - Não | Não se aplica. |
| Mecanismos de segurança nos processos de desenvolvimento e suporte? | 0 - Não | Não se aplica. |
| **Resultado** | **0** | |

*Tabela 15 – Análise dos sistemas.*

| 9. GESTÃO DA CONTINUIDADE DO NEGÓCIO | Avaliação | OBS |
|---|---|---|
| Requisitos de segurança de sistemas? | 1 - Parcialmente | Precisa revisar permissões e autorizações. |
| **Resultado** | **1** | |

*Tabela 16 – Análise da continuidade do negócio.*

| 10. CONFORMIDADE | Avaliação | OBS |
|---|---|---|
| Gestão de conformidades técnicas e legais? | 0 - Não | Não identificado. |
| Recursos e critérios para auditoria de sistemas? | 0 - Não | Não identificado. |
| **Resultado** | **0** | |

*Tabela 17 – Análise da conformidade.*

| **Resultado Geral** | **10** |
|---|---|

O resultado obtido mostra que a Ytech possui um nível de conformidade Ruim com a norma. Tecnicamente, isso destaca a importância de implementar melhorias e controles essenciais importantes na empresa, visando conformidade com a norma.

### 9.6 – Análise dos requisitos da ISO 27701

A ISO 27701 – Sistemas de Gestão de Informação Privada, foi publicada no dia 05 de agosto de 2019 e tem como objetivo estabelecer controles de segurança para proteção de dados, sendo uma adequação lógica para LGPD e GDPR. Para a garantia do cumprimento dos requisitos da norma ISO 27701, foi feita uma análise sobre cada controle sugerido pelo documento. Todos os controles que ainda não foram completamente implementados no ambiente farão parte do plano de ações fornecido pela ADX e serão monitorados pelo Dashboard de conformidade disponibilizado para o acompanhamento do cliente. O gráfico a seguir mostra um resumo da situação de cada controle no ambiente da Ytech.

| RESUMO DE PONTUAÇÃO – ISO/IEC 27701:2019 | | | | | |
|---|---|---|---|---|---|
| Seção / Anexo | Conformes (C) | Não Conformes (NC) | Não Aplicável (NA) | Parcialmente | Total Avaliado |
| 5 – Contexto da Organização | 0 | 4 | 0 | 0 | 4 |
| 6 – Liderança | 0 | 3 | 0 | 1 | 4 |
| 7 – Planejamento | 0 | 4 | 0 | 0 | 4 |
| 8 – Suporte | 0 | 4 | 0 | 0 | 4 |
| 9 – Operação | 0 | 12 | 1 | 2 | 14 |
| 10 – Avaliação de Desempenho | 0 | 3 | 0 | 0 | 3 |
| 11 – Melhoria | 0 | 2 | 0 | 0 | 2 |
| Anexo A – Controles para Controladores de Dados Pessoais | 0 | 16 | 0 | 0 | 16 |
| Anexo B – Controles para Operadores de Dados Pessoais | 0 | 6 | 0 | 2 | 8 |
| Extensões aos Controles da ISO/IEC 27001 com Foco em Privacidade – Extensões aos Controles da ISO/IEC 27001 com Foco em Privacidade | 0 | 9 | 0 | 1 | 10 |
| TOTAL GERAL | 0 | 63 | 1 | 6 | 69 |

*Figure 5 – Requisitos da ISO 27701.*

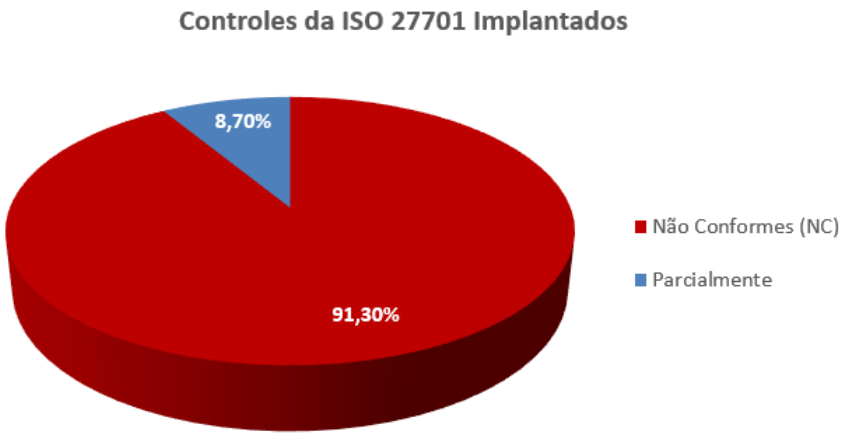



*Figure 6 - Avaliação ISO 27701.*

### 9.7 – Análise das configurações dos servidores e serviços de rede

Durante a análise de segurança, alguns problemas críticos pontuais foram encontrados e precisam de remediação urgente. Eles serão descritos nessa sessão do documento.

O ambiente interno não possui infraestrutura de servidores, serviços de rede ou controlador de domínio, consequentemente não há políticas de ambiente que definam regras para contas de usuários e equipamentos.

Mesmo não havendo política de senhas implementada, é valido citar a importância de seguir boas práticas para definição das mesmas pelos usuários, criando-se assim uma camada de proteção a mais. A imagem a seguir mostra as configurações recomendadas pela CIS para uma configuração mais segura da política de senhas.

| **Account Policies** |
|---|
| **Password Policy** |
| (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored) |
| (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored) |
| (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Scored) |
| (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Scored) |
| (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Scored) |
| (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Scored) |
| **Account Lockout Policy** |
| (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored) |
| (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored) |
| (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Scored) |

*Figure 7 - Política de senhas sugerida pelo CIS.*

O antivírus usado nas estações de trabalho é o Windows Defender, solução nativa e gratuita presente em sistemas operacionais da Microsoft. Além deste há outras soluções gratuitas instaladas nas máquinas dos colaboradores, mas sem padrão estabelecido, validação ou gerenciamento.

Não é utilizada solução de gerenciamento de patches de segurança no ambiente. A definição de instalação dos patches no Windows Update está como automática. Cada usuário é responsável por realizar este monitoramento.

Não há serviço de gerenciamento e monitoramento de identidades ou dispositivos no ambiente. Os usuários possuem todas as permissões administrativas sobre seus respectivos dispositivos.

#### 9.7.1 – Análise das vulnerabilidades da rede, servidores e links externos

A análise de Vulnerabilidades externas e das aplicações foi realizada durante o período de 31/03/2026 até 29/04/2026. As constatações e recomendações refletem as informações coletadas durante a avaliação e estado do ambiente naquele momento e não quaisquer alterações realizadas posteriormente fora deste período. As informações detalhadas sobre cada vulnerabilidade encontrada foram registradas no documento **2026 - Ytech - Análise de Vulnerabilidades Externa**.

# 10 – Análise jurídica

Essa sessão do documento visa elucidar todos os pontos críticos referentes à LGPD que foram analisados durante o diagnóstico. Será sempre exibido um referencial teórico sobre o tema o resultado da análise no contexto atual da empresa.

Vale ressaltar que todo tratamento de dados pessoais deve sempre atender aos dez princípios descritos na lei e explicados na imagem a seguir.

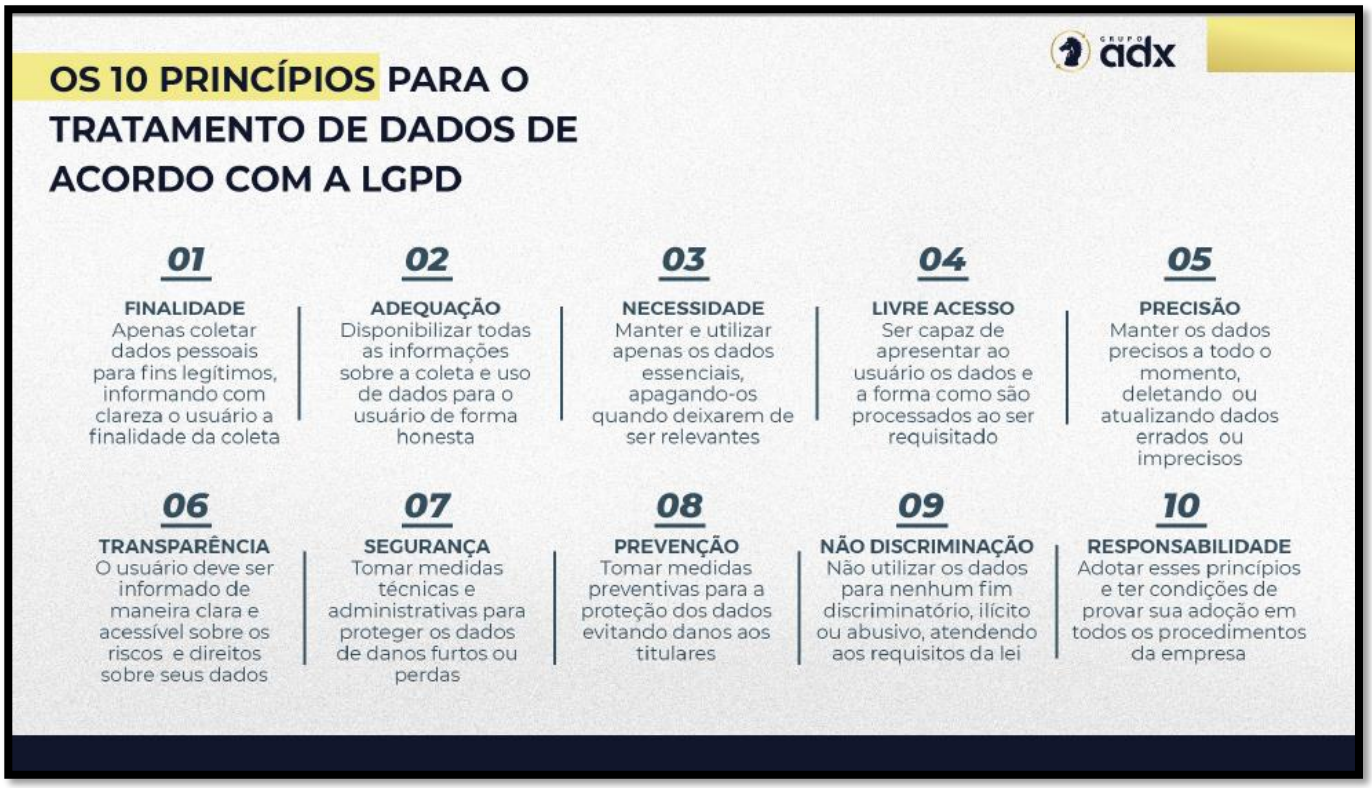



*Figure 8 - Princípios da LGPD.*

10.1 – Transferência internacional de dados

A LGPD trouxe uma redação específica para a transferência internacional de dados pessoais. Na mesma linha das previsões sobre tratamentos de dados pessoais e dados pessoais sensíveis, conforme artigos 7º e 11, respectivamente, a LGPD listou as bases legais da transferência internacional de dados pessoais no artigo 33, a saber:

- Países ou organismos internacionais destinatários com grau de proteção de dados pessoais adequado ao previsto na LGPD (a ser avaliado pela autoridade nacional);
- Mediante o oferecimento e a comprovação de garantias, pelo controlador, de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD (na forma de cláusulas contratuais específicas e padrão; normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos – cuja análise será realizada pela autoridade nacional);

- Se necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

- Se necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros;

- Mediante autorização pela autoridade nacional;

- Se resultante de compromisso assumido em acordo de cooperação internacional;

- Se necessária para a execução de política pública ou atribuição legal do serviço público (assegurada a publicidade nos termos do artigo 23, inciso I da LGPD);

- Mediante consentimento específico e destacado do titular do dado pessoal, com informação prévia sobre o caráter internacional da operação e com finalidade distinta de qualquer outra eventualmente existente; e

- Se necessária para cumprimento de obrigação legal ou regulatória pelo controlador, para a execução de contrato ou de procedimentos preliminares contratuais, ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral (vide artigo 7º, incisos II, V e VI da LGPD).


*Figure 9 - Transferência Internacional de dados.*

Ao final do mapeamento de todos os processos de negócio da empresa que fazem transferência internacional de dados, chegamos ao resultado visto a seguir:

| **Nome dos processos que fazem transferência internacional de dados** |
|---|
| TEC 04 – Realizar licenciamento no Zebra |
| TEC 03 – Gerenciar chamados |
| TEC 06 – Criar e-mail para novo colaborador |
| ADM 03 – Realizar Admissão |
| TEC 01 – Atender chamado |
| ADM 02 - Gerenciar exames periódicos |
| FIN 01 – Gerenciar recebimento de contratos |
| ADM 01 - Atender solicitações de clientes |
| FIN 03 – Elaborar relatório de espelho do ponto |
| FIN 02 – Realizar pagamentos para os funcionários |
| ADM 05 – Cadastrar colaborador em benefícios |
| DIR 01 – Elaborar contrato |
| TEC 05 – Cadastrar cliente nos portais de soluções Cloud |
| TEC 02 – Coletar assinatura da NF no Notas Ytech |

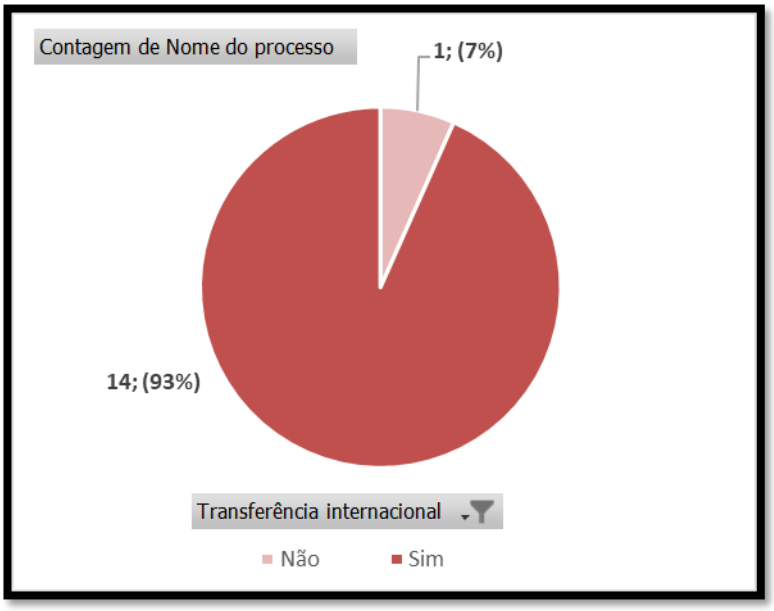



*Figure 10 - Processos que fazem internacionalização de dados.*

10.2 – Tratamento de dados de crianças e adolescentes

O tratamento de dados de crianças e adolescentes deverá ser realizado (i) no melhor interesse da criança ou adolescente (art. 14, caput), (ii) mediante o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (art. 14, §1º) e (iii) de acordo com a obrigação que os controladores têm de manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos Ciente da importância cada vez maior da internet na vida das crianças e dos adolescentes. O § 5º prevê que "O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis." Trata-se de mais um dispositivo em que a LGPD impõe aos controladores o devido dever de cuidado, a ser analisado no contexto das tecnologias disponíveis e dos meios razoáveis para tal. direitos do titular (art. 14, § 2º).

As únicas exceções ao consentimento são (i) quando a coleta dos dados for necessária para contatar os pais ou o responsável legal e, mesmo nessa hipótese, os dados devem ser utilizados uma única vez e sem armazenamento, e (ii) para a proteção da criança ou adolescente, sendo que, em qualquer caso, os dados não podem ser repassados a

terceiros sem o consentimento de pelo menos um dos pais ou do responsável legal (art. 14, § 3º, LGPD).

Outro ponto importante é o § 4º, segundo o qual “Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.”

Neste sentido, dos processos mapeados no diagnóstico realizado no Ytech, **1** (7**%)** tratam dados pessoais de crianças e adolescentes. O que requer uma atenção especial na definição dos processos de controle contra vazamento de dados.

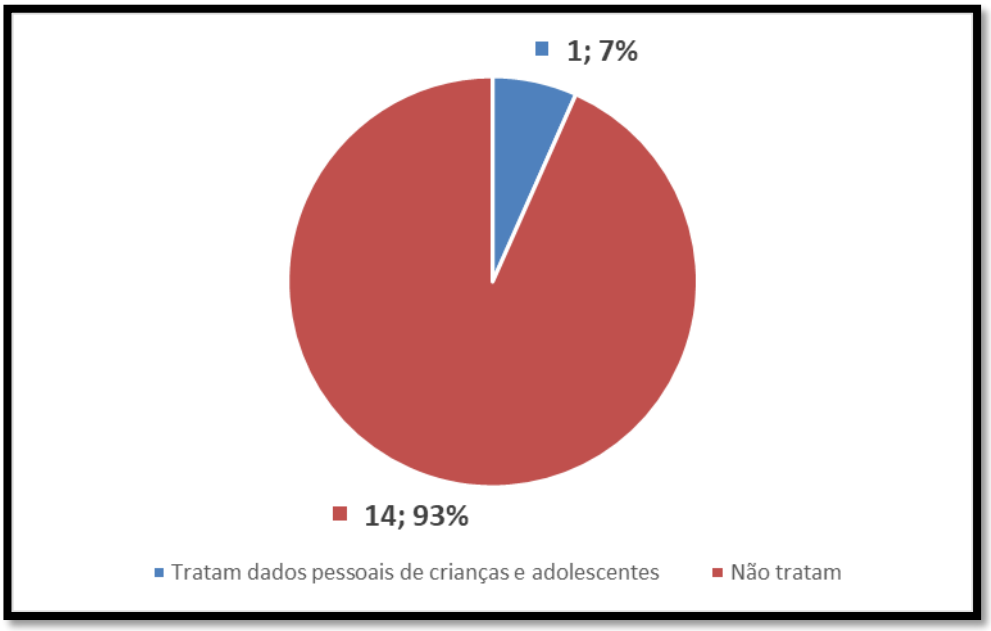



*Figura 12 - Processos que tratam dados de menores.*

10.3 – Atendimento aos direitos dos titulares de dados

A LGPD assegurou 10 direitos aos titulares dos dados pessoais e os controladores desses dados precisam estar prontos para cumprimento dessa obrigação. Como esse requisito não existia, novos processos de negócio precisarão ser criados para garantir o

perfeito funcionamento dessa solicitação, livrando a empresa de futuras sanções. Para o melhor controle dos processos, será necessário usar alguma ferramenta para apoio tecnológico como interface para os titulares de dados.


*Figure 11 - Direitos dos Titulares de dados.*

10.4 – Relatório de impacto à proteção dos dados pessoais

O relatório de impacto à proteção de dados pessoais (RIPD), também conhecido como DPIA – Data Protection Impact Assessment, é definido como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais. Ele também apresenta as medidas, salvaguardas e mecanismos de mitigação de riscos, conforme o artigo 5º, inciso XVII da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). A análise de impacto de todos os processos críticos foi realizada na auditoria de segurança e a partir de agora será preciso definir um modelo para esse documento, bem como quais processos precisam ter esse modelo preenchido para futuras solicitações da ANPD.

10.5 – Processo de tratamento de incidentes de segurança e privacidade de dados

A LGPD exige que as empresas gerenciem de forma completa os incidentes de segurança e privacidade ocorridos para prestação de contas aos titulares e para a ANPD. Um incidente é sempre gerado pela exploração de alguma vulnerabilidade existente nos ativos organizacionais. A figura a seguir descreve esse fluxo.

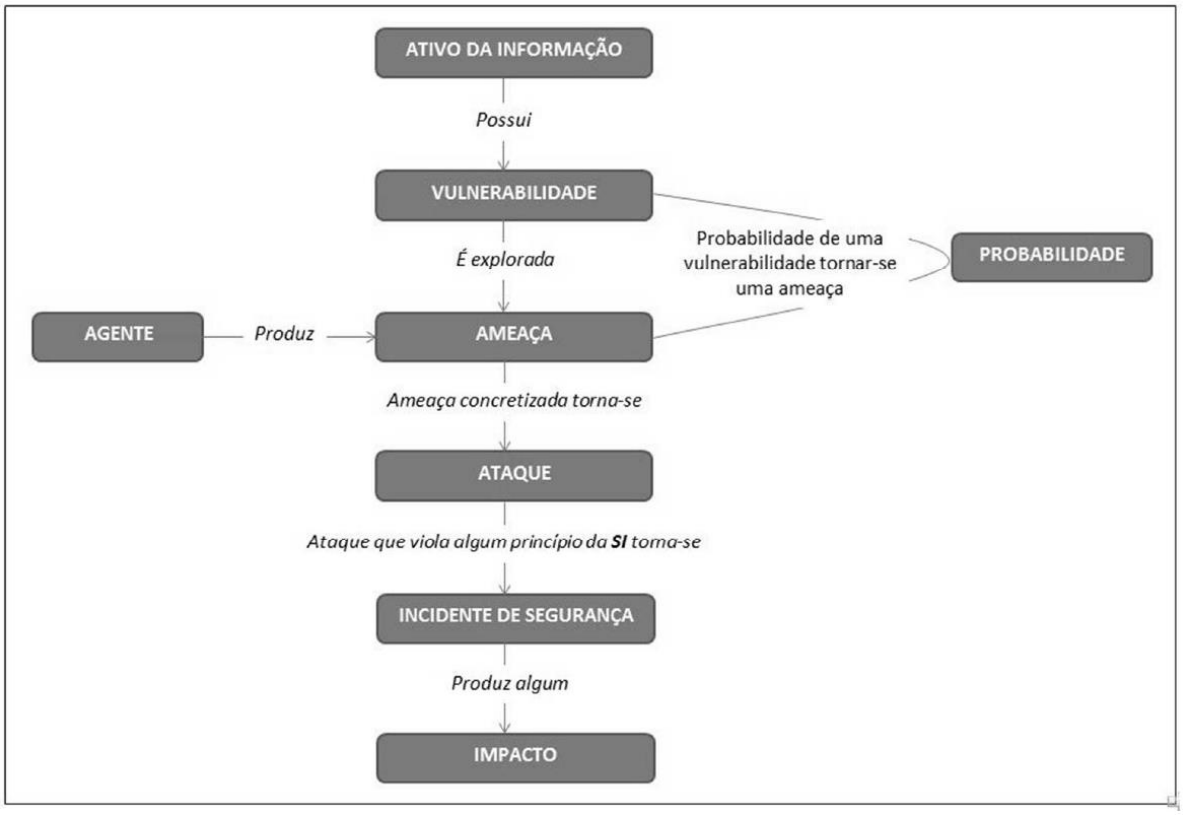



*Figure 12 - Fluxo de um incidente de segurança da informação.*

É importante diferenciar uma violação de segurança de uma violação de privacidade. A figura a seguir mostra que a violação de dados pode ou não acontecer quando uma violação de segurança ocorre. No exemplo dado, se o pen drive ou laptop perdido tiver os dados criptografados, não será categorizada uma violação de dados.

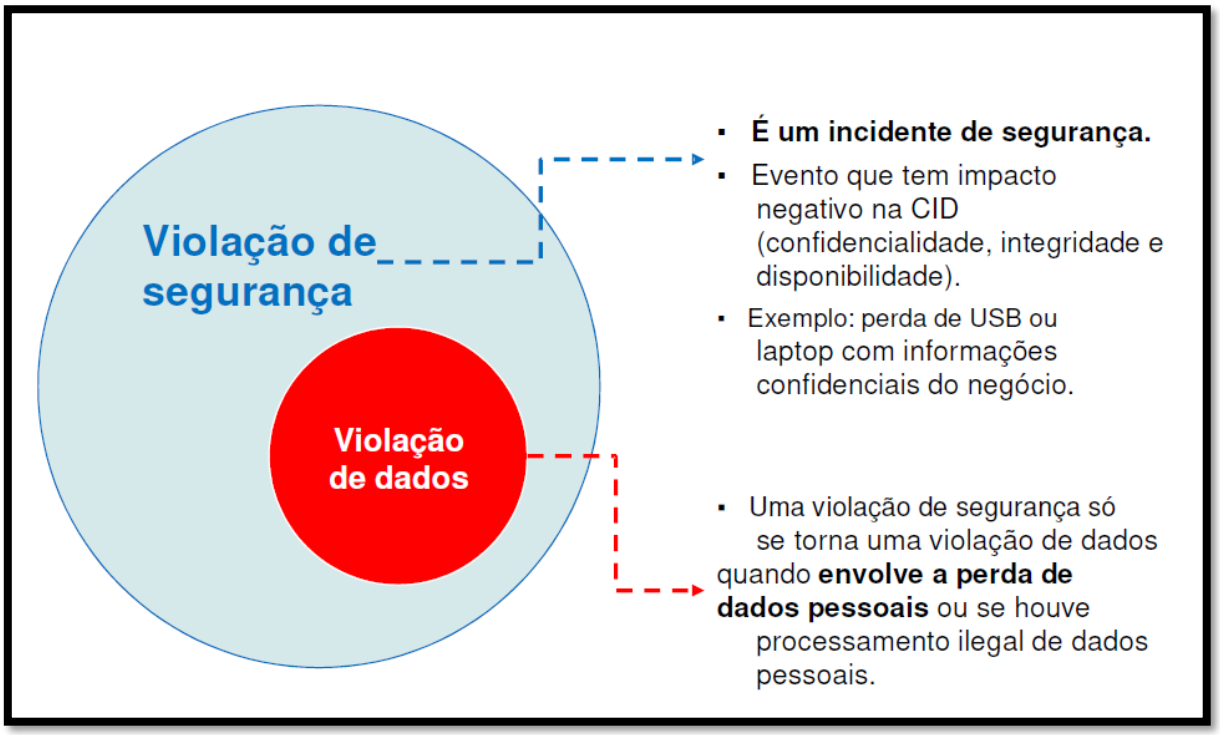



*Figure 13 - Violação de segurança X Violação de dados.*

No texto da lei, a previsão legal para a resposta a incidentes de segurança vem no capítulo VII, justamente o que trata da segurança da informação e das boas práticas a serem adotadas para tanto. Em seu artigo 48, consta:

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

- § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
- I - a descrição da natureza dos dados pessoais afetados;
- II - as informações sobre os titulares envolvidos;
- III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente;
- V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Dessa forma, será extremamente importante a criação de um processo para gerenciamento de todos os incidentes, bem como para o registro das deliberações realizadas pelo comitê de privacidade e pelo DPO. Para potencializar esse processo, recomenda-se que seja usado um software especialista nessa função. Esse software deve catalogar cada registro de incidentes ocorridos dentro da empresa. O registro de incidente normalmente contempla os seguintes dados:

• Quando ocorreu o incidente;

• Quais dados foram afetados;

• Quais e quantos titulares foram afetados;

• Quais as causas do incidente;

• Quais seus efeitos e consequências;

• Qual o plano para mitigação desses efeitos e suas respectivas consequências;

• Uma linha do tempo do incidente, incluindo quando houve o primeiro alerta quanto ao incidente e quando de fato foi determinado que o mesmo ocorreu;

• As decisões relativas à notificação.

Após a análise do incidente pela equipe de segurança, comitê e DPO, as seguintes informações devem ser registradas para determinação do plano ação.

• O tipo do incidente/vazamento;

• O tipo de dados pessoais afetados;

• A sensibilidade dos dados afetados;

• O volume de dados afetados;

• O número de titulares atingidos;

• A natureza do processamento;

• A facilidade ou não de identificação dos titulares (se por exemplo, os dados estavam criptografados ou anonimizados, o risco reduz);

• A gravidade das consequências para os titulares;

• A extensão das consequências para os titulares;

• Se houve menores entre os titulares;

• Caso haja uma falha de confidencialidade, quais as possíveis intenções de quem perpetrou o ataque que gerou o incidente.

10.6 – Bases legais para tratamento dos dados

A LGPD definiu dez bases legais para tratamento de dados pessoais. Isso significa que todos os dados pessoais manipulados pela empresa devem pertencer a pelo menos uma dessas categorias. Se não for possível o enquadramento, o dado não deve ser tratado e deve ser excluído, caso esteja armazenado em poder da empresa.

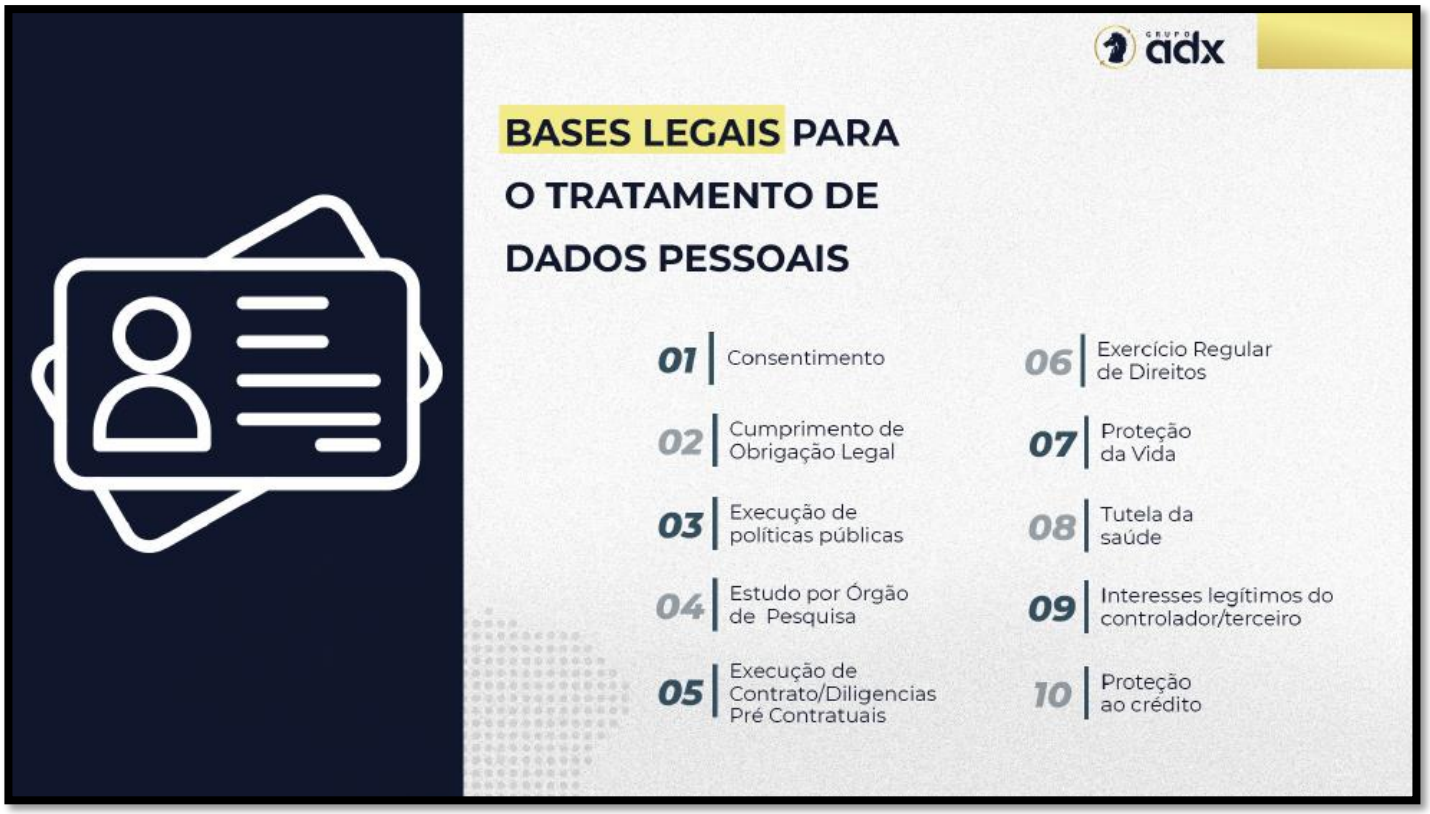



*Figure 14 - Bases Legais para tratamento de dados.*

Depois de uma análise minuciosa em todos os processos que tratam dados pessoais, foi definida a base legal que concede o direito do tratamento pela Ytech. A documentação geral será entregue no **Anexo II** desse documento e um resumo das bases usadas em cada processo podem ser vistas na figura a seguir.

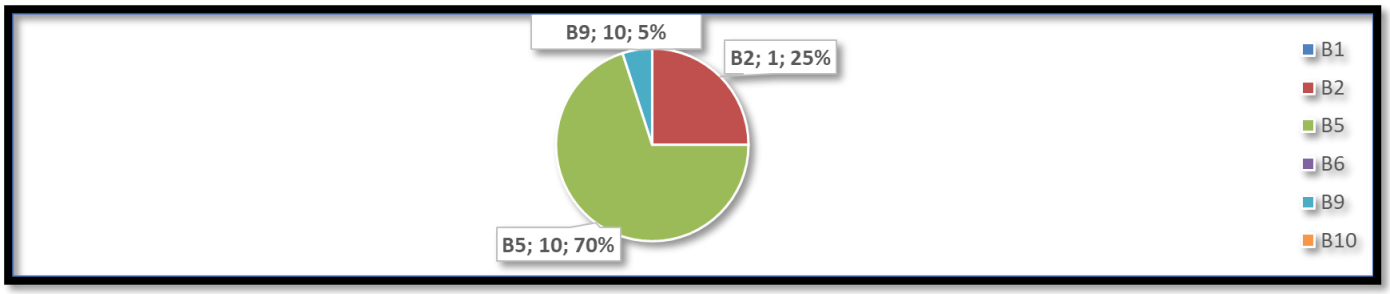



*Figure 15 - Percentual de processos por Base Legal.*

*Quadro 1 - Lista de processos por Base Legal.*

| Bases legais | Processos |
|---|---|
| B1 | |
| B2 | ADM 03 – Realizar Admissão;<br>ADM 02 - Gerenciar exames periódicos;<br>FIN 03 – Elaborar relatório de espelho do ponto;<br>FIN 02 – Realizar pagamentos para os funcionários;<br>TEC 02 – Coletar assinatura da NF no Notas Ytech |
| B3 | |
| B4 | |
| B5 | TEC 04 – Realizar licenciamento no Zebra;<br>TEC 03 – Gerenciar chamados;<br>TEC 06 – Criar e-mail para novo colaborador;<br>ADM 03 – Realizar Admissão;<br>TEC 01 – Atender chamado;<br>FIN 01 – Gerenciar recebimento de contratos;<br>ADM 01 - Atender solicitações de clientes;<br>FIN 03 – Elaborar relatório de espelho do ponto;<br>FIN 02 – Realizar pagamentos para os funcionários;<br>ADM 04 – Coletar assinatura do colaborador em termo de responsabilidade;<br>ADM 05 – Cadastrar colaborador em benefícios;<br>DIR 01 – Elaborar contrato;<br>TEC 05 – Cadastrar cliente nos portais de soluções Cloud;<br>TEC 02 – Coletar assinatura da NF no Notas Ytech |
| B6 | |
| B7 | |
| B8 | |
| B9 | TEC 03 – Gerenciar chamados |
| B10 | |

Portanto, conforme estabelece o caput e inciso IX do artigo 7° da LGPD:

“Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

(...)

IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;”

Além disso, o artigo 10 da LGPD estabelece que o controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas. Elas incluem, mas não se limitam a:

“I – apoio e promoção de atividades do controlador; e

II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.”

Para os processos que usam a base B9 (Legítimo interesse) é extremamente importante a realização da avaliação de legítimo interesse (LIA) com teste de balanceamento.

A responsabilidade adicional ao agente de tratamento decorrente da utilização dessa base legal é inerente, portanto conduzir uma avaliação como um LIA pode ajudar bastante a decidir pelo legítimo interesse.

Um LIA basicamente coloca de forma estruturada e documentada o teste em quatro partes que se recomenda ao avaliar a adequação do interesse legítimo. Os detalhes estão na figura a seguir.

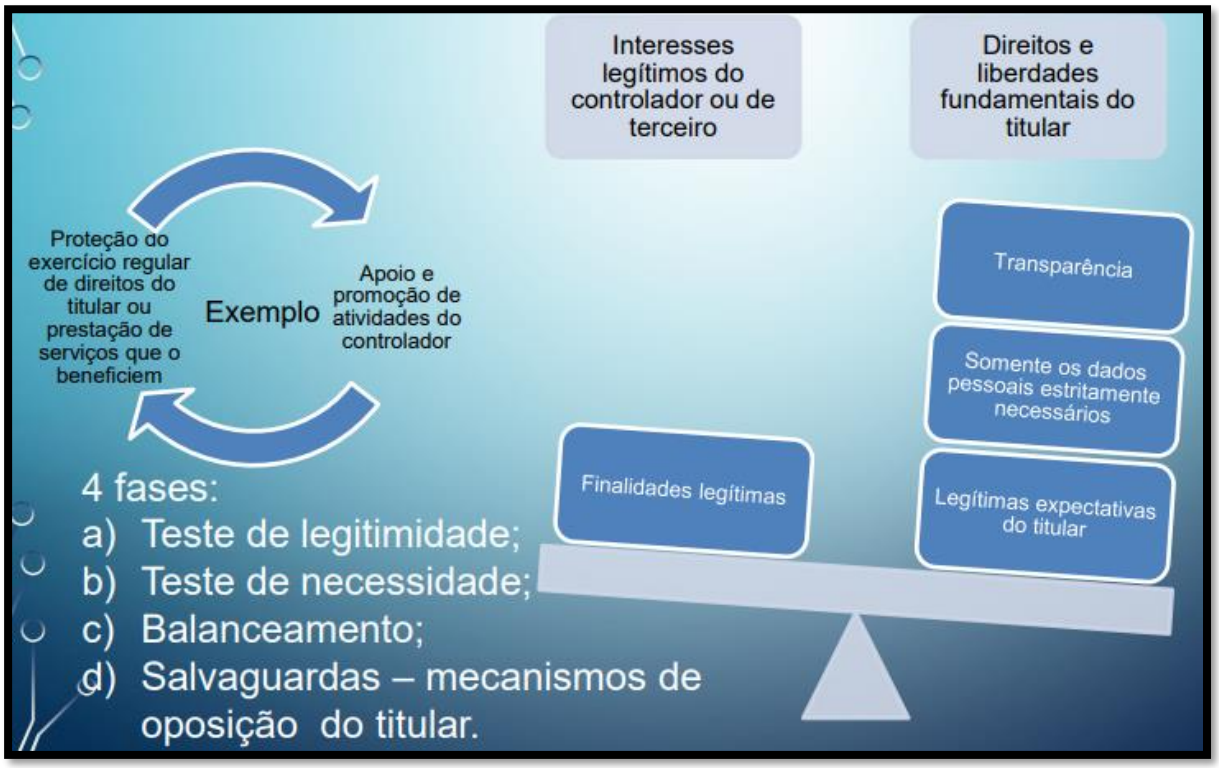



*Figure 16 - Avaliação de legítimo interesse.*

10.7 – Dados sensíveis

Um dado sensível contém informações que ninguém gostaria que fossem compartilhadas e que podem causar uma grande exposição tanto na vida social quanto profissional do cidadão.

Essa preocupação com os dados sensíveis advém do fenômeno da publicidade comportamental, utilizada para formação de perfis das pessoas. Os dados sensíveis possibilitam conclusões a respeito de um indivíduo, como por exemplo, a sua orientação sexual, sua religião, alguma doença que possa ter e com essas informações, torna-se muito perigoso que as pessoas venham a ser classificadas de forma preconceituosa, interferindo diretamente em seus direitos e liberdades individuais. A figura a seguir lista as categorias de dados sensíveis.


*Figure 17 - Dados Pessoais Sensíveis.*

Os dados pessoais sensíveis são regulados pelos artigos 11 a 13 da LGPD. A lei os define no art. 5º, inciso II (1). É o 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.

Estas sete categorias de informação são especialmente protegidas pela lei, em busca do atendimento, principalmente, do Princípio da Não-Discriminação. O art. 11 da LGPD define as hipóteses exclusivas que permitem o tratamento desse tipo de dado.

A primeira hipótese é dada pelo consentimento do titular. Esse consentimento, além de seguir as regras gerais do art. 8º, exige forma destacada a respeito dos dados sensíveis, além de mencionar a finalidade específica. Seguem valendo as regras de Boa-fé, Finalidade, vícios de consentimento, entre outras.

No entanto, o processamento de dados sensíveis poderá ser feito sem o consentimento do titular em sete hipóteses:

- Cumprimento de obrigação legal ou regulatória pelo controlador.
- Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.
- Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis.
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem).
- Proteção da vida ou da incolumidade física do titular ou de terceiros.
- Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.
- Garantia da prevenção à fraude e à segurança do titular.

Foi avaliado que **47%** dos processos da Ytech tratam dados pessoais sensíveis. O gráfico a seguir descreve essa situação por setor.

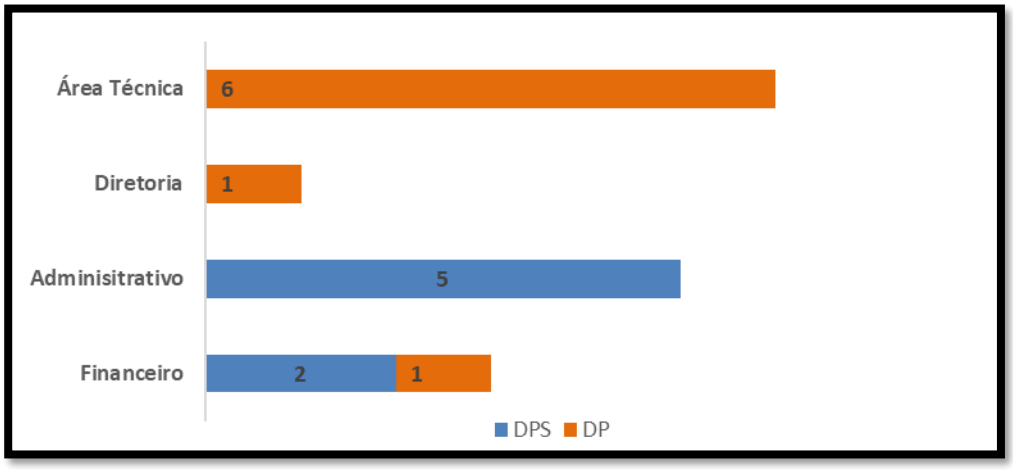



*Figure 18 - Processos que tratam dados sensíveis.*

# 11 – Gerenciamento de riscos

Riscos são eventos ou condições incertas que, se ocorrerem, geram efeitos positivos ou negativos sobre o negócio. No caso específico de efeitos negativos, existem sanções previstas na lei e descritas na área em vermelho da imagem a seguir. É importante também ressaltar que a imagem mostra o que será levado em consideração no momento da definição da sanção pela autoridade nacional de proteção de dados.


*Figure 19 - Sanções da LGPD.*

Para cada risco identificado é adotada uma estratégia de tratamento e resposta. As estratégias possíveis de respostas às ameaças e/ou oportunidades são:

- **Aceitar:** Não fazer nada previamente. Os riscos se enquadram nos critérios de aceitação e ficam em observação, sem ação pré-definida. Pode envolver criar um plano de contingência, para o caso de o risco ocorrer (Aceitação ativa);
- **Eliminar:** Eliminar a ameaça destruindo a sua causa. Esse é o critério a ser utilizado para riscos não toleráveis pela organização.
- **Mitigar:** Minimizar os impactos negativos e a probabilidade de o risco ocorrer, reduzindo sua criticidade e tornando-o um risco menor.
- **Transferir:** Tornar outra parte responsável pelo risco, como por exemplo, contratando seguros ou terceirizando trabalhos.
- **Explorar:** Em caso de oportunidades (riscos positivos) determinar ações para maximizar as possibilidades de um risco ocorrer e otimizar seu impacto caso ele ocorra.

Os riscos identificados possuem um atributo chamado de criticidade do risco. A criticidade é o resultado da multiplicação de probabilidade x impacto. O resultado dessa operação possui valores possíveis de 1 a 9. Dessa forma os riscos se enquadram de acordo com a matriz a seguir:

| Probabilidade | Valor |
|---|---|
| Baixa | 1 |
| Média | 2 |
| Alta | 3 |

| Impacto | Valor |
|---|---|
| Baixo | 1 |
| Médio | 2 |
| Alto | 3 |

*Figure 20 - Probabilidade X Impacto dos riscos.*

Foi definido que os riscos de exposição inferior a 3 possuem exposição baixa, entre 4 e 6 possuem exposição média e acima de 6 exposição alta. Os riscos serão classificados por prioridade e impacto, de acordo com o gráfico a seguir.

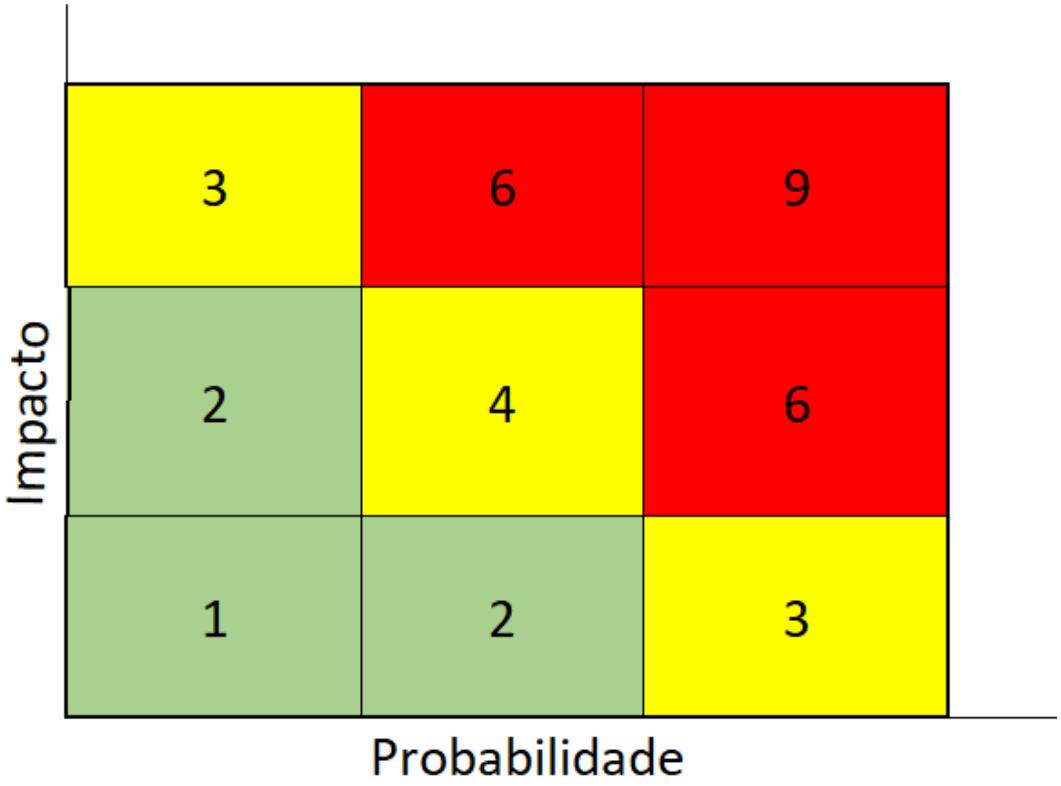



*Figure 21 - Matriz de avaliação de riscos.*

Após a realização da análise de riscos em todos os processos mapeados e definição de seus respectivos controles de segurança da informação ou jurídicos, para adequação à LGPD, foi gerado o gráfico a seguir como resumo das informações de cada setor.

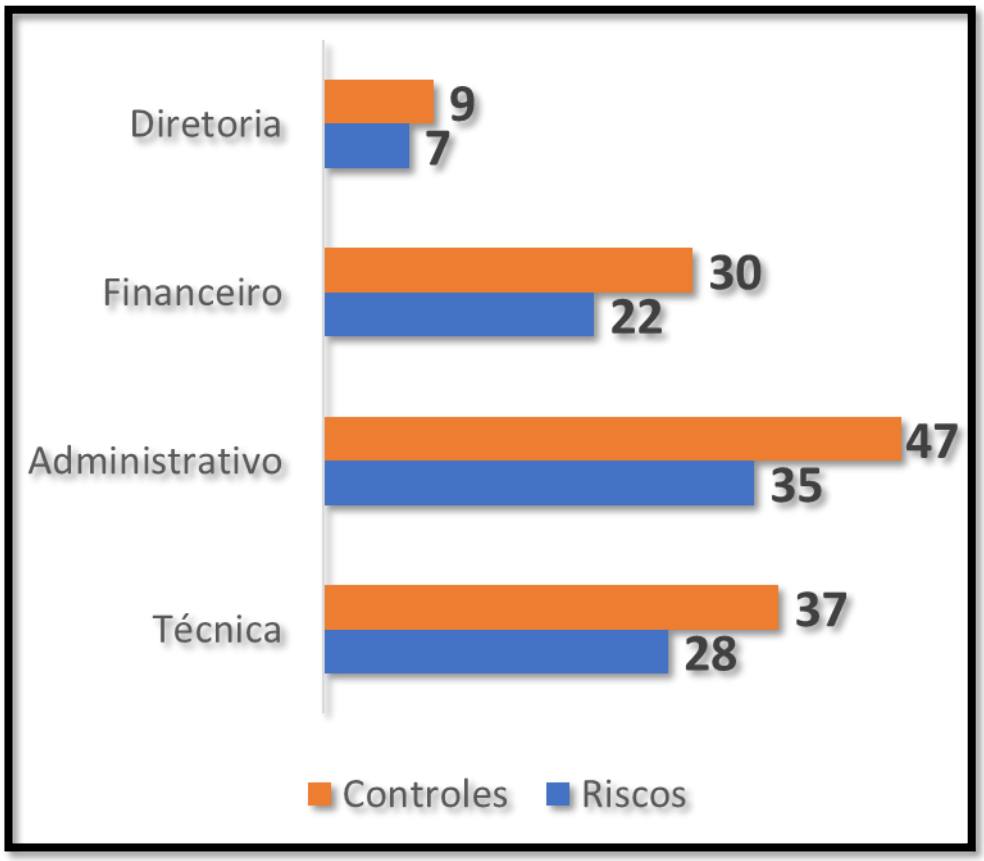



*Figura 48 - Nº de riscos e controles por setor.*

A tabela a seguir agrupa os processos de acordo com cada faixa de criticidade definidas no plano de gerenciamento de riscos.

| **Criticidade 6** |
|---|
| ADM 03 – Realizar Admissão |
| ADM 02 - Gerenciar exames periódicos |
| ADM 05 – Cadastrar colaborador em benefícios |
| **Criticidade 3** |
| ADM 01 - Atender solicitações de clientes |
| **Criticidade 2** |
| TEC 03 – Gerenciar chamados |
| TEC 01 – Atender chamado |
| FIN 01 – Gerenciar recebimento de contratos |
| FIN 03 – Elaborar relatório de espelho do ponto |

| |
|---|
| FIN 02 – Realizar pagamentos para os funcionários |
| DIR 01 – Elaborar contrato |
| **Criticidade 1** |
| TEC 04 – Realizar licenciamento no Zebra |
| TEC 06 – Criar e-mail para novo colaborador |
| ADM 04 – Coletar assinatura do colaborador em termo de responsabilidade |
| TEC 05 – Cadastrar cliente nos portais de soluções Cloud |
| TEC 02 – Coletar assinatura da NF no Notas Ytech |

*Tabela 18 - Processos por criticidade.*

O plano de gerenciamento dos riscos foi elaborado tendo como base a análise do ambiente e suas necessidades. Para cada risco levantado e priorizado foram calculados a categoria, probabilidade, impacto e exposição. Em seguida foram definidas as medidas preventivas e/ou de contingência. A tabela a seguir descreve cada item avaliado no plano de gerenciamento de riscos:

| ITEM | DESCRIÇÃO |
|---|---|
| **ID** | Identificador do processo. |
| **Setor** | Setor responsável pelo processo. |
| **Processo** | Nome do processo. |
| **Riscos** | Descritivo dos riscos. |
| **Probabilidade** | Probabilidade estimada de um risco ocorrer. |
| **Impacto** | Impacto estimado se um risco ocorrer. |
| **Criticidade** | Probabilidade multiplicada pelo Impacto. |
| **Estratégia** | Atitude a ser tomada em relação ao risco. |
| **Controles de segurança** | Controles aplicados para garantir a estratégia de tratamento do risco. |

*Tabela 19 – Informações do plano de gestão de riscos.*

Segue abaixo a tabela com os riscos e o respectivo plano de tratamento:

| Nome do processo | Risco | Controle | Resposta ao risco | Probabilidade | Impacto | Criticidade |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| TEC 04 – Realizar licenciamento no Zebra | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Descumprimento de obrigações legais pelo operador Google (e-mail); Descumprimento de obrigações legais pelo operador Zebra Technologies | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Zebra Technologies referente ao tratamento de dados pessoais [Jurídico] | Mitigar | 2 | 3 | 6 |

| | | | | | | |
|---|---|---|---|---|---|---|
| TEC 03 – Gerenciar chamados | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Descumprimento de obrigações legais pelo operador Google (e-mail); Não há rotina ou processo para o descarte de dados após conclusão da finalidade de tratamento; Descumprimento de obrigações legais pelo operador AUVO | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Criar rotina de descarte | Mitigar | 3 | 3 | 9 |
| TEC 06 – Criar e-mail para novo colaborador | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Descumprimento de obrigações legais pelo operador Google (e-mail) | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico] | Mitigar | 2 | 2 | 4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| ADM 03 – Realizar Admissão | Falta de transparência ao colaborador; Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Perda definitiva de dados pessoais devido ao armazenamento apenas na máquina; Descumprimento de obrigações legais pelo operador GR Protection; Descumprimento de obrigações legais pelo operador ASSESCOM; Descumprimento de obrigações legais pelo operador Google (e-mail); Descumprimento de obrigações legais pelo operador Whatsapp; Retenção excessiva de documentos; Acesso indevido às informações físicas no setor | Comunicar formalmente aos colaboradores, no onboarding, sobre o compartilhamento com clientes. [Organizacional]; Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Definir repositório central oficial para armazenamento de documentos. [Organizacional]; Revisão do contrato ou notificação dos operador GR Protection referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador ASSESCOM referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Whatsapp referente ao tratamento de dados pessoais [Jurídico]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Criar rotina de descarte periódico de documentos antigos | Mitigar | 3 | 3 | 9 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | [Organizacional]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional] | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| TEC 01 – Atender chamado | Vazamento por intermédio do funcionário ; Não há rotina ou processo para o descarte de dados após conclusão da finalidade de tratamento; Descumprimento de obrigações legais pelo operador AUVO | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Criar rotina de revisão e descarte de termos antigos. [Organizacional]; Revisão do contrato ou notificação dos operador AUVO referente ao tratamento de dados pessoais [Jurídico] | Mitigar | 2 | 2 | 4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| ADM 02 - Gerenciar exames periódicos | Vazamento por intermédio do funcionário ; Perda definitiva de dados pessoais devido ao armazenamento apenas na máquina; Descumprimento de obrigações legais pelo operador GR Protection; Descumprimento de obrigações legais pelo operador ASSESCOM; Descumprimento de obrigações legais pelo operador Google (e-mail); Retenção excessiva de documentos; Acesso indevido aos exames médicos; Compartilhamento indevido com terceiros (contabilidade); Acesso indevido às informações físicas no setor | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Definir repositório central oficial para armazenamento de documentos. [Organizacional]; Revisão do contrato ou notificação dos operador GR Protection referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador ASSESCOM referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Criar rotina de descarte periódico de documentos antigos [Organizacional]; Armazenar ASO em repositório seguro, com controle de acesso. [Segurança da Informação]; Enviar à contabilidade apenas documentos estritamente necessários (sem laudos). [Organizacional]; Redigir ou mascarar informações sensíveis antes do envio. [Segurança da Informação]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional] | Mitigar | 3 | 3 | 9 |

| | | | | | | |
|---|---|---|---|---|---|---|
| FIN 01 – Gerenciar recebimento de contratos | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Descumprimento de obrigações legais pelo operador Google (e-mail); Descumprimento de obrigações legais pelo operador Whatsapp; Não há rotina ou processo para o descarte de dados após conclusão da finalidade de tratamento; Descumprimento de obrigações legais pelo operador CyberSul; Armazenamento de documentos descentralizado | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Whatsapp referente ao tratamento de dados pessoais [Jurídico]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Criar rotina de revisão e descarte de termos antigos. [Organizacional]; Revisão do contrato ou notificação dos operador CyberSul referente ao tratamento de dados pessoais [Jurídico]; Centralizar contratos e NFs em repositório único corporativo [Organizacional]; Restringir acesso aos contratos apenas a perfis autorizados [Organizacional]; Proibir envio de documentos contratuais por WhatsApp [Organizacional] | Mitigar | 2 | 3 | 6 |

| | | | | | | |
|---|---|---|---|---|---|---|
| ADM 01 - Atender solicitações de clientes | Vazamento de dados por envio de documentos sem proteção; Falta de transparência ao colaborador; Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Perda definitiva de dados pessoais devido ao armazenamento apenas na máquina | Utilizar pasta centralizada com controle de acesso para armazenamento de documentos. [Segurança da Informação]; Utilizar links com prazo de expiração para compartilhamento de documentos. [Segurança da Informação]; Comunicar formalmente aos colaboradores, no onboarding, sobre o compartilhamento com clientes. [Organizacional]; Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Definir repositório central oficial para armazenamento de documentos. [Organizacional] | Mitigar | 2 | 3 | 6 |
| FIN 03 – Elaborar relatório de espelho do ponto | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Perda definitiva de dados pessoais devido ao armazenamento apenas na máquina; Descumprimento de obrigações legais pelo operador Google (e-mail); Acesso indevido às informações físicas no setor; Não há rotina ou processo para o descarte de dados após conclusão da | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Definir repositório central oficial para armazenamento de | Mitigar | 2 | 3 | 6 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | finalidade de tratamento; Descumprimento de obrigações legais pelo operador SIMIX | documentos. [Organizacional]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Criar rotina de revisão e descarte de termos antigos. [Organizacional]; Revisão do contrato ou notificação dos operador SIMIX referente ao tratamento de dados pessoais [Jurídico] | | | | |
| FIN 02 – Realizar pagamentos para os funcionários | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Descumprimento de obrigações legais pelo operador ASSESCOM; Descumprimento de obrigações legais pelo operador Google (e-mail); Descumprimento de obrigações legais pelo operador Whatsapp; Não há rotina ou processo para o descarte de dados após conclusão da finalidade de tratamento; Armazenamento de documentos descentralizado; Descumprimento de obrigações legais pelo operador Banco Bradesco | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Revisão do contrato ou notificação dos operador ASSESCOM referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Whatsapp referente ao tratamento de dados pessoais [Jurídico]; Criar rotina de descarte periódico de documentos | Mitigar | 3 | 3 | 9 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | antigos [Organizacional]; Criar rotina de revisão e descarte de termos antigos. [Organizacional]; Definir repositório central oficial para armazenamento de documentos. [Organizacional]; Revisão do contrato ou notificação dos operador Banco Bradesco referente ao tratamento de dados pessoais [Jurídico] | | | | |
| ADM 04 – Coletar assinatura do colaborador em termo de responsabilidade | Vazamento por intermédio do funcionário ; Retenção excessiva de documentos; Extravio do termo físico; Acesso indevido às informações físicas no setor | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Digitalizar os termos e armazenar cópia em repositório seguro. [Segurança da Informação]; Criar rotina de revisão e descarte de termos antigos. [Organizacional]; Controlar acesso ao | Mitigar | 2 | 2 | 4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | local de armazenamento de documentos físicos [Organizacional] | | | | |
| ADM 05 – Cadastrar colaborador em benefícios | Falta de transparência ao colaborador; Acesso indevido às informações dos e-mails; Perda definitiva de dados pessoais devido ao armazenamento apenas na máquina; Descumprimento de obrigações legais pelo operador Unimed; Descumprimento de obrigações legais pelo operador Pluxee; Retenção indefinida de dados de benefícios; Acesso indevido às informações físicas no setor | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Definir repositório central oficial para armazenamento de documentos. [Organizacional]; Revisão do contrato ou notificação dos operador Unimed referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Pluxee referente ao tratamento de dados pessoais [Jurídico]; Criar rotina de revisão e descarte de termos antigos. [Organizacional]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional] | Mitigar | 2 | 3 | 6 |

| | | | | | | |
|---|---|---|---|---|---|---|
| DIR 01 – Elaborar contrato | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Perda definitiva de dados pessoais devido ao armazenamento apenas na máquina; Descumprimento de obrigações legais pelo operador Google (e-mail); Descumprimento de obrigações legais pelo operador Whatsapp; Descumprimento de obrigações legais pelo operador D4Sign; Não há rotina ou processo para o descarte de dados após conclusão da finalidade de tratamento | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Definir repositório central oficial para armazenamento de documentos. [Organizacional]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Whatsapp referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador D4Sign referente ao tratamento de dados pessoais [Jurídico]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Criar rotina de descarte periódico de documentos antigos [Organizacional] | Mitigar | 2 | 3 | 6 |

| | | | | | | |
|---|---|---|---|---|---|---|
| TEC 05 – Cadastrar cliente nos portais de soluções Cloud | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Descumprimento de obrigações legais pelo operador Google (e-mail); Descumprimento de obrigações legais pelo operador Whatsapp; Descumprimento de obrigações legais pelo operador Extreme Cloud IQ; Descumprimento de obrigações legais pelo operador URMOBO; Recebimento via WhatsApp | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Whatsapp referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador Extreme Cloud IQ referente ao tratamento de dados pessoais [Jurídico]; Revisão do contrato ou notificação dos operador URMOBO referente ao tratamento de dados pessoais [Jurídico]; Proibir envio de dados de acesso por WhatsApp. [Organizacional] | Mitigar | 2 | 3 | 6 |

| | | | | | | |
|---|---|---|---|---|---|---|
| TEC 02 – Coletar assinatura da NF no Notas Ytech | Vazamento por intermédio do funcionário ; Acesso indevido às informações dos e-mails; Descumprimento de obrigações legais pelo operador Google (e-mail); Não há rotina ou processo para o descarte de dados após conclusão da finalidade de tratamento; Descumprimento de obrigações legais pelo operador Google Drive; Armazenamento duplicado (celular e Drive) | Capacitar os colaboradores em segurança da informação e privacidade [Segurança da Informação]; Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo [Jurídico]; Revisar a política de atualização de senhas dos e-mails [Segurança da Informação]; Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais [Jurídico]; Definir prazos legais de retenção por tipo de documento [Jurídico]; Criar rotina de descarte periódico de documentos antigos [Organizacional]; Revisão do contrato ou notificação dos operador Google Drive referente ao tratamento de dados pessoais [Jurídico]; Definir repositório oficial único para arquivamento fiscal (Google Drive) [Organizacional] | Mitigar | 2 | 2 | 4 |

# 12 – Plano de ações

O tratamento dos riscos foi totalmente elaborado em forma de planos de ações, deixando claro como será a sua execução, o responsável e o prazo de conclusão.

Os planos de ações têm o objetivo de descrever todas as ações e projetos que devem ser executados para a completa adequação à LGPD.

Os planos de ações sugeridos surgiram através dos controles estabelecidos, o número total de controles sugeridos para os processos foi de 833, sendo resumido pelas 73 ações da planilha do plano de ações. A figura a seguir mostra a divisão entre controles de segurança da informação, organizacionais e para adequação jurídica.

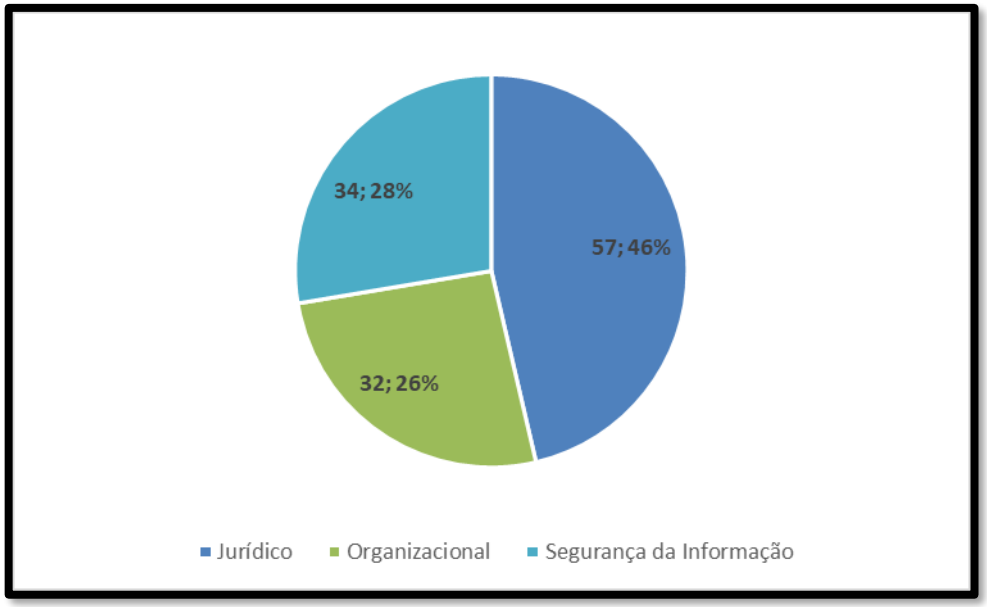



*Figure 22 - Controles por tipo.*

Para facilitar o trabalho de alocação dos responsáveis por cada plano de ação, a ADX fez uma sugestão a ser aprovada pelo cliente na tabela a seguir.

| N° | Controles | Tipo | Processos | Responsável | Quando |
|---|---|---|---|---|---|
| **1** | Utilizar pasta centralizada com controle de acesso para armazenamento de documentos. | Segurança da Informação | ADM 01 - Atender solicitações de clientes | Ytech | Q3/2026 |
| **2** | Utilizar links com prazo de expiração para compartilhamento de documentos. | Segurança da Informação | ADM 01 - Atender solicitações de clientes | Ytech | Q2/2026 |

| | | | | | |
|---|---|---|---|---|---|
| **3** | Comunicar formalmente aos colaboradores, no onboarding, sobre o compartilhamento com clientes. | Organizacional | ADM 03 – Realizar Admissão;<br>ADM 01 - Atender solicitações de clientes | Ytech | Q3/2026 |
| **4** | Capacitar os colaboradores em segurança da informação e privacidade | Segurança da Informação | Todos os processos | ADX | Q2/2026 |
| **5** | Revisar o contrato de trabalho para inclusão de cláusulas (independentes) que tratam de confidencialidade e sigilo | Jurídico | Todos os processos | ADX | Q3/2026 |
| **6** | Revisar as permissões de acesso | Segurança da Informação | ADM 03 – Realizar Admissão;<br>ADM 01 - Atender solicitações de clientes | Ytech | Q3/2026 |
| **7** | Revisar a política de atualização de senhas dos e-mails | Segurança da Informação | Todos os Processos | ADX | Q4/2026 |
| **8** | Definir repositório central oficial para armazenamento de documentos. | Organizacional | Todos os Processos | Ytech | Q2/2026 |
| **9** | Revisão do contrato ou notificação dos operador GR Protection referente ao tratamento de dados pessoais | Jurídico | ADM 03 – Realizar Admissão;<br>ADM 02 - Gerenciar exames periódicos | ADX | Q3/2026 |
| **10** | Revisão do contrato ou notificação dos operador ASSESCOM referente ao tratamento de dados pessoais | Jurídico | ADM 03 – Realizar Admissão;<br>ADM 02 - Gerenciar exames periódicos;<br>FIN 02 – Realizar pagamentos para os funcionários | ADX | Q2/2026 |

| | | | | | |
|---|---|---|---|---|---|
| **11** | Revisão do contrato ou notificação dos operador Google (e-mail) referente ao tratamento de dados pessoais | Jurídico | TEC 04 – Realizar licenciamento no Zebra;<br>TEC 03 – Gerenciar chamados;<br>TEC 06 – Criar e-mail para novo colaborador;<br>ADM 03 – Realizar Admissão;<br>ADM 02 - Gerenciar exames periódicos;<br>FIN 01 – Gerenciar recebimento de contratos;<br>FIN 03 – Elaborar relatório de espelho do ponto;<br>FIN 02 – Realizar pagamentos para os funcionários;<br>DIR 01 – Elaborar contrato;<br>TEC 05 – Cadastrar cliente nos portais de soluções Cloud;<br>TEC 02 – Coletar assinatura da NF no Notas Ytech | ADX | Q3/2026 |
| **12** | Revisão do contrato ou notificação dos operador Whatsapp referente ao tratamento de dados pessoais | Jurídico | ADM 03 – Realizar Admissão; | ADX | Q3/2026 |

| | | | | | |
|---|---|---|---|---|---|
| | | | FIN 01 – Gerenciar recebimento de contratos;<br>FIN 02 – Realizar pagamentos para os funcionários;<br>DIR 01 – Elaborar contrato;<br>TEC 05 – Cadastrar cliente nos portais de soluções Cloud | | |
| **13** | Definir prazos legais de retenção por tipo de documento | Jurídico | Todos os Processos | ADX | Q3/2026 |
| **14** | Criar rotina de descarte periódico de documentos antigos | Organizacional | Todos os Processos | Ytech | Q3/2026 |
| **15** | Armazenar ASO em repositório seguro, com controle de acesso. | Segurança da Informação | ADM 02 - Gerenciar exames periódicos | Ytech | Q3/2026 |
| **16** | Enviar à contabilidade apenas documentos estritamente necessários (sem laudos). | Organizacional | ADM 02 - Gerenciar exames periódicos | Ytech | Q2/2026 |
| **17** | Redigir ou mascarar informações sensíveis antes do envio. | Segurança da Informação | ADM 02 - Gerenciar exames periódicos | Ytech | Q2/2026 |
| **18** | Digitalizar os termos e armazenar cópia em repositório seguro. | Segurança da Informação | ADM 04 – Coletar assinatura do colaborador em termo de responsabilidade | Ytech | Q4/2026 |
| **19** | Criar rotina de revisão e descarte de termos antigos. | Organizacional | Todos os Processos | Ytech | Q3/2026 |

| | | | | | |
|---|---|---|---|---|---|
| **20** | Revisão do contrato ou notificação dos operador Unimed referente ao tratamento de dados pessoais | Jurídico | ADM 05 – Cadastrar colaborador em benefícios | ADX | Q4/2026 |
| **21** | Revisão do contrato ou notificação dos operador Pluxee referente ao tratamento de dados pessoais | Jurídico | ADM 05 – Cadastrar colaborador em benefícios | ADX | Q4/2026 |
| **22** | Controlar acesso ao local de armazenamento de documentos físicos | Organizacional | ADM 03 – Realizar Admissão;<br>ADM 02 - Gerenciar exames periódicos;<br>FIN 03 – Elaborar relatório de espelho do ponto;<br>ADM 04 – Coletar assinatura do colaborador em termo de responsabilidade;<br>ADM 05 – Cadastrar colaborador em benefícios | ADX | Q3/2026 |
| **23** | Revisão do contrato ou notificação dos operador D4Sign referente ao tratamento de dados pessoais | Jurídico | DIR 01 – Elaborar contrato | ADX | Q3/2026 |
| **24** | Revisão do contrato ou notificação dos operador CyberSul referente ao tratamento de dados pessoais | Jurídico | FIN 01 – Gerenciar recebimento de contratos | ADX | Q3/2026 |
| **25** | Centralizar contratos e NFs em repositório único corporativo | Organizacional | Todos os Processos | Ytech | Q3/2026 |
| **26** | Restringir acesso aos contratos apenas a perfis autorizados | Organizacional | Todos os Processos | Ytech | Q3/2026 |

| | | | | | |
|---|---|---|---|---|---|
| **27** | Proibir envio de documentos contratuais por WhatsApp | Organizacional | Todos os Processos | Ytech | Q4/2026 |
| **28** | Revisão do contrato ou notificação dos operador Banco Bradesco referente ao tratamento de dados pessoais | Jurídico | FIN 02 – Realizar pagamentos para os funcionários | ADX | Q2/2026 |
| **29** | Revisão do contrato ou notificação dos operador SIMIX referente ao tratamento de dados pessoais | Jurídico | FIN 03 – Elaborar relatório de espelho do ponto | ADX | Q2/2026 |
| **30** | Revisão do contrato ou notificação dos operador AUVO referente ao tratamento de dados pessoais | Jurídico | TEC 03 – Gerenciar chamados;<br>TEC 01 – Atender chamado | ADX | Q2/2026 |
| **31** | Revisão do contrato ou notificação dos operador Google Drive referente ao tratamento de dados pessoais | Jurídico | TEC 02 – Coletar assinatura da NF no Notas Ytech | ADX | Q2/2026 |
| **32** | Definir repositório oficial único para arquivamento fiscal (Google Drive) | Organizacional | Todos os Processos | Ytech | Q4/2026 |
| **33** | Revisão do contrato ou notificação dos operador Zebra Technologies referente ao tratamento de dados pessoais | Jurídico | TEC 04 – Realizar licenciamento no Zebra | ADX | Q3/2026 |
| **34** | Revisão do contrato ou notificação dos operador Extreme Cloud IQ referente ao tratamento de dados pessoais | Jurídico | TEC 05 – Cadastrar cliente nos portais de soluções Cloud | ADX | Q3/2026 |
| **35** | Revisão do contrato ou notificação dos operador URMOBO referente ao tratamento de dados pessoais | Jurídico | TEC 05 – Cadastrar cliente nos portais de soluções Cloud | ADX | Q2/2026 |
| **36** | Proibir envio de dados de acesso por WhatsApp. | Organizacional | TEC 05 – Cadastrar cliente nos portais de soluções Cloud | Ytech | Q4/2026 |

*Tabela 20 - Plano de Ações.*

# 13 – Conclusão

Um programa de privacidade e Proteção de dados é um plano para incorporar mudanças atuais e recebidas em processos de negócios acionáveis e operacionalizados.

Desenvolver um programa de Compliance sobre privacidade e segurança de dados exige um investimento substancial de tempo profissional e gerencial, além de recursos financeiros para adquirir, instalar e operar os sistemas tecnológicos necessários que servem como fundamentos para coletar, utilizar, transferir e descartar informações pessoais não públicas.

Esse sistema deve ter uma abrangência holística, pois no ritmo em que as regulamentações estão se desenvolvendo, uma abordagem pontual resulta em uma resposta lenta, expondo a organização ao risco de não conformidade. Como sempre, os danos causados por violações de privacidade de dados podem ser graves financeiramente e para a reputação da empresa.

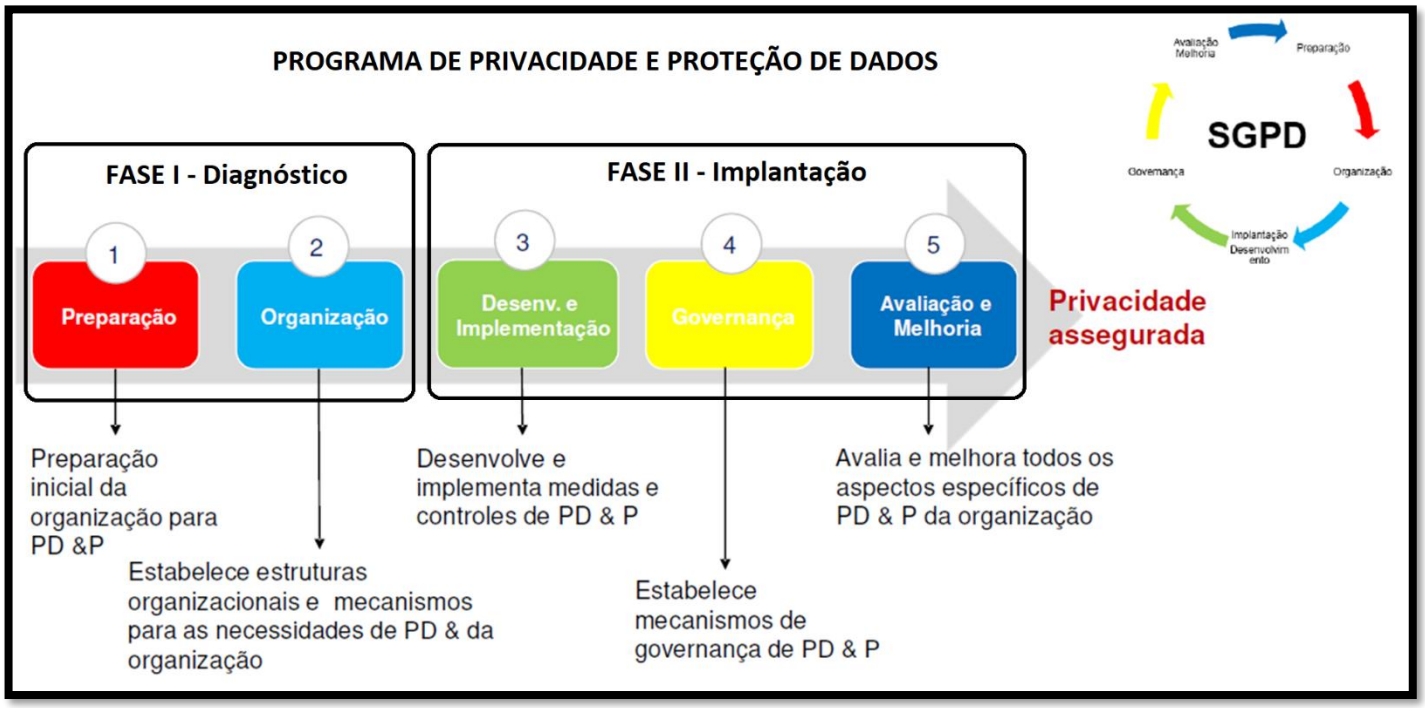



*Figure 23 - Programa de Privacidade e Proteção de Dados.*

# 14 - Aprovações

A assinatura desse documento atesta que a ADX concluiu com sucesso todas as atividades do projeto de diagnóstico para adequação da LGPD da Ytech.

| | |
|---|---|
| _____ _____<br>Nome Assinatura | _____ _____<br>Nome Assinatura |
| ADX | YTECH |
| Aracaju, 14/04/2026. | |