YTECH
SOLUÇÕES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

adx movidos por transformação

VERSÃO 1.0 – 03 DE MARÇO DE 2026

DENOMINAÇÃO DO DOCUMENTO: Política de Segurança da Informação	**DATA DA PUBLICAÇÃO:** 03/03/2026
ÁREA REPONSÁVEL: Diretoria Geral	**CLASSIFICAÇÃO:** **Uso interno**
RESPONSÁVEL PELA ELABORAÇÃO: ADX Governança e Gestão	**RESPONSÁVEL PELA APROVAÇÃO:** Comitê Gestor de Privacidade

Comitê Gestor de Privacidade da Ytech Soluções

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

Equipe Técnica do Grupo ADX

Adriano Lima Head de Operações	**Adgenison Nascimento** Head de Expansão
Hendrick Arcanjo Head de Tecnologia	**Gessica Alcântara** Head de Projetos
Laís Gomes Head de Processos	Saulo Santos **Advogado**

Sigilo e direitos de propriedade
As informações contidas nesse documento são propriedade da Ytech Soluções e não poderão ser disseminadas, distribuídas ou de qualquer outra forma passadas a terceiros, sem o expresso consentimento escrito.

Histórico de revisões			
Versão	**Data**	**Autor**	**Descrição**
1.0	02/03/2026	ADX	Documento elaborado

Sumário

1 – Introdução

Este documento declara o comprometimento da diretoria em estabelecer a PSI - Política de Segurança da Informação da Ytech Soluções, que é um conjunto das diretrizes, normas e procedimentos necessários à preservação e segurança dos bens de informação utilizados na empresa.

São bens de informação os seguintes componentes da TI - Tecnologia da Informação: sistemas aplicativos desenvolvidos e adquiridos, softwares básicos e de apoio, dados, hardware, instalações físicas, equipamentos de infraestrutura e documentos em qualquer forma de armazenamento.

Conforme definição da norma **NBR ISO/IEC 27001**, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A segurança da informação objetiva proteger a informação de diversos tipos de ameaças, para garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A informação pode existir em muitas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

2 – Objetivo

Estabelecer as políticas, normas e procedimentos a serem seguidas pela organização, no que diz respeito às atividades relacionadas à segurança da informação

3 – Escopo e abrangência

O escopo e abrangência dessa política de segurança da informação engloba não apenas os requisitos de segurança lógica, mas também os de segurança física, segurança dos processos e de pessoal, direta ou indiretamente relacionados com todos os departamentos da empresa.

4 – Integração com os procedimentos existentes

Os seguintes documentos são parte integrante dessa política e devem ter todo o seu conteúdo respeitado como todas as regras e diretrizes aqui descritas:

- Política de Privacidade Interna;
- Política de Privacidade Externa;
- Política de Proteção de Dados Pessoais;
- Termo de Confidencialidade dos Colaboradores;
- Contrato de Trabalho;
- Contratos com Fornecedores;

5 – Princípios

Os seguintes princípios são endereçados por esse documento:

- **Confidencialidade:** Somente pessoas devidamente autorizadas pela organização devem ter acesso à informação;
- **Integridade:** A informação deve sempre ser alterada de forma íntegra para não gerar falsas interpretações;
- **Disponibilidade:** A informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;
- **Autenticidade:** Princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;
- **Criticidade:** Princípio de segurança que define a importância da informação para a continuidade da atividade fim da organização;
- **Não-Repúdio:** Garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;
- **Responsabilidade:** As responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas.
- **Conhecimento:** Todos os colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência de normas, procedimentos,

orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

- **Ética:** todos os direitos e interesses legítimos de colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação devem ser respeitados;
- **Legalidade:** as ações de Segurança da Informação levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e direitos de uso;

6 – Diretrizes

As seguintes diretrizes de alto nível serão utilizadas como origem dessa política, norteando todo o documento:

- **D1** - Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;
- **D2** - Assegurar que os recursos colocados à disposição dos colaboradores sejam utilizados apenas para as finalidades aprovadas pela organização;
- **D3** - Garantir a continuidade dos negócios;
- **D4** - Atender às leis que regulamentam as atividades da organização e seu mercado de atuação;
- **D5** - Selecionar os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- **D6** - Comunicar imediatamente ao Comitê qualquer descumprimento da política corporativa de segurança da informação;
- **D7** – Inventariar e proteger os ativos de informação, além de ter os seus proprietários identificados;
- **D8** – Analisar os principais processos de negócios sob a ótica da segurança da informação, ajustando-os de acordo com as melhores práticas;

7 – Estrutura normativa

A estrutura normativa da Segurança da Informação da Ytech Soluções é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- **Política de Segurança da Informação (Política):** Constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- **Normas de Segurança da Informação (Normas):** Estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- **Procedimentos de Segurança da Informação (Procedimentos):** Instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da empresa.

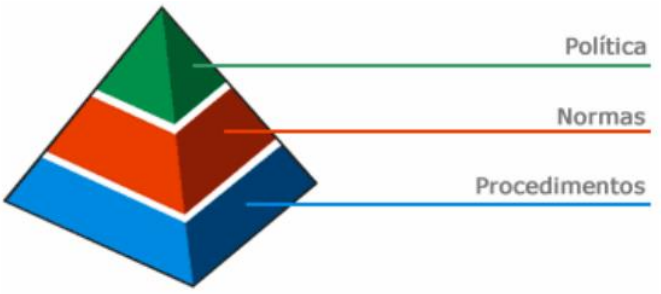

Figura 01 – Estrutura normativa da Segurança da Informação.

8 – Análise dos processos de negócio

Para o perfeito entendimento do funcionamento da empresa, em busca das customizações e ajustes necessários pelas boas práticas de segurança, foi feito o mapeamento dos principais processos de negócio existentes. Esses processos foram detalhadamente analisados, pela ótica da segurança da informação, e as sugestões de melhoria foram registradas no plano de ações para adequação à LGPD. Cada ação desse plano possui uma data limite para implementação e responsável, detalhados em outro documento que foi apresentado à diretoria da empresa. A figura a seguir demonstra, de forma macro, quais processos de negócio foram analisados:

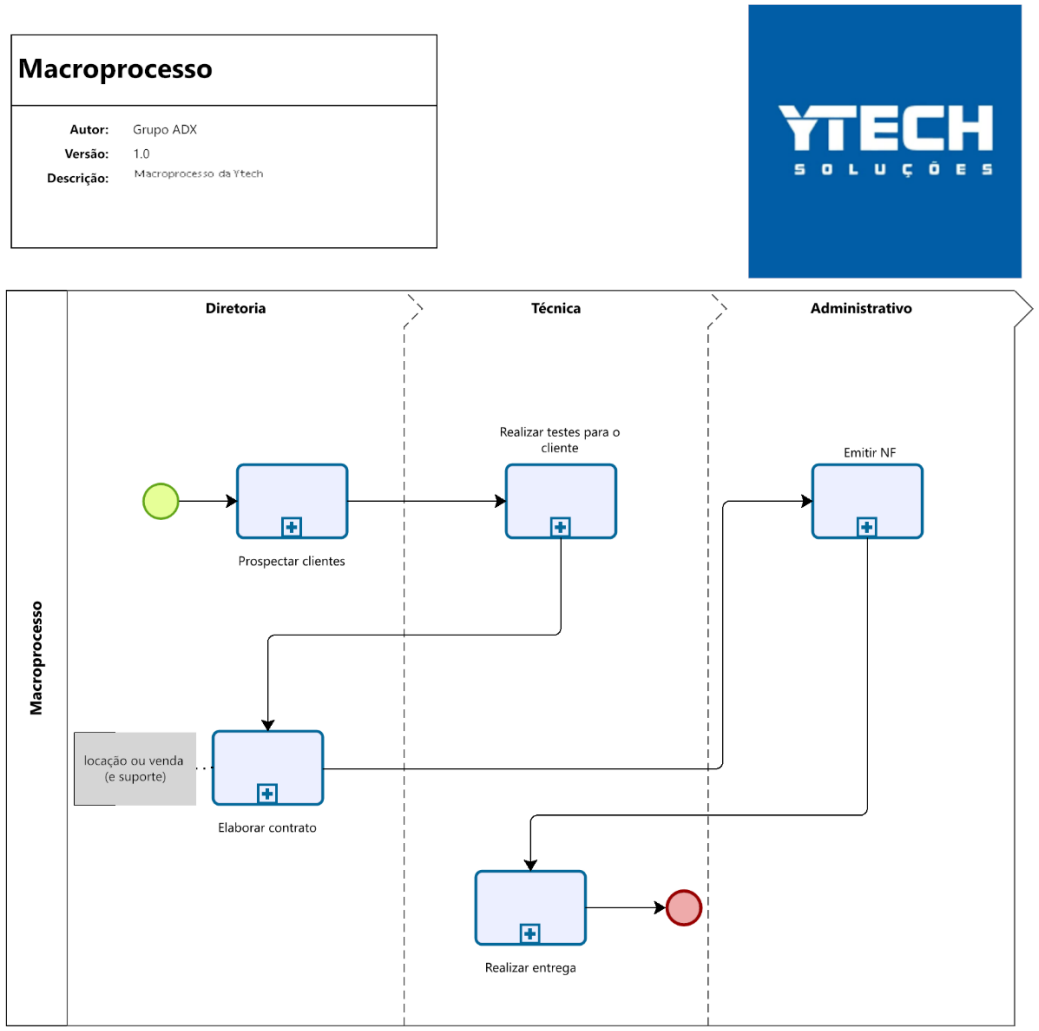

Figura 02 – Macroprocesso de negócio.

9 – Gerenciamento da versão e manutenção da política

A política de segurança deve ser revisada constantemente para adequar as normas e procedimentos aos novos requisitos do negócio e avanços tecnológicos.

Os documentos integrantes da estrutura normativa da Segurança da Informação deverão ser aprovados e revisados conforme os seguintes critérios:

- **Política:**
    - Nível de Aprovação: Diretoria e Gestão de TI;
    - Periodicidade de Revisão: anual;
- **Normas:**
    - Nível de Aprovação: Comitê Gestor de Privacidade;
    - Periodicidade de Revisão: anual;
- **Procedimentos:**
    - Nível de Aprovação: Supervisor responsável pela área envolvida;
    - Periodicidade de Revisão: Semestral;

10 – Atribuições e responsabilidades na gestão da PSI

Cabe a todos os colaboradores (funcionários, estagiários, jovens aprendizes e prestadores de serviços) da Ytech Soluções:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

- Assinar Termo de Conhecimento (**Anexo II**) desse documento, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento. As sanções pelo não cumprimento da política de segurança da informação estão descritas no item **29 – Punições;**

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados;

- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela organização;

- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;

- Comunicar imediatamente ao comitê gestor de segurança da informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

Adicionalmente, são definidas as seguintes responsabilidades e atribuições específicas relacionadas à segurança da informação:

Atribuições e responsabilidades da Diretoria:

- Aprovar a Política de Segurança da Informação e suas revisões;

- Aprovar a nomeação dos “proprietários” da informação;

- Aprovar os investimentos necessários para manter a segurança dentro da organização;

- Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Comitê Gestor de Segurança da Informação;

Atribuições e responsabilidades do comitê gestor de privacidade

- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor melhorias e aprovar as Normas de Segurança da Informação;
- Definir a classificação das informações pertencentes ou sob a guarda da Ytech Soluções, com base no inventário de informações apresentado pela Área de TI e nos critérios de classificação constantes de Norma específica;
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando-os à diretoria, quando for o caso;
- Propor projetos e iniciativas relacionados à melhoria da segurança da informação;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
- Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;
- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação e propor a relação de “proprietários” das informações;

Atribuições e responsabilidades do departamento de TI

- Convocar, coordenar, lavrar atas e prover apoio às reuniões do Comitê;
- Prover todas as informações de gestão de segurança da informação solicitadas pelo Comitê;
- Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores;
- Oferecer orientação e treinamento sobre segurança e sobre a Política de Segurança da Informação e suas Normas a todos os colaboradores;

- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;

- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;

- Analisar os riscos relacionados à segurança da informação e apresentar relatórios periódicos sobre tais riscos ao Comitê, acompanhados de proposta de aperfeiçoamento do ambiente de controle, quando for o caso;

- Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações;

- Requisitar informações às demais áreas (diretorias, gerências, supervisões etc.), realizar testes e averiguações em sistemas e equipamentos com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação e estabelecer mecanismo de registro e controle de não conformidade a esta Política e às Normas de Segurança da Informação, comunicando sempre ao Comitê.

- Configurar os bloqueios de acesso à Internet não permitindo o acesso a conteúdo improdutivo, seja através de websites, redes sociais ou ferramentas de comunicação instantânea não homologadas pela diretoria;

- Configurar o acesso remoto dos colaboradores a qualquer serviço da rede da Ytech Soluções, e-mails, sistemas, ferramentas de comunicação etc., apenas durante o horário comercial;

- Auditar os computadores dos visitantes em relação a ferramenta de antivírus atualizada e conexão em segmento de rede separado, quando for preciso se conectar na rede da Ytech Soluções;

- Criar um perfil de acesso, detalhando todas as permissões necessárias em todos os sistemas, para cada colaborador ou prestador de serviço da Ytech Soluções;

Atribuições e responsabilidades da assessoria jurídica

- Manter as áreas da empresa informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;
- Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação e LGPD, com o objetivo de proteger os interesses da Ytech Soluções e avaliar, quando solicitada, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas da empresa;

Atribuições e responsabilidades do departamento de recursos humanos

- Obter referências pessoais e profissionais de todos os colaboradores a serem contratados pela empresa;
- Verificar a exatidão e inteireza do curriculum vitae, profissional e acadêmico;
- Obter pelo menos uma referência bancária;
- Providenciar o ajuste do perfil de acesso aos sistemas, quando houver transferência de setor;
- Colher a assinatura do Termo de Conhecimento dos funcionários e estagiários, arquivando-o nos respectivos prontuários;
- Informar, previamente, à área de TI, todos os desligamentos, afastamentos e modificações no quadro funcional da empresa;
- Providenciar a eliminação do *login*, quando houver saída de pessoal, quer seja por demissão ou por suspensão de contrato;

- Solicitar ao departamento de TI que bloqueie os acessos dos colaboradores durante o período de férias ou licenças.

Atribuições e responsabilidades dos usuários da TI

- Os usuários são responsáveis por qualquer atividade desenvolvida através de suas contas na Ytech Soluções e pelos eventuais custos dela decorrentes em atividades não autorizadas;

- Os usuários, a menos que tenham uma autorização específica para esse fim, não podem permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na Ytech Soluções ou de sua propriedade;

- Os recursos computacionais não podem ser utilizados para constranger, assediar, ofender, caluniar ou ameaçar qualquer pessoa. Esses recursos não podem ser usados para alterar ou destruir recursos computacionais de outras instituições. Se a partir de uma conta, um usuário estiver, de qualquer maneira, interferindo no trabalho de outro, este deve comunicar o fato ao responsável pelo equipamento onde está a conta, ou comunicar o caso à TI;

- É proibida a distribuição voluntária de mensagens não desejadas, como circulares, manifestos políticos, correntes de cartas ou outros sistemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas computacionais;

- Sem uma autorização específica, os usuários não podem ligar ou desligar fisicamente ou eletricamente recursos computacionais da Ytech Soluções, especialmente as estações de trabalho, e componentes externos, como cabos, impressoras, discos ou sistemas de vídeo, exceto os PC's do setor ao qual o funcionário pertença;

- Não é permitida a utilização dos recursos computacionais da Ytech Soluções para benefício financeiro direto ou indireto, próprio ou de terceiros fora da instituição, sujeitando-se o infrator a imediata suspensão de sua conta, sem

prejuízo da aplicação das demais penalidades cabíveis previstas no Regimento Interno;

- Não é permitido o uso, para fins particulares ou de recreação, de serviços que sobrecarreguem as redes de computadores da Ytech Soluções tais como: escuta de rádio, páginas de animação e serviços de telefone via Internet.
- Não é permitida a manutenção não autorizada de páginas pessoais ou de serviços particulares envolvendo comercialização na Internet, utilizando os recursos computacionais da Ytech Soluções;
- Não é permitido o uso de material de consumo de informática da Ytech Soluções para fins particulares;
- Os usuários devem comunicar ao Comitê qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros.
- Os usuários não podem, deliberadamente, efetuar ou tentar efetuar qualquer tipo de acesso não autorizado a dados dos recursos computacionais da Ytech Soluções, ou tentar sua alteração, como por exemplo, ler mensagens pessoais de terceiros ou acessar arquivos confidenciais;
- Os usuários não podem violar ou tentar violar os sistemas de segurança dos recursos computacionais da Ytech Soluções, como quebrar ou tentar adivinhar identificação ou senhas de terceiros;
- Os usuários não podem interceptar ou tentar interceptar transmissão de dados não destinados ao seu próprio acesso, seja monitorando barramentos de dados, seja através da rede;
- Equipamentos devem ser mantidos nas suas perfeitas condições de uso, na forma como lhes foram entregues. Não movê-los dos locais onde foram instalados, exceto os "notebooks". Evitar colocar objetos sobre o equipamento de maneira que prejudique o seu sistema de ventilação. Não manipular líquidos

ou substâncias que possam danificar os equipamentos quando os estiver operando.

- É terminantemente proibida a instalação de "softwares" e/ ou pacotes aditivos aos "softwares" pré-instalados, sejam eles licenciados ou não;
- Não é permitido instalar qualquer software de propriedade da Ytech Soluções em computadores pessoais usados na empresa ou fora dela;
- Comunicar imediatamente à Coordenação Administrativa qualquer dano ou extravio de material de consumo e mobiliário diretamente ligado à informática.
- É extremamente proibida a utilização de qualquer referência à Ytech Soluções, sem expressa autorização da diretoria, em mídias sociais, propagandas ou eventos;

Atribuições e responsabilidades do DPO

- Contribuir na Definição das Políticas e Diretrizes do Programa de Governança em Privacidade;
- Assegurar o cumprimento das políticas de Privacidade e Proteção de Dados através de auditorias mensais;
- Articular a aderência do corpo diretivo com as políticas, estratégias, diretrizes e regulações referentes à proteção de dados pessoais;
- Gerir a Revisão da posição da organização como agente de tratamento de Dados Pessoais;
- Auxiliar na definição e gerir o fluxo de atendimento a requisições de direitos dos Titulares de Dados Pessoais;
- Revisar práticas de Segurança da Informação voltadas a tratamento de Dados Pessoais e Dados Pessoais Sensíveis;

- Propor oportunidades de Anonimização e Pseudoanonimização dos dados pessoais tratados pela empresa;
- Revisar e Propor melhorias no Processo de Gestão de Incidentes voltado a Dados Pessoais e Dados Pessoais Sensíveis;
- Revisar e Propor métodos de armazenamento e compartilhamento de dados seguros;
- Auxiliar na definição e gerir processo de mapeamento de ciclo de vida dos dados, aplicações e terceiros;
- Realizar avaliação do impacto da proteção de dados (RIPD), de acordo com a metodologia definida;
- Acompanhamento e apoio nos projetos de software que envolvem Gestão de Privacidade de Dados Pessoais e Dados Pessoais Sensíveis;
- Aconselhar sobre proteção de dados na arquitetura de TI na organização;
- Aconselhar programadores e administradores de sistemas sobre a proteção prática de sistemas de acordo com as boas práticas;
- Aconselhar sobre tecnologias de aprimoramento da privacidade, incluindo criptografia, anonimização e pseudonimização;
- Atender as solicitações dos titulares dos Dados através da plataforma contratada e dentro dos SLAs acordados;
- Coletar informações de violações de segurança;
- Ajudar o cliente a manter, armazenar e documentar as revogações da gestão de consentimento dos titulares dos dados;
- Apoiar o cliente no registro e documentação dos incidentes relacionados a privacidade e proteção de dados;

- Apoiar nas decisões do comitê de privacidade e acompanhar as ações relacionados aos incidentes;
- Apoiar o cliente na investigação de incidentes de segurança e privacidade;
- Entender o impacto do incidente e ajudar o cliente a gerir as crises objetivando evitar sanções;
- Ajudar o cliente a Notificar a Agência de Proteção e Dados sobre uma violação de segurança dentro do prazo estabelecido em Lei;
- Ajudar o cliente a Notificar os titulares dos dados da violação de segurança;
- Garantir a conformidade com os requisitos da LGPD;
- Realizar controle anual de conformidade de segurança de TI para Dados Pessoais e Dados Pessoais Sensíveis;
- Ajudar o cliente a Garantir mais foco na segurança de TI para Dados Pessoais e Dados Pessoais Sensíveis;
- Recomendações técnicas e operacionais para proteger sistemas, redes e dispositivos;
- Apresentar relatórios de acompanhamento de nível de conformidade com a LGPD e segurança da TI para a Administração.

11 – Classificação da informação

A classificação da informação é o processo de estabelecer o grau de importância das informações mediante o seu impacto para o negócio, ou seja, quanto mais estratégica e decisiva para a manutenção ou sucesso da organização, maior será a sua importância. A classificação deve ser realizada a todo instante, em qualquer meio de armazenamento.

Existem regras que devem ser consideradas durante a classificação e a principal delas é a determinação de proprietários para todas as informações, sendo este o responsável por auxiliar na escolha do meio de proteção.

Nos casos em que houver um conjunto de informações armazenadas em um mesmo local, e elas possuírem diferentes níveis, deve-se adotar o critério de classificar todo o local com o mais alto nível de classificação.

As informações armazenadas em qualquer local devem estar de acordo com os critérios de classificação e devem possuir uma identificação que facilite o reconhecimento do seu grau de sigilo. O inventário dos ativos de informação da Ytech Soluções seguirá o seguinte padrão:

Documentos em papel	• Contratos; • Documentos da empresa; • Relatórios
Software	• Aplicativos; • Sistemas operacionais; • Ferramentas de desenvolvimento; • Utilatários de sistema; • Atestados médicos
Hardware	• Servidores, desktops, netbooks, talets; • Storages, unidades de backup, fitas de backup; • Impressoras e copiadoras; • Equipamentos de comuicação (FAX, modem, access points, roteadores, switches etc.); • Mídias magnéticas; • Nobreak, ar condicionados; • Móveis, prédios e salas
Pessoa	• Empregados; • Estagiários; • Jovem aprendiz; • Terceirizados; • Fornecedores
Serviço ou atividade	• Computação (Aplicação de paths, backup etc); • Comunicação (Ligações telefônicas, vídeo conferência etc.); • Atendimento a usuários

12 – Reclassificação da informação

Toda informação classificada, quando passar por alteração de conteúdo, deve ser submetida a novo processo de classificação, com o objetivo de rever o nível mais adequado.

13 – Níveis de classificação

A classificação quanto ao sigilo obedecerá aos seguintes critérios:

- **Públicas** – São aquelas que não necessitam de sigilo algum. Podendo ter livre acesso para os colaboradores. Não há necessidade de investimentos em recursos de proteção. São informações que se forem divulgadas fora da organização, não trarão impactos para os negócios.

- **Internas** – O acesso externo a essas informações devem ser evitadas. Entretanto, se esses dados se tornarem públicos, as consequências não serão críticas. Exemplo: agendas de telefones e ramais, benefícios da organização para os colaboradores, procedimentos operacionais simples;

- **Confidenciais** – As informações dessa classe devem ser confidenciais dentro da organização e protegidas do acesso externo. Se alguns desses dados forem acessados por pessoas não autorizadas, as operações da organização poderão ser comprometidas, causando perdas financeiras e de competitividade. Exemplos: Salários, dados pessoais, dados dos clientes, estratégias de mercado e senhas.

14 – Formas de classificação

A classificação das informações deve ser implementada de acordo com a tabela a seguir:

Tipo do documento	Procedimento
Documento em papel	Caso seja confidencial e gerado dentro da organização, deve apresentar o nível de segurança na primeira página do documento. Caso venha de fora, deve ser marcado com uma etiqueta ou carimbo.
E-mail	Caso seja confidencial, deve ter o assunto iniciado com "[Confidencial]".
Documento eletrônico	Deve conter o nível de segurança no rodapé na primeira página do documento.
Outros tipos de mídia	A classificação de segurança deve ser visível por etiquetas ou outros recursos que se façam necessários

15 - Proprietário da informação

O proprietário da informação é um diretor ou um gestor da Ytech Soluções, formalmente indicado pelos sócios, responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações sob a sua guarda. Cabe ao proprietário da informação:

- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções com as autorizações de acesso concedidas;
- Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a Política e as Normas de Segurança da Informação;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;
- Analisar os relatórios de controle de acesso fornecidos pela área de Gestão de Segurança da Informação, com o objetivo de identificar desvios em relação à

Política e às Normas de Segurança da Informação, tomando as ações corretivas necessárias;

- Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões do Comitê de Gestão de Privacidade, prestando os esclarecimentos solicitados.

A tabela a seguir descreve os proprietários das informações de cada departamento da Ytech Soluções:

Proprietário da Informação	Departamento
Jairo Soirefmann	Diretoria
Lorena Bandeira	Administrativo
Carla Mendes	Financeiro
Matheus Santana	Administrativa

16 - Usuários da informação

É todo funcionário interno, trabalhador temporário, estagiário ou terceirizado, que tenham acesso aos bens de informação da Ytech Soluções.

O usuário da informação terá responsabilidade de:

- Zelar por todo acesso ao ambiente computadorizado executado e registrado com a sua identificação de acesso;
- Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
- Utilizar os recursos tecnológicos (equipamentos, programas e sistemas) e as informações somente para desempenho das suas atividades profissionais, sendo assim vedado o seu uso para fins pessoais;

- Notificar não conformidades de segurança.

17 - Controle da Divulgação

- **Informações Confidenciais** – Só devem ser divulgadas para quem precisa da informação em função da necessidade de serviço. Para acessá-la, é preciso que se faça parte de uma lista formal de autorização elaborada pelo proprietário da informação ou seu representante autorizado;

- **Informações de uso interno** – Podem ser divulgadas para qualquer funcionário da Ytech Soluções;

- **Informações Públicas** – Podem ser divulgadas livremente sem nenhum controle de acesso;

18 - Armazenamento

- **Informações Confidenciais** – Devem ser armazenadas em locais que garantam apenas o acesso das pessoas permitidas. Ferramentas como servidores de arquivos, sistemas de gerenciamento de documentos e locais com acesso restrito devem ser utilizadas para garantia da confidencialidade. As listas de controle de acesso devem ser periodicamente auditadas para identificar inconformidades de acesso;

- **Informações de uso interno** – Devem ser disponibilizadas em meios onde os colaboradores possam ter apenas o mínimo acesso necessário. As ferramentas de armazenamento utilizadas devem garantir que as informações não serão indevidamente alteradas, copiadas ou excluídas.

19 - Transporte interno e expedição

- **Informações Confidenciais** – Em recipiente simples com identificação do grau de sensibilidade, evitando-se a entrega em malotes internos. Deve-se dar preferência à entrega pessoal por pessoa devidamente autorizada, com registro de protocolo;

- **Informações de uso interno** – Pode ser transportada aberta;

20 - Transporte externo

- **Informações Confidenciais** – Em recipiente de segurança com identificação do grau de sensibilidade. O transporte e a entrega devem sempre ser realizados por pessoa devidamente autorizada, com registro de protocolo;
- **Informações de uso interno** – Em recipiente simples;

21 - Transmissão de voz

- **Informações Confidenciais** – Permitida a transmissão através de linhas telefônicas, apenas dentro de ambientes controlados.
- **Informações de uso interno** – Sem restrições.

22 - Transmissão de dados

- **Informações Confidenciais** – Se o meio de transmissão estiver totalmente em área sob o controle da organização, pode ser transmitido em texto claro (sem encriptação), caso contrário deve ser criptografado.

- **Informações de uso interno** – Permitida a transmissão em texto livre para qualquer caso.

23 - Descarte de informações

Toda mídia impressa que contenha informações relevantes deve ser destruída antes de ser descartada. Essa destruição deve ser feita com o picotador de papel existente na empresa. CDs, DVDs, pen drives, discos externos e qualquer outro tipo de mídia física devem ser totalmente destruídos antes de serem descartados.

24 – Controle de mudanças no ambiente

Toda e qualquer mudança crítica que precise ser realizada no ambiente de TI da Ytech Soluções deve ser feita fora do horário de expediente e, sempre que possível, prioritariamente validada no ambiente de homologação.

25 – Manutenção de equipamentos de informática

Quando qualquer equipamento de informática como computadores pessoais, celulares, *notebooks*, *tablets*, servidores, *storages etc.*, necessitarem de assistência técnica fora da empresa, a equipe de TI deve apagar ou remover todos os dispositivos de armazenamento como discos, cartões de memória, pen drives etc. Essa ação evitará que os dados sejam acessados por pessoas não autorizadas.

26 - Computação móvel e trabalho remoto

Os trabalhos remotos, sempre que necessários, só estão liberados através de acesso VPN para alguns membros da equipe de TI, de acordo com a necessidade. Para os funcionários, só será permitido esse acesso em situações especiais e com aprovação prévia do diretor de cada área, observando o período e os horários em que os acessos serão permitidos.

Para os fornecedores, o acesso só será permitido depois da criação de um perfil de acesso que libere apenas os servidores envolvidos nas atividades. As contas deles devem ser desabilitadas imediatamente após a conclusão dos trabalhos e por padrão só poderão ocorrer em horário comercial. Casos especiais serão tratados pontualmente.

27 - Níveis de Operação

- **Rotina** – Caracteriza a situação em que não existe suspeita de falhas na segurança do sistema, que deve estar monitorado continuamente;

- **Emergência** – Existe a suspeita de algum ataque à segurança, com possíveis danos ao funcionamento seguro do sistema;

- **Crise** – Situação na qual um problema à segurança está confirmado e ações devem ser tomadas para tratar o ataque e suas consequências.

Todo e qualquer incidente de segurança deve ser imediatamente informado ao Comitê, ao DPO e a equipe de TI para que as medidas cabíveis sejam tomadas no menor espaço de tempo possível;

28 – Segurança Física

- A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. As seguintes regras devem ser obedecidas por todos:
- Todos os visitantes, colaboradores e prestadores de serviço devem usar o crachá de identificação em local visível;
- Os visitantes não podem ficar circulando nas dependências da empresa. Devem ser conduzidos da portaria diretamente para o setor que deseja visitar;
- Todo e qualquer equipamento ou material só poderá ser retirado das instalações da Ytech Soluções com a devida autorização dos gestores ou da diretoria;
- Todas as áreas de circulação, incluindo as salas de aula, devem ser monitoradas através de circuitos internos de TV;
- A sala dos servidores e equipamentos de TI, Datacenter, tem acesso reservado aos funcionários desse setor. É terminantemente proibido o uso de qualquer tipo de alimentos ou líquidos devido aos riscos de dano aos ativos existentes;
- As portarias de acesso à empresa são monitoradas continuamente por profissionais de empresa especializada em segurança;
- Todos os colaboradores devem manter a política da mesa limpa, evitando que informações confidenciais fiquem expostas e possam ser observadas por pessoas não autorizadas;

- Uma cópia das mídias de backups semanais, mensais e anuais devem ser removidas continuamente das instalações da Ytech Soluções para garantir a continuidade dos negócios em caso de incidentes com a estrutura física;
- Ao encaminhar qualquer equipamento para assistência técnica, as informações existentes nas mídias de armazenamento devem ser definitivamente excluídas para evitar acesso indevido;

28 – Gestão de incidentes de segurança

Um incidente de segurança da informação é qualquer ação ou omissão que pode ter impacto na segurança das informações, no negócio ou nos ativos da instituição. A tabela a seguir descreve quem deve ser acionado a depender da natureza do incidente:

Tipo de incidente	Empresa	Telefone
Problemas envolvendo privacidade de dados pessoais	ADX	3013-4140
Problemas com energia elétrica	SULGIPE ENERGISA	(079) 3530-1000 0800 079 01 96
Problemas com incêndios	BOMBEIROS	193
Problemas de roubo ou assalto	Polícia Militar Polícia Civil	190 3213-1119
Problemas de infraestrutura civil	Defesa Civil	3246-3453

Problemas de saúde com alunos, colaboradores ou visitantes	SAMU	192

29 – Punições

Quando qualquer item da política de segurança da informação for violado, por um colaborador que tenha assinado o Termo de Conhecimento, o Comitê vai levar ao conhecimento da diretoria para definir a punição aplicada. As punições possíveis são:

- Advertência verbal;
- Advertência por escrito;
- Desconto de período de trabalho;
- Desligamento do colaborador sem justa causa;
- Desligamento do colaborador por justa causa;

30 – Referências bibliográficas

[1] ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 270005 e ISO/IEC 22301;

[2] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet**, versão 3.1. São Paulo: Comitê Gestor da Internet no Brasil, 2006. Disponível em: <http://cartilha.cert.br/livro/>.

[3] Ferreira, Fernando Nicolau Freitas; Araújo, Márcio Tadeu. Política da Segurança da Informação: Guia Prático para Elaboração e Implementação. Editora Ciência Moderna, 2006.

[4] Sêmola Marcos. Gestão da segurança da informação, uma visão executiva. Editora CAMPUS 2003.

[5] Fontes Edilson. Políticas e Normas para a Segurança da Informação. Editora Brasport, 2012.

[6] FONTES, Edson. Praticando a Segurança da Informação. Brasport, 2008.

[7] Ferreira Fernando e Araújo Márcio. Política de Segurança da Informação. Ciência Moderna, 2008.

ANEXOS

ANEXO I – Conceitos e definições

- **Ameaça**: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;
- **Ativos de informação**: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- **Capacitação em SIC**: saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;
- **Classificação da informação**: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;
- **Comitê Gestor de Privacidade**: Comitê de caráter deliberativo, responsável pela normatização e supervisão da segurança da informação;
- **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada;
- **Conscientização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;
- **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

- **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;
- **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;
- **Gestão de continuidade dos negócios**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;
- **Gerenciamento de operações e comunicações**: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;
- **Gestão de riscos de segurança da informação e comunicações - GRSIC**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;
- **Gestão de segurança da informação e comunicações - GSIC**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;
- **Incidente de Segurança**: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
- **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
- **Infraestrutura de TI**: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;
- **Integridade**: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental;
- **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

- **Recursos criptográficos**: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;
- **Risco**: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
- **Segurança física e do ambiente**: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;
- **Sensibilização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional;
- **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos à Ytech Soluções;
- **Tratamento de incidentes**: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências;
- **Tratamento da informação**: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação; e
- **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

ANEXO II - Termo de Conhecimento para os Colaboradores

NOME:	
MATRÍCULA:	
CPF:	

AFIRMO QUE ESTOU CIENTE E COMPROMETO-ME a cumprir a Política de Segurança da Informação da Ytech Soluções na sua íntegra, respondendo em todas as instâncias pelas consequências das ações ou omissões da minha parte, que possam pôr em risco ou comprometer qualquer diretiva descrita nesse documento.

Manaus, _____ de _____ de 20___.

_____

Assinatura do Colaborador/Estagiário/Jovem Aprendiz/Fornecedor