PROGRAMA DE GOVERNANÇA EM PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÃO

- LGPD -

Responsável pelo Programa de Governança em Privacidade
Thiago Marcos Montagner
Encarregado pelo Tratamento de Dados Pessoais (DPO)

Dois Vizinhos
2026

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÃO - LGPD

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.
CNPJ: 53.695.158/0001-90

INTRODUÇÃO

ORGANIZAÇÃO DO PROGRAMA

BLOCO 1 — GOVERNANÇA, COMPLIANCE E ÉTICA (NÍVEL ESTRATÉGICO)

BLOCO 2 — PRIVACIDADE, DIREITOS E RELAÇÃO COM TITULARES

BLOCO 3 — SEGURANÇA DA INFORMAÇÃO E CONTINUIDADE

INTRODUÇÃO

A Ê-Sistemas é uma empresa de software que desenvolve e opera soluções digitais voltadas ao atendimento e à gestão de interações. Com destaque para chatbots integrados ao WhatsApp, painel de atendimento humano, rotinas de suporte, registros de atendimento, logs técnicos e de segurança, integrações e infraestrutura de backup e continuidade. Nesse contexto, dados pessoais podem ser tratados em diferentes etapas da operação, de forma automatizada e/ou com intervenção humana, sempre vinculados à entrega do serviço contratado.

Este documento apresenta a estrutura de governança em proteção de dados pessoais da Ê-Sistemas, em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). Seu objetivo é explicitar como a empresa organiza, documenta e executa seus deveres de privacidade e segurança da informação, oferecendo previsibilidade jurídica, operacional e institucional a clientes, titulares de dados, parceiros e órgãos de controle.

Como regra geral, especialmente em contratos com entes públicos, a Ê-Sistemas atua como OPERADORA de dados pessoais, tratando informações conforme as instruções do CONTROLADOR (cliente), nos limites contratuais e legais aplicáveis. Em situações específicas — como comunicações próprias, gestão interna e cumprimento de obrigações legais — a empresa pode atuar como CONTROLADORA, assumindo diretamente as responsabilidades correspondentes.

A governança descrita neste Programa não se limita a declarações formais. Ela se baseia em políticas, procedimentos e registros efetivos, orientados pelos princípios da finalidade, necessidade, transparência, segurança, responsabilização e melhoria contínua. O enfoque adotado é prático e defensivo — sem prejuízo da eficiência operacional —, para reduzir riscos, proteger os titulares, sustentar a operação e assegurar capacidade de resposta diante de auditorias, incidentes ou mudanças regulatórias.

Este conjunto de documentos deve ser compreendido como um sistema vivo de conformidade, ajustado à realidade operacional da Ê-Sistemas e passível de evolução conforme o crescimento da empresa, a ampliação de produtos, as exigências contratuais e o ambiente regulatório.

ORGANIZAÇÃO DO PROGRAMA

O programa de privacidade da Ê-Sistemas foi estruturado para combinar transparência externa com governança interna, formando um sistema único e coerente de conformidade com a LGPD. De forma objetiva, os documentos se organizam em dois eixos:

Documentos externos (transparência): apresentam, em linguagem clara, como os dados pessoais são tratados, quais são os direitos dos titulares e quais canais estão disponíveis para contato e solicitações.

Documentos internos (governança e controle): reúnem os registros, avaliações e procedimentos necessários para a gestão de riscos, a comprovação de conformidade e a resposta a auditorias e incidentes, incluindo ROPA, DPIA, políticas internas e planos de ação. A Ê-Sistemas adota medidas técnicas e organizacionais compatíveis com o risco de sua operação e mantém procedimento formal de resposta a incidentes, com foco em contenção, avaliação de impacto, comunicação responsável e registro das medidas adotadas.

Os titulares podem exercer seus direitos previstos na LGPD por meio de canal institucional dedicado, com tratamento organizado, prazos razoáveis e rastreabilidade das solicitações.

Este programa é dinâmico e passa por revisões periódicas, sob responsabilidade da estrutura de governança da empresa, acompanhando a evolução da operação, dos produtos, das exigências contratuais e do ambiente regulatório.

1 PLANO DE GOVERNANÇA EM PRIVACIDADE

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

1.1 OBJETIVO

Este Plano de Governança em Privacidade tem por objetivo estabelecer a estrutura, diretrizes, papéis, processos e controles adotados pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA para assegurar a conformidade contínua com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), promovendo a proteção de dados pessoais, a mitigação de riscos e a cultura de privacidade.

1.2 FUNDAMENTAÇÃO LEGAL

Este Plano é elaborado com base nos artigos 46 a 50 da LGPD, bem como nas boas práticas de governança, segurança da informação e accountability recomendadas pela Autoridade Nacional de Proteção de Dados (ANPD).

1.3 PRINCÍPIOS NORTEADORES

O Programa de Governança em Privacidade observará, de forma transversal:

I – Finalidade.

II – Adequação.

III – Necessidade.

IV – Livre acesso.

V – Qualidade dos dados.

VI – Transparência.

VII – Segurança.

VIII – Prevenção.

IX – Não discriminação.

X – Responsabilização e prestação de contas.

1.4 ESTRUTURA DE GOVERNANÇA

1.4.1 Controlador de Dados

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA atua como Controladora dos dados pessoais tratados no âmbito de suas operações.

1.4.2 Encarregado de Proteção de Dados (DPO)

Nome: Thiago Marcos Montagner.

E-mail: thiagomarcosmontagner@hotmail.com

Compete ao DPO:

I – Atuar como canal de comunicação entre a empresa, os titulares e a ANPD.

II – Orientar colaboradores e parceiros quanto às práticas de proteção de dados.

III – Monitorar a conformidade com a LGPD.

IV – Coordenar a resposta a incidentes de segurança.

V – Manter e atualizar o ROPA.

1.4.3 Alta Administração

Compete à Administração:

I – Aprovar políticas e procedimentos de privacidade.

II – Garantir recursos técnicos e organizacionais adequados.

III – Apoiar a cultura de proteção de dados.

1.5 POLÍTICAS E DOCUMENTOS DE APOIO

Integram este Plano, entre outros:

I – Política de Privacidade.

II – Código de Ética e Conduta.

III – Registro das Operações de Tratamento de Dados (ROPA).

IV – Procedimento de Resposta a Incidentes de Segurança.

V – Termo de Ciência e Compromisso.

VI – Contratos e cláusulas de proteção de dados com terceiros.

VII – Política de Retenção e Destruição de Dados.

VIII – Plano de Continuidade de Negócios.

1.6 MAPEAMENTO E CONTROLE DOS TRATAMENTOS

A empresa mantém mapeadas todas as operações de tratamento de dados pessoais por meio do ROPA, contendo:

I – Finalidades.

II – Bases legais.

III – Categorias de dados.

IV – Compartilhamentos.

V – Prazos de retenção.

VI – Medidas de segurança.

1.7 GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO

São adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais, incluindo:

I – Controle de acesso.

II – Autenticação e gestão de credenciais.

III – Criptografia, quando aplicável.

IV – Backups e registros de logs.

V – Monitoramento e prevenção de incidentes.

A Ê-SISTEMAS adota os princípios de *Privacy by Design* e *Privacy by Default* no desenvolvimento e evolução de seus sistemas e soluções tecnológicas.

1.8 DIREITOS DOS TITULARES

A Ê-SISTEMAS assegura aos titulares o exercício dos direitos previstos no art. 18 da LGPD, mediante solicitação ao DPO, observando prazos e procedimentos internos.

1.9 GESTÃO DE TERCEIROS E OPERADORES

A contratação de terceiros que tratem dados pessoais observará:

I – Avaliação prévia de riscos.

II – Cláusulas contratuais de proteção de dados.

III – Dever de confidencialidade.

IV – Responsabilização conforme a LGPD.

1.10 TREINAMENTO E CONSCIENTIZAÇÃO

A empresa promoverá treinamentos periódicos sobre proteção de dados, segurança da informação e ética, visando consolidar a cultura de privacidade.

1.11 MONITORAMENTO, AUDITORIA E MELHORIA CONTÍNUA

O Programa de Governança em Privacidade será monitorado continuamente, podendo ser realizadas:

I – Revisões internas.

II – Atualizações de documentos.

III – Adequações a novas exigências legais ou orientações da ANPD.

Quando aplicável, serão realizadas Avaliações de Impacto à Proteção de Dados Pessoais (DPIA), conforme orientação da ANPD.

A empresa poderá utilizar indicadores internos para monitorar a efetividade do Programa de Governança em Privacidade.

1.12 REVISÃO E ATUALIZAÇÃO

Este Plano será revisado periodicamente ou sempre que houver alterações relevantes nos tratamentos de dados, nos serviços prestados ou na legislação aplicável.

1.13 VIGÊNCIA

Este Plano entra em vigor na data de sua aprovação pela Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Data da última atualização: 31/01/2026.

Responsável pela aprovação: Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

2 DECLARAÇÃO DE CONFORMIDADE À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

2.1 FINALIDADE DA DECLARAÇÃO

A presente Declaração de Conformidade à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) tem por finalidade demonstrar, de forma transparente e objetiva, que a Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA. adota medidas técnicas, administrativas e organizacionais adequadas para a proteção de dados pessoais, em conformidade com a legislação brasileira vigente e com as boas práticas de governança, segurança da informação e privacidade.

2.2 COMPROMISSO COM A LGPD

A Ê-SISTEMAS declara que:

I – Observa os princípios da LGPD, em especial finalidade, adequação, necessidade, segurança, prevenção, transparência e accountability.

II – Implementou um Programa de Governança em Privacidade, Proteção de Dados Pessoais e Segurança da Informação, estruturado e documentado.

III – Adota controles proporcionais aos riscos identificados, inclusive para dados pessoais sensíveis, quando aplicável.

IV – Atua de forma diligente na prevenção, detecção e resposta a incidentes de segurança.

V – Mantém mecanismos de melhoria contínua e revisão periódica de seus processos.

2.3 ESTRUTURA DE GOVERNANÇA EM PRIVACIDADE

A Ê-SISTEMAS mantém, entre outros, os seguintes instrumentos e documentos de governança:

- Política de Compliance.
- Política de Privacidade e Política de Privacidade do Cliente.
- Política de Segurança da Informação (PSI).
- Política de Retenção e Descarte de Dados.
- Plano de Governança em Privacidade.
- Registro das Operações de Tratamento de Dados (ROPA).
- Avaliação de Impacto à Proteção de Dados Pessoais (DPIA), inclusive específica para dados sensíveis (saúde).
- Matriz de Risco, Heatmap de Riscos e Plano de Ação para Tratamento de Riscos Altos.

- Procedimento de Resposta a Incidentes de Segurança.
- Plano de Continuidade de Negócios (BCP) e Procedimento de Backup e Recuperação.
- Programa de Awareness Contínuo.
- Programa de Due Diligence de Terceiros.
- Registro Centralizado de Riscos Aceitos.
- Termos jurídicos aplicáveis (Termo do Usuário, Termo de Ciência e Compromisso, entre outros).

2.4 PAPÉIS E RESPONSABILIDADES

A empresa possui definição clara de papéis e responsabilidades, incluindo:

- Administração, responsável por decisões estratégicas e alocação de recursos.
- Encarregado de Proteção de Dados (DPO), responsável por orientar, monitorar e zelar pela conformidade com a LGPD.
- Áreas técnicas e operacionais, responsáveis pela implementação e manutenção dos controles.

2.5 RELAÇÃO COM CLIENTES E TERCEIROS

Quando aplicável, a Ê-SISTEMAS poderá atuar como Controladora ou Operadora de dados pessoais, observando rigorosamente:

- As bases legais previstas na LGPD.
- As instruções documentadas do Controlador.
- Contratos e acordos de proteção de dados.
- Boas práticas de segurança e confidencialidade.

2.6 LIMITAÇÕES DA DECLARAÇÃO

Esta Declaração:

I – Não constitui garantia absoluta contra incidentes de segurança.

II – Não substitui contratos, políticas específicas ou obrigações legais individuais.

III – Reflete o estado atual das práticas de governança da empresa, sujeitas a aprimoramento contínuo.

2.7 ATUALIZAÇÃO

Esta Declaração poderá ser atualizada sempre que houver alterações relevantes nos processos, na legislação ou no Programa de Governança em Privacidade da Ê-SISTEMAS.

2.8 APROVAÇÃO

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Responsável pela aprovação:

Administração

Assinatura: _____

Data: ____ / ____ / _____

3 WHITEPAPER DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

3.1 APRESENTAÇÃO

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA. (“Ê-SISTEMAS”) apresenta este Whitepaper de Segurança da Informação e Privacidade de Dados com o objetivo de demonstrar, de forma transparente, clara e técnica, seu compromisso com a proteção de dados pessoais, a segurança da informação e a conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

Este documento destina-se a clientes, parceiros, fornecedores, auditorias, órgãos reguladores e demais partes interessadas, servindo como material institucional e informativo sobre as práticas adotadas pela empresa.

3.2 VISÃO GERAL DE GOVERNANÇA EM PRIVACIDADE

A Ê-SISTEMAS mantém um Programa de Governança em Privacidade, Proteção de Dados Pessoais e Segurança da Informação, estruturado com base nos princípios da LGPD, nas boas práticas de mercado e em referenciais normativos como ISO/IEC 27001 e ISO/IEC 27701.

Esse programa é composto por políticas, procedimentos, registros, avaliações de impacto, controles técnicos e administrativos, além de ações contínuas de conscientização.

3.3 PRINCÍPIOS NORTEADORES

O tratamento de dados pessoais realizado pela Ê-SISTEMAS observa, entre outros, os seguintes princípios:

- Finalidade.
- Adequação.
- Necessidade.
- Livre acesso.
- Qualidade dos dados.
- Transparência.
- Segurança.
- Prevenção.
- Não discriminação.
- Responsabilização e prestação de contas (accountability).

3.4 ESTRUTURA DE COMPLIANCE E RESPONSABILIDADES

A Ê-SISTEMAS possui estrutura formal de compliance, incluindo:

- Política de Compliance.
- Código de Ética e Conduta.
- Plano de Governança em Privacidade.
- Encarregado de Proteção de Dados (DPO) designado.
- Definição clara de papéis como Controlador e Operador, conforme o contexto do tratamento.

As responsabilidades são formalizadas e periodicamente revisadas.

3.5 SEGURANÇA DA INFORMAÇÃO

A proteção das informações é regida pela Política de Segurança da Informação (PSI), complementada por procedimentos específicos, incluindo:

- Controle de acessos lógicos e físicos.
- Gestão de credenciais.
- Criptografia, quando aplicável.
- Monitoramento e registros de logs.
- Procedimentos de backup e recuperação.
- Plano de Continuidade de Negócios (BCP).
- Plano de Comunicação de Crise.

3.6 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A empresa mantém políticas específicas, entre elas:

- Política de Privacidade.
- Política de Privacidade do Cliente.
- Política de Retenção e Descarte de Dados Pessoais.

Os dados pessoais são tratados com base em fundamentos legais adequados, de forma transparente e segura.

3.7 AVALIAÇÃO DE RISCOS E DPIA

A Ê-SISTEMAS realiza:

- Registro das Operações de Tratamento (ROPA).
- Avaliações de Impacto à Proteção de Dados (DPIA).
- DPIA específico para dados sensíveis (saúde).

- Matrizes de risco (impacto × probabilidade).
- Heatmaps de risco (geral e saúde).
- Planos de ação para riscos altos.

Além disso, mantém:

- Política de Aceitação de Riscos.
- Registro Centralizado de Riscos Aceitos.
- Formulário de Aceitação Formal de Risco.

3.8 GESTÃO DE INCIDENTES

A empresa dispõe de Procedimento de Resposta a Incidentes de Segurança da Informação e Dados Pessoais, que contempla:

- Identificação e contenção.
- Análise de impacto.
- Comunicação interna.
- Comunicação à ANPD, titulares e clientes, quando aplicável.
- Registro e lições aprendidas.

Modelos de comunicação formal fazem parte do programa.

3.9 TREINAMENTO E AWARENESS

A Ê-SISTEMAS executa um Programa de Awareness Contínuo, voltado à conscientização de colaboradores e parceiros sobre:

- Segurança da informação.
- Privacidade e proteção de dados.
- Boas práticas e condutas esperadas.
- Responsabilidades legais.

3.10 GESTÃO DE TERCEIROS

O relacionamento com terceiros é tratado por meio de:

- Programa de Due Diligence de Terceiros.
- Questionários de avaliação de risco (baixo, médio e alto).
- Cláusulas contratuais de proteção de dados.
- Avaliação periódica de fornecedores críticos.

3.11 DIREITOS DOS TITULARES

A Ê-SISTEMAS respeita e viabiliza o exercício dos direitos dos titulares de dados, conforme previsto na LGPD, por meio de canais adequados, definidos na Política de Privacidade.

3.12 SEGURO CIBERNÉTICO

Como medida adicional de mitigação de riscos, a empresa avalia e mantém Seguro Cibernético (Cyber Insurance), compatível com seu perfil de risco e operações.

3.13 EVIDÊNCIAS E ACCOUNTABILITY

O programa é sustentado por um robusto conjunto de evidências, incluindo:

- Checklist de Evidências LGPD
- Kit de Governança em Privacidade
- Pacote de Evidências LGPD para Clientes
- Registros formais, políticas, planos e relatórios

Esses materiais permitem comprovar conformidade em auditorias, fiscalizações e processos de due diligence.

3.14 CONFORMIDADE LEGAL

A Ê-SISTEMAS declara que seu programa está estruturado para atender às exigências da LGPD, bem como às orientações da Autoridade Nacional de Proteção de Dados (ANPD), adotando postura preventiva, diligente e transparente.

3.15 CONSIDERAÇÕES FINAIS

Este Whitepaper não substitui contratos, políticas internas ou documentos legais específicos, mas reflete, de forma consolidada, o compromisso institucional da Ê-SISTEMAS com a segurança da informação e a privacidade de dados pessoais.

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Programa de Governança em Privacidade, Proteção de Dados Pessoais e Segurança da Informação.

4 POLÍTICA DE COMPLIANCE

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

4.1 OBJETIVO

A presente Política de Compliance tem por objetivo estabelecer os princípios, diretrizes e responsabilidades que orientam a conduta ética, legal e transparente da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA. (“Ê-SISTEMAS”), assegurando a conformidade com a legislação aplicável, normas regulatórias, boas práticas de governança corporativa, segurança da informação e proteção de dados pessoais.

Esta Política integra o Programa de Governança em Privacidade, Segurança da Informação e Compliance da Ê-SISTEMAS.

4.2 ABRANGÊNCIA

Esta Política aplica-se a:

- Sócios, administradores e dirigentes.
- Colaboradores, empregados e estagiários.
- Prestadores de serviços e fornecedores.
- Parceiros comerciais.
- Clientes e usuários, quando aplicável.
- Terceiros que atuem em nome ou no interesse da Ê-SISTEMAS.

4.3 PRINCÍPIOS DE COMPLIANCE

A Ê-SISTEMAS pauta suas atividades nos seguintes princípios:

I – Legalidade e conformidade regulatória.

II – Ética, integridade e boa-fé.

III – Transparência e responsabilidade.

IV – Prevenção de riscos e melhoria contínua.

V – Segurança da informação e privacidade por padrão e por design.

VI – Responsabilização e prestação de contas (accountability).

4.4 ESTRUTURA DO PROGRAMA DE COMPLIANCE

O Programa de Compliance da Ê-SISTEMAS é composto, entre outros, pelos seguintes instrumentos:

- Política de Compliance.

- Código de Ética e Conduta.
- Política de Privacidade.
- Política de Segurança da Informação (PSI).
- Termo de Uso Aceitável da Informação (TUA).
- ROPA (Registro das Operações de Tratamento).
- DPIA (Avaliações de Impacto à Proteção de Dados).
- Matriz de Riscos, Heatmaps e Planos de Ação.
- Política de Aceitação de Riscos e Risk Register.
- Procedimento de Incidentes de Segurança.
- Plano de Continuidade de Negócios (BCP) e Procedimento de Backup.
- Programa de Awareness Contínuo.
- Plano de Comunicação de Crise.
- Programa de Due Diligence de Terceiros.
- Checklists e Pacotes de Evidências LGPD.

4.5 RESPONSABILIDADES

4.5.1 Da Ê-SISTEMAS

A Ê-SISTEMAS compromete-se a:

I – Manter e atualizar o Programa de Compliance.

II – Implementar controles internos adequados.

III – Promover treinamentos e ações de conscientização.

IV – Monitorar riscos legais, regulatórios e operacionais.

V – Adotar medidas corretivas em caso de não conformidade.

VI – Proteger dados pessoais e informações confidenciais, nos termos da LGPD.

4.5.2 Dos Colaboradores e Terceiros

Todos os abrangidos por esta Política devem:

I – Conhecer e cumprir esta Política e documentos correlatos.

II – Atuar de forma ética, legal e responsável.

III – Comunicar suspeitas de irregularidades ou violações.

IV – Cooperar com auditorias e investigações internas.

V – Proteger informações e dados sob sua responsabilidade.

4.6 PREVENÇÃO E GESTÃO DE RISCOS

A Ê-SISTEMAS adota abordagem sistemática de gestão de riscos, incluindo:

- Identificação, análise e avaliação de riscos.
- Classificação por impacto e probabilidade.
- Elaboração de planos de ação para riscos altos.
- Aceitação formal de riscos residuais, quando aplicável.
- Registro centralizado de riscos aceitos.
- Revisões periódicas e melhoria contínua.

4.7 COMPLIANCE EM PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO

O tratamento de dados pessoais observa rigorosamente a Lei Geral de Proteção de Dados Pessoais (LGPD), bem como princípios de segurança da informação.

A Ê-SISTEMAS poderá atuar como Controladora ou Operadora, conforme o contexto contratual, observando:

- Bases legais adequadas.
- Minimização de dados.
- Segurança técnica e administrativa.
- Direitos dos titulares.
- Gestão de incidentes e comunicação adequada.

4.8 CANAIS DE COMUNICAÇÃO E INCIDENTES

A Ê-SISTEMAS mantém canais adequados para:

- Comunicação de dúvidas sobre compliance.
- Relato de incidentes de segurança.
- Comunicação de violações éticas ou legais.

Todos os relatos serão tratados com confidencialidade, boa-fé e sem retaliação.

4.9 TREINAMENTO E AWARENESS

A empresa mantém Programa de Awareness Contínuo, com ações periódicas de capacitação sobre:

- Compliance.
- Ética.
- Proteção de dados pessoais.
- Segurança da informação.
- Boas práticas operacionais.

4.10 SANÇÕES E MEDIDAS DISCIPLINARES

O descumprimento desta Política poderá resultar em:

- Medidas corretivas.
- Advertências.
- Suspensão.
- Rescisão contratual.
- Responsabilização civil, administrativa ou penal, conforme o caso.

4.11 DO ACEITE ELETRÔNICO E VALIDADE JURÍDICA

O presente documento poderá ser aceito por meio eletrônico, possuindo o aceite eletrônico plena validade jurídica, produzindo os mesmos efeitos legais de uma assinatura manuscrita, nos termos da legislação brasileira aplicável, em especial o Código Civil, o Marco Civil da Internet (Lei nº 12.965/2014), a Lei nº 14.063/2020 e a Lei Geral de Proteção de Dados Pessoais – LGPD.

O aceite ocorrerá mediante manifestação inequívoca de concordância, incluindo, mas não se limitando a:

I – Marcação de caixa de seleção (“checkbox”) indicando concordância.

II – Clique em botão identificado como “Li e concordo”, “Aceito” ou equivalente.

III – Assinatura eletrônica por plataformas digitais.

IV – Continuidade do vínculo contratual ou uso dos sistemas após a disponibilização desta Política.

A Ê-SISTEMAS poderá manter registros eletrônicos do aceite, incluindo data, hora, endereço IP, identificação do usuário e versão do documento, exclusivamente para fins de comprovação, auditoria e cumprimento legal, em conformidade com a LGPD.

4.12 ATUALIZAÇÕES

Esta Política poderá ser revisada e atualizada a qualquer tempo. A versão vigente estará disponível nos canais oficiais da Ê-SISTEMAS, sendo a continuidade do vínculo considerada como aceitação das alterações.

4.13 LEGISLAÇÃO APLICÁVEL E FORO

Esta Política é regida pelas leis da República Federativa do Brasil.

Fica eleito o foro da comarca da sede da Ê-SISTEMAS, salvo disposição legal diversa.

4.14 DISPOSIÇÕES FINAIS

Esta Política integra formalmente o Programa de Governança, Compliance, Privacidade e Segurança da Informação da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., devendo ser interpretada em conjunto com os demais documentos institucionais.

5 CÓDIGO DE ÉTICA E CONDUTA

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

5.1 OBJETIVO E ABRANGÊNCIA

O presente Código de Ética e Conduta estabelece os princípios, valores e diretrizes que norteiam a atuação da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA, devendo ser observado por seus sócios, administradores, colaboradores, prestadores de serviços, parceiros comerciais e fornecedores, em todas as atividades profissionais, internas ou externas.

O cumprimento deste Código é condição essencial para a manutenção de qualquer vínculo com a empresa.

5.2 PRINCÍPIOS FUNDAMENTAIS

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA pauta suas atividades pelos seguintes princípios:

I – Legalidade e conformidade com a legislação vigente.

II – Ética, integridade e boa-fé.

III – Transparência nas relações comerciais e institucionais.

IV – Respeito às pessoas, à diversidade e à dignidade humana.

V – Responsabilidade social, profissional, ambiental e tecnológica.

VI – Proteção de dados pessoais e informações confidenciais.

VII – Compromisso com práticas sustentáveis no desenvolvimento e operação de soluções tecnológicas.

5.3 CONFORMIDADE LEGAL E REGULATÓRIA

Todos os envolvidos devem cumprir integralmente as leis, normas e regulamentos aplicáveis às atividades da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA, incluindo, mas não se limitando à legislação civil, comercial, trabalhista, tributária, anticorrupção e à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

Nenhuma conduta ilegal ou antiética será tolerada, ainda que sob alegação de interesse comercial ou orientação hierárquica.

5.4 CONDUTA PROFISSIONAL

É esperado que todos atuem com profissionalismo, respeito e responsabilidade, sendo expressamente vedado:

I – Práticas discriminatórias, abusivas ou ofensivas.

II – Assédio moral ou sexual.

III – Uso indevido de informações, sistemas ou recursos da empresa.

IV – Atos que comprometam a reputação, imagem ou credibilidade da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA ou de terceiros.

A empresa providenciará treinamento periódico sobre este Código a todos os destinatários, sempre que necessário ou quando houver atualização relevante.

As relações com clientes, parceiros e colegas devem ser pautadas pela urbanidade, transparência e boa-fé.

5.5 ANTICORRUPÇÃO E INTEGRIDADE

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA adota política de tolerância zero à corrupção, sendo proibido:

I – Oferecer, prometer, solicitar ou aceitar vantagens indevidas.

II – Praticar atos de corrupção, fraude ou suborno, direta ou indiretamente.

III – Manipular informações, documentos ou resultados.

IV – Facilitar ou acobertar práticas ilegais por terceiros.

5.6 CONFLITO DE INTERESSES

Todos devem evitar situações em que interesses pessoais, financeiros ou profissionais possam influenciar ou aparentar influenciar decisões tomadas em nome da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Situações de potenciais conflitos de interesses devem ser comunicadas imediatamente à administração da empresa.

Incluem-se, a título exemplificativo, situações em que:

I – Há relação familiar com fornecedor.

II – Possui participação em empresa concorrente.

III – Presta serviços paralelos que competem com a empresa.

5.7 PROTEÇÃO DE DADOS E CONFIDENCIALIDADE

As informações confidenciais, estratégicas, comerciais, técnicas ou relacionadas a dados pessoais devem ser tratadas com sigilo absoluto.

É dever de todos:

I – Utilizar dados pessoais apenas para finalidades legítimas e autorizadas.

II – Cumprir integralmente a LGPD e as políticas internas de proteção de dados.
III – Adotar medidas de segurança para prevenir acessos, usos ou divulgações indevidas.

A obrigação de confidencialidade permanece vigente mesmo após o encerramento do vínculo com a empresa.

5.8 USO DE SISTEMAS E RECURSOS TECNOLÓGICOS

Os sistemas, softwares, equipamentos e acessos disponibilizados pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA devem ser utilizados exclusivamente para fins profissionais, de forma ética, segura e responsável.
É vedado:
I – Compartilhar senhas ou credenciais de acesso.
II – Utilizar sistemas para fins ilícitos ou não autorizados.
III – Tentar burlar controles de segurança ou auditoria.

5.9 COMUNICAÇÃO E RELACIONAMENTO COM O MERCADO

A comunicação institucional da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA deve ser clara, verdadeira e responsável.
É proibida a divulgação de informações falsas, enganosas ou que possam induzir terceiros a erro, bem como o uso indevido da marca, nome, imagem ou reputação da empresa.
Atuar em conformidade com as leis de defesa da concorrência, não praticando dumping, cartelização ou outras práticas anticompetitivas.

5.10 CONFORMIDADE COM SANÇÕES INTERNACIONAIS

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA observa e cumpre todas as sanções e embargos internacionais aplicáveis, não realizando negócios com pessoas, empresas ou países sob restrições.

5.11 PRESENTES E ENTRETENIMENTO

Presentes, cortesias ou entretenimento oferecidos a ou recebidos de clientes/fornecedores devem ser simbólicos, não frequentes e não podem influenciar decisões comerciais. Devendo, quando aplicável, ser previamente comunicados à administração.

5.12 PROPRIEDADE INTELECTUAL

Respeitar direitos de propriedade intelectual de terceiros e proteger os ativos de PI da empresa, incluindo códigos-fonte, algoritmos, marcas e know-how.

5.13 CANAL DE COMUNICAÇÃO E DENÚNCIAS

Qualquer violação a este Código, à legislação vigente ou às políticas internas poderá ser comunicada por meio dos canais oficiais da empresa.

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA assegura confidencialidade e veda qualquer forma de retaliação contra quem, de boa-fé, realizar comunicações ou denúncias.

5.14 CONSEQUÊNCIAS PELO DESCUMPRIMENTO

O descumprimento deste Código poderá resultar na aplicação de medidas disciplinares, incluindo advertência, rescisão contratual e demais responsabilizações cabíveis nas esferas civil, administrativa e penal, conforme o caso.

5.15 DISPOSIÇÕES FINAIS

Este Código entra em vigor na data de sua publicação e deverá ser observado por todos os seus destinatários.

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA poderá revisá-lo e atualizá-lo sempre que necessário, comprometendo-se a divulgar as alterações de forma adequada.

Todos os destinatários deverão declarar por escrito que leram, compreenderam e comprometem-se a cumprir este Código.

6 KIT DE GOVERNANÇA EM PRIVACIDADE

ÍNDICE GERAL DE GOVERNANÇA (MASTER INDEX)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento consolidado do Programa de Governança em Privacidade e Segurança da Informação, nos termos da Lei nº 13.709/2018 (LGPD), especialmente do art. 50.

6.1 FINALIDADE DO KIT DE GOVERNANÇA

O presente Kit de Governança Ê-SISTEMAS tem por finalidade organizar, integrar e indexar todos os documentos, políticas, procedimentos, registros e evidências relacionados à proteção de dados pessoais, segurança da informação, gestão de riscos e continuidade de negócios da empresa.

Este Índice Geral:

- Facilita auditorias e fiscalizações (ANPD).
- Demonstra **accountability** e governança estruturada.
- Permite rápida localização de evidências.
- Consolida a maturidade do Programa de Privacidade.

6.2 ESTRUTURA DO PROGRAMA DE GOVERNANÇA

O Programa de Governança da Ê-SISTEMAS está estruturado nos seguintes eixos fundamentais:

I – Governança e Compliance.

II – Privacidade e Proteção de Dados.

III – Segurança da Informação.

IV – Gestão de Riscos.

V – Continuidade e Resiliência.

VI – Relacionamento com Titulares e Clientes

VII – Terceiros e Cadeia de Tratamento.

VIII – Conscientização (Awareness).

IX – Resposta a Incidentes e Crise

X – Evidências, Monitoramento e Melhoria Contínua

6.3 ÍNDICE GERAL DOS DOCUMENTOS DE GOVERNANÇA

6.3.1 Governança, Compliance e Direcionamento Estratégico

- Programa de Governança em Privacidade.

- Código de Ética e Conduta.
- Termo de Ciência e Compromisso (assinatura eletrônica).
- Política de Aceitação de Riscos.
- Checklist de Evidências LGPD.
- Kit de Governança – Índice Geral (este documento).

6.3.2 Privacidade e Proteção de Dados Pessoais

- Política de Privacidade (clientes e usuários).
- Aviso de Privacidade / Privacidade do Cliente.
- Termo do Usuário (Termos de Uso).
- Cláusula de Aceite Eletrônico.
- Registro de consentimentos (quando aplicável).
- Procedimento de Atendimento aos Titulares (DSAR).

6.3.3 Segurança da Informação

- Política de Segurança da Informação (PSI).
- Termo de Uso Aceitável da Informação (TUA).
- Procedimento de Controle de Acesso.
- Procedimento de Backup e Recuperação.
- Registros de logs e monitoramento.
- Inventário de ativos e sistemas.

6.3.4 Gestão de Riscos e Avaliações de Impacto

- Avaliação de Impacto à Proteção de Dados (DPIA – Geral).
- DPIA específico para tratamento de dados sensíveis (saúde).
- Matriz de Risco (Impacto × Probabilidade).
- Heatmap de Riscos – Geral.
- Heatmap de Riscos – Dados Sensíveis (Saúde / nível ANPD).
- Plano de Ação para Tratamento de Riscos Altos.

6.3.5 Aceitação e Registro de Riscos

- Registro Centralizado de Riscos Aceitos (Risk Register).
- Formulário de Aceitação Formal de Risco (Risk Acceptance Form).
- Pareceres do DPO.

- Registros de reavaliação de riscos.

6.3.6 Continuidade de Negócios e Resiliência

- Plano de Continuidade de Negócios (BCP).
- Procedimento de Backup e Recuperação (anexo ao BCP).
- Plano de Recuperação de Desastres (quando aplicável).
- Testes de continuidade e evidências de execução.

6.3.7 Incidentes de Segurança e Comunicação de Crise

- Procedimento de Incidentes de Segurança.
- Plano de Comunicação de Crise.
- Modelos de comunicação:
    - Comunicação à ANPD.
    - Comunicação aos titulares.
    - Comunicação a clientes e parceiros.
- Registro de incidentes e lições aprendidas

6.3.8 Terceiros e Cadeia de Tratamento

- Programa de Due Diligence de Terceiros.
- Questionário de fornecedores (baixo, médio e alto risco).
- Classificação de risco de fornecedores.
- Contratos com cláusulas de proteção de dados.
- Acordos de Operador (DPA / Data Processing Agreement).

6.3.9 Conscientização e Cultura Organizacional

- Programa de Awareness contínuo em LGPD e Segurança.
- Materiais de treinamento.
- Registros de participação.
- Comunicações internas periódicas.

6.3.10 Evidências, Auditoria e Melhoria Contínua

- Checklist de Evidências LGPD.
- Registros de auditorias internas.
- Planos de melhoria continua.

- Indicadores de maturidade.
- Alinhamento à ISO 27001 / ISO 27701.

6.4 PAPÉIS E RESPONSABILIDADES

- **Administração:** direção estratégica, aprovação e apetite de risco.
- **DPO / Encarregado:** supervisão, pareceres e conformidade LGPD.
- **TI / Segurança:** controles técnicos e operacionais.
- **Colaboradores:** cumprimento das políticas e procedimentos.

6.5 ORGANIZAÇÃO E CONTROLE DO KIT

Todos os documentos integrantes deste Kit:

- Possuem versão, data e responsável.
- Estão sujeitos a revisão periódica.
- Devem ser armazenados em ambiente seguro.
- Podem ser apresentados à ANPD, clientes ou auditores quando solicitado.

6.6 VIGÊNCIA E APROVAÇÃO

Este Índice Geral entra em vigor na data de sua aprovação e deverá refletir sempre a versão mais atual do Programa de Governança em Privacidade da Ê-SISTEMAS.

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: ____ / ____ / _____

7 PROGRAMA DE AWARENESS CONTÍNUO

Privacidade, LGPD e Segurança da Informação.

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade e Segurança da Informação.

7.1 OBJETIVO

O presente Programa de Awareness Contínuo tem por objetivo promover a conscientização permanente de colaboradores, prestadores de serviço e parceiros da Ê-SISTEMAS quanto à proteção de dados pessoais, à segurança da informação e às responsabilidades legais decorrentes da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

O programa visa:

I – Reduzir riscos operacionais e regulatórios.

II – Prevenir incidentes de segurança e violações de dados.

III – Fortalecer a cultura organizacional de privacidade e segurança.

IV – Demonstrar conformidade com os princípios da accountability, prevenção e governança.

7.2 ABRANGÊNCIA

Este Programa aplica-se a:

I – Colaboradores internos, independentemente do vínculo ou cargo.

II – Prestadores de serviços, terceirizados e parceiros com acesso a dados pessoais ou sistemas.

III – Estagiários, trainees e temporários.

IV – Administração e alta gestão.

7.3 FUNDAMENTAÇÃO LEGAL E NORMATIVA

O Programa está fundamentado em:

I – Lei nº 13.709/2018 (LGPD).

II – Marco Civil da Internet (Lei nº 12.965/2014).

III – Normas de boas práticas de segurança da informação.

IV – Política de Segurança da Informação (PSI).

V – Política de Privacidade.

VI – DPIA, Matriz de Risco, Heatmap e Plano de Ação.

VII – Política de Aceitação de Riscos.

VIII – Procedimento de Gestão de Incidentes.

7.4 PRINCÍPIOS DO PROGRAMA

O Programa de Awareness é regido pelos seguintes princípios:

I – Continuidade e atualização permanente.

II – Clareza e acessibilidade das informações.

III – Proporcionalidade ao nível de risco.

IV – Responsabilização individual.

V – Registro e rastreabilidade das ações educativas.

7.5 CONTEÚDOS ABORDADOS

O Programa contempla, no mínimo, os seguintes temas:

7.5.1 Privacidade e LGPD

I – Conceitos básicos de dados pessoais e dados sensíveis.

II – Papéis de Controlador, Operador e DPO.

III – Bases legais de tratamento.

IV – Direitos dos titulares.

V – Responsabilidades individuais.

7.5.2 Segurança da Informação

I – Confidencialidade, integridade e disponibilidade da informação.

II – Uso seguro de sistemas, senhas e dispositivos.

III – Prevenção contra phishing, engenharia social e malware.

IV – Uso aceitável da informação e dos recursos tecnológicos.

7.5.3 Incidentes e Riscos

I – Identificação de incidentes de segurança.

II – Procedimento de comunicação interna de incidentes.

III – Importância do monitoramento e do reporte imediato.

IV – Consequências legais, administrativas e reputacionais.

7.5.4 Continuidade e Governança

I – Noções básicas de continuidade de negócios (BCP).

II – Backup e recuperação.

III – Cultura de prevenção e melhoria contínua.

7.6 FORMAS DE EXECUÇÃO DO AWARENESS

O Awareness será realizado de forma contínua, por meio de:

I – Treinamentos periódicos (presenciais ou online).

II – Materiais educativos (cartilhas, e-mails, comunicados internos).

III – Campanhas de conscientização.

IV – Comunicados sobre incidentes reais ou simulados.

V – Atualizações sempre que houver mudanças relevantes nos processos ou legislação.

7.7 PERIODICIDADE

O Programa observará, no mínimo:

I – Treinamento inicial na admissão ou início da prestação de serviços.

II – Atualizações periódicas obrigatórias.

III – Treinamentos extraordinários em caso de:

III.I – Incidentes relevantes.

III.II – Atualizações da LGPD ou normas internas.

III.III – Alterações significativas nos tratamentos de dados.

7.8 RESPONSABILIDADES

7.8.1 Encarregado de Proteção de Dados (DPO)

I – Coordenar o Programa de Awareness.

II – Definir conteúdos e prioridades.

III – Manter registros das ações realizadas.

IV – Reportar à Administração os resultados e necessidades de melhoria.

7.8.2 Administração

I – Apoiar institucionalmente o Programa.

II – Garantir recursos e engajamento.

III – Promover a cultura de privacidade e segurança.

7.8.3 Colaboradores e Terceiros

I – Participar das ações de awareness.

II – Cumprir políticas e procedimentos internos.

III – Comunicar incidentes ou riscos identificados.

7.9 REGISTRO E COMPROVAÇÃO

As ações do Programa serão documentadas por meio de:

I – Listas de presença ou registros eletrônicos.

II – Logs de treinamentos online.

III – Materiais distribuídos

IV – Evidências de campanhas internas.

Os registros serão mantidos para fins de:

I – Auditorias internas e externas.

II – Fiscalização da ANPD.

III – Demonstração de accountability.

7.10 MEDIDAS DISCIPLINARES

O descumprimento das diretrizes de privacidade e segurança, quando decorrente de negligência, imprudência ou dolo, poderá resultar em medidas administrativas, sem prejuízo das responsabilidades civis, trabalhistas e legais aplicáveis.

7.11 REVISÃO E ATUALIZAÇÃO

Este Programa será revisado:

I – Periodicamente.

II – Sempre que houver mudanças relevantes na legislação ou nos processos.

III – Após incidentes relevantes de segurança da informação.

7.12 VIGÊNCIA E APROVAÇÃO

Este Programa entra em vigor na data de sua aprovação e integra o Programa de Governança em Privacidade e Segurança da Informação da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: ____ / ____ / _____

8 TERMO DE CIÊNCIA E COMPROMISSO

CÓDIGO DE ÉTICA E CONDUTA

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Pelo presente instrumento eletrônico, eu, _____,

CPF nº _____, declaro, para os devidos fins, que:

1. Recebi, li e compreendi integralmente o Código de Ética e Conduta da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA, estando plenamente ciente de seus princípios, regras e diretrizes.
2. Comprometo-me a cumprir integralmente todas as disposições previstas no referido Código, bem como a legislação vigente aplicável, especialmente as normas relacionadas à ética, integridade, anticorrupção, confidencialidade, uso adequado de recursos tecnológicos e proteção de dados pessoais, nos termos da Lei nº 13.709/2018 (LGPD).
3. Tenho ciência de que o descumprimento das normas estabelecidas no Código de Ética e Conduta poderá ensejar a aplicação de medidas disciplinares, incluindo advertência, rescisão contratual e demais responsabilizações cabíveis nas esferas civil, administrativa e penal, conforme a natureza do vínculo e a legislação aplicável.
4. Declaro estar ciente de que eventuais situações de conflito de interesses, bem como dúvidas éticas ou suspeitas de irregularidades, deverão ser comunicadas imediatamente à administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA, por meio dos canais oficiais disponibilizados.
5. Reconheço que a obrigação de confidencialidade sobre informações estratégicas, comerciais, técnicas ou dados pessoais subsiste antes, durante e após o encerramento do vínculo com a empresa.
6. Declaro que este Termo é celebrado em meio eletrônico, possuindo plena validade jurídica, nos termos do art. 10, §2º, da Medida Provisória nº 2.200-2/2001, sendo a assinatura eletrônica suficiente para comprovar minha manifestação de vontade.
7. Estou ciente de que este Termo integra o meu vínculo profissional, contratual ou comercial com a Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA, produzindo todos os efeitos legais.

E, por estar de pleno acordo com seu conteúdo, assino eletronicamente o presente Termo.

Assinatura Eletrônica do(a) Declarante:

Nome completo: _____

CPF: _____

Local (opcional): _____ Data (opcional):_____/_____/_____

Assinatura Eletrônica da Empresa:

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Registro eletrônico:

Data e hora da assinatura eletrônica: Registradas automaticamente pela plataforma de assinatura digital.

9 POLÍTICA DE PRIVACIDADE

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Esta Política de Privacidade descreve como o sistema de chatbot da Ê-Sistemas coleta, usa e compartilha suas informações quando você utiliza nossos serviços. Valorizamos a sua privacidade e estamos comprometidos em proteger seus dados pessoais de acordo com a Lei nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados) e outras regulamentações aplicáveis.

9.1 QUAIS DADOS PESSOAIS SÃO COLETADOS

Para fornecer e melhorar nossos serviços de chatbot, podemos coletar e tratar os seguintes tipos de dados pessoais, conforme necessário para as finalidades específicas:

Dados de Cadastro: Quando você interage com nosso chatbot, podemos solicitar informações como seu nome, e-mail, CPF (somente será solicitado quando estritamente necessário para fins de identificação, cumprimento legal ou execução contratual), e número de telefone para identificação e personalização do atendimento. Esses dados são coletados apenas se você os fornecer voluntariamente.

Dados de Utilização e Interação: Coletamos informações sobre como você interage com o chatbot, incluindo o conteúdo das suas mensagens, comandos utilizados, data e hora das interações, e informações técnicas sobre o dispositivo que você usa (como tipo de dispositivo, sistema operacional e endereço IP). Esses dados nos ajudam a entender o uso do serviço e a aprimorar a experiência do usuário.

Dados para Funcionamento do Chatbot: Para o correto funcionamento do chatbot, podemos tratar dados como o histórico de conversas, preferências de idioma, status e horário de trabalho; o conteúdo das mensagens pré formatadas do chatbot e as suas respostas; dados para configuração do chatbot e outras configurações que você possa definir. Em alguns casos, se o chatbot for integrado a outros sistemas, dados adicionais podem ser processados para fornecer a funcionalidade solicitada.

Dados Pessoais Sensíveis: O chatbot não tem como finalidade a coleta ou o tratamento de dados pessoais sensíveis, nos termos do art. 5º, II, da Lei nº 13.709/2018 (LGPD). Eventualmente, o titular poderá, por iniciativa própria, informar dados sensíveis (como dados de saúde, convicção religiosa, filiação sindical, opinião política ou outros), hipótese em que tais informações serão tratadas de forma pontual e limitada, exclusivamente para possibilitar a resposta à solicitação

realizada. A empresa não solicita nem incentiva o fornecimento de dados pessoais sensíveis, recomendando que o titular evite o seu compartilhamento, salvo quando estritamente necessário. O tratamento desses dados observará as bases legais do art. 11 da LGPD e adotará medidas de segurança técnicas e administrativas para a proteção das informações.

Outras Informações: Qualquer outra informação que você voluntariamente nos forneça durante suas interações com o chatbot ou através de outros canais de comunicação.

9.2 COMO UTILIZAMOS SEUS DADOS PESSOAIS

Utilizamos seus dados pessoais para diversas finalidades, sempre de acordo com a sua interação com o nosso sistema de chatbot. Os principais propósitos para os quais coletamos, processamos ou tratamos seus dados pessoais incluem:

Para Fornecer e Gerenciar o Serviço de Chatbot: Utilizamos seus dados para permitir a funcionalidade do chatbot, responder às suas perguntas, executar comandos e fornecer as informações ou serviços solicitados.

Para Melhorar a Experiência do Usuário: Analisamos os dados de utilização e interação para entender como o chatbot é utilizado, identificar áreas de melhoria e desenvolver novas funcionalidades que tornem a sua experiência mais eficiente e agradável.

Para Comunicação: Podemos usar seus dados para responder a dúvidas, elogios, reclamações ou sugestões que você nos envie, bem como para comunicar informações importantes sobre o serviço, atualizações ou problemas técnicos.

Para Marketing e Promoção (com seu consentimento): Com seu consentimento explícito, podemos utilizar seus dados para enviar newsletters, informações sobre novos recursos, promoções ou outros conteúdos relacionados aos nossos serviços de chatbot.

Para Segurança e Prevenção de Fraudes: Tratamos seus dados para garantir a segurança do nosso sistema de chatbot, monitorar atividades suspeitas e proteger contra acessos não autorizados ou outras ameaças cibernéticas.

Para Cumprimento de Obrigações Legais: Em certas situações, podemos ser obrigados a tratar ou compartilhar seus dados pessoais para cumprir com obrigações legais, regulatórias ou ordens judiciais.

9.3 SEUS DIREITOS COMO TITULAR DOS DADOS PESSOAIS

Como titular dos dados pessoais, você possui os seguintes direitos, garantidos pela LGPD:

Confirmação e Acesso: Você tem o direito de confirmar a existência de tratamento de seus dados e de acessá-los.

Correção: Você pode solicitar a correção de dados incompletos, inexatos ou desatualizados.

Anonimização, Bloqueio ou Eliminação: Você pode solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
Portabilidade: Você tem o direito à portabilidade dos seus dados a outro fornecedor de serviço ou produto, mediante requisição expressa.
Eliminação: Você pode solicitar a eliminação dos dados pessoais tratados com o seu consentimento, exceto nas hipóteses previstas em lei.
Informação sobre Compartilhamento: Você tem o direito de ser informado sobre as entidades públicas e privadas com as quais seus dados são compartilhados.
Revogação do Consentimento: Você pode revogar o consentimento a qualquer momento, sem que isso afete a legalidade do tratamento realizado antes da revogação.
Oposição: Você pode se opor a tratamentos de dados que não estejam em conformidade com a LGPD.

9.4 MECANISMO DE EXERCÍCIO DE DIREITOS DOS TITULARES

O titular dos dados pessoais poderá exercer, a qualquer momento, os direitos previstos na Lei Geral de Proteção de Dados, mediante solicitação formal encaminhada pelos canais disponibilizados nesta Política.
O processo de atendimento às solicitações observará as seguintes etapas:
I – Recebimento da solicitação, por meio dos canais oficiais indicados.
II – Verificação da identidade do titular, com a finalidade de garantir a segurança e evitar acessos não autorizados.
III – Análise da viabilidade da solicitação, considerando a natureza do pedido e as obrigações legais e regulatórias aplicáveis.
IV – Resposta ao titular, de forma clara e objetiva, no prazo de até 15 (quinze) dias, contado a partir do recebimento da solicitação válida, conforme previsto na legislação vigente.
Em determinadas hipóteses, a solicitação poderá ser parcialmente atendida ou indeferida, mediante justificativa fundamentada, quando houver impedimento legal, regulatório ou técnico, nos termos da LGPD.

9.5 MECANISMO DE EXERCÍCIO DE DIREITOS DOS TITULARES - ATUAÇÃO COMO OPERADOR DE DADOS

Na condição de operador de dados pessoais, o tratamento das informações é realizado de acordo com as instruções do controlador, nos termos da Lei Geral de Proteção de Dados.

Caso o operador receba diretamente solicitações de titulares relacionadas ao exercício de direitos previstos na LGPD, o operador adotará as seguintes medidas:

I – Registro da solicitação recebida.

II – Verificação da identidade do solicitante, quando aplicável, para fins de segurança.

III – Encaminhamento da solicitação ao controlador, em prazo razoável, para análise e deliberação.

IV – Apoio técnico e operacional ao controlador, quando necessário, para viabilizar o atendimento da solicitação, conforme as instruções recebidas.

O atendimento ao titular, a análise do pedido e o prazo de resposta observarão as diretrizes legais aplicáveis e serão de responsabilidade exclusiva do controlador.

9.6 TEMPO DE TRATAMENTO DOS DADOS COLETADOS

Os dados pessoais coletados pelo nosso sistema de chatbot serão armazenados e tratados pelo tempo necessário para cumprir as finalidades para as quais foram coletados, conforme descrito nesta Política de Privacidade, e em conformidade com a legislação aplicável.

Os períodos de retenção podem variar dependendo do tipo de dado, da finalidade do tratamento e das obrigações legais ou regulatórias.

Após o término do período de tratamento, os dados pessoais serão eliminados, a menos que a manutenção seja autorizada por lei, como para cumprimento de obrigação legal ou regulatória, estudo por órgão de pesquisa (garantindo a anonimização sempre que possível), ou para uso exclusivo do controlador, vedado seu acesso por terceiros, e desde que anonimizados.

9.7 BASE LEGAL PARA O TRATAMENTO DE DADOS

O tratamento dos seus dados pessoais é realizado com base nas seguintes hipóteses legais, conforme o Artigo 7º da LGPD:

Consentimento do titular: Quando você nos dá permissão para tratar seus dados para uma finalidade específica.

Execução de contrato: Para cumprir um contrato ou realizar procedimentos preliminares relacionados a um contrato do qual você seja parte.

Cumprimento de obrigação legal ou regulatória: Para atender a determinações legais ou regulatórias.

Exercício regular de direitos: Para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais.

Legítimo interesse: Quando o tratamento é necessário para atender aos interesses legítimos do nosso sistema de chatbot ou de terceiros, desde que seus direitos e liberdades fundamentais não sejam violados.

Proteção da vida ou incolumidade física: Quando o tratamento é essencial para proteger a vida ou a segurança física do titular ou de terceiros.

Proteção ao crédito: Para a proteção do crédito, conforme a legislação aplicável.

Para dados pessoais sensíveis (Artigo 11 da LGPD), o tratamento pode ocorrer com base em:

. Consentimento específico e destacado do titular.

. Cumprimento de obrigação legal ou regulatória.

. Exercício regular de direitos.

. Proteção da vida ou incolumidade física.

. Garantia da prevenção à fraude e à segurança do titular.

9.8 POLÍTICA DE COOKIES

Nosso site e sistema de chatbot podem utilizar cookies e tecnologias similares para melhorar sua experiência de navegação, personalizar conteúdo, analisar o tráfego e para fins de marketing. Cookies são pequenos arquivos de texto armazenados em seu dispositivo que nos permitem reconhecê-lo em visitas futuras.

Utilizamos cookies para diversas finalidades, como lembrar suas preferências, manter você logado e coletar informações sobre como você interage com nossos serviços. Podemos utilizar, tanto cookies primários (definidos por nós) quanto cookies de terceiros (definidos por parceiros, como serviços de análise ou publicidade).

O uso de cookies não essenciais dependerá do consentimento prévio do usuário, conforme aplicável.

As práticas de privacidade de cookies de terceiros são regidas pelas políticas de privacidade desses terceiros, sobre as quais não temos controle. Recomendamos que você consulte as políticas de privacidade desses terceiros para entender como eles utilizam seus dados.

Você pode, a qualquer momento, gerenciar suas preferências de cookies através das configurações do seu navegador. A maioria dos navegadores permite que você bloqueie ou exclua cookies. No entanto, ao desativar os cookies, algumas funcionalidades do nosso site ou sistema de chatbot podem não funcionar corretamente.

9.9 ATUALIZAÇÃO DA POLÍTICA

Esta Política de Privacidade poderá ser alterada a qualquer momento, para refletir mudanças na legislação ou em nossos serviços. Sempre que isso ocorrer, comunicaremos de forma clara os usuários sobre as atualizações relevantes. As atualizações relevantes serão comunicadas por meio do site, do sistema ou por outros canais oficiais. Recomendamos a leitura periódica deste documento.

9.10 FALE CONOSCO

Se você tiver dúvidas sobre esta Política de Privacidade, sobre como seus dados são tratados ou se desejar exercer seus direitos como titular dos dados, entre em contato conosco através do seguinte canal:

Encarregado e DPO (Data Protection Officer): Thiago Marcos Montagner.

E-mail: thiagomarcosmontagner@hotmail.com

Nosso Encarregado de Proteção de Dados estará à disposição para atendê-lo e esclarecer quaisquer questões relacionadas à proteção de seus dados pessoais.

9.11 BANNER DE COOKIES PARA INSERIR NO SITE

Ao selecionar 'Aceitar todos os cookies', você autoriza a manutenção dos cookies em seu dispositivo. Isso possibilita melhorar a navegação no site e personalizar a experiência do usuário. Consulte nossa Política de Privacidade.

Comandos do usuário:

I – Aceitar todos os cookies.

II – Rejeitar todos.

III – Customizar.

10 POLÍTICA DE PRIVACIDADE DO CLIENTE

(Proteção de Dados Pessoais – LGPD)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

10.1 OBJETIVO

A presente Política de Privacidade do Cliente tem por objetivo informar, de forma clara, transparente e acessível, como a Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA. realiza o tratamento de dados pessoais de seus clientes, usuários e representantes, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e com as boas práticas de governança em privacidade e segurança da informação.

Esta Política demonstra o compromisso da empresa com a proteção da privacidade, a segurança da informação e os direitos dos titulares de dados.

10.2 APLICAÇÃO E ABRANGÊNCIA

Esta Política aplica-se aos dados pessoais tratados pela Ê-SISTEMAS no contexto de:

I – Prestação de serviços tecnológicos.

II – Uso de sistemas, plataformas, softwares e chatbots.

III – Relacionamento comercial com clientes e parceiros.

IV – Suporte técnico, atendimento e comunicação.

V – Cumprimento de obrigações legais e contratuais.

10.3 DEFINIÇÕES IMPORTANTES

Para fins desta Política, aplicam-se as definições da LGPD, especialmente:

I – Dados pessoais: informação relacionada a pessoa natural identificada ou identificável.

II – Dados pessoais sensíveis: dados sobre saúde, biometria, origem racial, convicções religiosas, entre outros definidos em lei.

III – Titular: pessoa natural a quem se referem os dados pessoais.

IV – Controlador: quem decide sobre o tratamento de dados pessoais.

V – Operador: quem realiza o tratamento em nome do controlador.

VI – Tratamento: toda operação realizada com dados pessoais.

10.4 PAPEL DA Ê-SISTEMAS NO TRATAMENTO DE DADOS

A Ê-SISTEMAS poderá atuar:

I – Como controladora, quando define as finalidades e meios do tratamento.

II – Como operadora, quando trata dados pessoais conforme instruções documentadas de seus clientes (controladores).

10.5 DADOS PESSOAIS TRATADOS

10.5.1 Dados pessoais comuns

Podem incluir, conforme a relação estabelecida:

I – Nome completo.

II – CPF ou CNPJ.

III – E-mail.

IV – Telefone.

V – Dados profissionais.

VI – Registros de acesso e logs.

VII – Informações fornecidas em formulários ou sistemas.

10.5.2 Dados pessoais sensíveis

Somente tratados quando estritamente necessários, como:

I – Dados relacionados à saúde, quando vinculados à finalidade específica do serviço contratado (ex.: chatbot de saúde).

10.6 FINALIDADES DO TRATAMENTO

Os dados pessoais são tratados para:

I – Prestação e gestão dos serviços contratados.

II – Execução de contratos e obrigações assumidas.

III – Suporte técnico e atendimento ao cliente.

IV – Comunicação operacional e institucional.

V – Segurança da informação e prevenção a fraudes.

VI – Cumprimento de obrigações legais e regulatórias.

10.7 BASES LEGAIS

O tratamento de dados pessoais ocorre com fundamento, conforme o caso, em:

I – Execução de contrato (art. 7º, V, LGPD).

II – Cumprimento de obrigação legal ou regulatória (art. 7º, II).

III – Exercício regular de direitos (art. 7º, VI).

IV – Consentimento do titular, quando aplicável (art. 7º, I).

V – Para dados sensíveis, hipóteses do art. 11 da LGPD.

10.8 COMPARTILHAMENTO DE DADOS

Os dados pessoais poderão ser compartilhados:

I – Com parceiros e fornecedores contratualmente vinculados.

II – Com operadores de dados, conforme instruções do controlador.

III – Com autoridades públicas, mediante obrigação legal.

Todo compartilhamento observa princípios de necessidade, finalidade e segurança.

10.9 SEGURANÇA DA INFORMAÇÃO

A Ê-SISTEMAS adota medidas técnicas e administrativas aptas a proteger os dados pessoais, incluindo, entre outras:

I – Política de Segurança da Informação (PSI).

II – Controle de acesso baseado em perfis.

III – Criptografia de dados, quando aplicável.

IV – Monitoramento, registros de logs e auditorias.

V – Backup, recuperação e plano de continuidade.

VI – Procedimento de resposta a incidentes.

VII – Treinamento e conscientização de colaboradores.

10.10 RETENÇÃO E ELIMINAÇÃO DOS DADOS

Os dados pessoais são armazenados apenas pelo tempo necessário para cumprir as finalidades informadas, obrigações legais ou contratuais, e posteriormente eliminados ou anonimizados, conforme a Política de Retenção e Destruição de Dados.

10.11 DIREITOS DOS TITULARES

Nos termos da LGPD, o titular poderá solicitar:

I – Confirmação da existência de tratamento.

II – Acesso aos dados.

III – Correção de dados incompletos ou desatualizados.

IV – Anonimização, bloqueio ou eliminação.

V – Portabilidade, quando aplicável.

VI – Informação sobre compartilhamentos.

VII – Revogação do consentimento, quando aplicável.

As solicitações serão tratadas dentro dos prazos legais.

10.12 CANAL DE ATENDIMENTO AO TITULAR (DPO)

Para exercer seus direitos ou esclarecer dúvidas, o titular poderá entrar em contato com o Encarregado de Proteção de Dados (DPO):

E-mail: thiagomarcosmontagner@hotmail.com

Responsável: Thiago Marcos Montagner

10.13 INCIDENTES DE SEGURANÇA

Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, a Ê-SISTEMAS adotará as medidas cabíveis, incluindo comunicação ao controlador, aos titulares e à Autoridade Nacional de Proteção de Dados (ANPD), quando aplicável.

10.14 ALTERAÇÕES DESTA POLÍTICA

Esta Política poderá ser atualizada a qualquer tempo para refletir:

I – Alterações legais ou regulatórias.

II – Mudanças nos tratamentos de dados.

III – Evolução tecnológica ou operacional.

A versão vigente estará sempre disponível aos clientes.

10.15 VIGÊNCIA

Esta Política entra em vigor na data de sua publicação e integra o Programa de Governança em Privacidade da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

11 POLÍTICA DE RETENÇÃO E DESCARTE DE DADOS PESSOAIS

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

11.1 OBJETIVO

Esta Política de Retenção e Descarte de Dados Pessoais estabelece os critérios, prazos e procedimentos adotados pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA para a retenção, armazenamento e eliminação segura de dados pessoais tratados no âmbito de suas atividades, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

11.2 ABRANGÊNCIA

Esta Política aplica-se a todos os sócios, administradores, colaboradores, prestadores de serviços, parceiros e terceiros que realizem operações de tratamento de dados pessoais em nome da Ê-SISTEMAS, independentemente do meio ou formato utilizado.

11.3 FUNDAMENTAÇÃO LEGAL

Esta Política fundamenta-se, especialmente, nos seguintes dispositivos da LGPD:

I – Art. 6º, incisos I (finalidade), III (necessidade) e X (responsabilização).

II – Art. 15 – Término do tratamento de dados pessoais.

III – Art. 16 – Hipóteses legais de conservação dos dados.

IV – Art. 37 – Registro das operações de tratamento (ROPA).

V – Art. 46 – Segurança da informação.

11.4 PRINCÍPIOS APLICÁVEIS À RETENÇÃO DE DADOS

A retenção de dados pessoais observará os seguintes princípios:

I – Limitação da finalidade.

II – Necessidade e minimização de dados.

III – Proporcionalidade.

IV – Segurança e confidencialidade.

V – Responsabilização e prestação de contas.

11.5 PRAZOS DE RETENÇÃO

Os dados pessoais tratados pela Ê-SISTEMAS serão mantidos apenas pelo tempo necessário para cumprir as finalidades que justificaram seu tratamento, observando-se:

11.5.1 Critérios gerais de retenção

Os dados poderão ser conservados enquanto:

I – Houver relação contratual vigente.

II – Forem necessários para cumprimento de obrigação legal ou regulatória.

III – Forem necessários para exercício regular de direitos em processo judicial, administrativo ou arbitral.

IV – Existir legítimo interesse devidamente justificado.

V – Houver consentimento válido do titular, quando aplicável.

11.5.2 Referência aos prazos

Os prazos específicos de retenção estão detalhados no Registro das Operações de Tratamento de Dados (ROPA) e em obrigações legais aplicáveis (trabalhistas, fiscais, contratuais, regulatórias), conforme detalhado no Registro das Operações de Tratamento de Dados (ROPA), parte integrante do Programa de Governança em Privacidade da empresa.

11.6 TÉRMINO DO TRATAMENTO

Encerrada a finalidade do tratamento, os dados pessoais serão eliminados, ressalvadas as hipóteses legais previstas no art. 16 da LGPD.

Exceções: Estudos por órgão de pesquisa (anonimizados), obrigação legal, processo judicial ativo.

11.7 PROCEDIMENTOS DE DESCARTE E ELIMINAÇÃO DE DADOS

A eliminação de dados pessoais será realizada de forma segura, conforme a natureza do dado e o meio de armazenamento, podendo incluir:

I – Exclusão definitiva de bases digitais e sistemas.

II – Anonimização irreversível, quando aplicável.

- II.I Anonimização: Remoção completa de identificadores diretos e indiretos, impossibilitando reidentificação.

III – Destruição física de documentos impressos (fragmentação, trituração ou método equivalente).

IV – Sobrescrita segura de mídias eletrônicas.

A eliminação deverá impedir a recuperação, reconstrução ou acesso indevido às informações.

Descarte programado: Aprovação do DPO + Administração.

Descarte emergencial: DPO pode autorizar, com comunicação posterior.

11.8 RESPONSABILIDADES

11.8.1 Encarregado de Proteção de Dados (DPO)

Compete ao DPO:

I – Orientar sobre os prazos de retenção.

II – Supervisionar os procedimentos de descarte.

III – Garantir alinhamento com o ROPA e demais políticas.

IV – Registrar e documentar as eliminações relevantes, quando necessário.

11.8.2 Colaboradores e Terceiros

Devem:

I – Cumprir esta Política.

II – Não reter dados além do prazo autorizado.

III – Comunicar qualquer retenção indevida ou falha no descarte.

11.9 DADOS TRATADOS POR TERCEIROS

Terceiros e operadores contratados pela Ê-SISTEMAS deverão observar esta Política, comprometendo-se contratualmente a:

I – Respeitar os prazos de retenção definidos.

II – Eliminar os dados ao término da relação contratual.

III – Comprovar o descarte, quando solicitado.

11.10 AUDITORIA E MONITORAMENTO

O cumprimento desta Política poderá ser objeto de:

I – Revisões internas.

II – Auditorias contratuais.

III – Avaliações periódicas de conformidade.

11.11 REVISÃO E ATUALIZAÇÃO

Esta Política será revisada periodicamente ou sempre que houver:

I – Alterações na legislação.

II – Mudanças relevantes nos tratamentos de dados.

III – Novas orientações da ANPD.

11.12 VIGÊNCIA

Esta Política entra em vigor na data de sua aprovação pela Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Data da última atualização: 01/02/2026.

Responsável pela aprovação: Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

12 TERMO DO USUÁRIO

(TERMOS DE USO DOS SISTEMAS, PLATAFORMAS E SERVIÇOS)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

12.1 ACEITAÇÃO DOS TERMOS

Ao acessar, utilizar ou se cadastrar em quaisquer sistemas, plataformas, softwares, aplicações, chatbots ou serviços fornecidos pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA. ("Ê-SISTEMAS"), o Usuário declara ter lido, compreendido e concordado integralmente com o presente Termo do Usuário, bem como com a Política de Privacidade e demais documentos que integram o Programa de Governança em Privacidade da empresa.

O Usuário declara ser maior de 18 (dezoito) anos e plenamente capaz, ou, se menor, que possui autorização expressa de seus responsáveis legais.

A Ê-SISTEMAS não direciona seus serviços a menores de 18 anos, sendo vedado o uso sem autorização expressa dos responsáveis legais.

Caso o Usuário não concorde com estes Termos, deverá interromper imediatamente o uso dos serviços.

12.2 DEFINIÇÕES

Para fins deste Termo:

I – Usuário: pessoa física que acessa ou utiliza os serviços da Ê-SISTEMAS.

II – Serviços: sistemas, plataformas, softwares, aplicações e chatbots disponibilizados.

III – Dados pessoais: informações relacionadas a pessoa natural identificada ou identificável.

IV – LGPD: Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

12.3 OBJETO

Este Termo regula as condições de acesso e uso dos serviços tecnológicos disponibilizados pela Ê-SISTEMAS, estabelecendo direitos, deveres e responsabilidades do Usuário e da empresa.

12.4 CONDIÇÕES DE USO

O Usuário compromete-se a:

I – Utilizar os serviços de forma lícita, ética e em conformidade com a legislação vigente.

II – Fornecer informações verdadeiras, completas e atualizadas quando solicitadas.

III – Não utilizar os sistemas para fins ilegais, fraudulentos ou que violem direitos de terceiros.

IV – Não tentar acessar áreas restritas ou sistemas sem autorização.

V – Não introduzir códigos maliciosos, vírus ou qualquer mecanismo que comprometa a segurança dos sistemas.

12.5 RESPONSABILIDADES DO USUÁRIO

O Usuário é exclusivamente responsável:

I – Pelo uso que fizer dos serviços.

II – Pela confidencialidade de suas credenciais de acesso, quando aplicável.

III – Pelas informações inseridas, transmitidas ou processadas nos sistemas.

IV – Por eventuais danos causados à Ê-SISTEMAS ou a terceiros em decorrência de uso indevido.

12.6 RESPONSABILIDADES DA Ê-SISTEMAS

A Ê-SISTEMAS compromete-se a:

I – Empregar boas práticas de segurança da informação.

II – Proteger os dados pessoais tratados, nos termos da LGPD.

III – Manter políticas e procedimentos internos de segurança, privacidade e governança.

IV – Atuar com diligência na prestação dos serviços, ressalvadas limitações técnicas ou operacionais.

V - A Ê-SISTEMAS empenha seus melhores esforços para manter a disponibilidade dos serviços, mas não garante que estes serão ininterruptos, seguros ou livres de erros, estando isenta de responsabilidade por eventuais indisponibilidades decorrentes de fatores fora de seu controle razoável, incluindo casos fortuitos ou de força maior.

12.7 TRATAMENTO DE DADOS PESSOAIS

O tratamento de dados pessoais do Usuário ocorre conforme descrito na Política de Privacidade, que é parte integrante deste Termo.

O Usuário declara ciência de que:

I – Seus dados poderão ser tratados para execução dos serviços.

II – Poderão ser adotadas medidas de segurança e monitoramento.

III – Os dados serão tratados conforme bases legais previstas na LGPD.

IV – A depender do contexto do serviço, a Ê-SISTEMAS poderá atuar como Controladora ou como Operadora dos dados pessoais tratados. Quando atuar como Operadora, o tratamento será regido pelas instruções documentadas do cliente contratante (Controlador) e por contrato

específico de proteção de dados, sendo as disposições sobre finalidade e bases legais definidas pelo referido Controlador.

12.8 DIREITOS DO USUÁRIO (TITULAR DOS DADOS)

Nos termos da LGPD, o Usuário poderá exercer seus direitos, incluindo:

I – Confirmação da existência de tratamento.

II – Acesso aos dados pessoais.

III – Correção de dados incompletos ou desatualizados.

IV – Solicitação de eliminação ou anonimização, quando aplicável.

V – Revogação do consentimento, quando utilizado como base legal.

As solicitações poderão ser realizadas pelos canais indicados na Política de Privacidade.

12.9 DO ACEITE ELETRÔNICO

O Usuário declara que o aceite eletrônico deste Termo possui plena validade jurídica, produzindo os mesmos efeitos legais de uma assinatura manuscrita, nos termos da legislação brasileira aplicável.

O aceite ocorrerá mediante ação inequívoca do Usuário, incluindo, mas não se limitando a:

I – Marcação de caixa de seleção (“checkbox”) indicando concordância com este Termo.

II – Clique em botão identificado como “Li e concordo”, “Aceito os Termos” ou equivalente.

III – Continuidade de uso dos sistemas, plataformas, aplicações ou serviços após a disponibilização deste Termo.

A Ê-SISTEMAS poderá manter registros eletrônicos do aceite, incluindo data, hora, endereço IP, identificação do usuário e versão do Termo aceito, exclusivamente para fins de comprovação, segurança jurídica e cumprimento legal, em conformidade com a LGPD.

O Usuário reconhece que a ausência de aceite implicará na impossibilidade de acesso ou utilização dos serviços disponibilizados.

12.10 LIMITAÇÕES DE RESPONSABILIDADE

A Ê-SISTEMAS não se responsabiliza por:

I – Falhas decorrentes de culpa exclusiva do Usuário ou de terceiros.

II – Indisponibilidades temporárias por manutenção, força maior ou fatores externos.

III – Conteúdos, dados ou informações inseridos pelos próprios usuários.

IV – Danos decorrentes de uso inadequado ou em desacordo com este Termo.

V – Em nenhuma circunstância a Ê-SISTEMAS será responsável por quaisquer danos indiretos, especiais, incidentais, consequenciais ou por perda de lucros. A responsabilidade total da empresa, por qualquer motivo, será limitada ao valor efetivamente pago pelo usuário pelo serviço no último ano.

VI – Exceto nos casos de dolo ou culpa grave, quando aplicável nos termos da legislação.

12.11 PROPRIEDADE INTELECTUAL

Todos os direitos sobre os sistemas, softwares, interfaces, marcas, códigos-fonte, conteúdos e materiais disponibilizados são de titularidade da Ê-SISTEMAS ou de seus licenciadores, sendo vedada a reprodução, modificação ou distribuição sem autorização expressa.

12.12 SUSPENSÃO E ENCERRAMENTO DE ACESSO

A Ê-SISTEMAS poderá, a seu critério, suspender ou encerrar o acesso do Usuário aos serviços, sem aviso prévio, em caso de:

I – Violação deste Termo.

II – Uso indevido ou ilegal dos sistemas.

III – Risco à segurança da informação ou à privacidade de dados.

12.13 ALTERAÇÕES DOS TERMOS

Este Termo poderá ser atualizado a qualquer tempo. A versão vigente estará sempre disponível nos canais oficiais da Ê-SISTEMAS, sendo o uso contínuo dos serviços considerado como aceitação das alterações. Sempre que houver alteração relevante, o Usuário será informado por meio dos canais disponíveis.

12.14 VIGÊNCIA E RESCISÃO

Este Termo permanece vigente enquanto o Usuário utilizar os serviços da Ê-SISTEMAS, podendo ser rescindido a qualquer momento mediante interrupção do uso.

12.15 LEGISLAÇÃO APLICÁVEL E FORO

Este Termo é regido pelas leis da República Federativa do Brasil. Fica eleito o foro da comarca do domicílio da sede da Ê-SISTEMAS, salvo disposição legal diversa.

12.16 DISPOSIÇÕES FINAIS

Este Termo integra o Programa de Governança em Privacidade e Segurança da Informação da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., juntamente com a Política de Privacidade, PSI, DPIA e demais documentos correlatos.

13. TERMO DE USO ACEITÁVEL DA INFORMAÇÃO (TUA)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

13.1 OBJETIVO

Este Termo de Uso Aceitável da Informação ("TUA") tem por objetivo estabelecer regras, responsabilidades e condições para o uso adequado dos ativos de informação, sistemas, dados pessoais e recursos tecnológicos disponibilizados pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA, em conformidade com a Política de Segurança da Informação (PSI), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e demais normativos internos.

13.2 ABRANGÊNCIA

Este Termo aplica-se a todos os sócios, administradores, colaboradores, estagiários, prestadores de serviços, parceiros, fornecedores e quaisquer terceiros que tenham acesso, direto ou indireto, a:

I – Sistemas da Ê-SISTEMAS.

II – Informações corporativas.

III – Dados pessoais ou dados pessoais sensíveis.

IV – Infraestrutura tecnológica e recursos de TI.

13.3 ATIVOS DE INFORMAÇÃO ABRANGIDOS

Para fins deste Termo, consideram-se ativos de informação, entre outros:

I – Sistemas, softwares, plataformas e aplicações.

II – Equipamentos, servidores, redes e serviços em nuvem.

III – Bases de dados, arquivos digitais e documentos físicos.

IV – Informações estratégicas, técnicas, comerciais e operacionais.

V – Dados pessoais e dados pessoais sensíveis.

13.4 DIRETRIZES DE USO ACEITÁVEL

O usuário compromete-se a:

I – Utilizar os recursos de informação exclusivamente para fins profissionais e autorizados.

II – Acessar apenas informações estritamente necessárias ao desempenho de suas funções.

III – Respeitar a classificação da informação e o princípio do menor privilégio.

IV – Proteger credenciais de acesso, mantendo-as pessoais e intransferíveis.

V – Observar as políticas internas de segurança, privacidade e proteção de dados.

VI – Comunicação e Redes Sociais.

VI.I – Identificação: Não representar a empresa em redes sociais sem autorização.

VI.II – Confidencialidade: Não divulgar informações internas, mesmo em contas pessoais.

VI.III – Segurança: Não publicar fotos/vídeos que revejam informações sensíveis, inclusive após o encerramento do vínculo, quando aplicável.

13.5 CONDUTAS VEDADAS

É expressamente proibido ao usuário:

I – Compartilhar senhas, logins ou credenciais de acesso.

II – Acessar, copiar, divulgar ou alterar informações sem autorização.

II.I – Exportar dados para dispositivos de armazenamento não controlados.

III – Utilizar sistemas ou dados para fins ilícitos, pessoais ou não autorizados.

IV – Instalar softwares, extensões ou aplicações sem autorização prévia.

IV.I – Autorização: Via solicitação formal ao gestor/departamento de TI.

V – Armazenar dados corporativos em dispositivos ou serviços não autorizados.

VI – Tentar burlar controles de segurança ou explorar vulnerabilidades.

VII – Divulgar informações corporativas em redes sociais sem autorização.

VIII – Exportação e Transferência de Dados.

VIII.I – Proibido: Copiar dados para dispositivos de armazenamento pessoal.

VIII.II – Proibido: Enviar dados corporativos para e-mail pessoal.

VIII.III – Proibido: Fazer upload de informações para serviços de nuvem não autorizados.

VIII.IV – Permitido: Apenas através de canais aprovados.

13.6 PROTEÇÃO DE DADOS PESSOAIS

O usuário declara ciência de que:

I – Dados pessoais somente podem ser tratados para finalidades legítimas e autorizadas.

II – O acesso a dados pessoais é restrito e monitorado.

III – Dados pessoais sensíveis exigem nível reforçado de proteção.

IV – Qualquer uso indevido poderá gerar responsabilização administrativa, civil e legal.

13.7 INCIDENTES DE SEGURANÇA

O usuário compromete-se a:

I – Comunicar imediatamente qualquer suspeita ou ocorrência de incidente de segurança.

II – Cooperar com investigações internas e medidas de contenção.

III – Seguir as orientações previstas no Procedimento de Resposta a Incidentes de Segurança da Informação.

13.8 MONITORAMENTO E REGISTROS

O usuário declara estar ciente de que:

I – O uso dos sistemas poderá ser monitorado, registrado e auditado.

II – Logs de acesso e atividades poderão ser utilizados para fins de segurança, auditoria e conformidade legal.

III – O monitoramento observará a legislação aplicável e os princípios da proporcionalidade e transparência.

IV – O monitoramento não tem por finalidade violar a intimidade do usuário, limitando-se à proteção dos ativos de informação e ao cumprimento de obrigações legais.

13.9 RESPONSABILIDADES E SANÇÕES

O descumprimento deste Termo poderá acarretar, conforme o caso:

I – Medidas disciplinares internas.

II – Rescisão contratual.

III – Responsabilização civil, administrativa e/ou penal.

Sem prejuízo das sanções previstas na legislação vigente.

13.10 DISPOSITIVOS PESSOAIS E TRABALHO REMOTO

I – BYOD: Permitido apenas com política específica de segurança.

II – Requisitos: Antivirus atualizado, tela de bloqueio, criptografia.

III – Separação: Dados corporativos em container/partição separada.

IV – Revogação: Direito da empresa de apagar dados remotamente se dispositivo for perdido/roubado.

V – A adesão ao BYOD é facultativa, condicionada à aceitação expressa das regras de segurança.

13.11 VINCULAÇÃO ÀS POLÍTICAS INTERNAS

Este Termo integra e deve ser interpretado em conjunto com:

I – Política de Segurança da Informação (PSI).

II – Política de Privacidade.

III – Política de Retenção e Descarte de Dados.

IV – Procedimento de Resposta a Incidentes.

V – Plano de Continuidade de Negócios (BCP).

VI – Código de Ética e Conduta.

13.12 VIGÊNCIA

Este Termo entra em vigor na data de sua assinatura e permanecerá válido enquanto o usuário mantiver vínculo ou acesso aos ativos de informação da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

TERMO DE CIÊNCIA E COMPROMISSO

Declaro que li, compreendi e concordo integralmente com os termos deste Termo de Uso Aceitável da Informação, comprometendo-me a cumpri-lo integralmente.

Nome: _____

CPF: _____

Cargo/Função: _____

Data: ____ / ____ / _____

☐ Assinatura eletrônica

☐ Assinatura manual

14 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

14.1 OBJETIVO

A presente Política de Segurança da Informação (PSI) tem por objetivo estabelecer diretrizes, princípios, responsabilidades e controles para a proteção das informações e dos dados pessoais tratados pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA, assegurando sua confidencialidade, integridade, disponibilidade e autenticidade, em conformidade com a legislação vigente, especialmente a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

14.2 ABRANGÊNCIA

Esta Política aplica-se a todos os sócios, administradores, colaboradores, estagiários, prestadores de serviços, parceiros, fornecedores e quaisquer terceiros que tenham acesso, direto ou indireto, às informações e aos ativos de informação da Ê-SISTEMAS, independentemente do meio ou formato utilizado.

O acesso de terceiros às informações estará condicionado à realização de due diligence de segurança, à formalização de cláusulas contratuais específicas e à possibilidade de auditorias periódicas.

14.3 FUNDAMENTAÇÃO LEGAL E REFERÊNCIAS

Esta Política fundamenta-se, especialmente:

I – Na Lei nº 13.709/2018 (LGPD), em especial nos arts. 6º, 37, 46 a 49.

II – Nas boas práticas de governança corporativa, gestão de riscos e segurança da informação.

III – Nos princípios da proteção de dados pessoais e da responsabilidade demonstrável (accountability).

14.4 DEFINIÇÕES

Para fins desta Política, considera-se:

I – Informação: todo dado ou conjunto de dados, independentemente do formato ou meio.

II – Ativo de Informação: qualquer recurso que armazene, processe ou transmita informações.

III – Dados Pessoais: informações relacionadas a pessoa natural identificada ou identificável.

IV – Incidente de Segurança: evento que comprometa ou possa comprometer a segurança da informação.

V – Usuário: qualquer pessoa autorizada a acessar informações ou sistemas da empresa.

14.5 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação na Ê-SISTEMAS observa os seguintes princípios:

I – Confidencialidade: acesso às informações apenas por pessoas autorizadas.

II – Integridade: proteção contra alterações indevidas ou não autorizadas.

III – Disponibilidade: acesso às informações sempre que necessário.

IV – Autenticidade: garantia da identidade das partes envolvidas.

V – Responsabilização: atribuição clara de responsabilidades.

VI – Prevenção e gestão de riscos.

14.6 CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser classificadas conforme seu nível de sensibilidade, incluindo, mas não se limitando a:

I – Informações públicas.

II – Informações internas.

III – Informações confidenciais.

IV – Informações contendo dados pessoais ou dados pessoais sensíveis.

O nível de proteção adotado deverá ser proporcional à classificação da informação.

14.7 CONTROLES DE ACESSO

I – O acesso às informações e sistemas será concedido conforme o princípio do menor privilégio.

II – Cada usuário deverá possuir credenciais individuais e intransferíveis.

III – É vedado o compartilhamento de senhas, acessos ou credenciais.

IV – O acesso deverá ser revogado imediatamente em caso de desligamento, mudança de função ou término de contrato.

14.8 SEGURANÇA DOS SISTEMAS E INFRAESTRUTURA

A Ê-SISTEMAS adotará medidas técnicas e administrativas adequadas, incluindo:

I – Uso de autenticação segura.

II – Monitoramento de sistemas e acessos.

III – Atualizações e correções de segurança.

IV – Proteção contra acessos não autorizados, malware e ataques cibernéticos.

V – Backups periódicos, conforme política específica.

14.9 PROTEÇÃO DE DADOS PESSOAIS

I – O tratamento de dados pessoais deverá observar estritamente as bases legais previstas na LGPD.

II – Dados pessoais serão tratados apenas para finalidades legítimas, específicas e informadas.

III – O acesso a dados pessoais será restrito às pessoas autorizadas e necessárias ao desempenho de suas funções.

IV – Dados pessoais sensíveis receberão nível reforçado de proteção.

V – Sempre que possível, serão adotadas técnicas de anonimização ou pseudo minimização, conforme a finalidade do tratamento.

14.10 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

I – Todo incidente ou suspeita de incidente deverá ser comunicado imediatamente ao responsável designado ou ao Encarregado de Proteção de Dados (DPO).

II – A resposta a incidentes seguirá o Procedimento de Resposta a Incidentes de Segurança da Informação adotado pela empresa.

III – Incidentes relevantes poderão ser comunicados à ANPD e aos titulares, quando exigido por lei.

14.11 USO ADEQUADO DOS RECURSOS

Os recursos tecnológicos e informacionais da Ê-SISTEMAS devem ser utilizados exclusivamente para fins profissionais e autorizados, sendo vedado:

I – Uso para atividades ilícitas ou não autorizadas.

II – Instalação de softwares sem autorização.

III – Compartilhamento indevido de informações.

14.12 RESPONSABILIDADES

14.12.1 Administração

Compete à Administração:

I – Aprovar esta Política e suas revisões.

II – Garantir recursos para sua implementação.

14.12.2 Encarregado de Proteção de Dados (DPO)

Compete ao DPO:

I – Orientar quanto à segurança da informação e proteção de dados.

II – Atuar em incidentes de segurança.

III – Garantir alinhamento com a LGPD e demais políticas internas.

14.12.3 Usuários

Compete a todos os usuários:

I – Cumprir esta Política.

II – Proteger as informações sob sua responsabilidade.

III – Comunicar falhas, riscos ou incidentes.

14.13 TREINAMENTO E CONSCIENTIZAÇÃO

A Ê-SISTEMAS promoverá, sempre que viável, ações de conscientização e orientação sobre segurança da informação e proteção de dados.

14.14 AUDITORIA E MONITORAMENTO

O cumprimento desta Política poderá ser monitorado por meio de:

I – Auditorias internas.

II – Revisões técnicas e administrativas.

III – Avaliações de conformidade.

14.15 VIOLAÇÕES E SANÇÕES

O descumprimento desta Política poderá resultar em medidas disciplinares, contratuais e legais cabíveis, sem prejuízo de outras sanções previstas em lei.

14.16 REVISÃO E ATUALIZAÇÃO

Esta Política será revisada:

I – Periodicamente.

II – Após incidentes relevantes.

III – Em caso de alterações legais, regulatórias ou operacionais.

14.17 CONFORMIDADE E DOCUMENTAÇÃO

I – Documentação: Esta PSI integra o Programa de Governança em Privacidade.

II – Referências: Alinha-se com ROPA, Plano de Continuidade, Procedimento de Incidentes.

III – Evidências: Registros de acesso, logs de segurança, relatórios de auditoria.

IV – Registros de treinamentos e termos de ciência.

14.18 VIGÊNCIA

Esta Política entra em vigor na data de sua aprovação pela Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Data da última atualização: 01/02/2026.

15 PROCEDIMENTO DE BACKUP E RECUPERAÇÃO DE DADOS

(Anexo ao Plano de Continuidade de Negócios – BCP).

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

15.1 OBJETIVO

Este Procedimento de Backup e Recuperação estabelece as diretrizes, responsabilidades e processos adotados pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA para garantir a proteção, integridade, disponibilidade e recuperação das informações e dos dados pessoais tratados pela empresa, assegurando a continuidade das operações em conformidade com o Plano de Continuidade de Negócios (BCP), a Política de Segurança da Informação (PSI) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

15.2 ABRANGÊNCIA

Este Procedimento aplica-se a todos os sistemas, bancos de dados, aplicações, ambientes em nuvem, servidores, dispositivos e informações críticas da Ê-SISTEMAS, incluindo dados pessoais e dados pessoais sensíveis, bem como a todos os colaboradores, prestadores de serviço e terceiros envolvidos na gestão ou operação da infraestrutura tecnológica.

15.3 FUNDAMENTAÇÃO LEGAL E NORMATIVA

Este Procedimento fundamenta-se, especialmente:

I – Na Lei nº 13.709/2018 (LGPD), arts. 46 a 49.

II – No Plano de Continuidade de Negócios (BCP).

III – Na Política de Segurança da Informação (PSI).

IV – No Registro das Operações de Tratamento de Dados (ROPA).

V – Em boas práticas de segurança da informação e continuidade de negócios.

15.4 DEFINIÇÕES

Para fins deste Procedimento:

I – Backup: Cópia de segurança dos dados e sistemas, realizada para fins de recuperação.

II – Recuperação: Processo de restauração de dados ou sistemas a partir de backups válidos.

III – Dados Críticos: Informações essenciais à continuidade das operações e à prestação dos serviços.

IV – Ambiente de Produção: Ambiente principal onde os sistemas operam.

V – Ambiente de Contingência: Ambiente alternativo para recuperação.

15.5 CLASSIFICAÇÃO DOS DADOS PARA BACKUP

Os backups deverão contemplar, no mínimo:

I – Bases de dados dos sistemas e aplicações.

II – Informações operacionais e técnicas críticas.

III – Dados pessoais e dados pessoais sensíveis tratados pela empresa.

IV – Configurações essenciais de sistemas e infraestrutura.

A criticidade dos dados seguirá a classificação definida na Política de Segurança da Informação.

15.6 POLÍTICA DE BACKUP

15.6.1 Frequência dos Backups

Os backups serão realizados conforme a criticidade do ativo:

I – Backups diários: Dados operacionais e bancos de dados críticos.

II – Backups semanais: Sistemas, configurações e arquivos estruturais.

III – Backups mensais: Backups completos para retenção prolongada.

15.6.2 Tipos de Backup

Poderão ser utilizados:

I – Backup completo.

II – Backup incremental.

III – Backup diferencial.

A escolha do tipo dependerá da arquitetura técnica e da criticidade do sistema.

15.6.3 Armazenamento dos Backups

I – Os backups serão armazenados em ambiente seguro, preferencialmente em nuvem ou infraestrutura segregada.

II – Deve haver separação lógica ou física entre ambiente de produção e backup.

III – O acesso aos backups será restrito a pessoas autorizadas.

15.6.4 Segurança dos Backups

I – Backups contendo dados pessoais deverão ser protegidos por criptografia, sempre que tecnicamente viável.

II – Credenciais de acesso deverão ser protegidas e controladas.

III – Os backups estarão sujeitos às mesmas regras de confidencialidade e segurança dos dados originais.

15.7 RETENÇÃO DOS BACKUPS

Os backups serão mantidos conforme critérios definidos na Política de Retenção e Descarte de Dados Pessoais e no ROPA, observando:

I – Necessidade operacional.

II – Obrigações legais e regulatórias.

III – Continuidade de negócios e recuperação de desastres.

Encerrado o prazo de retenção, os backups deverão ser eliminados de forma segura.

A eliminação deverá ocorrer por exclusão lógica e, quando aplicável, física, com registro ou certificado de destruição das mídias.

15.8 PROCEDIMENTO DE RECUPERAÇÃO

15.8.1 Situações de Recuperação

A recuperação poderá ser acionada em casos de:

I – Falhas de sistema.

II – Incidentes de segurança da informação.

III – Perda, corrupção ou indisponibilidade de dados.

IV – Eventos disruptivos previstos no BCP.

15.8.2 Processo de Recuperação

O processo seguirá as seguintes etapas:

I – Identificação do incidente.

II – Avaliação do impacto e definição da prioridade.

III – Seleção do backup adequado.

IV – Restauração dos dados ou sistemas.

V – Validação da integridade e funcionalidade.

VI – Retomada controlada das operações.

15.8.2.1 Procedimento Técnico de Recuperação

Cenário Leve (dados corrompidos):

I – Identificar backup mais recente pré-corrupção.

II – Restaurar em ambiente staging.

III – Validar integridade.

IV – Aplicar em produção durante janela de manutenção.

Cenário Grave (perda total):

I – Provisionar ambiente contingência.

II – Restaurar último backup completo.

III – Aplicar backups incrementais sequenciais.

IV – Validar todos sistemas interconectados.

V – Comunicar clientes sobre interrupção programada.

15.8.3 Prioridade de Recuperação

A recuperação priorizará:

I – Sistemas e dados críticos à continuidade do serviço.

II – Dados pessoais necessários ao atendimento de obrigações legais.

III – Serviços essenciais aos clientes.

15.9 TESTES DE BACKUP E RECUPERAÇÃO

I – Os backups deverão ser testados periodicamente para garantir sua integridade e efetividade.

II – Testes de restauração poderão ser realizados em ambiente controlado.

III – Os resultados dos testes deverão ser registrados e avaliados.

IV - Os testes deverão ser realizados, no mínimo, anualmente ou sempre que houver alterações relevantes na infraestrutura.

15.10 RESPONSABILIDADES

15.10.1 Administração

I – Garantir recursos para execução deste Procedimento.

II – Apoiar decisões estratégicas em situações críticas.

15.10.2 Responsáveis Técnicos

I – Executar os backups conforme definido.

II – Garantir a segurança e integridade dos dados.

III – Realizar e documentar testes de recuperação.

15.10.3 Encarregado de Proteção de Dados (DPO)

I – Avaliar impactos relacionados a dados pessoais.

II – Garantir alinhamento com a LGPD e políticas internas.

III – Atuar em conjunto com a Administração em incidentes relevantes.

15.11 REGISTROS E DOCUMENTAÇÃO

Devem ser mantidos registros de:

I – Execução dos backups.

II – Testes de recuperação.

III – Incidentes e acionamentos do procedimento.

IV – Falhas e medidas corretivas adotadas.

15.12 REVISÃO E ATUALIZAÇÃO

Este Procedimento será revisado:

I – Periodicamente.

II – Após incidentes relevantes.

III – Em caso de alterações tecnológicas ou legais.

IV – Quando houver mudanças nos serviços ou infraestrutura.

15.13 VIGÊNCIA

Este Procedimento entra em vigor na data de sua aprovação e integra o Plano de Continuidade de Negócios (BCP) da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Data da última atualização: 01/02/2026.

Responsável pela aprovação: Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

16 PLANO DE CONTINUIDADE DE NEGÓCIOS (BCP)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

16.1 OBJETIVO

O presente Plano de Continuidade de Negócios (Business Continuity Plan – BCP) tem por objetivo estabelecer diretrizes, responsabilidades e procedimentos a serem adotados pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA para assegurar a continuidade de suas atividades essenciais diante de incidentes, crises ou eventos disruptivos que possam impactar pessoas, processos, sistemas, informações ou infraestrutura tecnológica.

16.2 FUNDAMENTAÇÃO E REFERÊNCIAS

Este Plano está alinhado:

I – À Lei nº 13.709/2018 (LGPD), especialmente quanto à segurança da informação e continuidade dos serviços.

II – Às boas práticas de governança corporativa e gestão de riscos.

III – Às diretrizes de segurança da informação e proteção de dados adotadas pela empresa.

16.3 ABRANGÊNCIA

Este BCP aplica-se a todos os sócios, administradores, colaboradores, prestadores de serviços, parceiros e terceiros que atuem em processos críticos da Ê-SISTEMAS, incluindo ambientes físicos, digitais e em nuvem.

16.4 PRINCÍPIOS NORTEADORES

O Plano de Continuidade de Negócios observará os seguintes princípios:

I – Prevenção e antecipação de riscos.

II – Minimização de impactos operacionais, financeiros, reputacionais e legais.

III – Proteção da informação e dos dados pessoais.

IV – Rápida resposta e recuperação.

V – Comunicação clara e coordenada.

VI – Melhoria contínua.

16.5 GOVERNANÇA E RESPONSABILIDADES

16.5.1 Alta Administração

Compete à Administração:

I – Aprovar este Plano e suas revisões.

II – Garantir recursos necessários para sua implementação.

III – Apoiar decisões estratégicas durante situações de crise.

16.5.2 Encarregado de Proteção de Dados (DPO)

Nome: Thiago Marcos Montagner

E-mail: thiagomarcosmontagner@hotmail.com

Compete ao DPO:

I – Avaliar impactos relacionados à segurança da informação e dados pessoais.

II – Atuar em conjunto com a Administração em incidentes relevantes.

III – Avaliar necessidade de comunicação à ANPD e aos titulares, quando aplicável.

16.5.3 Responsáveis Técnicos e Operacionais

Compete aos responsáveis técnicos:

I – Executar os procedimentos de contingência.

II – Restaurar sistemas, dados e serviços críticos.

III – Reportar status e evolução das ações à Administração.

16.6 IDENTIFICAÇÃO DE PROCESSOS CRÍTICOS

São considerados processos críticos, entre outros:

I – Operação e disponibilidade do sistema de chatbot.

II – Infraestrutura de servidores, bancos de dados e serviços em nuvem.

III – Segurança da informação e proteção de dados pessoais.

IV – Atendimento a clientes e suporte técnico.

V – Comunicação institucional e canais oficiais.

16.7 ANÁLISE DE RISCOS E CENÁRIOS

O BCP considera, de forma não exaustiva, os seguintes cenários:

I – Falha ou indisponibilidade de sistemas.

II – Incidentes de segurança da informação.

III – Vazamento ou comprometimento de dados pessoais.

IV – Falhas de provedores de tecnologia ou energia.

V – Desastres naturais.

VI – Indisponibilidade de pessoal-chave.

VII – Ataques cibernéticos.

16.8 ESTRATÉGIAS DE CONTINUIDADE

16.8.1 Medidas Preventivas

I – Backups periódicos e testados.

II – Uso de infraestrutura redundante, quando aplicável.

III – Controles de acesso e autenticação.

IV – Monitoramento contínuo dos sistemas.

V – Contratos com cláusulas de continuidade e segurança.

16.8.2 Estratégias de Resposta

Em caso de incidente:

I – Ativação imediata deste BCP.

II – Comunicação interna à Administração e responsáveis técnicos.

III – Isolamento de sistemas afetados, se necessário.

IV – Adoção das medidas previstas no Procedimento de Resposta a Incidentes.

V – Prioridade à restauração dos processos críticos.

16.8.2.1 Procedimento de Ativação

Passo 1: Identificação do incidente (qualquer pessoa).

Passo 2: Acionamento do Administrador.

Passo 3: Classificação (leve/moderado/grave) com base no impacto.

Passo 4: Ativação do nível correspondente do BCP.

Passo 5: Comunicação inicial à equipe.

16.9 RECUPERAÇÃO E RESTAURAÇÃO

As ações de recuperação incluem:

I – Restauração de backups.

II – Validação da integridade dos dados.

III – Retomada gradual dos serviços.

IV – Monitoramento pós-incidente.

V – Registro detalhado das ações adotadas.

16.10 COMUNICAÇÃO EM SITUAÇÃO DE CRISE

A comunicação durante incidentes deverá:

I – Ser centralizada e coordenada pela Administração.

II – Garantir clareza, transparência e tempestividade.

III – Observar obrigações legais e contratuais.

IV – Preservar a imagem e a credibilidade da empresa.

16.11 TREINAMENTO E TESTES

A Ê-SISTEMAS realizará, sempre que viável:

I – Treinamentos internos sobre continuidade de negócios.

II – Testes periódicos de backup e recuperação.

III – Simulações de cenários críticos.

16.12 REVISÃO E MELHORIA CONTÍNUA

Este BCP será revisado:

I – Periodicamente.

II – Após incidentes relevantes.

III – Em caso de mudanças significativas nos serviços, tecnologias ou estrutura organizacional.

IV – Quando houver alterações legais ou regulatórias aplicáveis.

16.13 VIGÊNCIA

Este Plano de Continuidade de Negócios entra em vigor na data de sua aprovação pela Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Data da última atualização: 01/02/2026

Responsável pela aprovação: Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

17 PROCEDIMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DADOS PESSOAIS

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

17.1 OBJETIVO

Este Procedimento estabelece as diretrizes, responsabilidades e etapas a serem observadas pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA em caso de incidente de segurança da informação ou de dados pessoais, visando:

I – Mitigar danos e impactos aos titulares de dados.

II – Garantir a conformidade com a Lei nº 13.709/2018 (LGPD).

III – Preservar a continuidade das operações.

IV – Assegurar transparência e rastreabilidade das ações adotadas.

17.2 ABRANGÊNCIA

Aplica-se a todos os sócios, administradores, colaboradores, prestadores de serviço, parceiros e terceiros que tratem dados pessoais ou tenham acesso a sistemas, informações ou infraestrutura tecnológica da Ê-SISTEMAS.

17.3 DEFINIÇÃO DE INCIDENTE DE SEGURANÇA

Considera-se incidente de segurança qualquer evento confirmado ou suspeito que resulte em:

I – Acesso não autorizado a dados pessoais.

II – Vazamento, perda, destruição ou alteração indevida de dados.

III – Indisponibilidade de sistemas que impactem dados pessoais.

IV – Comprometimento da confidencialidade, integridade ou disponibilidade das informações.

17.4 PRINCÍPIOS NORTEADORES

O tratamento de incidentes observará os princípios da:

I – Prevenção.

II – Responsabilização e prestação de contas.

III – Transparência.

IV – Minimização de danos.

V – Boa-fé e cooperação.

17.5 PAPÉIS E RESPONSABILIDADES

17.5.1 Administração

I – Garantir recursos técnicos e organizacionais adequados.

II – Apoiar a tomada de decisões estratégicas.

III – Aprovar comunicações externas relevantes.

17.5.2 Encarregado de Proteção de Dados (DPO)

I – Coordenar a resposta ao incidente.

II – Avaliar riscos e impactos aos titulares.

III – Definir a necessidade de notificação à ANPD e aos titulares.

IV – Manter registros do incidente.

V – Orientar medidas corretivas e preventivas.

17.5.3 Colaboradores e Terceiros

I – Comunicar imediatamente qualquer suspeita ou ocorrência de incidente.

II – Cooperar com as investigações internas.

III – Cumprir as orientações de contenção e mitigação.

17.6 Identificação e Comunicação do Incidente

I – Qualquer pessoa que identifique ou suspeite de um incidente deve comunicar imediatamente a Administração ou o DPO.

II – A comunicação deve conter, sempre que possível, data, hora, descrição do evento, sistemas afetados e dados envolvidos.

17.6.1 Classificação do Incidente, o incidente será classificado pelo DPO considerando:

I – Tipo de dado pessoal envolvido.

II – Volume de dados afetados.

III – Número de titulares impactados.

IV – Risco de dano material ou moral.

V – Facilidade de identificação dos titulares.

17.6.2 Contenção e Mitigação:

I – Isolamento de sistemas afetados.

II – Revogação ou redefinição de credenciais.

III – Correção de vulnerabilidades.

IV – Preservação de evidências técnicas.

V – Adoção de medidas para reduzir impactos aos titulares.

17.6.3 Avaliação de Risco e Impacto, o DPO realizará análise técnica e jurídica para avaliar:

I – Probabilidade e gravidade dos danos.

II – Necessidade de notificação à ANPD.

III – Necessidade de comunicação aos titulares.

IV – Medidas adicionais de segurança.

17.6.4 Notificação à ANPD, quando o incidente puder acarretar risco ou dano relevante aos titulares, a Ê-SISTEMAS notificará a ANPD em prazo razoável, preferencialmente em até 2 (dois) dias úteis, contendo, no mínimo:

I – Descrição da natureza do incidente.

II – Dados pessoais afetados.

III – Medidas técnicas e de segurança adotadas.

IV – Riscos relacionados.

V – Medidas para mitigar os efeitos.

17.6.5 Comunicação aos Titulares, quando aplicável, os titulares afetados serão comunicados de forma clara, objetiva e transparente, informando:

I – Natureza do incidente.

II – Dados afetados.

III – Riscos envolvidos.

IV – Medidas adotadas pela empresa.

V – Orientações para proteção do titular.

17.6.6 Registro do Incidente, todos os incidentes, independentemente de notificação externa, deverão ser registrados internamente, contendo:

I – Data e hora do evento.

II – Descrição detalhada.

III – Dados e sistemas envolvidos.

IV – Medidas adotadas.

V – Responsáveis.

VI – Conclusões e lições aprendidas.

VII – Evidências técnicas, quando aplicável.

17.6.7 Medidas Corretivas e Preventivas, após o encerramento do incidente, poderão ser adotadas:

I – Revisão de políticas e procedimentos.

II – Treinamento adicional.

III – Atualização de controles de segurança.

IV – Melhorias técnicas e organizacionais.

17.6.8 Treinamento e Conscientização

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA promoverá treinamentos periódicos sobre segurança da informação e proteção de dados, reforçando a prevenção e a correta resposta a incidentes.

17.6.9 Revisão do Procedimento, este procedimento será revisado periodicamente ou sempre que houver:

I – Alterações relevantes na legislação.

II – Mudanças tecnológicas significativas.

III – Ocorrência de incidentes relevantes.

17.7 VIGÊNCIA

Este Procedimento entra em vigor na data de sua aprovação pela Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Data da última atualização: 31**/**01/2026

Responsável pela aprovação: Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

18 PLANO DE COMUNICAÇÃO DE CRISE

Privacidade, Proteção de Dados e Segurança da Informação

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade e Segurança da Informação.

18.1 OBJETIVO

O presente Plano de Comunicação de Crise tem por objetivo estabelecer diretrizes, fluxos, responsabilidades e procedimentos claros para a comunicação interna e externa em situações de crise relacionadas a:

I – Incidentes de segurança da informação.

II – Violações ou suspeitas de violação de dados pessoais.

III – Eventos que possam gerar impacto aos titulares, clientes, parceiros, imagem institucional ou continuidade dos negócios.

O plano visa assegurar:

I – Transparência.

II – Agilidade.

III – Consistência das informações.

IV – Conformidade com a LGPD.

V – Preservação da reputação e da confiança.

18.2 ESCOPO E APLICAÇÃO

Este Plano aplica-se a crises decorrentes de:

I – Incidentes de segurança da informação.

II – Vazamento, acesso não autorizado ou perda de dados pessoais.

III – Ataques cibernéticos relevantes.

IV – Falhas sistêmicas com impacto significativo.

V – Determinações ou fiscalizações da ANPD relacionadas a incidentes.

Aplica-se a:

I – Colaboradores.

II – Administração.

III – DPO.

IV – Prestadores de serviço envolvidos na gestão da crise.

18.3 FUNDAMENTAÇÃO LEGAL E NORMATIVA

Este Plano observa:

I – Lei nº 13.709/2018 (LGPD), especialmente arts. 6º, 46 a 48.

II – Marco Civil da Internet (Lei nº 12.965/2014).

III – Normas de boas práticas de segurança da informação.

IV – DPIA e Matriz de Risco.

V – Procedimento de Gestão de Incidentes.

VI – Plano de Continuidade de Negócios (BCP).

VII – Política de Segurança da Informação.

VIII – Programa de Awareness Contínuo.

18.4 PRINCÍPIOS DA COMUNICAÇÃO DE CRISE

A comunicação durante a crise deverá observar:

I – Veracidade e precisão das informações.

II – Rapidez compatível com a apuração técnica.

III – Proporcionalidade ao impacto do incidente.

IV – Centralização da comunicação.

V – Proteção aos titulares e à empresa.

VI – Registro e rastreabilidade.

18.5 CLASSIFICAÇÃO DA CRISE

Para fins de comunicação, as crises são classificadas em:

18.5.1 Crise Nível 1 – Baixo Impacto

I – Incidente sem dados pessoais ou com impacto mínimo.

II – Comunicação restrita ao time interno.

III – Sem necessidade de comunicação externa.

18.5.2 Crise Nível 2 – Médio Impacto

I – Incidente com dados pessoais comuns.

II – Potencial impacto limitado aos titulares.

III – Comunicação interna ampliada e avaliação de comunicação externa.

18.5.3 Crise Nível 3 – Alto Impacto

I – Incidente envolvendo dados pessoais sensíveis.

II – Risco relevante aos titulares.

III – Comunicação obrigatória à ANPD e aos titulares, quando aplicável.

IV – Comunicação externa estruturada.

18.6 COMITÊ DE COMUNICAÇÃO DE CRISE

Em caso de crise, será instituído o Comitê de Comunicação de Crise, composto por:

I – Administração.

II – Encarregado de Proteção de Dados (DPO).

III – Responsável pela Segurança da Informação / TI.

IV – Responsável Jurídico (interno ou externo).

V – Responsável pela Comunicação, quando aplicável.

18.7 PAPÉIS E RESPONSABILIDADES

18.7.1 Administração

I – Tomar decisões estratégicas.

II – Aprovar comunicações externas.

III – Avaliar impactos reputacionais e financeiros.

18.7.2 DPO

I – Avaliar impacto aos titulares.

II – Definir necessidade de comunicação à ANPD.

III – Redigir ou validar comunicações relacionadas à LGPD.

IV – Manter registros para accountability.

18.7.3 TI / Segurança da Informação

I – Apurar tecnicamente o incidente.

II – Fornecer informações precisas ao Comitê.

III – Implementar medidas de contenção.

18.7.4 Comunicação Institucional

I – Padronizar linguagem.

II – Evitar divulgação indevida ou especulativa.

III – Garantir coerência da mensagem.

18.8 FLUXO DE COMUNICAÇÃO

18.8.1 Comunicação Interna

I – Notificação imediata do incidente ao DPO.

II – Ativação do Comitê de Comunicação de Crise.

III – Comunicação interna restrita às áreas envolvidas.

IV – Orientações claras sobre sigilo e conduta.

18.8.2 Comunicação à Administração

Relatório inicial com:

I – Natureza do incidente.

II – Dados afetados.

III – Medidas adotadas.

IV – Riscos estimados.

18.8.3 Comunicação à ANPD

Quando aplicável, será realizada:

I – Em prazo razoável.

II – Com informações claras e objetivas.

III – Conforme art. 48 da LGPD.

Conteúdo mínimo:

I – Descrição do incidente.

II – Dados pessoais afetados.

III – Medidas técnicas e administrativas adotadas.

IV – Riscos aos titulares.

V – Medidas de mitigação.

18.8.4 Comunicação aos Titulares

Quando houver risco ou dano relevante:

I – Linguagem clara e acessível.

II – Orientações práticas aos titulares.

III – Canais de contato disponibilizados.

18.8.5 Comunicação Externa (Clientes, Parceiros e Público)

I – Centralizada e aprovada pelo Comitê.

II – Evitar especulações ou exposição excessiva.

III – Preservar segredos comerciais e dados pessoais.

18.9 CANAIS DE COMUNICAÇÃO

Poderão ser utilizados:

I – E-mail institucional.

II – Comunicado interno.

III – Plataforma ou sistema afetado.

IV – Site institucional.

V – Comunicação direta ao cliente, quando aplicável.

18.10 REGISTRO E DOCUMENTAÇÃO

Toda comunicação de crise deverá ser documentada, incluindo:

I – Linha do tempo do incidente.

II – Decisões tomadas.

III – Comunicações enviadas.

IV – Evidências de envio e recebimento.

Os registros integrarão o DPIA, o Risk Register e o Programa de Governança.

18.11 CONFIDENCIALIDADE E CONDUTA

Durante a crise:

I – Somente porta-vozes autorizados poderão se manifestar.

II – É vedada divulgação não autorizada de informações.

III – O descumprimento poderá gerar medidas disciplinares.

18.12 TREINAMENTO E AWARENESS

Este Plano será:

I – Divulgado internamente.

II – Integrado ao Programa de Awareness Contínuo.

III – Testado periodicamente por meio de simulações.

18.13 REVISÃO E ATUALIZAÇÃO

O Plano será revisado:

I – Periódicamente.

II – Após crises ou incidentes relevantes.

III – Em alterações regulatórias.

IV – Por solicitação da Administração ou da ANPD.

18.14 PÓS-CRISE E LIÇÕES APRENDIDAS

I. Após a contenção da crise, o Comitê se reunirá para realizar uma análise post-mortem.

II. O objetivo é documentar as lições aprendidas, identificar pontos de melhoria nos processos, na segurança e no próprio Plano de Comunicação.

III. Um relatório de lições aprendidas será elaborado e suas conclusões serão incorporadas à revisão dos documentos do Programa de Governança (PSI, DPIA, este Plano, etc.).

IV. As lições aprendidas relevantes serão compartilhadas (de forma anonimizada) no Programa de Awareness Contínuo.

18.15 VIGÊNCIA E APROVAÇÃO

Este Plano entra em vigor na data de sua aprovação e integra o Programa de Governança em Privacidade e Segurança da Informação da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: ____ / ____ / _____

19 MODELO DE COMUNICAÇÃO À ANPD

(Art. 48 da LGPD – Comunicação de Incidente de Segurança)

Assunto: Comunicação de Incidente de Segurança – Art. 48 da LGPD

Controlador: Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

À

Autoridade Nacional de Proteção de Dados – ANPD

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., na qualidade de Controladora e/ou Operadora de dados pessoais, conforme o caso, vem, respeitosamente, comunicar a ocorrência de incidente de segurança da informação, nos termos do art. 48 da Lei nº 13.709/2018 (LGPD), conforme segue:

19.1 DESCRIÇÃO DO INCIDENTE

Em [data], foi identificado um incidente de segurança envolvendo [descrever de forma objetiva: acesso não autorizado, vazamento, indisponibilidade, ataque cibernético etc.].

19.2 NATUREZA DOS DADOS PESSOAIS AFETADOS

Os dados potencialmente afetados envolvem:

☐ Dados pessoais comuns

☐ Dados pessoais sensíveis

Descrição: [especificar categorias, sem expor dados individuais].

19.3 TITULARES AFETADOS

Estimativa de titulares impactados: [quantidade estimada ou “em apuração”].

19.4 RISCOS AOS TITULARES

Avaliação preliminar indica os seguintes riscos:

[ex.: exposição indevida, fraude, uso não autorizado, impacto reputacional].

19.5 MEDIDAS TÉCNICAS E ADMINISTRATIVAS ADOTADAS

Foram adotadas imediatamente as seguintes medidas:

I – Contenção do incidente.

II – Ativação do Plano de Resposta a Incidentes.

III – Reforço dos controles de segurança.

IV – Análise forense e monitoramento contínuo.

19.6 MEDIDAS PARA MITIGAR EFEITOS DO INCIDENTE

I – Revisão de acessos.

II – Comunicação aos titulares, quando aplicável.

III – Atualização de políticas e controles.

IV – Treinamento adicional.

19.7 Contato do Encarregado (DPO)

Nome: _____

E-mail: _____

Telefone: _____

A empresa permanece à disposição da ANPD para prestar informações adicionais e colaborar integralmente com eventuais orientações ou determinações.

Atenciosamente,

19.8 Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

[Nome do responsável legal]

[Cargo]

[Data]

19.9 MODELO DE COMUNICAÇÃO AOS TITULARES DE DADOS

(Clara, acessível e protetiva)

Assunto: Comunicação Importante sobre Segurança de Dados

Prezada(o) Titular,

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA. preza pela transparência e pela proteção dos seus dados pessoais.

Identificamos recentemente um incidente de segurança da informação que pode ter envolvido alguns de seus dados pessoais tratados em nossos sistemas.

O que aconteceu?

Em [data], detectamos [descrição objetiva do incidente, sem linguagem técnica excessiva].

Quais dados podem ter sido afetados?

Os dados potencialmente envolvidos incluem:

[ex.: nome, e-mail, informações cadastrais].

Não houve acesso a [ex.: senhas, dados bancários, dados sensíveis], quando aplicável.

O que estamos fazendo?

Imediatamente após a identificação:

I – Contivemos o incidente.

II – Reforçamos nossas medidas de segurança.

III – Ativamos nossos protocolos internos de resposta.

IV – Comunicamos as autoridades competentes, quando aplicável.

O que você pode fazer?

Recomendamos, por precaução:

I – Atenção a comunicações suspeitas.

II – Não compartilhar senhas ou códigos.

III – Entrar em contato conosco em caso de dúvida.

Seus direitos

Você pode exercer seus direitos previstos na LGPD, inclusive solicitar informações adicionais, por meio do nosso Encarregado de Proteção de Dados:

E-mail: _____

Telefone: _____

Reafirmamos nosso compromisso com a proteção dos seus dados e lamentamos qualquer transtorno.

Atenciosamente,

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

[Data]

19.20 MODELO DE COMUNICAÇÃO A CLIENTES / PARCEIROS

(Mais técnica, preservando relação comercial)

Assunto: Comunicado sobre Incidente de Segurança da Informação

Prezados(as),

A Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA. informa que identificou um incidente de segurança da informação em seus ambientes tecnológicos, relacionado a [descrever genericamente].

Impacto identificado

Até o momento:

☐ Não há evidências de impacto relevante aos dados de clientes

☐ Há impacto limitado e controlado

(ajustar conforme o caso)

Medidas adotadas

I – Ativação imediata do Plano de Resposta a Incidentes.

II – Contenção do evento.

III – Reforço dos controles técnicos e organizacionais.

IV – Monitoramento contínuo.

Conformidade legal

As medidas adotadas estão alinhadas à LGPD, às boas práticas de segurança da informação e ao nosso Programa de Governança em Privacidade.

Caso o incidente gere qualquer impacto específico relacionado a dados sob sua titularidade ou controle, o contato será realizado de forma individualizada.

Permanecemos à disposição para esclarecimentos.

Atenciosamente,

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

[Responsável]

[Cargo]

[Contato]

[Data]

20. SEGURO CIBERNÉTICO (CYBER INSURANCE)

Diretrizes e Avaliação de Contratação

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade, da Matriz de Risco, do DPIA e do Plano de Ação para Tratamento de Riscos.

20.1 OBJETIVO

Este documento tem por objetivo estabelecer as diretrizes para avaliação, eventual contratação e gestão de Seguro Cibernético (Cyber Insurance), como medida complementar de mitigação de riscos relacionados a incidentes de segurança da informação e proteção de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

O seguro cibernético visa reduzir impactos financeiros, operacionais, legais e reputacionais decorrentes de incidentes digitais.

20.2 FUNDAMENTAÇÃO LEGAL E REGULATÓRIA

A avaliação da contratação de seguro cibernético está alinhada aos seguintes dispositivos da LGPD:

I – Art. 6º, X (Accountability) – demonstração de medidas eficazes de governança.

II – Art. 46 – adoção de medidas técnicas e administrativas aptas a proteger dados pessoais.

III – Art. 48 – mitigação de danos em caso de incidente de segurança.

IV – Art. 50 – boas práticas e governança em privacidade.

O seguro não substitui controles internos, mas atua como camada adicional de proteção.

20.3 ESCOPO DO SEGURO CIBERNÉTICO

O seguro cibernético poderá abranger, conforme apólice contratada:

20.3.1 Riscos Cobertos (exemplos)

I – Vazamento de dados pessoais e dados pessoais sensíveis.

II – Incidentes cibernéticos (ataques, ransomware, malware).

III – Acesso não autorizado a sistemas.

IV – Interrupção de serviços (indisponibilidade).

V – Responsabilização civil por falhas de segurança.

VI – Custos de resposta a incidentes.

20.3.2 Custos Possivelmente Cobertos

I – Investigação forense digital.

II – Notificação de titulares e autoridades.

III – Honorários advocatícios e custas judiciais.

IV – Multas administrativas (quando legalmente seguráveis).

V – Serviços de comunicação e gestão de crise.

VI – Recuperação de sistemas e dados.

VII – Monitoramento de crédito para titulares afetados (quando aplicável).

20.4 LIMITAÇÕES DO SEGURO

A Ê-SISTEMAS reconhece que o seguro cibernético:

I – Não substitui medidas técnicas e organizacionais de segurança.

II – Não afasta responsabilidade legal em caso de negligência.

III – Pode excluir eventos decorrentes de dolo, fraude interna ou descumprimento deliberado da LGPD.

IV – Está sujeito a franquias, limites e exclusões contratuais.

V – A contratação de seguro cibernético não implica transferência integral ou automática da responsabilidade legal da Ê-SISTEMAS perante titulares, controladores ou autoridades competentes.

20.5 CRITÉRIOS PARA AVALIAÇÃO E CONTRATAÇÃO

A eventual contratação do seguro deverá considerar:

I – Perfil de risco identificado no DPIA e na Matriz de Risco.

II – Tratamento de dados pessoais sensíveis (ex.: chatbot de saúde).

III – Volume e criticidade dos dados tratados.

IV – Dependência operacional de sistemas digitais.

V – Custos potenciais de incidentes.

VI – Limites de cobertura e franquias.

VII – Requisitos de segurança exigidos pela seguradora.

VIII – Compatibilidade com a legislação brasileira.

IX – Requisitos Mínimos de Segurança (para obter cobertura).

IX.I - MFA para acesso administrativo.

IX.II - Backups diários testados mensalmente.

IX.III - Política de senhas.

IX.IV - Treinamento anual de segurança.

IX.V - Plano de resposta a incidentes.

IX.VI - Firewall + antivirus atualizados.

IX.VII - Logs centralizados.

X – Checklist de Avaliação de Apólice.

X.I - Cobre ransomware.

X.II - Cobre custos de notificação.

X.III - Cobre forense digital.

X.IV - Cobre interrupção de negócios.

X.V - Cobre responsabilidade civil.

X.VI - Não exclui falta de controles básicos.

X.VII - Não tem franquia proibitiva.

X.VIII - Jurisdição Brasil.

20.6 INTEGRAÇÃO COM A GOVERNANÇA EM PRIVACIDADE

O seguro cibernético será tratado como medida complementar, integrada a:

I – Política de Segurança da Informação (PSI).

II – Procedimento de Resposta a Incidentes.

III – Plano de Continuidade de Negócios (BCP).

IV – Procedimento de Backup e Recuperação.

V – Plano de Ação para Riscos Altos.

VI – DPIA e Heatmap de Riscos.

A existência do seguro não reduz a obrigação de prevenção, mas fortalece a capacidade de resposta.

20.7 PAPÉIS E RESPONSABILIDADES

I – Administração: decisão estratégica sobre contratação, limites e orçamento.

II – DPO: avaliação de aderência à LGPD e impactos regulatórios.

III – TI: fornecimento de informações técnicas e cumprimento dos requisitos de segurança.

IV – Jurídico (interno ou externo): análise contratual da apólice.

20.8 DECISÃO ATUAL SOBRE CONTRATAÇÃO

Com base na Matriz de Risco, Heatmap e Plano de Ação:

I – Foi identificada exposição a riscos cibernéticos relevantes, especialmente envolvendo dados pessoais sensíveis.

II – A contratação de seguro cibernético é considerada medida recomendável, porém não obrigatória.

III – A decisão final deverá considerar custo-benefício, maturidade dos controles internos e cenário operacional.

A ausência de contratação não configura descumprimento da LGPD, desde que mantidas medidas técnicas e organizacionais adequadas.

20.9 PROCESSO DE CONTRATAÇÃO E NEGOCIAÇÃO

I – Fase 1: Due diligence técnica e jurídica.

II – Fase 2: Análise comparativa de coberturas, limites e exclusões.

III – Fase 3: Negociação contratual e adequação à LGPD.

IV – Fase 4: Implementação e alinhamento com controles internos.

V – Fase 5: Gestão contínua e revisão periódica da apólice.

20.10 REVISÃO E ATUALIZAÇÃO

Este documento será revisado:

I – Periodicamente.

II – Em caso de alteração significativa no perfil de risco.

III – Após incidentes relevantes.

IV – Em caso de contratação, renovação ou alteração da apólice.

V – Por solicitação da Administração ou da ANPD.

20.11 APROVAÇÃO

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: 02 / 02/ 2026

21. REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS (ROPA)

Empresa: Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA

CNPJ: 53.695.158/0001-90

Encarregado (DPO): Thiago Marcos Montagner

E-mail do DPO: thiagomarcosmontagner@hotmail.com

Base legal: Art. 37 da Lei nº 13.709/2018 (LGPD)

21.1 FINALIDADE DO DOCUMENTO

O presente Registro das Operações de Tratamento de Dados (ROPA) tem como objetivo documentar, de forma sistematizada, todas as operações de tratamento de dados pessoais realizadas pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA, demonstrando conformidade com os princípios e obrigações previstos na Lei Geral de Proteção de Dados Pessoais (LGPD).

Este documento possui natureza interna, devendo ser apresentado à Autoridade Nacional de Proteção de Dados (ANPD) ou a outros órgãos competentes sempre que solicitado.

21.2 ATIVIDADES DE TRATAMENTO DE DADOS

21.2.1 Atendimento e Operação do Chatbot

I – Titulares dos dados: Usuários do chatbot / clientes finais.

II – Categorias de dados pessoais: Nome, e-mail, telefone, conteúdo das mensagens, dados de interação.

III – Dados sensíveis: Não aplicável (eventual fornecimento espontâneo pelo titular).

IV – Finalidade do tratamento: Prestação do serviço de atendimento automatizado, resposta a solicitações e melhoria da experiência do usuário.

V – Base legal: Execução de contrato (art. 7º, V) e, subsidiariamente, legítimo interesse (art. 7º, IX), observado o princípio da minimização.

VI – Forma de coleta: Inserção direta pelo titular no chatbot.

VII – Compartilhamento: Clientes contratantes do sistema e provedores de infraestrutura tecnológica, quando necessário.

VIII – Prazo de retenção: Pelo período de vigência contratual e, após o término, pelo prazo necessário para defesa de direitos ou cumprimento de obrigações legais.

IX – Medidas de segurança: Controle de acesso, autenticação, criptografia e registros de logs.

21.2.2 Cadastro de Clientes e Usuários

I – Titulares dos dados: Clientes pessoa física e representantes de clientes pessoa jurídica.

II – Categorias de dados pessoais: Nome, e-mail, telefone, CPF (quando necessário).

III – Dados sensíveis: Não aplicável.

IV – Finalidade do tratamento: Identificação, formalização contratual, faturamento e suporte técnico.

V – Base legal: Execução de contrato (art. 7º, V) e cumprimento de obrigação legal (art. 7º, II).

VI – Forma de coleta: Formulários digitais, contratos e comunicação direta.

VII – Compartilhamento: Plataformas de pagamento, contabilidade e autoridades competentes, quando exigido por lei.

VIII – Prazo de retenção: Conforme prazos legais fiscais e contratuais.

IX – Medidas de segurança: Acesso restrito, armazenamento seguro e backups controlados.

21.2.3 Marketing e Comunicação Institucional

I – Titulares dos dados: Leads e clientes.

II – Categorias de dados pessoais: Nome, e-mail, telefone.

III – Dados sensíveis: Não aplicável.

IV – Finalidade do tratamento: Envio de comunicações institucionais, informativos e ofertas de serviços.

V – Base legal: Consentimento do titular (art. 7º, I).

VI – Forma de coleta: Formulários de consentimento e interações voluntárias.

VII – Compartilhamento: Plataformas de e-mail marketing.

VIII – Prazo de retenção: Até a revogação do consentimento.

IX – Medidas de segurança: Gestão de consentimento, controle de listas e acesso restrito.

21.2.4 Gestão de Colaboradores e Prestadores de Serviço

I – Titulares dos dados: Colaboradores e prestadores de serviço.

II – Categorias de dados pessoais: Nome, CPF, dados de contato, dados contratuais.

III – Dados sensíveis: Não aplicável.

IV – Finalidade do tratamento: Gestão contratual, obrigações trabalhistas e administrativas.

V – Base legal: Cumprimento de obrigação legal (art. 7º, II) e execução de contrato (art. 7º, V).

VI – Forma de coleta: Contratos, formulários internos e documentos oficiais.

VII – Compartilhamento: Contabilidade, órgãos governamentais e instituições financeiras.

VIII – Prazo de retenção: Conforme legislação trabalhista e previdenciária.

IX – Medidas de segurança: Arquivamento seguro, controle de acesso e confidencialidade.

21.3 MAPEAMENTO DE FLUXO DE DADOS

I – Coleta → Processamento → Armazenamento → Destruição (se necessário).

21.4 PROCEDIMENTO PARA INCIDENTES DE SEGURANÇA

I – Em caso de incidente: Registro imediato no sistema interno.

II – Avaliação: DPO analisa gravidade em 72h.

III – Notificação: ANPD em prazo razoável, preferencialmente em até 2 (dois) dias úteis.

IV – Titulares afetados: Comunicação clara e transparente.

21.5 TRANSFERÊNCIA INTERNACIONAL DE DADOS

Atualmente, a Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA poderá utilizar provedores de tecnologia em nuvem localizados no exterior. Nesses casos, a transferência internacional de dados observará os requisitos previstos nos arts. 33 a 36 da LGPD, adotando cláusulas contratuais e medidas de segurança adequadas.

Observando-se, sempre que aplicável, a adoção de cláusulas contratuais padrão, medidas técnicas equivalentes e avaliação do nível de proteção do país destinatário.

21.6 DIREITOS DOS TITULARES

A empresa assegura aos titulares o exercício de todos os direitos previstos no art. 18 da LGPD, mediante solicitação encaminhada ao Encarregado de Proteção de Dados, observando-se os prazos e procedimentos internos estabelecidos.

21.7 RESPONSABILIDADES E TREINAMENTO

I – DPO: Responsável pela manutenção deste ROPA.

II – Colaboradores: Treinamento anual em LGPD.

III – Revisão: Periodicamente ou quando nova atividade surgir.

21.8. ATUALIZAÇÃO E REVISÃO

Este ROPA deverá ser revisado periodicamente e sempre que houver alterações relevantes nas operações de tratamento de dados, novos serviços, tecnologias ou exigências legais.

Data da última atualização: 31/01/2026.

Responsável pela aprovação: Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

22 AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (DPIA)

22.1 IDENTIFICAÇÃO DO OPERADOR

Razão Social: Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90.

Papel: Operadora de Dados Pessoais.

Atividade: Desenvolvimento, fornecimento e operação de soluções tecnológicas com tratamento de dados pessoais sob instruções do controlador.

22.2 RESPONSÁVEL PELA ELABORAÇÃO

Área responsável: Governança, Compliance e Segurança da Informação.

Encarregado de Proteção de Dados (DPO):Thiago Marcos Montagner.

Data da avaliação: 01/02/2026.

Versão: 1.0.

22.3 DESCRIÇÃO DO TRATAMENTO DE DADOS

22.3.1 Finalidade do Tratamento

O tratamento de dados pessoais realizado pela Ê-SISTEMAS tem como finalidades principais:

I – Prestação de serviços tecnológicos.

II – Execução de contratos.

III – Suporte técnico e atendimento ao cliente.

IV – Cumprimento de obrigações legais e regulatórias.

V – Segurança da informação e prevenção a fraudes.

22.3.2 Categorias de Titulares

I – Clientes (pessoas físicas).

II – Usuários de sistemas e plataformas.

III – Colaboradores e prestadores de serviço.

IV – Representantes legais de clientes pessoa jurídica.

22.3.3 Categorias de Dados Tratados

I – Dados pessoais comuns: nome, CPF, e-mail, telefone, dados profissionais, registros de acesso.

II – Dados pessoais sensíveis: apenas quando estritamente necessário, como dados relacionados à saúde, quando vinculados à finalidade específica do serviço contratado.

22.3.4 Bases Legais

O tratamento fundamenta-se, conforme o caso, em:

I – Execução de contrato (art. 7º, V, LGPD).

II – Cumprimento de obrigação legal (art. 7º, II).

III – Exercício regular de direitos (art. 7º, VI).

IV – Consentimento do titular, quando aplicável (art. 7º, I).

V – Para dados sensíveis: art. 11 da LGPD.

22.3.5 Cenários de Tratamento Específicos

Cenário A: Chatbot geral (baixo risco).

Dados: Nome, e-mail, mensagens.

Risco: Baixo.

Cenário B: Chatbot para saúde (alto risco).

- Dados: Condições saúde, medicamentos.

- Risco: Alto.

O tratamento de dados pessoais sensíveis no Cenário B fundamenta-se no art. 11, II, 'a' ou 'f', da LGPD, conforme a finalidade específica e o vínculo contratual com o controlador.

O risco residual varia conforme o cenário de tratamento, sendo baixo para tratamentos comuns e médio para tratamentos envolvendo dados sensíveis.

22.4 NECESSIDADE E PROPORCIONALIDADE

O tratamento:

I – Limita-se aos dados estritamente necessários.

II – Observa os princípios da finalidade, adequação, necessidade e minimização.

III – Não realiza coleta excessiva ou desvinculada da finalidade informada ao titular.

22.5 MAPEAMENTO DOS FLUXOS DE DADOS

I – Coleta: plataformas, formulários, sistemas internos, integrações.

II – Armazenamento: ambientes controlados, preferencialmente em nuvem segura.

III – Acesso: restrito a pessoas autorizadas.

IV – Compartilhamento: apenas com operadores ou parceiros contratualmente vinculados.

V – Eliminação: conforme Política de Retenção e Destruição de Dados.

22.6 IDENTIFICAÇÃO DOS RISCOS ÀS LIBERDADES E DIREITOS DOS TITULARES

22.6.1 Riscos Identificados

I – Acesso não autorizado.

II – Vazamento de dados pessoais.

III – Perda ou indisponibilidade de informações.

IV – Uso indevido ou fora da finalidade.

V – Incidentes de segurança cibernética.

22.6.2 Impactos Potenciais

I – Violação da privacidade dos titulares.

II – Danos morais ou patrimoniais.

III – Responsabilização administrativa, civil ou reputacional da empresa.

22.7 - MEDIDAS DE MITIGAÇÃO ADOTADAS

A Ê-SISTEMAS adota, entre outras:

I – Política de Segurança da Informação (PSI).

II – Controle de acesso lógico.

III – Criptografia de dados, sempre que viável.

IV – Procedimento de Backup e Recuperação.

V – Plano de Continuidade de Negócios (BCP).

VI – Procedimento de Incidentes de Segurança.

VII – Treinamento e conscientização de colaboradores.

VIII – Contratos com cláusulas de proteção de dados com terceiros.

22.8 - AVALIAÇÃO DO NÍVEL DE RISCO RESIDUAL

Após a adoção das medidas técnicas e administrativas, o risco residual é considerado:

☐ Baixo

☐ Médio

☐ Alto

Justificativa:

O tratamento é realizado de forma controlada, com medidas de segurança adequadas e monitoramento contínuo, reduzindo significativamente os riscos aos titulares.

22.9 RELACIONAMENTO COM CONTROLADORES

I - Instruções: Processamos apenas conforme instruções documentadas do controlador.

II – Due diligence: Avaliamos legalidade das instruções recebidas.

III – Notificação: Comunicamos ao controlador se instrução violar LGPD.

IV – Cooperação: Apoiamos controlador no exercício de direitos dos titulares.

22.10 CONCLUSÃO DA AVALIAÇÃO

Com base na análise realizada, conclui-se que:

I – O tratamento de dados pessoais é necessário, proporcional e legítimo.

II – Os riscos identificados são mitigados por controles técnicos e organizacionais adequados.

III – O tratamento está em conformidade com a LGPD, não sendo identificada, no momento, necessidade de consulta prévia à ANPD.

22.11 REVISÃO E ATUALIZAÇÃO

Este DPIA deverá ser revisado:

I – Periodicamente.

II – Sempre que houver mudança relevante no tratamento.

III – Em caso de incidentes de segurança relevantes.

IV – Por solicitação da Autoridade Nacional de Proteção de Dados (ANPD).

22.12 APROVAÇÃO

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Ciente e validado pelo Encarregado de Proteção de Dados (DPO).

Data: 01/02/2026

23 AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

DPIA – TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS (SAÚDE)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade, da Política de Segurança da Informação, da Matriz de Risco, do Heatmap de Riscos, do Plano de Ação para Riscos Altos e do Registro Centralizado de Riscos Aceitos.

23.1 OBJETIVO

Esta Avaliação de Impacto à Proteção de Dados Pessoais (DPIA) tem por objetivo identificar, avaliar e mitigar os riscos decorrentes do tratamento de dados pessoais sensíveis relacionados à saúde, realizado pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., especialmente por meio de soluções tecnológicas, sistemas e chatbots voltados à área da saúde, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

23.2 DESCRIÇÃO DO TRATAMENTO

23.2.1 Natureza do tratamento

O tratamento envolve a coleta, registro, armazenamento, processamento, análise e eventual exclusão de dados pessoais sensíveis de saúde, fornecidos diretamente pelos titulares por meio de interfaces digitais, incluindo chatbots e plataformas tecnológicas.

23.2.2 Finalidade do tratamento

Os dados são tratados exclusivamente para:

I – Prestação de serviços tecnológicos de apoio à área da saúde.

II – Interação automatizada com usuários (chatbot).

III – Organização e direcionamento de informações relacionadas a atendimento, triagem ou suporte.

IV – Cumprimento de obrigações legais e regulatórias do cliente controlador.

Não há tratamento para fins discriminatórios, comerciais abusivos ou incompatíveis com a finalidade informada.

23.3 CATEGORIAS DE DADOS PESSOAIS SENSÍVEIS

Os dados pessoais sensíveis tratados podem incluir:

I – Informações sobre estado de saúde.

II – Dados relacionados a sintomas, histórico clínico ou condições médicas informadas voluntariamente.

III – Dados associados a atendimentos, triagens ou orientações automatizadas.

O tratamento observa o princípio da minimização, sendo coletados apenas os dados estritamente necessários.

23.4 TITULARES DOS DADOS

Os titulares dos dados pessoais sensíveis são:

I – Usuários finais das plataformas e chatbots.

II – Pacientes ou potenciais pacientes, conforme o contexto do serviço.

Não há tratamento deliberado de dados de crianças e adolescentes sem consentimento ou base legal adequada, quando aplicável.

23.5 BASE LEGAL PARA O TRATAMENTO

O tratamento de dados pessoais sensíveis fundamenta-se, conforme o caso, nas seguintes bases legais previstas no art. 11 da LGPD:

I – Consentimento específico e destacado do titular, quando exigido.

II – Cumprimento de obrigação legal ou regulatória pelo controlador.

III – Execução de políticas públicas ou contratos.

IV – Tutela da saúde, quando aplicável, em conformidade com a legislação.

Quando a Ê-SISTEMAS atuar como Operadora, o tratamento ocorrerá conforme instruções documentadas do Controlador.

23.6 PAPÉIS E RESPONSABILIDADES

I – Controlador: cliente contratante, responsável pelas finalidades e decisões sobre o tratamento.

II – Operadora: Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., responsável pela execução técnica do tratamento.

III – Encarregado (DPO): responsável pela supervisão da conformidade com a LGPD e mitigação de riscos.

23.7 AVALIAÇÃO DE NECESSIDADE E PROPORCIONALIDADE

O tratamento:

I – É necessário para a finalidade pretendida.

II – É proporcional ao serviço prestado.

III – Observa os princípios da finalidade, adequação, necessidade, segurança e prevenção.

IV – Evita tratamento excessivo ou desnecessário de dados sensíveis.

Foram avaliadas alternativas menos invasivas, não sendo tecnicamente viáveis sem comprometer a funcionalidade do serviço.

23.8 IDENTIFICAÇÃO DOS RISCOS AOS TITULARES

Foram identificados, entre outros, os seguintes riscos:

I – Vazamento de dados pessoais sensíveis de saúde.

II – Acesso não autorizado por falha de credenciais.

III – Uso indevido ou fora da finalidade.

IV – Incidentes cibernéticos direcionados.

V – Impacto à dignidade, privacidade e direitos fundamentais dos titulares.

Os riscos foram classificados conforme a Matriz de Risco (Impacto × Probabilidade) e representados no Heatmap de Riscos.

23.9 MEDIDAS DE MITIGAÇÃO ADOTADAS

A Ê-SISTEMAS adota, entre outras, as seguintes medidas técnicas e organizacionais:

I – Política de Segurança da Informação.

II – Controle de acesso baseado em menor privilégio.

III – Autenticação multifator (MFA) para acessos críticos.

IV – Criptografia de dados em repouso e em trânsito, quando viável.

V – Monitoramento contínuo, logs e auditorias.

VI – Procedimento de Backup e Recuperação.

VII – Plano de Continuidade de Negócios (BCP).

VIII – Procedimento de Resposta a Incidentes.

IX – Treinamento específico sobre tratamento de dados sensíveis.

23.10 AVALIAÇÃO DO RISCO RESIDUAL

Após a implementação das medidas de mitigação:

I – Os riscos inerentes classificados como altos foram reduzidos.

II – O risco residual foi classificado como Médio, considerado controlado e aceitável, nos termos do art. 46 da LGPD.

III – Não foi identificada, no momento, necessidade de consulta prévia à ANPD, conforme art. 38 da LGPD.

23.11 DECISÃO SOBRE A CONTINUIDADE DO TRATAMENTO

Com base nesta DPIA:

I – O tratamento de dados pessoais sensíveis de saúde é considerado legítimo, necessário e proporcional.

II – Os riscos aos titulares estão adequadamente mitigados.

III – A continuidade do tratamento é autorizada, condicionada à manutenção dos controles existentes e à revisão periódica deste DPIA.

23.12 MONITORAMENTO, REVISÃO E ATUALIZAÇÃO

Este DPIA deverá ser revisado:

I – Periodicamente.

II – Em caso de alteração relevante no tratamento.

III – Após incidentes de segurança.

IV – Por solicitação do Controlador ou da ANPD.

23.13 CONCLUSÃO

Esta Avaliação de Impacto demonstra que a Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.:

I – Atua em conformidade com a LGPD no tratamento de dados sensíveis de saúde.

II – Adota medidas técnicas e organizacionais adequadas ao nível de risco.

III – Mantém postura de accountability, prevenção e governança em privacidade.

23.14 APROVAÇÃO

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: ____ / ____ / _____

24 MATRIZ DE RISCO

(Impacto × Probabilidade)

Anexo à Avaliação de Impacto à Proteção de Dados Pessoais – DPIA

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

24.1 OBJETIVO

Esta Matriz de Risco tem por objetivo identificar, avaliar e classificar os riscos associados às operações de tratamento de dados pessoais realizadas pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., considerando a probabilidade de ocorrência e o impacto potencial sobre os direitos e liberdades dos titulares de dados, nos termos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

Este documento integra e complementa a Avaliação de Impacto à Proteção de Dados Pessoais (DPIA).

24.2 METODOLOGIA DE AVALIAÇÃO DE RISCO

A avaliação de riscos foi realizada com base em:

I – Identificação dos riscos inerentes ao tratamento de dados.

II – Análise da probabilidade de ocorrência.

III – Análise do impacto potencial aos titulares.

IV – Consideração das medidas técnicas e administrativas existentes.

V – Determinação do nível de risco residual.

24.3 CRITÉRIOS DE PROBABILIDADE

Nível	Descrição
Baixa	Evento raro, controles eficazes, histórico inexistente ou remoto.
Média	Evento possível, controles existentes, mas com dependência operacional.
Alta	Evento provável, histórico conhecido ou alta exposição.

24.4 CRITÉRIOS DE IMPACTO

Nível	Descrição
Baixo	Impacto limitado, sem prejuízo relevante aos titulares.
Médio	Possível dano moral, operacional ou desconforto ao titular.
Alto	Dano significativo, violação de direitos fundamentais, sanções legais ou reputacionais.

24.5 MATRIZ DE CLASSIFICAÇÃO DE RISCO

Impacto \ Probabilidade	Baixa	Média	Alta
Baixo Impacto	Risco Baixo	Risco Baixo	Risco Médio
Médio Impacto	Risco Baixo	Risco Médio	Risco Alto
Alto Impacto	Risco Médio	Risco Alto	Risco Alto

24.6 IDENTIFICAÇÃO E AVALIAÇÃO DOS RISCOS

24.6.1 Riscos Gerais (Tratamentos Comuns)

Nº	Risco Identificado	Probabilidade	Impacto	Nível de Risco
1	Acesso não autorizado a sistemas	Média	Médio	**Médio**
2	Vazamento acidental de dados pessoais comuns	Baixa	Médio	**Baixo**
3	Uso de dados fora da finalidade	Baixa	Médio	**Baixo**
4	Indisponibilidade temporária de dados	Média	Baixo	**Baixo**

24.6.2 Riscos Específicos – Dados Sensíveis (ex.: Chatbot Saúde)

Nº	Risco Identificado	Probabilidade	Impacto	Nível de Risco
5	Vazamento de dados pessoais sensíveis	Média	Alto	**Alto**
6	Acesso indevido por falha de credencial	Média	Alto	**Alto**
7	Incidente cibernético direcionado	Baixa	Alto	**Médio**
8	Tratamento excessivo de dados sensíveis	Baixa	Alto	**Médio**

24.7 PLANO DE TRATAMENTO DE RISCOS

I – Riscos Alto/Médio: sujeitos a monitoramento contínuo e revisão periódica.

II – Indicadores: Nº incidentes por risco, eficácia controles.

III – Investimento: Orçamento anual para mitigação de riscos altos.

IV – Seguro: Avaliar contratação de cyber insurance para riscos catastróficos.

24.8 MEDIDAS DE CONTROLE E MITIGAÇÃO

Para os riscos identificados, a Ê-SISTEMAS adota, entre outras, as seguintes medidas:

I – Política de Segurança da Informação (PSI).

II – Controle de acesso baseado em perfil e menor privilégio.

III – Criptografia de dados em repouso e em trânsito, sempre que viável.

IV – Monitoramento, logs e auditorias.

V – Procedimento de Backup e Recuperação.

VI – Plano de Continuidade de Negócios (BCP).

VII – Procedimento de Resposta a Incidentes.

VIII – Cláusulas contratuais de proteção de dados com controladores e terceiros.

IX – Treinamento e conscientização periódica.

24.9 AVALIAÇÃO DO RISCO RESIDUAL

Após a aplicação das medidas técnicas e administrativas:

I – Tratamentos comuns: Risco residual Baixo.

II – Tratamentos envolvendo dados sensíveis: Risco residual Médio, considerado aceitável e controlado, nos termos do art. 46 da LGPD.

III – Risco residual Médio, considerado aceitável do ponto de vista regulatório, desde que mantidas as medidas de controle.

Não foi identificada, no momento, necessidade de consulta prévia à ANPD.

24.10 CONCLUSÃO

A Matriz de Risco demonstra que:

I – Os riscos aos direitos e liberdades dos titulares foram devidamente identificados e avaliados.

II – As medidas de mitigação adotadas são proporcionais à natureza dos dados tratados.

III – O tratamento de dados pessoais realizado pela Ê-SISTEMAS apresenta nível de risco compatível com as boas práticas de governança em privacidade e segurança da informação.

24.11 REVISÃO E ATUALIZAÇÃO

Esta Matriz de Risco deverá ser revisada:

I – Periodicamente.

II – Em caso de alterações relevantes nos tratamentos de dados.

III – Após incidentes de segurança relevantes.

IV – Por solicitação da ANPD ou do controlador.

24.12 APROVAÇÃO

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: 02/02/2026

25 MAPA VISUAL DE CALOR DE RISCOS

(Heatmap de Risco – Impacto × Probabilidade)

Anexo à Matriz de Risco e à Avaliação de Impacto à Proteção de Dados (DPIA)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

25.1 OBJETIVO

O presente Mapa Visual de Calor de Riscos (Heatmap) tem por objetivo representar graficamente os riscos identificados nas operações de tratamento de dados pessoais da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., considerando a probabilidade de ocorrência e o impacto potencial aos direitos e liberdades dos titulares de dados, conforme a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

Este documento complementa a Matriz de Risco (Impacto × Probabilidade) e integra a Avaliação de Impacto à Proteção de Dados Pessoais (DPIA).

25.2 METODOLOGIA DO HEATMAP

O Heatmap foi construído a partir:

I – Dos riscos identificados no DPIA.

II – Da classificação de impacto (Baixo, Médio, Alto).

III – Da classificação de probabilidade (Baixa, Média, Alta).

IV – Da combinação Impacto × Probabilidade para definição do nível de risco.

V – Da avaliação do risco residual após aplicação dos controles existentes.

25.3 LEGENDA DE CORES DO HEATMAP

Cor	Nível de Risco	Significado
Verde	Risco Baixo	Risco controlado, aceitável, apenas monitoramento
Amarelo	Risco Médio	Risco relevante, exige controles contínuos
Vermelho	Risco Alto	Risco crítico, exige mitigação prioritária

25.4 MAPA VISUAL DE CALOR (IMPACTO × PROBABILIDADE)

Heatmap Geral de Riscos

PROBABILIDADE			
	Baixa	Média	Alta
IMPACTO			
Baixo	Baixo	Baixo	Médio
Médio	Baixo	Médio	Alto
Alto	Médio	Alto	Alto

25.5 POSICIONAMENTO DOS RISCOS NO HEATMAP

25.5.1 Riscos Gerais (Dados Pessoais Comuns)

Risco	**Impacto**	**Probabilidade**	**Nível**	**Cor**
Acesso não autorizado	Médio	Média	Médio	Amarelo
Vazamento acidental de dados comuns	Médio	Baixa	Baixo	Verde
Uso fora da finalidade	Médio	Baixa	Baixo	Verde
Indisponibilidade temporária	Baixo	Média	Baixo	Verde

25.5.2 Riscos Específicos – Dados Pessoais Sensíveis (ex.: Chatbot Saúde)

Risco	**Impacto**	**Probabilidade**	**Nível**	**Cor**
Vazamento de dados sensíveis	Alto	Média	Alto	Vermelho

Acesso indevido por falha de credencial	Alto	Média	Alto	Vermelho
Ataque cibernético direcionado	Alto	Baixa	Médio	Amarelo
Tratamento excessivo de dados sensíveis	Alto	Baixa	Médio	Amarelo

25.6 INTERPRETAÇÃO DO HEATMAP

I – Áreas verdes indicam riscos aceitáveis, controlados e monitorados.

II – Áreas amarelas representam riscos relevantes que exigem atenção contínua, revisão periódica de controles e monitoramento.

III – Áreas vermelhas indicam riscos críticos, prioritários para mitigação, especialmente quando envolvem dados pessoais sensíveis.

25.7 RISCO RESIDUAL E DECISÃO DE ACEITAÇÃO

Após a aplicação das medidas técnicas e administrativas previstas:

I – Os riscos relacionados a dados pessoais comuns apresentam risco residual baixo.

II – Os riscos relacionados a dados pessoais sensíveis apresentam risco residual médio, considerado aceitável do ponto de vista regulatório e proporcional aos riscos inerentes à natureza dos dados tratados, desde que mantidos os controles existentes.

III – Não foi identificada necessidade de consulta prévia à ANPD, nos termos do art. 38 da LGPD.

25.8 GOVERNANÇA E USO DO HEATMAP

O Heatmap de Risco será utilizado para:

I – Apoiar decisões de gestão e priorização de controles.

II – Subsidiar auditorias internas e externas.

III – Demonstrar accountability e governança em privacidade.

IV – Atualizar o DPIA sempre que houver mudanças relevantes no tratamento de dados.

V – Apoiar decisões sobre necessidade de novas avaliações de impacto ou revisão de bases legais.

25.9 REVISÃO E ATUALIZAÇÃO

Este Mapa Visual de Calor deverá ser revisado:

I – Periodicamente.

II – Em caso de alteração relevante nos tratamentos de dados.

III – Após incidentes de segurança relevantes.

IV – Por solicitação da ANPD ou do controlador.

25.10 APROVAÇÃO

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: 02 / 02 / 2026

26 HEATMAP DE RISCOS

Tratamento de Dados Pessoais Sensíveis – Saúde

(Nível Reforçado – LGPD / ANPD)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade, da Política de Segurança da Informação, do DPIA de Dados Sensíveis (Saúde), do Plano de Ação para Riscos Altos e do Registro Centralizado de Riscos Aceitos.

26.1 FINALIDADE DO HEATMAP ESPECÍFICO

Este Heatmap tem por finalidade visualizar, priorizar e classificar os riscos associados exclusivamente ao tratamento de dados pessoais sensíveis relacionados à saúde, conforme definido no art. 5º, II, e art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD).

A elaboração de um heatmap segregado atende às boas práticas de governança, à accountability e às expectativas regulatórias da ANPD, especialmente para tratamentos de alto impacto aos titulares.

26.2 ESCOPO DE APLICAÇÃO

Este Heatmap aplica-se a:

I – Sistemas, plataformas e chatbots que tratem dados sensíveis de saúde.

II – Processos de coleta, armazenamento, processamento, transmissão e exclusão desses dados.

III – Ambientes próprios ou de terceiros (cloud, APIs, integrações).

IV – Atuação da Ê-SISTEMAS como Controladora ou Operadora.

26.3 METODOLOGIA DE CLASSIFICAÇÃO

A classificação dos riscos considera dois eixos fundamentais:

26.3.1 Impacto ao titular

Avaliado com foco ampliado, considerando:

I – Violação da intimidade e da vida privada.

II – Risco à dignidade, à honra e à não discriminação.

III – Potencial dano psicológico, social ou econômico.

IV – Risco à continuidade de tratamentos de saúde.

Os níveis possíveis são: Baixo, Médio e Alto, com critério mais rigoroso do que para dados comuns.

26.3.2 Probabilidade de ocorrência

Avaliada considerando:

I – Complexidade tecnológica do tratamento.

II – Volume e sensibilidade dos dados.

III – Histórico de incidentes.

IV – Exposição a ameaças cibernéticas direcionadas à área da saúde.

26.4 NÍVEIS DE RISCO CONSIDERADOS

A combinação entre impacto e probabilidade resulta nos seguintes níveis de risco:

26.4.1 Risco Crítico

Caracteriza-se por:

I – Impacto alto e probabilidade média ou alta.

II – Potencial de dano grave ou irreversível aos titulares.

III – Possibilidade de atuação imediata da ANPD, inclusive com sanções.

Riscos classificados como críticos não podem ser aceitos, exigindo mitigação imediata ou suspensão do tratamento.

26.4.2 Risco Alto

Caracteriza-se por:

I – Impacto alto com probabilidade baixa ou média.

II – Exposição relevante de dados sensíveis de saúde.

III – Necessidade de Plano de Ação formal e acompanhamento reforçado.

A aceitação é excepcional, condicionada a justificativa técnica, DPIA atualizado e aprovação formal da alta administração.

26.4.3 Risco Médio

Caracteriza-se por:

I – Impacto médio com probabilidade média.

II – Possibilidade de dano controlável ao titular.

III – Existência de controles técnicos e organizacionais eficazes.

Pode ser aceito, desde que monitorado continuamente e registrado no Risk Register.

26.4.4 Risco Baixo

Caracteriza-se por:

I – Impacto e probabilidade reduzidos.

II – Tratamento limitado, controlado e bem segregado.

Pode ser aceito sem necessidade de plano de ação específico, mantendo-se o monitoramento padrão.

26.5 DISTRIBUIÇÃO DOS RISCOS NO HEATMAP

No contexto de dados sensíveis de saúde, observou-se que:

I – Riscos relacionados a vazamento de dados de saúde concentram-se na zona Alta ou Crítica.

II – Riscos de acesso não autorizado tendem a variar entre Médio e Alto, dependendo do controle de identidade.

III – Riscos de uso indevido ou fora da finalidade situam-se majoritariamente em Médio, com possibilidade de escalonamento.

IV – Riscos de indisponibilidade do sistema podem alcançar Alto impacto, considerando a continuidade assistencial.

26.6 CRITÉRIOS ESPECIAIS PARA DADOS DE SAÚDE

Para fins deste Heatmap, aplicam-se critérios reforçados:

I – Qualquer incidente envolvendo dados de saúde é presumido como potencialmente grave.

II – O impacto ao titular é avaliado com presunção de sensibilidade ampliada.

III – A probabilidade é reavaliada sempre que houver mudança tecnológica.

IV – O apetite de risco é significativamente mais restritivo.

26.7 INTEGRAÇÃO COM DPIA E PLANOS DE AÇÃO

Este Heatmap:

I – Complementa o DPIA específico para dados sensíveis (saúde).

II – Fundamenta a elaboração do Plano de Ação para riscos altos e críticos.

III – Alimenta o Registro Centralizado de Riscos Aceitos.

IV – Serve como evidência documental para auditorias e fiscalização da ANPD.

26.8 GOVERNANÇA E RESPONSABILIDADES

I – A área de Segurança da Informação é responsável pela atualização técnica.

II – O Encarregado (DPO) supervisiona a aderência à LGPD.

III – A Administração valida riscos residuais e decisões de aceitação.

26.9 REVISÃO E ATUALIZAÇÃO

Este Heatmap deverá ser revisado:

I – Anualmente.

II – Após incidentes de segurança.

III – Em alterações relevantes no tratamento.

IV – Mediante solicitação da ANPD ou do Controlador.

26.10 CONCLUSÃO

O Heatmap específico para dados pessoais sensíveis de saúde:

I – Reflete abordagem de risco compatível com o nível exigido pela ANPD.

II – Demonstra maturidade em governança e accountability.

III – Permite tomada de decisão consciente, documentada e defensável.

27 PLANO DE AÇÃO PARA TRATAMENTO DE RISCOS ALTOS

(Action Plan – LGPD)

Anexo ao DPIA, Matriz de Risco e Heatmap de Riscos

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

27.1 OBJETIVO

Este Plano de Ação para Tratamento de Riscos Altos ("Action Plan") tem por objetivo definir medidas técnicas, administrativas e organizacionais específicas para mitigar, reduzir ou controlar os riscos classificados como Alto na Matriz de Risco e no Mapa de Calor de Riscos, especialmente aqueles relacionados ao tratamento de dados pessoais sensíveis, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

27.2 ESCOPO E VINCULAÇÃO

Este Plano aplica-se aos riscos classificados como Alto Impacto e/ou Alta Probabilidade, identificados no:

I – DPIA – Avaliação de Impacto à Proteção de Dados.

II – Matriz de Risco (Impacto × Probabilidade).

III – Heatmap de Risco.

Integra o Programa de Governança em Privacidade da Ê-SISTEMAS.

27.3 METODOLOGIA DE TRATAMENTO DE RISCOS

Os riscos altos são tratados conforme as seguintes estratégias:

I – Mitigação: redução da probabilidade e/ou impacto.

II – Controle: manutenção do risco em nível aceitável com monitoramento contínuo.

III – Evitação: interrupção ou redesign do tratamento, quando aplicável.

IV – Aceitação condicionada: apenas quando tecnicamente justificada e documentada.

27.4 RISCOS CLASSIFICADOS COMO ALTOS

Conforme a Matriz de Risco e o Heatmap, foram identificados como Riscos Altos:

Nº	Risco Identificado	Contexto
R1	Vazamento de dados pessoais sensíveis	Chatbot Saúde

R2	Acesso indevido por falha de credenciais	Sistemas com dados sensíveis

27.5 PLANO DE AÇÃO POR RISCO

27.5.1 RISCO R1 – Vazamento de Dados Pessoais Sensíveis

Classificação:

I – Impacto: Alto.

II – Probabilidade: Média.

III – Nível: Alto.

Ações de Mitigação:

Ação	Descrição	Responsável	Prazo
A1	Criptografia de dados sensíveis em repouso e em trânsito	Técnico/TI	Curto prazo
A2	Revisão de minimização de dados coletados	DPO + Produto	Curto prazo
A3	Segregação lógica de bases com dados sensíveis	TI	Médio prazo
A4	Revisão de logs e monitoramento de acessos	TI	Contínuo
A5	Testes de segurança periódicos (pentest/scan)	TI / Terceiro	Longo Prazo
A6	Treinamento específico sobre dados sensíveis	DPO	Médio prazo

Risco Residual Esperado: Médio (controlado).

27.5.2 RISCO R2 – Acesso Indevido por Falha de Credenciais

Classificação:

I – Impacto: Alto.

II – Probabilidade: Média.

III – Nível: Alto.

Ações de Mitigação:

Ação	Descrição	Responsável	Prazo

B1	Implementação de autenticação multifator (MFA)	TI	Curto prazo
B2	Política de senhas fortes e rotação periódica	TI	Curto prazo
B3	Revisão periódica de perfis e acessos	DPO + TI	Longo prazo
B4	Revogação imediata de acessos após desligamento	RH + TI	Contínuo
B5	Monitoramento de acessos suspeitos	TI	Contínuo
B6	Conscientização sobre phishing e engenharia social	DPO	Curto Prazo

Risco Residual Esperado: Médio (controlado).

27.6 INDICADORES DE ACOMPANHAMENTO (KPIs)

Serão utilizados, entre outros:

I – Número de incidentes envolvendo dados sensíveis.

II – Tempo médio de resposta a incidentes.

III – Percentual de usuários com MFA ativo.

IV – Conformidade com revisões periódicas de acesso.

V – Resultados de testes de backup e recuperação.

27.7 GOVERNANÇA E ACOMPANHAMENTO

I – O DPO será responsável por monitorar a execução deste Plano.

II – A Administração acompanhará riscos críticos e decisões estratégicas.

III – A evolução das ações será registrada e documentada.

IV – O Plano poderá ser ajustado conforme mudanças nos tratamentos ou riscos.

27.8 ACEITAÇÃO DO RISCO RESIDUAL

Após a implementação das ações previstas:

I – Os riscos inicialmente classificados como Altos passam a Risco Residual Médio.

II – O risco residual é considerado aceitável, desde que mantidos os controles técnicos e organizacionais.

III – Não foi identificada necessidade de consulta prévia à ANPD, nos termos do art. 38 da LGPD.

27.9 REVISÃO E ATUALIZAÇÃO

Este Plano de Ação será revisado:

I – Periodicamente.

II – Após incidentes relevantes.

III – Em caso de alteração significativa nos tratamentos.

IV – Por solicitação do controlador ou da ANPD.

27.10 – APROVAÇÃO

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: 02 / 02 / 2026.

28 POLÍTICA DE ACEITAÇÃO DE RISCOS

(Privacy & Security Risk Acceptance Policy)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade, da Avaliação de Impacto à Proteção de Dados (DPIA), da Matriz de Risco, do Heatmap de Riscos e do Plano de Ação para Tratamento de Riscos.

28.1 OBJETIVO

Esta Política de Aceitação de Riscos tem por objetivo estabelecer critérios, limites, responsabilidades e procedimentos para a aceitação formal de riscos residuais relacionados ao tratamento de dados pessoais e à segurança da informação pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e com as boas práticas de governança, compliance e gestão de riscos.

28.2 PRINCÍPIOS NORTEADORES

A aceitação de riscos observará, obrigatoriamente, os seguintes princípios:

I – Accountability: demonstração documentada de decisões conscientes e responsáveis.

II – Proporcionalidade: avaliação equilibrada entre risco, impacto, custo e benefício.

III – Prevenção: priorização da mitigação sempre que tecnicamente viável.

IV – Transparência interna: decisões formalmente registradas.

V – Proteção dos direitos dos titulares: preservação das liberdades fundamentais.

28.3 DEFINIÇÕES

Para fins desta Política:

I – Risco Inerente: risco existente antes da aplicação de controles.

II – Risco Residual: risco remanescente após a aplicação de medidas técnicas e administrativas.

III – Aceitação de Risco: decisão formal de conviver com determinado risco residual.

IV – Risco Aceitável: risco residual considerado tolerável dentro do apetite de risco da empresa.

V – Risco Não Aceitável: risco que exige mitigação, redesign ou evitação.

28.4 CLASSIFICAÇÃO DOS RISCOS PARA ACEITAÇÃO

Com base na Matriz de Risco e no Heatmap:

28.4.1 Riscos Aceitáveis

Podem ser aceitos formalmente:

I – Riscos classificados como Baixo.

II – Riscos classificados como Médio, desde que:

II.I - Existam controles técnicos e organizacionais adequados.

II.II - O risco residual seja considerado controlado.

II.III - Não haja impacto desproporcional aos titulares.

28.4.2 Riscos Não Aceitáveis

Não poderão ser aceitos automaticamente:

I – Riscos classificados como Alto, sem plano de mitigação.

II – Riscos que envolvam dados pessoais sensíveis sem controles reforçados.

III – Riscos que possam resultar em violação grave de direitos fundamentais.

IV – Riscos decorrentes de descumprimento deliberado da LGPD.

28.5 CRITÉRIOS PARA ACEITAÇÃO DE RISCO RESIDUAL

A aceitação de risco residual somente poderá ocorrer quando:

I – Todas as medidas razoáveis de mitigação tiverem sido avaliadas.

II – O risco residual for classificado como Baixo ou Médio.

III – O impacto aos titulares for limitado e controlável.

IV – A decisão estiver alinhada ao DPIA e ao Plano de Ação.

V – A aceitação estiver formalmente documentada.

28.6 PROCESSO FORMAL DE ACEITAÇÃO DE RISCO

A aceitação seguirá as seguintes etapas:

I – Identificação do risco no DPIA, Matriz ou Heatmap.

II – Avaliação do impacto e da probabilidade.

III – Análise das medidas de mitigação existentes.

IV – Classificação do risco residual.

V – Parecer técnico do DPO.

VI – Decisão da Administração.

VII – Registro formal da aceitação.

28.7 PROCEDIMENTO PARA RISCOS NÃO ACEITÁVEIS

Se classificado como Não Aceitável:

I – Desenvolvimento de plano de mitigação emergencial.

II – Consulta a especialista externo (opcional).

III – Reunião extraordinária dos sócios.

IV – Decisão por maioria qualificada.

V – Registro detalhado justificando exceção.

A eventual exceção não configura precedente automático para situações futuras.

28.8 RESPONSABILIDADES

28.8.1 Administração

I – Aprovar a aceitação de riscos residuais.

II – Definir o apetite de risco da empresa.

III – Garantir recursos para mitigação quando necessária.

28.8.2 Encarregado de Proteção de Dados (DPO)

I – Avaliar impactos à privacidade e aos titulares.

II – Emitir parecer técnico sobre a aceitabilidade do risco.

III – Garantir alinhamento com a LGPD.

28.8.3 Área de TI / Segurança da Informação

I – Informar riscos técnicos e operacionais.

II – Implementar controles aprovados.

III – Monitorar riscos aceitos.

28.9 DOCUMENTAÇÃO E REGISTROS

Toda aceitação de risco deverá ser documentada, contendo, no mínimo:

I – Descrição do risco.

II – Classificação de impacto e probabilidade.

III – Medidas de mitigação existentes.

IV – Justificativa da aceitação.

V – Nível de risco residual.

VI – Responsável pela decisão.

VII – Data e prazo de reavaliação.

Os registros integrarão o Programa de Governança em Privacidade.

28.10 REAVALIAÇÃO DOS RISCOS ACEITOS

Os riscos aceitos deverão ser reavaliados:

I – Periodicamente.

II – Em caso de incidentes de segurança.

III – Quando houver mudança no tratamento de dados.

IV – Por solicitação do controlador ou da ANPD.

V – Em revisões do DPIA.

28.11 CONSEQUÊNCIAS DA ACEITAÇÃO

Aceitação não significa:

I – Autorização para ignorar o risco.

II – Não precisa monitorar.

III – Isenta de responsabilidade em incidente.

IV – Dispensa compliance com LGPD.

Aceitação significa:

I – Decisão consciente com alternativas avaliadas.

II – Compromisso com monitoramento contínuo.

III – Reavaliação periódica obrigatória.

IV – Comunicação transparente internamente.

28.12 LIMITAÇÕES DA ACEITAÇÃO DE RISCO

A aceitação de risco:

I – Não elimina a responsabilidade legal da empresa.

II – Não afasta obrigações previstas na LGPD.

III – Não se aplica a situações de dolo, negligência grave ou descumprimento deliberado da lei.

IV – Não impede a adoção posterior de novas medidas de mitigação.

28.13 INTEGRAÇÃO COM OUTROS DOCUMENTOS

Esta Política está integrada a:

I – DPIA.

II – Matriz de Risco e Heatmap.

III – Plano de Ação para Riscos Altos.

IV – Política de Segurança da Informação (PSI).

V – Procedimento de Incidentes de Segurança.

VI – Seguro Cibernético (quando aplicável).

28.14 VIGÊNCIA E REVISÃO

Esta Política entra em vigor na data de sua aprovação e será revisada:

I – Periodicamente.

II – Após incidentes relevantes.

III – Em caso de alteração legislativa ou regulatória.

IV – Por decisão da Administração.

28.15 APROVAÇÃO

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: 02/ 02 / 2026.

29 FORMULÁRIO DE ACEITAÇÃO FORMAL DE RISCO

(Risk Acceptance Form – LGPD & Segurança da Informação)

Versão para Assinatura Eletrônica

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade, da Política de Aceitação de Riscos, do DPIA, da Matriz de Risco, do Heatmap de Riscos e do Registro Centralizado de Riscos Aceitos (Risk Register).

29.1 IDENTIFICAÇÃO DO RISCO

Identificador do Risco: _____

Descrição do Risco:

Contexto do Tratamento de Dados:

Tipo de dados envolvidos:

☐ Dados pessoais comuns

☐ Dados pessoais sensíveis

☐ Ambos

29.2 CLASSIFICAÇÃO DO RISCO

Risco Inerente:

I – Impacto: ☐ Baixo ☐ Médio ☐ Alto

II – Probabilidade: ☐ Baixa ☐ Média ☐ Alta

Risco Residual (após mitigação):

I – Impacto: ☐ Baixo ☐ Médio

II – Probabilidade: ☐ Baixa ☐ Média

Classificação Final do Risco Residual:

☐ Baixo ☐ Médio

29.3 MEDIDAS DE MITIGAÇÃO ADOTADAS

Medidas técnicas, administrativas e organizacionais implementadas:

Controles aplicáveis (quando pertinente):

☐ Política de Segurança da Informação

☐ Controles de acesso

☐ Criptografia

☐ Treinamento de colaboradores

☐ Monitoramento e logs

☐ Plano de Resposta a Incidentes

☐ Outros: _____

29.4 JUSTIFICATIVA PARA ACEITAÇÃO DO RISCO

A aceitação do risco residual fundamenta-se em:

☐ Risco residual classificado como Baixo

☐ Risco residual classificado como Médio; com controles adequados

☐ Impacto limitado e controlável aos titulares

☐ Avaliação de custo-benefício

☐ Alinhamento com DPIA e Plano de Ação

Justificativa técnica e jurídica:

29.5 DECLARAÇÃO DE ACEITAÇÃO FORMAL

Declaro que:

I – Todas as medidas razoáveis de mitigação foram avaliadas.

II – O risco residual encontra-se dentro do apetite de risco da empresa.

III – A aceitação não elimina a obrigação de monitoramento contínuo.

IV – A aceitação não afasta responsabilidades legais previstas na LGPD.

Decisão:

☐ Risco formalmente aceito

☐ Risco aceito com monitoramento reforçado

29.6 RESPONSÁVEIS E PARECER DO DPO

Responsável pelo Risco (Risk Owner):

Nome: _____

Cargo: _____

Parecer do Encarregado de Proteção de Dados (DPO):

☐ Favorável

☐ Favorável com ressalvas

☐ Desfavorável

Observações do DPO:

29.7 PRAZO DE REAVALIAÇÃO

Data da aceitação: ____ / ____ / _____

Data limite para reavaliação: ____ / ____ / _____

A reavaliação poderá ocorrer antecipadamente em caso de:

I - Incidente de segurança.

II - Alteração relevante no tratamento de dados.

III - Revisão do DPIA.

IV - Solicitação da Administração ou da ANPD.

V – Alteração legislativa ou regulatória relevante.

29.8 ASSINATURA ELETRÔNICA E VALIDADE JURÍDICA

As partes declaram que este documento é firmado por assinatura eletrônica, nos termos do art. 10 da Medida Provisória nº 2.200-2/2001, da Lei nº 14.063/2020 e demais normas aplicáveis, produzindo plenos efeitos jurídicos, com integridade, autenticidade e não repúdio.

As assinaturas eletrônicas abaixo vinculam os signatários ao conteúdo integral deste Formulário.

29.9 APROVAÇÃO ELETRÔNICA

Aprovador (Administração):

Nome: _____

Cargo: _____

DPO / Encarregado:

Nome: _____

29.10 REGISTRO E ARQUIVAMENTO

☐ Risco registrado no Risk Register

☐ Documento arquivado no Programa de Governança em Privacidade

☐ Documento disponível para auditorias internas, externas e fiscalização da ANPD

30 REGISTRO CENTRALIZADO DE RISCOS ACEITOS

(Risk Register – LGPD & Segurança da Informação)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade, da Política de Aceitação de Riscos, do DPIA, da Matriz de Risco, do Heatmap de Riscos e do Plano de Ação para Tratamento de Riscos.

30.1 OBJETIVO

O presente Registro Centralizado de Riscos Aceitos (“Risk Register”) tem por objetivo consolidar, documentar e acompanhar todos os riscos residuais formalmente aceitos pela Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., relacionados ao tratamento de dados pessoais e à segurança da informação, demonstrando conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), especialmente quanto aos princípios da accountability, prevenção e governança.

30.2 ABRANGÊNCIA

Este Registro aplica-se a:

I – Riscos identificados no DPIA.

II – Riscos classificados na Matriz de Risco e no Heatmap.

III – Riscos tratados no Plano de Ação para Riscos Altos.

IV – Riscos aceitos conforme a Política de Aceitação de Riscos.

Inclui riscos relacionados a:

I – Dados pessoais comuns.

II – Dados pessoais sensíveis.

III – Segurança da informação.

IV – Continuidade de negócios.

30.3 CRITÉRIOS PARA REGISTRO NO RISK REGISTER

Somente poderão constar neste Registro:

I – Riscos com classificação residual Baixa ou Média.

II – Riscos cuja aceitação tenha sido formalmente aprovada pela Administração.

III – Riscos com justificativa técnica documentada.

IV – Riscos com responsável definido e prazo de reavaliação.

Riscos classificados como Alto, sem mitigação, não poderão ser registrados como aceitos.

30.4 ESTRUTURA DO REGISTRO

Cada risco aceito deverá conter, no mínimo:

I – Identificador único do risco.

II – Descrição do risco.

III – Contexto do tratamento.

IV – Impacto e probabilidade.

V – Nível de risco inerente.

VI – Medidas de mitigação aplicadas.

VII – Nível de risco residual.

VIII – Justificativa da aceitação.

IX – Responsável.

X – Status do risco.

30.5 REGISTROS DE RISCOS ACEITOS

RISCO ACEITO Nº RA-01

Descrição: Possibilidade de vazamento acidental de dados pessoais comuns.

Contexto do tratamento: Operação de chatbot de atendimento geral.

Classificação inerente: Impacto médio, probabilidade baixa.

Medidas de mitigação aplicadas:

– Controle de acesso lógico.

– Política de Segurança da Informação.

– Registros de logs e monitoramento.

Risco residual: Baixo.

Justificativa da aceitação: Risco residual controlado, com impacto limitado aos titulares e medidas adequadas implementadas.

Responsável: Encarregado de Proteção de Dados (DPO).

Status: Aceito e monitorado.

RISCO ACEITO Nº RA-02

Descrição: Uso indevido pontual de dados pessoais fora da finalidade original.

Contexto do tratamento: Operações internas e acesso por colaboradores.

Classificação inerente: Impacto médio, probabilidade baixa.

Medidas de mitigação aplicadas:

– Treinamento contínuo de colaboradores.

– Política de Uso Aceitável da Informação.

– Revisão periódica de acessos.

Risco residual: Baixo.

Justificativa da aceitação: Controles administrativos suficientes e risco residual compatível com o apetite de risco da empresa.

Responsável: Encarregado de Proteção de Dados (DPO).

Status: Aceito e monitorado.

RISCO ACEITO Nº RA-03

Descrição: Ataque cibernético direcionado aos sistemas de chatbot.

Contexto do tratamento: Chatbot voltado à área da saúde.

Classificação inerente: Impacto alto, probabilidade baixa.

Medidas de mitigação aplicadas:

– Plano de Continuidade de Negócios (BCP).

– Procedimento de Backup e Recuperação.

– Monitoramento contínuo e Plano de Ação para riscos altos.

Risco residual: Médio.

Justificativa da aceitação: Risco residual reduzido a nível aceitável, com controles técnicos robustos e plano de resposta definido.

Responsável: Administração.

Status: Aceito com monitoramento reforçado.

Com base na existência de controles técnicos reforçados, plano de resposta estruturado e monitoramento contínuo.

30.6 GOVERNANÇA E ACOMPANHAMENTO

I – O DPO é responsável por manter este Registro atualizado.

II – A Administração deverá revisar riscos aceitos em reuniões periódicas.

III – Riscos aceitos devem ser monitorados continuamente.

IV – Qualquer alteração relevante no tratamento exige reavaliação imediata do risco.

30.7 REAVALIAÇÃO E ATUALIZAÇÃO

Os riscos registrados deverão ser reavaliados:

I – No prazo definido para cada risco.

II – Após incidentes de segurança.

III – Em caso de mudança no tratamento de dados.

IV – Em revisões do DPIA.

V – Por solicitação do controlador ou da ANPD.

A reavaliação poderá resultar em:

I - Manutenção da aceitação.

II - Reclassificação do risco.

III - Elaboração de novo plano de ação.

IV - Retirada do risco do status de aceito.

30.8 LIMITAÇÕES DA ACEITAÇÃO REGISTRADA

A inclusão de risco neste Registro:

I – Não elimina responsabilidade legal.

II – Não impede adoção futura de novas medidas.

III – Não se aplica a situações de dolo ou negligência grave.

IV – Não substitui a obrigação de prevenção contínua.

30.9 INTEGRAÇÃO COM OUTROS DOCUMENTOS

Este Registro está integrado a:

I – DPIA.

II – Matriz de Risco.

III – Heatmap de Riscos.

IV – Plano de Ação para Riscos Altos.

V – Política de Aceitação de Riscos.

VI – Política de Segurança da Informação (PSI).

VII – Procedimento de Incidentes de Segurança.

30.10 VIGÊNCIA E APROVAÇÃO

Este Registro entra em vigor na data de sua aprovação e deverá ser mantido atualizado como documento vivo do Programa de Governança em Privacidade.

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: 02 / 02 / 2026.

31 PROGRAMA DE DUE DILIGENCE DE TERCEIROS

(Third-Party Due Diligence Program – LGPD & Segurança da Informação)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade, da Política de Segurança da Informação, do DPIA, da Matriz de Risco, do Heatmap de Riscos, do Plano de Ação para Tratamento de Riscos e da Política de Aceitação de Riscos.

31.1 OBJETIVO

Este Programa de Due Diligence de Terceiros tem por objetivo estabelecer critérios, procedimentos e responsabilidades para a avaliação, seleção, contratação, monitoramento e reavaliação de terceiros que tenham acesso, tratem ou possam impactar dados pessoais, dados pessoais sensíveis, informações confidenciais ou ativos críticos da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA., em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e com as boas práticas de governança, compliance e segurança da informação.

31.2 FUNDAMENTAÇÃO LEGAL E NORMATIVA

Este Programa está fundamentado, especialmente, nos seguintes dispositivos da LGPD:

I – Art. 6º, X – Princípio da accountability.

II – Art. 39 – Responsabilidade do operador.

III – Art. 46 – Medidas técnicas e administrativas de segurança.

IV – Art. 48 – Prevenção e mitigação de incidentes.

V – Art. 50 – Boas práticas e governança em privacidade.

Também observa boas práticas de:

I – Gestão de riscos.

II – Segurança da informação.

III – Compliance e integridade.

IV – Terceirização responsável.

31.3 ABRANGÊNCIA

Este Programa aplica-se a todos os terceiros, pessoas físicas ou jurídicas, incluindo, mas não se limitando a:

I – Fornecedores de tecnologia e infraestrutura.

II – Desenvolvedores, provedores de nuvem e SaaS.

III – Prestadores de serviços com acesso a sistemas ou dados.

IV – Parceiros comerciais e estratégicos.

V – Consultorias, auditorias e suporte técnico.

VI – Suboperadores de dados pessoais.

31.4 DEFINIÇÕES

Para fins deste Programa:

I – Terceiro: qualquer pessoa física ou jurídica que mantenha relação contratual ou pré-contratual com a Ê-SISTEMAS.

II – Operador: terceiro que realiza tratamento de dados pessoais em nome do Controlador.

III – Suboperador: terceiro contratado pelo Operador para executar parte do tratamento.

IV – Due Diligence: processo de avaliação prévia e contínua de riscos.

V – Risco de Terceiros: risco decorrente da atuação, falha ou conduta de terceiros.

31.5 CLASSIFICAÇÃO DE TERCEIROS POR NÍVEL DE RISCO

Os terceiros serão classificados conforme o nível de risco:

31.5.1 Baixo Risco

I – Sem acesso a dados pessoais ou sistemas.

II – Serviços administrativos ou de apoio.

31.5.2 Médio Risco

I – Acesso limitado a dados pessoais comuns.

II – Acesso indireto a sistemas.

31.5.3 Alto Risco

I – Acesso a dados pessoais sensíveis.

II – Acesso direto a sistemas críticos.

III – Tratamento contínuo de dados.

IV – Subcontratação (suboperadores).

31.6 ETAPAS DO PROCESSO DE DUE DILIGENCE

31.6.1 Due Diligence Pré-Contratual

Antes da contratação, poderão ser avaliados:

I – Identificação e qualificação do terceiro.

II – Estrutura organizacional e capacidade técnica.

III – Práticas de segurança da informação.

IV – Conformidade com a LGPD.

V – Existência de políticas internas (PSI, Privacidade, Incidentes).

VI – Histórico de incidentes relevantes.

VII – Certificações ou auditorias (quando aplicável).

31.6.2 Avaliação de Risco

A avaliação considerará:

I – Tipo de dados tratados.

II – Volume e sensibilidade dos dados.

III – Criticidade do serviço.

IV – Dependência operacional.

V – Localização do tratamento e transferência internacional.

31.7 REQUISITOS MÍNIMOS PARA TERCEIROS COM ACESSO A DADOS

Terceiros classificados como Médio ou Alto Risco deverão, no mínimo:

I – Adotar medidas técnicas e administrativas adequadas.

II – Possuir controles de acesso e autenticação.

III – Manter políticas de segurança e privacidade.

IV – Treinar seus colaboradores.

V – Comunicar incidentes de segurança imediatamente.

VI – Submeter-se a auditorias ou avaliações, quando solicitado.

31.8 INSTRUMENTOS CONTRATUAIS

A contratação de terceiros que tratem dados pessoais deverá conter, conforme aplicável:

I – Cláusula de proteção de dados pessoais (DPA).

II – Definição clara de papéis (Controlador / Operador).

III – Obrigações de segurança da informação.

IV – Regras sobre subcontratação.

V – Dever de cooperação com a Ê-SISTEMAS e a ANPD.

VI – Cláusulas de responsabilização e sanções.

VII – Cláusulas de confidencialidade.

31.9 MONITORAMENTO CONTÍNUO

A Due Diligence não se limita à contratação inicial.

O monitoramento contínuo poderá incluir:

I – Reavaliações periódicas.

II – Atualização de informações.

III – Avaliação de incidentes.

IV – Auditorias documentais ou técnicas.

V – Revisão contratual.

31.10 TRATAMENTO DE NÃO CONFORMIDADES

Em caso de não conformidade identificada:

I – Solicitação de plano de correção.

II – Definição de prazo para adequação.

III – Reavaliação do risco.

IV – Aplicação de sanções contratuais.

V – Rescisão contratual, se necessário.

31.11 PAPÉIS E RESPONSABILIDADES

31.11.1 Administração

I – Aprovar critérios e decisões estratégicas.

II – Definir apetite de risco para terceiros.

31.11.2 Encarregado de Proteção de Dados (DPO)

I – Avaliar riscos à privacidade.

II – Emitir parecer técnico.

III – Acompanhar conformidade com a LGPD.

31.11.3 Área de TI / Segurança

I – Avaliar riscos técnicos.

II – Verificar requisitos de segurança.

III – Monitorar acessos e incidentes.

31.12 – REGISTROS E DOCUMENTAÇÃO

Todos os processos de Due Diligence deverão ser documentados, incluindo:

I – Avaliação inicial.

II – Classificação de risco.

III – Decisões de aprovação ou reprovação.

IV – Planos de ação.

V – Reavaliações periódicas.

Os registros integrarão o Programa de Governança em Privacidade.

31.13 REVISÃO E ATUALIZAÇÃO

Este Programa será revisado:

I – Periodicamente.

II – Em caso de incidentes relevantes.

III – Quando houver alteração regulatória.

IV – Por decisão da Administração ou da ANPD.

31.14 VIGÊNCIA E APROVAÇÃO

Este Programa entra em vigor na data de sua aprovação e aplica-se a todos os terceiros da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Responsável pela aprovação:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: 02 / 02 / 2026.

32 QUESTIONÁRIO DE DUE DILIGENCE PARA FORNECEDORES

(Third-Party Due Diligence Questionnaire – LGPD & Segurança da Informação)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Due Diligence de Terceiros, da Política de Segurança da Informação, do DPIA, da Matriz de Risco, do Heatmap de Riscos e do Programa de Governança em Privacidade.

32.1 IDENTIFICAÇÃO DO FORNECEDOR

1.1 Razão social:

1.2 Nome fantasia:

1.3 CNPJ / CPF:

1.4 Endereço:

1.5 Responsável pelo preenchimento:

1.6 Cargo / Função:

1.7 E-mail corporativo:

1.8 Telefone:

32.2 CLASSIFICAÇÃO INICIAL DO FORNECEDOR

(Preenchido pela Ê-SISTEMAS)

☐ Baixo Risco

☐ Médio Risco

☐ Alto Risco

Critério principal:

☐ Não trata dados pessoais

☐ Trata dados pessoais comuns

☐ Trata dados pessoais sensíveis

☐ Possui acesso a sistemas críticos

32.3 QUESTIONÁRIO GERAL (OBRIGATÓRIO PARA TODOS OS NÍVEIS)

32.3.1 O fornecedor trata dados pessoais em nome da Ê-SISTEMAS?

☐ Sim ☐ Não

32.3.2 Caso positivo, atua como:

☐ Operador

☐ Suboperador

☐ Controlador independente

32.3.3 Possui Política de Privacidade formalizada?

☐ Sim ☐ Não

32.3.4 Possui Política de Segurança da Informação (PSI)?

☐ Sim ☐ Não

32.3.5 Possui Encarregado de Proteção de Dados (DPO) ou responsável equivalente?

☐ Sim ☐ Não

32.3.6 Já sofreu incidente de segurança relevante nos últimos 24 meses?

☐ Não

☐ Sim (descrever):

32.3.7 Está ciente das obrigações previstas na LGPD?

☐ Sim ☐ Não

32.4 QUESTIONÁRIO PARA FORNECEDORES DE BAIXO RISCO

(Responder apenas se classificado como Baixo Risco)

32.4.1 Confirma que não terá acesso a dados pessoais da Ê-SISTEMAS?

☐ Sim ☐ Não

32.4.2 Confirma que não terá acesso a sistemas internos ou ambientes produtivos?

☐ Sim ☐ Não

32.4.3 Compromete-se a respeitar cláusulas de confidencialidade contratuais?

☐ Sim ☐ Não

32.5 QUESTIONÁRIO PARA FORNECEDORES DE MÉDIO RISCO

(Responder se classificado como Médio ou Alto Risco)

32.5.1 Quais tipos de dados pessoais poderão ser tratados?

☐ Dados pessoais comuns

☐ Dados cadastrais

☐ Dados profissionais

☐ Outros: _____

32.5.2 O acesso aos dados é:

☐ Limitado

☐ Temporário

☐ Contínuo

32.5.3 Possui controles de acesso lógico aos sistemas?

☐ Sim ☐ Não

32.5.4 Utiliza autenticação forte (ex.: MFA) para acessos administrativos?

☐ Sim ☐ Não

32.5.5 Mantém registros de logs de acesso?

☐ Sim ☐ Não

32.5.6 Possui plano de resposta a incidentes de segurança?

☐ Sim ☐ Não

32.5.7 Realiza treinamentos de segurança e privacidade para colaboradores?

☐ Sim ☐ Não

32.6 QUESTIONÁRIO PARA FORNECEDORES DE ALTO RISCO

(Obrigatório para fornecedores que tratam dados sensíveis ou acessam sistemas críticos)

32.6.1 Os dados tratados incluem dados pessoais sensíveis?

☐ Sim ☐ Não

32.6.2 Quais dados sensíveis poderão ser tratados?

☐ Saúde

☐ Biometria

☐ Dados financeiros

☐ Outros: _____

32.6.3 Os dados são armazenados:

☐ No Brasil

☐ No exterior (informar país): _____

32.6.4 Possui criptografia de dados em repouso e em trânsito?

☐ Sim ☐ Não

32.6.5 Realiza testes de segurança (pentest, vulnerability scan)?

☐ Sim ☐ Não

Periodicidade: _____

32.6.6 Possui backups regulares e testados?

☐ Sim ☐ Não

32.6.7 Subcontrata outros terceiros (suboperadores)?

☐ Não

☐ Sim (listar e descrever controles):

32.6.8 Compromete-se a comunicar incidentes de segurança imediatamente, no prazo máximo de ___ horas, à Ê-SISTEMAS?

☐ Sim ☐ Não

32.6.9 Aceita auditorias, questionários ou reavaliações periódicas de segurança e privacidade?

☐ Sim ☐ Não

32.7 – DECLARAÇÃO DO FORNECEDOR

Declaro que as informações prestadas neste Questionário são verdadeiras, completas e atualizadas, comprometendo-me a comunicar imediatamente qualquer alteração relevante que impacte segurança da informação, privacidade ou proteção de dados pessoais.

Nome do responsável:

Cargo:

Assinatura eletrônica:

Data: ____ / ____ / _____

32.8 AVALIAÇÃO INTERNA (Ê-SISTEMAS)

Parecer do DPO:

☐ Aprovado

☐ Aprovado com ressalvas

☐ Reprovado

Classificação final do risco do fornecedor:

☐ Baixo ☐ Médio ☐ Alto

Decisão:

☐ Contratação autorizada

☐ Contratação condicionada a plano de ação

☐ Contratação não recomendada

Responsável pela decisão:

Cargo:

Data: ____ / ____ / _____

32.9 REGISTRO E GOVERNANÇA

☐ Questionário arquivado no Programa de Due Diligence

☐ Fornecedor registrado no inventário de terceiros

☐ Avaliação vinculada ao DPIA e Matriz de Risco

☐ Reavaliação programada conforme nível de risco

33 TESTE DE BALANCEAMENTO

BANCO DE TALENTOS

Base Legal: Legítimo Interesse (Art. 7º, IX da LGPD)

Empresa: Ê-Sistemas - Recrutamento e Seleção

Operação/Tratamento: Realizar a coleta, armazenamento e análise de currículos e dados pessoais de candidatos, com a finalidade de constituir e manter um Banco de Talentos, visando a utilização em processos futuros de recrutamento e seleção, mesmo que o candidato não tenha sido selecionado no processo atual.

Data do teste: 03/02/2026.

Preenchido por: Thiago Marcos Montagner

Dados pessoais tratados:

Dados: Nome, sexo, nacionalidade, filiação, data de nascimento, CPF, RG, telefone, endereço, email, link de redes sociais, experiência profissional, formação acadêmica, pretensão salarial, cursos realizados, idiomas e proficiência.

Dados sensíveis: opcional; como: raça, deficiência (se fornecidos pelo candidato).

Forma de coleta: Envio direto pelo titular via e-mail, plataforma de RH, formulário online ou redes sociais.

Finalidade do tratamento: Constituir um banco de talentos com o objetivo de viabilizar a participação dos candidatos em processos de recrutamento e seleção promovidos pela Ê-Sistemas.

Os dados serão utilizados para:

- Contatar os candidatos em futuras oportunidades compatíveis com seu perfil profissional.
- Agilizar e facilitar processos seletivos futuros.
- Promover maior eficiência na identificação e contratação de talentos.

Hipótese legal utilizada: legítimo interesse. A empresa tem legítimo interesse em manter um banco de dados com candidatos qualificados, com o objetivo de agilizar futuras contratações, reduzir custos e tempo nos processos seletivos e responder de forma eficiente às necessidades de recrutamento.

Expectativa do Titular dos Dados

O titular, ao enviar seus dados para processos seletivos, espera que eles sejam armazenados por um período razoável e utilizados em futuras oportunidades de emprego.

É comum que o candidato tenha ciência de que seus dados podem ser considerados em seleções futuras, desde que armazenados com segurança, não compartilhados indevidamente e que ele possa solicitar a exclusão a qualquer momento.

33.1 FINALIDADE

Natureza dos dados pessoais: dados pessoais comuns, tais como nome, sexo, nacionalidade, filiação, data de nascimento, CPF, RG, telefone, endereço, e-mail, link de redes sociais, experiências profissionais, formação acadêmica, pretensão salarial, cursos realizados, idiomas e proficiência. Não há tratamento de dados sensíveis. Não é propósito da empresa tratar dados de menores (não há oferta para contratação de jovens aprendizes).

Interesse e finalidades legítimas: o interesse envolve (i) promover serviço de recrutamento e seleção de profissionais para Empresa Cliente XXX, bem como (ii) formação de um banco de talentos para facilitar e otimizar processos seletivos, ampliar as oportunidades de candidatos e atender demandas da Empresa Cliente XXX.

Situação concreta: a Empresa Cliente XXX contratou a XXXX Recrutamento e Seleção para promover a atividade de criação de banco de talentos que permitirá o recrutamento e seleção de profissionais para compor seu quadro de colaboradores.

33.2 NECESSIDADE

Tratamento e finalidade pretendida: o tratamento é necessário para (i) realizar a triagem inicial de candidatos adequada ao perfil das vagas; (ii) manter contato ágil e atualizado com profissionais que integram o banco de talentos; (iii) oferecer indicações de contratação para a Empresa Cliente XXX.

Minimização: apenas os dados estritamente necessários ao processo seletivo e à oferta de vagas são coletados e mantidos em banco de dados limitada (ex: 12 meses), com possibilidade de renovação mediante novo contato com o titular.

33.3 BALANCEAMENTO E SALVAGUARDAS

Legítima expectativa: o tratamento de dados para recrutamento e inclusão em banco de talentos são etapas necessárias para atingimento das expectativas dos titulares dos dados, que pretendem candidatar-se para vaga existente na Empresa Cliente XXX.

- Os dados são ofertados pelo próprio titular, via site.
- Os dados são mantidos pelo tempo necessário ao atingimento da finalidade (preenchimento de vagas).
- Os dados podem ser compartilhados com a Empresa Cliente XXX para a estrita finalidade de preenchimento de vagas e contratação de colaboradores.

Riscos e impactos aos direitos e liberdades fundamentais: o principal risco é o vazamento de informações ou uso não autorizado de dados.

Salvaguardas e mecanismos de oposição:

- A XXXX Recrutamento e Seleção conta com políticas internas voltadas à garantia da segurança da informação compatível com padrões de mercado (controles de acesso, auditoria, treinamento de equipe).
- Os titulares dos dados contam com canal de atendimento facilitado para exercício de direitos, incluindo o acesso aos dados, sua exclusão, correção, atualização ou limitação do tratamento.
- A XXXX Recrutamento e Seleção segue todos os normativos e diretrizes editadas pela ANPD.

33.4 CONCLUSÃO

Após análise das três fases, constatou-se que o tratamento de dados pessoais de candidatos para composição de banco de talentos fundamenta-se em legítimo interesse do controlador, é necessário à finalidade pretendida, atende às legítimas expectativas dos titulares e adota salvaguardas adequadas. O tratamento está aderente aos princípios e demais exigências dispostas na LGPD, assim como às orientações da ANPD.

Local/ Data

_____

Assinaturas

34 CHECKLIST DE EVIDÊNCIAS LGPD

(Documentos, registros e provas para fiscalização, auditoria e defesa administrativa/judicial)

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade e Segurança da Informação, nos termos do art. 50 da LGPD.

34.1 FINALIDADE DO CHECKLIST

Este Checklist tem por objetivo identificar, organizar e padronizar as evidências documentais, técnicas e operacionais que devem ser mantidas pela Ê-SISTEMAS para:

I – Demonstrar conformidade com a LGPD.

II – Atender fiscalizações da ANPD.

III – Responder a incidentes de segurança.

IV – Sustentar defesa administrativa ou judicial.

V – Evidenciar accountability, prevenção e governança.

34.2 EVIDÊNCIAS DE GOVERNANÇA E COMPLIANCE (ART. 50 LGPD)

✓ Programa de Governança em Privacidade (documento-mãe).

✓ Política de Privacidade externa (clientes/usuários).

✓ Política de Segurança da Informação (PSI).

✓ Política de Aceitação de Riscos.

✓ Programa de Awareness contínuo (treinamentos).

✓ Registro de revisões e atualizações dos documentos.

✓ Ata ou evidência de aprovação pela Administração.

Esses documentos demonstram cultura organizacional e compromisso institucional.

34.3 EVIDÊNCIAS DE MAPEAMENTO E AVALIAÇÃO DE RISCOS

✓ DPIA geral.

✓ DPIA específico para dados sensíveis (saúde).

✓ Matriz de Risco (Impacto × Probabilidade).

✓ Heatmap geral de riscos.

✓ Heatmap específico para dados sensíveis (nível ANPD/saúde).

✓ Plano de Ação para riscos altos.

✓ Registros de revisão do DPIA.

Essencial para comprovar prevenção e avaliação prévia de impacto.

34.4 EVIDÊNCIAS DE ACEITAÇÃO E TRATAMENTO DE RISCOS

✓ Registro Centralizado de Riscos Aceitos (Risk Register).

✓ Formulários de Aceitação Formal de Risco assinados eletronicamente.

✓ Justificativas técnicas e jurídicas de aceitação.

✓ Pareceres do DPO.

✓ Registros de monitoramento de riscos aceitos.

✓ Prazos e evidências de reavaliação periódica.

Fundamental para demonstrar decisões conscientes e documentadas.

34.5 EVIDÊNCIAS DE SEGURANÇA DA INFORMAÇÃO (ART. 46 LGPD)

✓ PSI aprovada e vigente.

✓ Procedimento de Backup e Recuperação.

✓ Plano de Continuidade de Negócios (BCP).

✓ Registros de testes de backup e recuperação.

✓ Registros de controle de acesso.

✓ Logs de acesso e monitoramento.

✓ Política de Uso Aceitável da Informação (TUA).

✓ Inventário de ativos e sistemas críticos.

Essas evidências são cruciais após incidentes.

34.6 EVIDÊNCIAS DE INCIDENTES DE SEGURANÇA

✓ Procedimento de Resposta a Incidentes.

✓ Plano de Comunicação de Crise.

✓ Modelos de comunicação (ANPD, titulares, clientes).

✓ Registro de incidentes ocorridos (mesmo sem dano).

✓ Lições aprendidas e medidas corretivas adotadas.

✓ Comunicações enviadas (quando aplicável).

A ANPD avalia mais a resposta do que o incidente em si.

34.7 EVIDÊNCIAS DE RELAÇÃO COM TITULARES

✓ Termo do Usuário / Termos de Uso.

✓ Cláusula de aceite eletrônico e registros de aceite.

✓ Política de Privacidade vigente à época do tratamento.

✓ Registros de solicitações de titulares (DSAR).

✓ Respostas fornecidas e prazos cumpridos.

✓ Canal de atendimento ao titular documentado.

Essencial para direitos do art. 18 da LGPD.

34.8 EVIDÊNCIAS DE BASE LEGAL E FINALIDADE

✓ Mapeamento de tratamentos e finalidades.

✓ Bases legais aplicáveis por operação.

✓ Contratos e termos que justifiquem execução contratual.

✓ Consentimentos (quando utilizados).

✓ Registros de revogação de consentimento (se aplicável).

Evita autuações por tratamento sem base legal.

34.9 EVIDÊNCIAS DE TERCEIROS E CADEIA DE TRATAMENTO

✓ Programa de Due Diligence de Terceiros.

✓ Questionários de fornecedores (baixo / médio / alto risco).

✓ Classificação de risco dos fornecedores.

✓ Contratos com cláusulas de proteção de dados.

✓ Aditivos ou DPAs (Data Processing Agreements).

✓ Registros de reavaliação periódica.

Responsabilização solidária é ponto sensível para a ANPD.

34.10 EVIDÊNCIAS DE TREINAMENTO E AWARENESS

✓ Programa de Awareness contínuo.

✓ Conteúdos de treinamento aplicados.

✓ Listas de presença ou logs de treinamento online.

✓ Treinamentos específicos (TI, saúde, DPO, gestores).

✓ Comunicações internas sobre privacidade e segurança.

Comprova prevenção e redução de erro humano.

34.11 EVIDÊNCIAS DE PRIVACIDADE DESDE A CONCEPÇÃO (PRIVACY BY DESIGN)

✓ Análises de privacidade em novos projetos.

✓ Registros de decisões de arquitetura.

✓ Integração com DPIA e Matriz de Risco.

✓ Documentação de controles técnicos adotados.

Muito valorizado em fiscalizações maduras.

34.12 EVIDÊNCIAS DE MATURIDADE E MELHORIA CONTÍNUA

✓ Documento de alinhamento à ISO 27001/27701.

✓ Roadmap de maturidade (se existente).

✓ Auditorias internas ou avaliações independentes.

✓ Planos de melhoria contínua.

✓ Revisões periódicas do Programa de Governança.

Demonstra evolução e não conformidade estática.

34.13 ORGANIZAÇÃO E ARQUIVAMENTO DAS EVIDÊNCIAS

Recomenda-se que todas as evidências sejam:

I – Centralizadas (repositório seguro).

II – Versionadas.

III – Datadas.

IV – Com controle de acesso.

V – Mantidas pelo prazo legal ou enquanto o tratamento existir.

34.14 CONSIDERAÇÃO FINAL

A manutenção deste Checklist atualizado não garante ausência de incidentes, mas fortalece significativamente a posição da empresa perante:

I – ANPD.

II – clientes.

III – parceiros.

IV – Judiciário.

A autoridade avalia boa-fé, diligência, prevenção e resposta, e este conjunto de evidências atende plenamente a esses critérios.

35 PACOTE DE EVIDÊNCIAS LGPD PARA CLIENTES

Proteção de Dados Pessoais e Segurança da Informação

Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

CNPJ: 53.695.158/0001-90

Documento integrante do Programa de Governança em Privacidade e Segurança da Informação.

35.1 FINALIDADE DO PACOTE DE EVIDÊNCIAS

O presente Pacote de Evidências LGPD para Clientes tem por finalidade demonstrar, de forma objetiva, organizada e proporcional, a conformidade da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA. com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), bem como com boas práticas de segurança da informação, governança e gestão de riscos.

Este pacote é destinado a:

- Clientes e parceiros comerciais.
- Processos de due diligence.
- Questionários de compliance e privacidade.
- Auditorias contratuais.
- Avaliação pré-contratual ou periódica.

35.2 PRINCÍPIOS DO COMPARTILHAMENTO DE EVIDÊNCIAS

A disponibilização das evidências observa:

- Accountability (art. 6º, X, LGPD).
- Necessidade e proporcionalidade.
- Confidencialidade e segurança.
- Segregação entre documentos públicos e internos.

Documentos sensíveis ou estratégicos poderão ser:

- Apresentados de forma resumida.
- Compartilhados sob NDA.
- Demonstrados apenas por evidência indireta (declarações, extratos ou pareceres).

35.3 ESTRUTURA DO PACOTE DE EVIDÊNCIAS

O Pacote está organizado por camadas de maturidade, permitindo fácil validação por áreas jurídica, compliance, segurança e privacidade do cliente.

35.4 EVIDÊNCIAS DE GOVERNANÇA E COMPLIANCE

Disponibilizáveis aos clientes:

- Declaração de Conformidade com a LGPD.
- Programa de Governança em Privacidade (sumário executivo).
- Código de Ética e Conduta.
- Termo de Ciência e Compromisso dos colaboradores.
- Política de Aceitação de Riscos (versão pública).
- Índice Geral do Kit de Governança.

Finalidade: demonstrar estrutura formal, comprometimento da alta direção e governança ativa.

35.5 EVIDÊNCIAS DE PRIVACIDADE E PROTEÇÃO DE DADOS

Disponibilizáveis aos clientes:

- Política de Privacidade.
- Aviso de Privacidade / Privacidade do Cliente.
- Termo do Usuário (quando aplicável).
- Procedimento de Atendimento aos Direitos dos Titulares (DSAR).
- Identificação do Encarregado de Proteção de Dados (DPO).

Finalidade: demonstrar transparência, legalidade e respeito aos direitos dos titulares.

35.6 EVIDÊNCIAS DE SEGURANÇA DA INFORMAÇÃO

Disponibilizáveis de forma controlada:

- Política de Segurança da Informação (PSI – versão resumida).
- Termo de Uso Aceitável da Informação (TUA).
- Procedimento de Controle de Acesso (descrição geral).
- Procedimento de Backup e Recuperação (visão macro).
- Declaração de uso de controles técnicos (MFA, logs, backups, antivírus, firewall).

Finalidade: comprovar adoção de medidas técnicas e administrativas (art. 46, LGPD).

35.7 EVIDÊNCIAS DE GESTÃO DE RISCOS E DPIA

Disponibilizáveis sob critério:

- Declaração de realização de DPIA.
- Sumário executivo do DPIA (sem exposição técnica sensível).
- Matriz de Risco (modelo).
- Heatmap de Riscos (visão consolidada).
- Plano de Ação para riscos altos (status geral).

Quando aplicável:

- Declaração de DPIA específico para dados sensíveis (ex.: saúde).

Finalidade: demonstrar avaliação de impacto, prevenção e gestão ativa de riscos.

35.8 EVIDÊNCIAS DE CONTINUIDADE E RESILIÊNCIA

Disponibilizáveis aos clientes:

- Declaração de existência de Plano de Continuidade de Negócios (BCP).
- Declaração de Procedimento de Backup e Recuperação.
- Evidência de testes periódicos (declaração ou extrato).

Finalidade: demonstrar resiliência operacional e proteção contra indisponibilidade.

35.9 EVIDÊNCIAS DE INCIDENTES E COMUNICAÇÃO

Disponibilizáveis sob solicitação:

- Procedimento de Incidentes de Segurança.
- Plano de Comunicação de Crise.
- Modelos de comunicação (ANPD, titulares e clientes).
- Declaração de histórico de incidentes relevantes (quando aplicável).

Finalidade: demonstrar prontidão, transparência e capacidade de resposta.

35.10 EVIDÊNCIAS DE TERCEIROS E CADEIA DE TRATAMENTO

Disponibilizáveis aos clientes:

- Programa de Due Diligence de Terceiros.
- Questionário de fornecedores (modelo).
- Classificação de risco de terceiros.
- Cláusulas contratuais de proteção de dados.
- Compromisso com suboperadores.

Finalidade: demonstrar controle da cadeia de tratamento (art. 39 e 42, LGPD).

35.11 EVIDÊNCIAS DE CONSCIENTIZAÇÃO (AWARENESS)

Disponibilizáveis:

- Programa de Awareness contínuo.
- Declaração de treinamentos periódicos.
- Evidência de comunicação interna em LGPD e segurança.

Finalidade: demonstrar cultura organizacional e redução de risco humano.

35.12 CERTIFICAÇÕES E REFERENCIAIS

Quando aplicável:

- Alinhamento às normas ISO 27001 e ISO 27701.
- Roadmap de certificação ou adequação contínua.
- Evidências de boas práticas reconhecidas pelo mercado.

35.13 LIMITAÇÕES DO PACOTE DE EVIDÊNCIAS

Este Pacote:

- Não substitui auditoria técnica completa.
- Não implica transferência de responsabilidade legal.
- Não autoriza acesso irrestrito a documentos internos.
- Pode ser atualizado periodicamente.

35.14 CONFIDENCIALIDADE E USO DAS INFORMAÇÕES

As informações fornecidas neste Pacote:

- Destinam-se exclusivamente à avaliação de conformidade.
- Não podem ser reproduzidas ou compartilhadas sem autorização.
- Estão protegidas por dever de confidencialidade e, quando aplicável, por NDA.

35.15 VIGÊNCIA E RESPONSABILIDADE

Este Pacote reflete a situação de governança vigente na data de sua emissão e integra o Programa de Governança em Privacidade da Ê-SISTEMAS.

Responsável:

Administração da Ê-SISTEMAS SOLUÇÕES TECNOLÓGICAS LTDA.

Assinatura: _____

Data: ____ / ____ / _____

gov.br Documento assinado digitalmente
THIAGO MARCOS MONTAGNER
Data: 26/03/2026 15:54:52-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
PEDRO HENRIQUE SILVEIRA
Data: 26/03/2026 08:06:35-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
VINICIUS RICARDO TREVISAN
Data: 26/03/2026 13:28:05-0300
Verifique em https://validar.iti.gov.br

CONSIDERAÇÕES FINAIS

A proteção de dados pessoais, para a Ê-Sistemas, é um componente estrutural da operação, nos termos da Lei nº 13.709/2018. Este conjunto normativo e operacional consolida o compromisso da empresa com a conformidade à LGPD, com a segurança da informação e com uma governança capaz de sustentar o serviço na rotina real, e também sob auditoria, diligência, incidentes ou exigências de clientes e órgãos de controle.

De forma prática, a Ê-Sistemas se orienta por cinco compromissos permanentes:

I – **Finalidade e necessidade**

Tratar dados pessoais de forma vinculada à entrega do serviço e às obrigações aplicáveis, evitando excesso e uso incompatível.

II – **Transparência e previsibilidade**

Manter comunicação clara sobre o tratamento de dados, distinguindo documentos públicos de governança interna e assegurando previsibilidade aos titulares e clientes.

III – **Segurança proporcional ao risco**

Aplicar medidas técnicas e organizacionais compatíveis com a operação, com controles, registros e boas práticas reconhecidas de segurança da informação, ajustadas ao contexto de uso.

IV – **Resposta e rastreabilidade**

Atuar com prontidão e método diante de solicitações de titulares e incidentes de segurança, com registro das ações, comunicação responsável, correção de falhas e incorporação das lições aprendidas.

V – **Melhoria contínua**

Revisar periodicamente políticas, procedimentos e registros, acompanhando a evolução dos produtos, integrações, exigências contratuais e mudanças no ambiente regulatório.

O Programa, aqui apresentado, é tratado como um sistema vivo. Seu conjunto integrado de documentos e rotinas existe para reduzir risco, proteger titulares, preservar a continuidade do serviço e fortalecer a confiança. Com isso, a Ê-Sistemas reforça sua postura de responsabilidade na gestão de dados pessoais, alinhando privacidade, segurança e operação como pilares do negócio. A governança em privacidade é tratada, assim, como fator de sustentabilidade, competitividade e credibilidade institucional.