PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS

1. CONSIDERANDOS

- Considerando que a RAPIDONET é uma empresa que atua no ramo de sistemas, com especialidade nas áreas de inteligência em gestão do trabalho, segurança patrimonial e sistemas de identificação.

- Considerando que nosso modelo de negócios e posicionamento institucional se baseiam em quatro pilares fundamentais que norteiam a atuação empresarial: ética, credibilidade, transparência, inovação. São obrigações inegociáveis, para os quais não existe tolerância/exceção a desvios.

- Considerando que a RAPIDONET adota critérios legais (aderência às leis nacionais), normas, padrões e regulamentos internos, princípios éticos, boas práticas em segurança da informação e transparência na relação com clientes e parceiros. Além de constante aprimoramento, treinamento e capacitação da equipe (força de trabalho) e governança (alta administração). Isso porque todos os empregados, colaboradores e parceiro são responsáveis por proteger nossos princípios, valores, compromissos e impedir eventuais condutas não conformes.

- Considerando que, no curso de suas atividades, a RAPIDONET processa Dados Pessoais relacionados a seus funcionários/parceiros, clientes, prestadores de serviços e fornecedores.

A RAPIDONET assume o compromisso de proteger tais dados, motivo pelo qual implanta este Programa de Governança em Proteção de Dados, nos termos da Lei nº. 20.489/2019 e artigo 50 da Lei Geral de Proteção de Dados (LGPD), cujo objetivo é : I) estar em consonância com as leis e regulamentações aplicáveis de proteção de Dados Pessoais e Privacidade; II) resguardar os direitos dos funcionários, clientes, fornecedores, contribuintes e parceiros contra os riscos de violações de Privacidade e Dados Pessoais; III) ser cristalino com relação aos procedimentos da entidade no

Tratamento de Dados Pessoais; e IV) incentivar e disseminar as diretrizes relacionadas a proteção de Dados Pessoais e questões de privacidade.

2. PRINCÍPIOS E DIREITOS

A proteção de dados pessoais caracteriza-se como expressão de garantia a direitos fundamentais expressamente albergados pela Constituição da República de 1988, resguardados pela Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) e lei nº. 20.489/2019.

É bem verdade que, para viabilizar a prestação de serviço (processar, faturar e enviar seus pedidos), responder as solicitações/questionamentos e cumprir obrigações contratuais e legais, a RAPIDONET efetua o tratamento de dados. Para tanto, adota os princípios da Adequação, Necessidade, Transparência, Livre Acesso, Qualidade dos Dados, Segurança, Prevenção e da Responsabilização e Prestação de Contas (Art. 6º da Lei Geral de Proteção de Dados). Isso porque:

- ✓ Serão coletados dados mínimos e indispensáveis para a finalidade da empresa;
- ✓ Solicita o consentimento expresso do cliente, parceiro ou prestador de serviço para manipular as informações cedidas;
- ✓ Informa o propósito (interesse legítimo) na captura de dados;
- ✓ Permite a alteração e retirada dos dados pessoais sempre que solicitado. e, neste caso, o tratamento de seus dados serão interrompidos no prazo de 24 (vinte e quatro) horas, exceto se existir alguma imposição contratual ou legal;
- ✓ Utiliza medidas técnicas e administrativas aptas a proteger os dados pessoais (mecanismos de segurança para impossibilitar vazamento de dados, perda e alteração);
- ✓ Limita os funcionários que manipulam os dados para reduzir os riscos de transferência de informações. Em paralelo, treinar e orientar os encarregados sobre o normativo legal, responsabilidade no manuseio e as respectivas penalidades;

- ✓ Proíbe a instalação ou remoção de software que coloque o sistema (rede) e/ou dados coletados em vulnerabilidade;
- ✓ Não permite a impressão de documentos ou backup, por qualquer meio e forma, de quaisquer documentos fornecidos.

A manipulação, venda e redirecionamento de informações à terceiros são condutas repudiadas e rechaçadas pela RAPIDONET.

3. ABRANGÊNCIA E RESPONSABILIDADES DOS INTEGRANTES

3.1 Relacionamento com os funcionários e alta administração

Os integrantes/parceiros da RAPIDONET são responsáveis por entender, observar, seguir e disseminar o presente Programa de Governança em Proteção de Dados. Como consequência lógica, comportamentos desconformes devem ser reportados para adoção de medidas de prevenção e/ou remediação de riscos.

Os líderes, como todos integrantes, devem de agir de forma ética, íntegra e transparente. Além de orientar, capacitar (incentivar o debate) e influenciar os liderados. Sempre de forma proativa, colaborando com a auditoria interna e o mapeamento de riscos.

A participação da alta administração (controlador), é fundamental para a concretização das ações relacionadas ao cumprimento das obrigações estipuladas pela Lei Geral de Proteção de Dados.

3.2 Relacionamento com fornecedores

As relações com fornecedores e prestadores de serviços devem ser abalizadas na transparência, respeito e confiança e na construção de relações negociais mutuamente satisfatórias.

A RAPIDONET assegura que o contrato firmado entre as partes possui cláusulas de privacidade e proteção de dados pessoais que assegure, no mínimo, medidas de

segurança, controles técnicos e administrativos apropriados para garantir a confidencialidade das informações.

Ademais, a RAPIDONET incentiva que os Terceiros implementem programas de Compliance próprios, compatíveis com os parâmetros estabelecidos neste Manual.

3.3 Relacionamento com cliente

A sustentabilidade dos negócios e a perenidade da empresa são objetivos estratégicos que dependem da satisfação dos clientes (ativos intangíveis). Para concretizar suas expectativas são implantados altos padrões éticos e as melhores práticas de mercado.

Os integrantes devem:

- ✓ Garantir a conformidade com a legislação, cumprir manuais de procedimento e boas práticas;
- ✓ Conduzir suas atividades com observância aos princípios éticos, responsabilidade, transparência, competência e diligência;
- ✓ Oferecer o melhor serviço/tratamento de forma clara, completa e precisa;
- ✓ Divulgar as informações dos clientes apenas quando estritamente necessário ao desempenho da atividade. É vedado a divulgação, em qualquer mídia, de quaisquer informações dos clientes, salvo em casos autorizados pelo cliente ou por ordem judicial;
- ✓ Proibir qualquer tipo de discriminação com base em etnia, credo, nacionalidade, sexo, idade, cidadania, religião, origem regional, deficiências físicas, estado civil, assédio;

4. COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Para fazer valer as disposições acima, este manual constitui a criação permanente do Comitê de Privacidade e Proteção de Dados Pessoais (“Comitê”) para administrar atividades relacionadas à Privacidade e Proteção de Dados e tem como desígnio

promover o conhecimento e garantir ações voltadas ao aperfeiçoamento das disposições legais relacionadas a Proteção de Dados.

Este comitê demonstrará o cumprimento deste manual, garantindo a implementação de diversas medidas que incluem, mas não se limitam a: assegurar que os Titulares dos Dados Pessoais possam exercer os seus direitos previsto no ordenamento jurídico, aconselhar que fornecedores/parceiros contratados pela empresa que tenham acesso aos Dados Pessoais também estejam agindo de acordo a legislação e avalizar que a empresa cumpra todas as exigências e solicitações da ANPD (Autoridade Nacional de Proteção de Dados).

Os integrantes do Comitê gozam de plena autonomia em relação aos dirigentes/líderes da Instituição e é composto por:

- Encarregado de Dados;
- Responsável Jurídico;
- Responsável por Pessoas (departamento pessoal ou recursos humanos).

A reunião ordinária deverá acontecer a cada semestre com a presença de todos os integrantes, preferencialmente em janeiro e julho, ou extraordinariamente sempre mediante convocação.

5. ENCARREGADO DE DADOS

A RAPIDONET, em consonância ao que dispõe o art. 5º, VIII, Lei nº. 13.709/2018 (Lei Geral de Proteção de Dados) nomeou o Sr. Cristhian Alessander de Queiroz, brasileiro, casado, inscrito no CPF sob o nº. 723.751.671-04, como Encarregado de dados (*Data Protection Officer*), para atuar como canal de comunicação e/ou intermediação entre a empresa, os titulares dos dados pessoais (funcionários, fornecedores e clientes) e o próprio governo através da Autoridade Nacional.

Em cumprimento ao que dispõe o art. 41 da LGPD, o Encarregado precisa ter sua identidade e informações de contatos divulgadas publicamente. Por isso, a comunicação

com o Encarregado é realizada através do e-mail institucional: cristhian@rapidonet.com.br.

O Encarregado possui, dentre suas funções:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências (Artigo 41, inciso I do parágrafo segundo). Isso significa atuar como ponto de contato para o exercício dos direitos dos titulares de dados, processamento de suas consultas e das solicitações pertinentes ao objeto da Lei;

- Receber comunicações da autoridade nacional e adotar providências (Artigo 41, inciso II do parágrafo segundo), ou seja, cooperar com a autoridade e demais órgãos administrativos e judiciais, sempre conciliando a proteção do titular e os direitos da Controladora;

- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (Artigo 41, inciso III do parágrafo segundo), garantindo a conscientização e treinamento do pessoal envolvido nas operações de tratamento de dados;

- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (Artigo 41, inciso IV do parágrafo segundo);

- Possui acesso direto à Alta Administração para alinhar com os demais integrantes as etapas da adequação à LGPD que serão priorizadas.

O Encarregado deve atuar de forma autônoma e independente em todas as suas atividades. Da mesma forma, precisará conduzir suas tarefas com sigilo e confidencialidade.

6. PADRÕES DE SEGURANÇA

A RAPIDONET, por si e por seus Representantes, se compromete, nos termos do art. 46 da LGPD, a aplicar medidas técnicas e organizacionais de segurança da informação e governança corporativa aptas a proteger os Dados Pessoais tratados.

São utilizados mecanismos de segurança para proteção contra invasões e/ou *hackers* que bloqueará vazamento, perda e alteração desconsentida de informações.

Em qualquer hipótese, os colaboradores deverão ficar atentos as seguintes situações:

- ✓ Encaminhamento de e-mails com caracteres e/ou arquivos suspeitos;
- ✓ Comportamento impróprio de dispositivos;
- ✓ Problema no acesso a determinados arquivos e/ou serviços;
- ✓ Roubo de dispositivos de armazenamento ou computadores com informações;
- ✓ Alerta de software antivírus;
- ✓ Consumo excessivo e repentino de memória em servidores ou computadores;
- ✓ Tráfego de rede incomum;
- ✓ Conexões bloqueadas por firewall;
- ✓ *logs* de tentativas de acesso não autorizado aos servidores;
- ✓ Não cumprimento dos procedimentos internos.

7. A RAPIDONET SEGUE AS SEGUINTES ETAPAS

7.1 Prevenção

Os recursos financeiros são, preferencialmente, canalizados na Prevenção, a fim de evitar danos na imagem, financeiros e legais. Para tanto, a atuação da liderança é fundamental, eis que inspira os demais integrantes a agir em conformidade com os pilares fundamentais que norteiam a atuação empresarial (ética, credibilidade, transparência, inovação, qualidade, respeito à vida e responsabilidade social), além da capacitação da equipe. Da mesma forma, o engajamento de parceiros/terceiros, independente do vínculo, é essencial.

As políticas e demais orientações devem ser difundidas e reiteradas (capacitação) de forma clara, precisa e compreensível para os integrantes.

Cabe ao Comitê de Governança em Proteção de Dados implantar plano de ação, avaliar o cumprimento do compromisso e estimular comportamentos que criam e sustentam a conformidade.
Seguem as principais medidas implementadas pela RAPIDONET:

- TERMO DE USO E POLÍTICA DE PRIVACIDADE - Através destes documentos, a RAPIDONET informa ao titular do dado que a empresa fornece a privacidade necessária para que a confidencialidade dos dados prestados seja garantida de forma eficiente. Dentre as cláusulas constam: arcabouço legal, descrição dos dados coletados, direito dos usuários, tecnologias adotadas, informações para contato e dúvidas, mudança no Termo, foro eleito);

- PLANO DE RESPOSTAS A INCIDENTES – Na referida Minuta, a RAPIDONET detalha as etapas/procedimentos em caso de incidentes;

- TERMO DE RESPONSABILIDADE, CONFIDENCIALIDADE/SIGILO E USO DE INTERNET E RECURSO DE INFORMÁTICA - Referido instrumento é assinado por todos os funcionários que manipulam dados;

- ADEQUAÇÃO DE CONTRATOS - inclusão de cláusulas que assegurem a proteção dos dados pessoais, tanto nos novos contratos como nas renovações dos vigentes através de Termo Aditivo. Na minuta é delimitada de forma claras e objetivas: as responsabilidades do controlador e operador; a forma que é realizada a coleta e o tratamento de dados; a existência da possibilidade de o titular acessar os seus dados coletados; a forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular; a existência da possibilidade de revogação do consentimento dado pelo titular; o detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias; as medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

- E-MAIL CORPORATIVO para denúncia de irregularidade/desconformidade;

- TERMO DE NOMEAÇÃO DE ENCARREGADO;

- POLÍTICA DE COOKIES;
- PLANO DE CAPACITAÇÕES E DE COMUNICAÇÕES (as campanhas de conscientização constante);

- ANÁLISE REGULAR DOS PRINCIPAIS INDICADORES DE DESEMPENHO para verificar lacunas (Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais; quantidade de treinamentos realizados/ quantidade de treinamentos previstos; analise das denúncias, etc).

Não obstante as ações preventivas, existindo incidentes, a RAPIDONET observará as etapas a seguir:

7.2 Notificação

Todos os funcionários e/ou parceiros da RAPIDONET são responsáveis por reportar qualquer tipo de eventos, que possam causar danos à segurança da informação e proteção de dados.

O incidente pode ser noticiado, por pessoa externa ou não, através dos mecanismos de comunicação – e-mail institucional do Encarregado pelo Tratamento de Dados Pessoais (DPO) ou endereço postal da empresa.

Encarregado pelo tratamento de dados pessoais:
Nome: Cristhian Alessander de Queiroz, brasileiro, casado, inscrito no CPF sob o nº. 723.751.671-04
E-mail: cristhian@rapidonet.com.br

O conhecimento de um incidente por qualquer pessoa enseja, necessariamente, uma notificação ao Encarregado, o mais rápido possível, para as adotar as medidas previstas na LGPD e no portal da Autoridade Nacional sobre comunicação de incidentes de segurança.

7.3 Triagem

Após a notificação, a equipe de Resposta a Incidentes vai fazer uma avaliação preliminar. Deverá verificar a quantidade de titulares de dados pessoais afetados, categoria e quantidade de dados afetados, consequências do incidente para os agentes de tratamento de dados pessoais. Poderá, inclusive, acionar técnico com expertise para auxiliar na avaliação, deverá buscar/colher informações, avaliar o risco da situação e, ainda, poderá, se for o caso, descartar as notificações nulas ou claramente improcedentes.

Em relação ao risco, será considerado ALTO se for atingido dados pessoais de crianças e/ou adolescentes, dados sensíveis, que possam gerar discriminação ao titular e dados bancários. Caso o incidente atinja dados pessoais imediatamente identificáveis (nome, e-mail, CPF, dentre outros), o risco será moderado. Por fim, se for atingido, tão somente, dados pessoais de difícil identificação o risco é caracterizado como leve.

7.4 Avaliação

Nesta fase será realizada uma avaliação mais detalhada/minuciosa. Para tanto, a equipe verificará a causa do incidente (endereços IP, credenciais e/ou *logins* envolvidos, varredura no sistema, os possíveis responsáveis e donos das informações, hora e data de cada ocorrência, transferências de dados irregulares, sistemas e serviços afetados, existência de outros eventos e alertas relacionados com o incidente).

Deve ser registrada toda a cadeia de diligências realizadas para entendimento do evento e mitigação dos danos.

7.5 Contenção e erradicação

O intuito desta fase é limitar o dano e isolar os sistemas afetados para inibir maiores problemas. Sistemas podem ser desligados após o *Snapshot*, procedimentos alterados, funcionários/parceiros afastados. Sempre com muito cuidado para não apagar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

7.6 Recuperação

É um conjunto de medidas que pode ser gradual ou total, a depender da situação. Neste momento, o Time/equipe de Resposta a Incidentes tem a responsabilidade de passar as informações que obteve para aplicação da solução.

Em regra, pode ser realizado restauração de *backups*, clonagem de máquinas virtuais e reinstalação de sistemas. Acaso o sistema afetado seja restabelecido, deve ser realizada uma análise técnica para examinar detalhadamente a integridade dos dados.

Após a resolução do incidente, um Relatório de Resposta a Incidentes (IRR) deverá ser elaborado e disponibilizado para gerenciamento da Área de Tecnologia da Informação (TI), Comitê de Privacidade e Proteção de Dados Pessoais e Setor Jurídico.

7.7 Documentação

Todo incidente deve ser documentado. Para tanto será registrado os atores envolvidos, informações/provas colhidas, decisões preliminares e finais, medidas de contenção ou reparação e, ainda, as lições aprendidas.

7.8 Comunicações

No caso de incidente com vazamento de dados pessoais, o Encarregado de Tratamento de Dados (DPO) deve, diante das informações levantadas internamente, de acordo com os parâmetros estabelecidos pelo Autoridade Nacional, realizar a comunicação. Existindo necessidade, as comunicações à Autoridade Nacional devem acontecer no prazo de 02 (dois) dias úteis. Eis que o art. 48 da LGPD determina que o controlador tem a obrigação de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que venha a gerar risco ou dano considerado relevante aos titulares.

Outrossim, o Relatório de Impacto à Proteção dos Dados Pessoais deve apresentar os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, preservações e mecanismos de mitigação de risco. Deve conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

7.9 M**edidas disciplinares**

Em caso de desvios de atuação ética, íntegra e transparente aplicar-se-á medidas disciplinares proporcionais ao tipo de violação e o grau de responsabilidade dos envolvidos, dentre elas: advertências verbais e formais, cancelamentos de contratos, suspensão de pagamentos, desligamento de funcionário/colaborador, entre outros.

No curso das investigações é possível a adoção de medidas cautelares, como o afastamento preventivo de integrantes para não atrapalhar as investigações/apuração da denúncia.

8. ESTÁGIO DA ADEQUAÇÃO À LGPD

Esse diagnóstico é uma importante ferramenta, já que incorpora as ações mais relevantes na busca pela conformidade com a LGPD.

É importante mencionar que a RAPIDONET adota integralmente as disposições da LGPD.

Isso porque já realizou um inventário dos serviços que tratam dados pessoais (rastreabilidade), os normativos internos estão em consonância com a LGPD, consagra o princípio da transparência na relação com os titulares de dados (possui Termo de Uso e Política de Privacidade), os instrumentos contratuais foram ajustados a LGPD, foi elaborado Plano de Respostas a Incidentes, adotou medidas de segurança, criou e-mail corporativo para denúncia de irregularidade/desconformidade, nomeou encarregado, criou politica de capacitação e treinamento, além de termo de responsabilidade para todos os funcionários que manipulam dados.

8 INVENTÁRIO DE DADOS PESSOAIS (IDP)

De acordo com o art. 37 da LGPD, o inventário de dados pessoais consiste no registro das operações de tratamento dos dados pessoais realizados pela RAPIDONET e descreve informações tais como:

- atores envolvidos (agentes de tratamento e o Encarregado);
- finalidade (o que a instituição faz com o dado pessoal);
- hipótese (arts. 7° e 11 da LGPD);
- previsão legal;
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 da LGPD); e
- medidas de segurança atualmente adotadas.

O levantamento considera o ciclo de vida dos dados, ou seja, coleta, uso, transferências, retenção e destruição, assim como compreende todas as atividades de tratamento previstas na LGPD.

Por fim, o presente Sistema de Conformidade deve ser lido e compreendido em conjunto com as demais políticas e normas/procedimentos internos. As regras/orientações aqui dispostas serão periodicamente revistas e atualizadas.

Última modificação: 01/06/2023.