LEI GERAL DE PROTEÇÃO DE DADOS

RELATÓRIO FINAL DE PROTEÇÃO DE DADOS

I – RELATÓRIO

O Programa de adequação da MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA. se desenvolveu primeiramente através da conscientização com palestra ao comitê de adequação e supervisores dos setores, como constam nas atas anexas, e sua implementação contou com a colaboração de todos os envolvidos.

Na fase de diagnóstico e mapeamento, foram feitas entrevistas com os responsáveis dos setores de Recursos Humanos, Recepção, Técnica, Financeiro e TI para identificação e análise de riscos dos fluxos de dados, bem como foi realizado o inventário de dados que segue anexo.

Identificados os compartilhamentos e vulnerabilidades de segurança, foi elaborado o plano de ação por setor, que segue anexo, relacionando os tópicos analisados, o problema identificado e a sugestão para solução.

Foi realizado a implantação de 100% dos tópicos do plano de ação pelos setores e o monitoramento e continuidade do programa será realizado pelo encarregado de dados.

II – ESCOPO DO PROJETO

O Programa de Adequação foi executado pelos profissionais:

a) Luciana de Carvalho Paulo Coelho, advogada, mestre e doutora em Ciência Jurídica, professora e consultora em LGPD

b) Sérgio Ari de Souza, formação em direito, administração, especialista em segurança da informação e consultor em LGPD.

c) Janaina Palma, advogada, mestranda em Ciência Jurídica, especialista em Direito Médico.

O trabalho foi realizado de março a novembro de 2022 através de 6 etapas que serão discriminadas a seguir.

III – NOMEAÇÃO DO ENCARREGADO

O encarregado de dados nomeado foi a Sr. Renato Sansigolo.

O critério para nomeação deste funcionário foi o fato de trabalhar na Empresa no setor de RH e conhecer de maneira completa todos os setores e os fluxos de dados pessoais. Além disso, foram levadas em considerações suas habilidades e competências técnicas e sociais, especialmente sua pró-atividade e acesso direto à gerência da empresa.

O funcionário Renato trabalha no setor de RH, havendo a possibilidade de cumular a função pela existência de tempo disponível no exercício de suas atividades.

Caso aumente a demanda em relação as tarefas para garantir a proteção de dados, o encarregado será retirado de outras funções para poder continuar exercendo esta função de forma eficaz.

IV – FASES DO PROJETO:

A realização do Programa se desenvolveu através das seguintes etapas: conscientização; diagnóstico e mapeamento; análise de riscos; plano de ação; implantação e monitoramento, conforme se demostra a seguir:

a) Conscientização e Definição inicial do Escopo de Trabalho: nomeação do comitê de Adequação, nomeação do encarregado de dados e realização de reunião para conscientização do comitê e gestores.

b) Diagnóstico e Mapeamento de Dados: realização de diagnóstico inicial com entrevistas individuais com membros do comitê representantes de cada setor. Objetivo desta etapa foi analisar e entender a empresa como um todo, realizando a identificação dos fluxos de dados e os sistemas de

armazenamento. Foi realizada manualmente a planilha do inventário de todos os dados coletados, identificados sua base legal, finalidade, controle de acesso, compartilhamentos realizados e demais parâmetros legais necessários.

d) Análise de Riscos: a partir do mapeamento foram analisados todos os riscos da empresa em relação aos dados tratados e classificados em baixo, médio e alto risco. Foi realizada, conforme identificado no mapeamento a revisão de todos os contratos vigentes em que há compartilhamento de dados, bem como a necessidade dos aditivos contratuais de parceiros e colaboradores.

e) Plano de Ação: de acordo com os riscos identificados, foram analisados cada tópico e elaboradas as medidas necessárias para correção. Além disso, foram criados os procedimentos necessários para garantir o cumprimento da lei.

f) Implementação: as medidas propostas foram repassadas para a empresa a fim de colocar em prática os mecanismos necessários para cumprimento da lei. Foram entregues os documentos finais, incluindo Relatório de Impacto de Proteção de dados e registro das operações de tratamento de dados.

g) Monitoramento: realização de reunião para diagnóstico final e análise da efetividade das medidas implementadas.

V – PROCESSOS CRIADOS

A empresa MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA. é controladora de dados em relação a seus funcionários e aos dados de clientes pessoas físicas, sendo compartilhados os dados de clientes e colaboradores com os terceiros listados abaixo:

-Empresa TI;

-Empresa Aplis;

-Empresa Unimed;

-Empresa Banricard;

-Empresa Ezepoint;

-Empresa RW;

-Empresa Quintas Contabilidade;

-Empresa Cabergs;

-Empresa Cassi;

-Empresa IPE;

-Empresa H Saúde;

-Empresa H Caridade;

-Empresa H Santa Terezinha;

Foram aditivados os contratos dos operadores listados acima, incluindo as cláusulas de cooperação, auxilio em caso de violação e não autorizando o compartilhamento ou comercialização dos dados. Sendo que os contratos da Unimed, Aplis, Banricard e RW já se encontravam adequados. Seguem as principais cláusulas dos aditivos:

A CONTRATADA, obriga-se, sempre que aplicável, a atuar no presente Contrato em conformidade com a legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial, a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (“LGPD”).

Caso exista modificação dos textos legais acima indicados ou de qualquer outro, de forma que exija modificações na estrutura do escopo deste Contrato ou na execução das atividades ligadas a este Contrato, a CONTRATADA deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade do Contrato conforme as disposições acordadas, a CONTRATANTE poderá resolvê-lo sem qualquer penalidade, apurando-se os serviços prestados e/ou produtos fornecidos até a data da rescisão e consequentemente os valores devidos correspondentes.

A CONTRATADA seguirá as instruções recebidas da CONTRATANTE em relação ao tratamento dos Dados Pessoais a que tiverem acesso unicamente para os fins e pelo tempo necessários para o cumprimento de suas obrigações e para a adequada execução do objeto contratual, além de observar e cumprir as normas legais vigentes aplicáveis, sob pena de arcar com as perdas e danos que eventualmente possa causar à CONTRATANTE, aos seus colaboradores, clientes e fornecedores, sem prejuízo das demais sanções aplicáveis.

Ambas as partes deverão implementar e manter as medidas técnicas e organizacionais necessárias para a proteção dos Dados Pessoais do Cliente contra destruição acidental ou ilegal, danos, perdas, alterações, divulgação ou acesso não autorizados, sem prejuízo do cumprimento de qualquer outra medida exigida pelas leis de proteção de dados aplicáveis. Constitui também

dever de ambas as partes assegurar que qualquer pessoa autorizada a tratar os Dados Pessoais coletados em decorrência deste contrato, esteja vinculada a obrigações contratuais de confidencialidade.

A CONTRATADA não poderá nomear qualquer subcontratada como Processador de Dados adicional para Processar Dados Pessoais do Cliente sem o consentimento prévio por escrito da CONTRATANTE. Caso a CONTRATADA nomeie qualquer subcontratada como Processador de Dados adicional e, uma vez tendo a CONTRATANTE consentido com tal nomeação, esta deverá vinculá-la a termos que forneçam proteções equivalentes às previstas neste aditivo.

A CONTRATADA deverá auxiliar a CONTRATANTE em qualquer caso de Violação de Dados e qualquer ameaça ou suspeita de Violação de Dados ("Incidente de Segurança"): notificando a outra Parte dentro de 72 horas após tomar conhecimento do Incidente de Segurança que possa acarretar risco ou dano relevante aos dados pessoais e/ou aos seus titulares, mencionando no mínimo o seguinte: i) a descrição da natureza dos dados pessoais afetados; ii) as informações sobre os titulares envolvidos; iii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; iv) os riscos relacionados ao incidente; v) os motivos da demora, no caso de a comunicação não ter sido imediata; e vi) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Deverá ainda cooperar e tomar as medidas que a CONTRATANTE possa razoavelmente solicitar para ajudar na investigação, mitigação e no remédio de qualquer Incidente de Segurança.

A CONTRATANTE poderá notificar a CONTRATADA sobre reclamações e solicitações dos titulares de Dados Pessoais que venha a receber (por exemplo, sobre a correção, exclusão, complementação e bloqueio de dados) e sobre as ordens de tribunais, autoridade pública e reguladores competentes, e quaisquer outras exposições ou ameaças em relação à conformidade com a proteção de dados identificadas pelo mesmo.

A CONTRATADA compromete-se a auxiliar a CONTRATANTE com as suas obrigações judiciais ou administrativas, de acordo com a Lei de Proteção de Dados aplicável, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança.

A CONTRATANTE terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da CONTRATADA com as obrigações de Proteção de Dados Pessoais, sem que isso implique qualquer diminuição da responsabilidade que a CONTRATADA possui perante a LGPD e este Contrato.

As previsões de exclusão de responsabilidade por fato de terceiro e força maior previstas no contrato original não se aplicam caso a CONTRATADA esteja em desconformidade com a LGPD ou com este aditivo contratual.

O presente Contrato não transfere a propriedade de quaisquer dados da CONTRATANTE ou dos clientes desta para a CONTRATADA.

A CONTRATANTE não autoriza a CONTRATADA a compartilhar ou comercializar quaisquer eventuais elementos de dados, que se originem ou sejam criados a partir do tratamento de Dados Pessoais estabelecido por este Contrato.

VI - PROCESSO CRIADO PARA O EXERCÍCIO DO DIREITO DOS TITULARES

Para cumprir a legislação e possibilitar o exercício do Direito dos Titulares foi criado o e-mail específico encarregado@medicinadiagnostica.med.br o qual está indicado no site da empresa.

Os direitos do titular no site são exercidos pelo próprio usuário, através do e-mail informado na página do site.

VII – PROCESSOS INTERNOS LIGADOS AOS COLABORADORES

Foi realizada reunião de conscientização no dia 17/05/22, com os funcionários responsáveis diretamente pelo tratamento de dados.

Foi criado manual de boas práticas e repassado aos colaboradores com foco em cuidados para garantir a segurança da informação na empresa.

IX – PROCEDIMENTOS CRIADOS

Conforme documentos anexos foram criados procedimentos com o objetivo de definir o processo de armazenamento e descarte de dados em vários setores da empresa.

1. Procedimento para coleta de currículos: define o procedimento e informações sobre coleta de currículos a serem seguidos na MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA.

2. Procedimento para admissão interna no Recursos Humanos: documento que define os procedimentos a serem seguidos na admissão de funcionários

internos realizado pela MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA.

3.Procedimento de coleta de dados de clientes: a política de Acesso aos laudos pelos médicos, clientes e hospitais na MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA.

4.Procedimento para descarte de dados de clientes: procedimentos e prazos a serem seguidos para armazenamento (físico e digital) de documentos pela Medicina Diagnóstica.

5.Procedimento para compartilhamento por email: define o termo a ser incluído como padrão ao final dos e-mails pela MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA.

6.Procedimento para coleta da dados para cadastro e descarte: o procedimento padrão para cadastramento do clientes na recepção pela MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA.

7.Procedimento para conscientização dos colaboradores: define os termos para conscientização no Manual dos Colaboradores pela MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA

6.Procedimento para atendimento do titular de dados: define os procedimentos a serem seguidos para atendimento de retificação e exclusão dos dados do titular no site pela MEDICINA DIAGNÓSTICA - CENTRO DE DIAGNÓSTICO PATOLÓGICO LTDA.

Em anexo consta o documento com a especificação e fluxo dos procedimentos criados

X – POLÍTICA DE DOCUMENTAÇÃO ADEQUADA

Foram elaborados os documentos listados abaixo com o objetivo de atender os direitos dos titulares de dados, sejam clientes ou funcionários da empresa.

1. Termo de Admissão dos funcionários: informa o compartilhamento dos dados do funcionário, e coleta o consentimento da coleta dos dados de menores de 12 anos

2. Manual de Boas Práticas: manual elaborado com temas de segurança da informação e noções básicas de LGPD, para divulgação interna através de e-mail periódicos.

3 Plano de Gestão de Crises: orientação em casos de incidentes de segurança na empresa.

4 Questionário de fornecedores: avaliar o nível de proteção de dados pessoais com o futuro fornecedor ou prestador de serviço, bem como sua conformidade com a LGPD.

5 Plano de Continuidade de Negócios: define estratégias de Gestão de Continuidade de negócios de acordo com a Política de Segurança da Informação e o Plano de Gestão de Incidentes.

XI – REGISTRO DE ATIVIDADES DE TRATAMENTO

O Registro das atividades de tratamento relatando quais dados são tratados, qual o fluxo dos dados, os compartilhamentos existentes e a vida útil dos dados estão especificados na tabela de data mapping.