RESOLUÇÃO NORMATIVA Nº 010/CA/2022

Institui o Comitê Permanente de Segurança da Informação, Privacidade de Dados e Imagens e dispõe sobre o seu funcionamento.

O CONSELHO DE ADMINISTRAÇÃO DA CAIXA DE ASSISTÊNCIA À SAÚDE DOS SERVIDORES PÚBLICOS DO ESTADO DE MATO GROSSO DO SUL (UNISAÚDEMS), no uso de suas atribuições previstas no art. 39 do Estatuto da entidade,

Considerando que, em vista do que dispõe a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a UNISAÚDEMS é responsável pela proteção de dados e imagens que obtém ou produz em razão da atividade que exerce na busca do atingimento do seu objetivo;

Considerando a necessidade de se instituir um Comitê com a finalidade específica de apoiar a administração da UNISAÚDEMS quanto às medidas a serem adotadas visando à segurança e à proteção desses dados e imagens,

RESOLVE:

CAPÍTULO I
DISPOSIÇÃO PRELIMINAR

Art. 1º Esta Resolução Normativa institui Comitê com a finalidade de apoiar a administração da UNISAÚDEMS em relação às medidas a serem adotadas visando ao atendimento da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), relativamente à segurança e à proteção de dados e imagens que obtém ou produz em razão da atividade que exerce com o objetivo de atender a sua finalidade, bem como dispõe sobre a sua estrutura e o seu funcionamento.

CAPÍTULO II
DO COMITÊ PERMANENTE DE SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE DE DADOS E IMAGENS

Seção I
Da Instituição

Art. 2º Fica instituído o Comitê Permanente de Segurança da Informação, Privacidade de Dados e Imagens (Comitê de Dados), com a finalidade específica de, nos termos desta Resolução Normativa, apoiar a administração da UNISAÚDEMS em relação às medidas e aos procedimentos que se fizerem necessários visando ao cumprimento da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de

Dados Pessoais), relativamente à segurança e à proteção de dados e imagens que a entidade obtém ou produz em razão da atividade que exerce no atendimento do seu objetivo.

§ 1º Para efeito desta Resolução Normativa, o Comitê Permanente de Segurança da Informação, Privacidade de Dados e Imagens fica denominado **Comitê de Dados**.

§ 2º O Comitê de Dados é órgão colegiado integrante da UNISAÚDEMS, de caráter permanente e autônomo.

Seção II
Das Atribuições do Comitê de Dados

Art. 3º São atribuições do Comitê de Dados apoiar a administração da UNISAÚDEMS, no cumprimento de suas obrigações em face da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), nas seguintes matérias ou atividades:

I. a política de Segurança da Informação e sobre a Política de Privacidade de Dados;
II. a definição de padrões e procedimentos internos de segurança da informação, com a aplicação de medidas fiscalizatórias e preventivas de segurança;
III. os trabalhos e os indicadores realizados pelo Gestor de Segurança da Informação e o Encarregado de Dados;
IV. o gerenciamento e a adoção de medidas sobre quaisquer incidentes de segurança da informação que possam impactar direta ou indiretamente a UNISAÚDEMS;
V. a confecção, atualização, gestão e aplicação do Plano de Gestão de Incidentes de Segurança de Dados Pessoais, Relatório de Impactos e *Data Mapping*/Matriz de Dados Pessoais;
VI. a identificação e avaliação de riscos, com aplicação de métrica matemática avaliativa e plano de ação para devidas correções e prevenções;
VII. as estratégias para assegurar a privacidade dos dados dos beneficiários, colaboradores, prestadores de serviços e fornecedores;
VIII. a implementação e verificação da aplicação de Política de Privacidade e Proteção de Dados no que tange ao sigilo, confidencialidade e imagens na matriz e filiais da UNISAÚDEMS;
IX. a abertura de procedimento para análise da quebra de sigilo de dados, privacidade e uso indevido de imagens que ocorram a partir de informações, vídeos e fotos coletadas nas filiais e matriz da UNISAÚDEMS. Os dados coletados/resultados apurados podem ser, inclusive, encaminhados para aplicação do Código de Conduta, Plano de Gestão de Incidentes de Segurança de Dados Pessoais e Relatório de Impactos;
X. a análise técnica da contratação de credenciados, prestadores de serviços e/ou fornecedores, para garantir que não haja exposição indevida da UNISAÚDEMS e dos dados dos beneficiários, colaboradores, credenciados e prestadores/fornecedores;
XI. a argumentação e aprovação de posicionamento público, que será redigido pela área jurídica, com a participação do Comitê e do setor Marketing, nos casos de vazamento de dados, quebra de privacidade de dados, incidente de segurança,

ou qualquer situação relacionada à exposição pública de colaborador, beneficiário, credenciados ou prestador/fornecedores;

XII. a correta adequação dos programas e ações existentes às exigências legais relacionadas à segurança da informação, proteção de dados e imagem;

XIII. a aprovação, apoio e/ou elaboração dos programas e treinamentos de sensibilização para os colaboradores, credenciados e prestadores/fornecedores de serviço sobre a relevância dos valores de segurança da informação, proteção de dados e imagem, em especial a aplicação da LGPD;

XIV. outros assuntos relacionados à segurança da informação, proteção de dados e imagem e aplicação da LGPD.

§ 1º São, também, atribuições do Comitê de Dados, quando não competir aos seus próprios membros em razão das funções que exercem na entidade:

I. sugerir à administração da UNISAÚDEMS que realize comunicações ou que determine fiscalizações que entende necessárias em razão de resultados decorrentes da atividade do Comitê;

II. propor a aplicação de sanções previstas para infrações que, na realização de sua atividade, verifique terem ocorridas;

III. propor política de segurança da informação simplificada, que estabeleça controles relacionados com o tratamento de dados pessoais, como cópias de segurança, uso de senhas, acesso à informação, compartilhamento de dados, atualização de softwares, uso de correio eletrônico e uso de antivírus, com a realização de revisões periódicas de política e segurança da informação.

§ 2º havendo necessidade para o desempenho de sua atividade, nos termos desta Resolução Normativa, o Comitê, por meio do seu coordenador, pode convocar qualquer colaborador, credenciado, prestador ou fornecedor da entidade para prestar informações pertinentes a essa atividade, ou exigir-lhes que apresentem documentos relativos à mesma.

Seção III
Da Composição do Comitê de Dados

Art. 4º O Comitê será composto por três membros natos, com suas atribuições estabelecidas nesta Resolução, sendo eles:

I. o responsável pela Gestão de Segurança da Informação;

II. o responsável pela Gestão de Dados (Encarregado de Dados);

III. o responsável pela Consultoria Jurídica e Representação Judicial.

§ 1º Os membros do Comitê de Dados atuarão, nos termos desta Resolução Normativa, de forma colegiada, nas atribuições do Comitê, e, de forma individualizada, segundo sua área de atuação.

§ 2º Na forma colegiada, o Comitê atuará sob a coordenação do membro responsável pela área jurídica.

Art. 5º Na impossibilidade de participação nas reuniões, os membros do Comitê

serão substituídos por colabores da UNISAUDEMS previamente designados pelo Conselho de Administração.

Parágrafo único. A designação de substitutos para os membros do Comitê de Dados deve recair em colaboradores contratados pela UNISAÚDEMS, para funções que guardem pertinência com as áreas a que se refere o artigo anterior desta Resolução Normativa.

Art. 6º Os colaboradores da UNISAÚDEMS, integrantes como membros do Comitê de Dados, ou seus substitutos, devem executar as atividades do Comitê concomitantemente com o exercício das funções para as quais foram contratados pela entidade.

§ 1º A integração como membro do Comitê de Dados, ou substituto, **não enseja** adicional à remuneração do colaborador da UNISAÚDEMS.

§ 2º Os membros do Comitê de Dados, inclusive substitutos, devem exercer com lealdade e zelo as suas atividades de apoio à administração da UNISAÚDEMS, nos termos desta Resolução Normativa, na busca de bem cumprir os deveres da entidade em face da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

Seção IV
Das Atribuições dos Membros do Comitê de Dados

Art. 7º Os membros do Comitê de Dados devem exercer, individual e continuamente, as atribuições pertinentes às áreas em relação às quais sãos os responsáveis no âmbito da entidade.

Parágrafo único. As decisões do Comitê, independentemente das áreas a que se referem, devem ser tomadas em conjunto, na forma estabelecida no Capítulo III desta Resolução Normativa.

Subseção I
Da Área de Dados

Art. 8º O responsável pela Gestão de Dados (Encarregado de Dados), no exercício de sua atividade no âmbito do Comitê de Dados, tem as seguintes atribuições:

I. atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
II. responder aos titulares dos dados pessoais conforme determinado no art. 18 da Lei Geral de Proteção de Dados Pessoais, recebendo reclamações, esclarecer dúvidas de beneficiários sobre os dados pessoais, fiscalizar a adequação da empresa à LGPD e orientar os colaboradores sobre como manter os dados seguros;
III. proceder à confecção e à atualização de documentos, termos, e processos relacionados a aplicação da LGPD (LGPD art. 6o, VII, o Princípio da Segurança);
IV. tomar ciência e manifestar-se sobre processos e/ou documentos relacionados

a LGPD, em especial ao tramite de informações pessoais, dados sensíveis ou anonimizados, tanto internamente quanto externamente (parceiros, credenciados, pessoas jurídicas, etc.);

V. apresentar parecer e/ou sugerir mudanças nas cláusulas de LGPD presentes em contratos confeccionados pelo jurídico ou de aprovação deste;

VI. avaliar, opinar, educar e monitorar o tratamento de dados pessoais na operadora, auxiliando a mesma no cumprimento das obrigações previstas na LGPD;

VII. providenciar a reestruturação de processos e fluxo de informações, com a implantação de novos métodos para conduzir processos de gestão de dados e informações;

VIII. realizar a conscientização dos funcionários, via treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais conforme disposto na LGPD e normas da ANPD, informando e sensibilizando todos os colaboradores da Operadora, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados.

IX. implementar soluções de anonimização ou pseudonimização, como a criptografia, quando necessário, para cifrar dados pessoais.

Subseção II
Da Área de Segurança da Informação

Art. 9º O responsável pela Gestão de Segurança da Informação, no exercício de sua atividade no âmbito do Comitê de Dados, tem as seguintes atribuições:

I. gerir os acessos aos sistemas e ferramentas, com a premissa do Princípio do Menor Privilégio, mantendo como regra o bloqueio a novos de acessos e/ou alterações, devendo ter a ciência do Encarregado de Dados, e quando necessário do jurídico, para mudanças de acesso, em especial os permanentes;

II. aplicar medidas preventivas e corretivas de segurança da informação e de dados digitais;

III. apresentar parecer técnico ou sugerir mudanças técnicas relacionadas à área de TI;

IV. administrar sistemas de informação e disponibilidade dos recursos, identificar vulnerabilidades em servidores, sistemas, aplicações e networking, a fim de garantir maior segurança e integridade dos dados da Operadora;

V. controlar e fiscalizar os acessos aos sistemas e ferramentas;

VI. monitorar a segurança e implementar processos e políticas de proteção de dados;

VII. proceder a ajustes de *data centers* e aquisição de infraestrutura para auditorias e fiscalizações das informações guardadas;

VIII. propor o emprego de programas para gerenciamento dos dados;

IX. implementar sistema de controle de acesso aplicável a todos os usuários/colaboradores, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais;

X. configurar funcionalidades no sistema de controle de acesso que possam detectar vulnerabilidades e não permitir o uso de senhas que não respeitem um certo nível de complexidade;

XI. implementar um adequado gerenciamento de senhas, estabelecendo

controles tais como: evitar o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos; utilizar apenas senhas complexas para acessar aplicativos e outros sistemas informáticos; não reutilizar senhas;

XII. utilizar como prioritário a autenticação multi-fator para acessar sistemas ou base de dados que contenham dados pessoais;
XIII. implementar um sistema de controle de acesso aplicável a todos os usuários que acessam o sistema de TI;
XIV. evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos;
XV. inventariar e cifrar dados de dispositivos externos e armazená-los em locais seguros;
XVI. realizar backups off line, periódicos e armazená-los de forma segura;
XVII. formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá-las, ou, quando não for possível a sobrescrita, destruir as mídias físicas;
XVIII. estabelecer no contrato de serviço o registro da destruição/descarte (caso o agente de tratamento utilize serviços de terceiros para o descarte);
XIX. utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia fim-a-fim para serviços de comunicação;
XX. manter sistema de Firewall dentro das aplicações internas e externas;
XXI. bloquear atividades web suspeitas e/ou não autorizadas;
XXII. proteger e-mails via adoção de ferramentas AntiSpam, filtros de e-mail e integrar o antivírus ao sistema de e-mail;
XXIII. remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas ou armazenados em duplicidade sem justificativa;
XXIV. atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os em sua versão atualizada (instalar patches de segurança disponibilizados pelos fornecedores);
XXV. adotar e atualizar periodicamente softwares antivírus e antimalwares;
XXVI. realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados;
XXVII. utilizar técnicas de autenticação multi-fator para controle de acesso de dispositivos móveis, como smartphones e laptops;
XXVIII. separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível;
XXIX. implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis;
XXX. realizar um contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados;
XXXI. avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende os demais requisitos de segurança da informação estabelecidos;
XXXII. analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado;
XXXIII. utilizar técnicas de autenticação multi-fator para acesso aos serviços em nuvem relacionados a dados pessoais;
XXXIV. sugerir a implementação de novos recursos dos sistemas e/ou funcionalidades;

XXXV. proceder ao gerenciamento da segurança de redes;
XXXVI. aplicar notificação de fragilidades e eventos de segurança da informação, a fim de evitar ou minimizar os danos causados por ataques;

Subseção III
Da Consultoria Jurídica e da Representação Judicial

Art. 10. O responsável pela Consultoria Jurídica e Representação Judicial, no exercício de sua atividade no âmbito do Comitê de Dados, tem as seguintes atribuições:

I. confeccionar e validar contratos com cláusulas da LGPD;
II. validar ou retificar documentos ou termos relacionados à aplicação da LGPD feitos pelo Encarregado de Dados;
III. analisar o teor de contratos sugerindo a inclusão de cláusulas de segurança da informação que assegurem a proteção de dados pessoais, tais como: regras para credenciados, fornecedores e parceiros; regras sobre compartilhamentos; relações entre controlador-operador; orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador.

CAPÍTULO III
DAS DELIBERAÇÕES DO COMITÊ DE DADOS

Art. 11. Os membros do Comitê de Dados devem reunir-se, ordinariamente, a cada três meses, e, extraordinariamente, sempre que convocados, para as suas deliberações.

§ 1º As reuniões serão convocadas e coordenadas pelo responsável pela Consultoria Jurídica e Representação Judicial, por iniciativa própria ou mediante provocação de qualquer membro.

§ 2º As reuniões deverão ser realizadas com a presença de, no mínimo, dois membros, ou seus respectivos substitutos.

§ 3º As reuniões poderão ser realizadas, presencialmente, na sede da UNISAÚDEMS ou em qualquer outro local previamente acordado, podendo ser realizada por videoconferência ou meio eletrônico equivalente.

Art. 12. As decisões do Comitê de Dados serão tomadas por consenso dos membros ou seus substitutos, participantes da reunião, ou pelos votos da maioria simples dos presentes.

Parágrafo único. No caso de empate, caberá ao Presidente do Conselho de Administração a decisão a respeito.

Art. 13. As reuniões, com as respectivas deliberações, devem ser registradas em ata, assinadas pelos membros presentes e, na hipótese do parágrafo único do artigo anterior, também pelo Presidente do Conselho de Administração.

Art. 14. Os colaboradores da UNISAÚDEMS que exercem atividades compreendidas no âmbito das atividades do Comitê de Dados podem, espontaneamente ou a convite dos membros do Comitê, ou, ainda, por convocação do Presidente do Conselho de Administração, participar das reuniões do Comitê, podendo apresentar sugestões ou orientações, que serão registradas na ata, sem direito a voto.

CAPÍTULO IV DISPOSIÇÕES FINAIS

Art. 15. Os casos omissos nesta Resolução Normativa serão supridos por decisão do Conselho de Administração.

Art. 16. Os documentos, pareceres e materiais decorrentes das atividades do Comitê deverão permanecer armazenados na UNISAÚDEMS, sendo seu acesso restrito aos seus membros, ao Conselho de Administração e a colaboradores, credenciados e prestadores/fornecedores autorizados pelo Comitê.

Art. 17. Esta Resolução Normativa entra em vigor na data de sua aprovação.

Campo Grande/MS, 02 de agosto de 2022.

Conselho de Administração da Caixa de Assistência à Saúde dos Servidores Públicos do Estado de Mato Grosso do Sul – UNISAÚDEMS