1. OBJETIVO

Estabelecer as diretrizes para a gestão e comunicação de informações em meio físico e digital, considerando: a coleta, a integração, a organização, o controle, a disponibilização, a movimentação, o recebimento, o compartilhamento, o armazenamento, a conservação e o descarte, a fim de garantir a segurança dos dados e informações processadas pela Irmandade da Santa Casa de Misericórdia de Curitiba (ISCMC), suas Unidades e seus *stakeholders*, com observância aos princípios da integridade, da confidencialidade e da disponibilidade, bem como em atenção ao quanto disposto pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e demais legislações correlatas vigentes.

Ademais, a presente Política visa auxiliar os titulares dos dados, os colaboradores e demais *stakeholders* (pacientes, seus familiares, fornecedores, prestadores de serviços, etc.) a compreenderem o compromisso da ISCMC e suas Unidades, com a sua privacidade.

2. ABRANGÊNCIA

Esta política aplica-se à toda estrutura organizacional da Irmandade da Santa Casa de Misericórdia de Curitiba (ISCMC), suas Unidades administradas e seus *stakeholders,* incluindo trabalhos executados externamente por colaboradores ou por terceiros que utilizem o ambiente de dados da Instituição ou tenham acesso às informações pertencentes a ela, seja em meio físico ou eletrônico.

3. DESCRIÇÃO

A ISCMC almeja garantir que os dados pessoais serão tratados dentro dos parâmetros da legislação vigente, da ética e do sigilo profissional. Para este fim, estabelece diretrizes para cumprimento dos princípios e das regras estabelecidos pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

3.1 DEFINIÇÕES

- **Confidencialidade**: garantia de que as informações serão acessadas apenas por pessoas previamente autorizadas;
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário;

- **Integridade:** preservação da exatidão e completude da informação e dos métodos de processamento.

3.2 DIRETRIZES

A ISCMC e suas Unidades realizarão o tratamento dos dados pessoais de forma adequada e dentro dos padrões legais e éticos e, a fim de assegurar a confiabilidade daqueles com quem assumiu responsabilidades, estabelece as seguintes diretrizes:

- Estabelecer diretrizes e orientar os colaboradores e demais *stakeholders* quanto às regras de segurança da informação e realização de tratamento de dados, seja em meio físico ou digital, em especial com relação às regras de acesso aos prontuários de pacientes e colaboradores, com observância ao sigilo ético e profissional e às regras estabelecidas pela Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018;
- Definir regras para que a disponibilização e utilização dos acessos, equipamentos e serviços de tecnologia da informação respeitem os manuais da instituição;
- Monitorar a atualização e a utilização de softwares, para que seja limitada àqueles que foram licenciados pela instituição (ou adquiridos mediante contrato de serviço), ou ainda que possuem licenciamento gratuito;
- Acompanhar o gerenciamento de lixo eletrônico, com observância à política ambiental e, especialmente, à Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018;
- Monitorar a rotina/cronograma de *backup* de dados;
- Monitorar a adoção de mecanismos que evitem/previnam eventuais ataques cibernéticos;
- Definir regras para utilização dos serviços de telecomunicações, através de mecanismos de controle de acesso e bloqueio de sites, programas, sistemas, etc., garantindo que os recursos são utilizados tão somente como ferramenta de trabalho;
- Estabelecer diretrizes para que o acesso à informação (física ou digital) de colaboradores e pacientes/clientes seja obtido apenas por pessoas autorizadas, com definição de graus de acessibilidade à diferentes profissionais e equipes, para estrito cumprimento de suas atividades profissionais relativas à ISCMC e Unidades, através da disponibilização de *logins* e senhas de acesso, cuja utilização é pessoal e intransferível, bem como através de controle de acesso aos espaços físicos da ISCMC e Unidades;
- Criar planos de contingência e de gerenciamento de riscos;
- Avaliar o desempenho de fornecedores críticos, os quais devem estar alinhados às políticas institucionais;

- Garantir a privacidade e a segurança das informações dos colaboradores e pacientes/clientes, através de diretrizes e monitoramento de acesso aos dados classificados como dados pessoais e dados pessoais sensíveis, nos termos da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018;
- Garantir aos colaboradores e pacientes/clientes o acesso às suas informações, cujas solicitações serão feitas através de canais de comunicação institucionais, conforme determina a Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018;

3.3 RESPONSABILIDADES

1) Departamento de Proteção de Dados:

- Monitorar e avaliar a implementação das ações de gestão e segurança da informação na ISCMC e suas Unidades;
- Desenvolver normas internas relativas à gestão e segurança da informação, em conformidade com a Lei nº 13.709/2018 e demais legislações correlatas;
- Realizar auditorias internas a fim de verificar se os departamentos e processos estão realizando o tratamento de dados conforme regramento da Lei nº 13.709/2018 e as diretrizes estabelecidas na presente política e demais documentos institucionais sobre o tema;
- Realizar treinamentos a fim de conscientizar os colaboradores da ISCMC e suas Unidades sobre os procedimentos para tratamento correto de informações.

2) Departamento de Tecnologia da Informação:

- Fornecer e monitorar a qualidade e eficiência das ferramentas necessárias (equipamentos, sistemas, senhas de acesso, etc.) para realização dos trabalhos dos demais departamentos;
- Manter as rotinas de backup das informações e atualização dos sistemas, softwares e programas, garantindo a confidencialidade, integridade e disponibilidade das informações;
- Monitorar e estabelecer diretrizes para evitar eventuais ataques cibernéticos, acessos não autorizados aos sistemas e demais meios eletrônicos.

3) Departamento de Hotelaria:

- Garantir que o acesso aos espaços físicos da ISCMC e de suas Unidades será feito apenas por pessoas autorizadas, estabelecendo graus de acessibilidade.

Todos os Departamentos da ISCMC e de suas Unidades devem, de forma imediata, informar ao Departamento de Proteção de Dados sobre qualquer evento, incidente ou suspeita de violação às informações (dados pessoais e dados pessoais sensíveis) de colaboradores e pacientes/clientes para que as medidas necessárias sejam adotadas com a maior brevidade possível.

4. DISPOSIÇÕES FINAIS

- A presente Política de Segurança da Informação passa a vigorar a partir da data de sua publicação;
- Ficam canceladas todas as diretrizes anteriores divergentes à presente Política;
- Os casos omissos nesta política devem ser submetidos ao Departamento de Proteção de Dados para apreciação e eventual deliberação com a Diretoria Corporativa Geral e demais responsáveis.

5. DOCUMENTOS RELACIONADOS

- Código de Ética e Conduta;
- Manual do Departamento de Proteção de Dados;
- Manual de Gestão de Documentos;
- Política de Gestão da Informação;
- Regulamento Interno de Trabalho.

6. ANEXOS

- Não se aplica