1. OBJETIVOS

1.1. A **Política de Segurança da Informação** ("Política") do A.C.Camargo Cancer Center ("Instituição") tem como objetivo estabelecer diretrizes para promover a proteção da informação produzida, recebida, utilizada, processada, armazenada e descartada pela Instituição, tanto em seus processos administrativos quanto naqueles relacionados à assistência ao paciente e aos projetos de pesquisas, independentemente de sua forma, sejam elas utilizadas interna ou externamente, com vistas a reforçar o compromisso da Instituição com suas partes relacionadas com relação à segurança das informações por ela manipuladas, e fomentar a cultura de segurança da informação, em linha com a regulamentação nacional e boas práticas internacionais.

2. APLICAÇÃO

2.1. Esta Política se aplica a todos os Profissionais do A.C.Camargo que, direta ou indiretamente, tenham acesso a informações e/ou utilizem recursos tecnológicos da Instituição para a execução de suas atividades profissionais.

3. ABRANGÊNCIA

3.1. Esta Política abrange todas as unidades organizacionais da Instituição.

4. DOCUMENTOS RELACIONADOS

4.1. **ACC-POL-0001:** Código de Conduta.

4.2. **ACC-POL-0014:** Política de Privacidade.

5. GLOSSÁRIO

5.1. **Ameaça:** Causa potencial de um Incidente de Segurança da Informação, que pode vir a prejudicar a Instituição.

5.2. **Ciclo de Vida:** A Informação possui um ciclo de vida, que pode contemplar a criação, o manuseio, o processamento, o armazenamento, o transporte, a transmissão, a exclusão e a sua destruição definitiva.

5.3. **Dado Pessoal:** refere-se a qualquer tipo de informação e dado, obtido por meios digitais ou não, capaz de identificar ou tornar identificáveis pessoas físicas, incluindo dados que possam ser combinados com outras informações para identificar um indivíduo e/ou que se relacionem com a identidade, características ou comportamento de um indivíduo ou influenciem na maneira como esse indivíduo é tratado ou avaliado, incluindo números identificativos, dados locacionais e/ou identificadores eletrônicos. O termo "Dados Pessoais" também inclui Dados Sensíveis.

5.4. **Dado Sensível:** qualquer Dado Pessoal referente a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural identificada ou identificável, ou, ainda, qualquer dado que, quando combinado com outras informações, possa inferir um Dado Sensível.

5.5. **Gestor da Informação:** Profissional da Instituição que criou a Informação ou a utilizou primariamente, sendo o responsável por assegurar que a Informação seja adequadamente classificada e protegida, durante todo o Ciclo de Vida da Informação.

5.6. **Incidente de Segurança da Informação:** Um evento ou conjunto de eventos indesejados de Segurança da Informação que tem possibilidade significativa de afetar as operações e/ou ameaçar a confidencialidade, a integridade ou a disponibilidade das Informações da Instituição.

5.7. **Informação:** Todo ativo de valor para a Instituição, de sua propriedade ou controle. Consiste em elemento fundamental para a execução dos seus negócios, podendo ser de caráter comercial, financeiro, administrativo, tecnológico, estratégico, mercadológico, legal, pessoal ou de qualquer outra natureza, incluindo-se a informação adquirida por contrato, associação, aquisição e licença, como também aquelas custodiadas relativas a clientes, colaboradores ou parceiros, criada, armazenada, processada, trafegada ou transmitida no ambiente da Instituição. O termo Informação também compreende Dados Pessoais e Dados Pessoais Sensíveis.

5.8. **Profissional(is) do A.C.Camargo:** refere-se aos conselheiros, diretores, empregados, estagiários, aprendizes, integrantes de seu corpo clínico e multiprofissional, residentes, alunos, pesquisadores internos e externos, voluntários e prestadores de serviços em geral, indiferente do regime jurídico a que estejam submetidos.

5.9. **Recursos Tecnológicos:** Todos os recursos e infraestrutura de tecnologia da informação de propriedade da Instituição, tais como, mas não se limitando a, hardwares (servidores, computadores, desktops, notebooks, tablets, telefones, smartphones, rádios comunicadores, pen drives, HDs, impressoras, copiadoras, scanners, etc.), softwares (sistemas de informação, programas de computador, bases de dados, aplicativos, etc.) e ferramentas de comunicação (linhas de telefonia fixa e celular, Internet, contas de e-mail, mensageira instantânea, voz sobre IP, etc.), entre outras ferramentas que venham a ser utilizadas no futuro em virtude da inovação tecnológica.

5.10. **Segurança da Informação:** Consiste na adoção de medidas de proteção da Informação, para que estas sejam protegidas e conhecidas somente por aqueles que devem conhecê-la para a execução de suas atividades, em qualquer forma ou suporte que se apresente (verbal, escrita, físico ou digital), durante todo o Ciclo de Vida da Informação, evitando o acesso de pessoas não autorizadas, bem como o uso da Informação de forma indevida, inadequada, ilegal ou em desconformidade com as políticas da Instituição.

5.11. **Usuário da Informação:** Profissional do A.C.Camargo ou outros indivíduos ou organizações devidamente autorizado a utilizar, manipular qualquer ativo de Informação da Instituição para o desempenho de suas atividades profissionais ou contratuais.

5.12. **Vulnerabilidade:** Causa potencial de um Incidente de Segurança da Informação, que pode vir a prejudicar as operações ou ameaçar as Informações da Instituição.

6. DESCRIÇÃO

6.1. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Todas as ações relacionadas à Segurança da Informação deverão ser norteadas pelos seguintes princípios:

(i) **Propriedade:** A Informação, em qualquer forma ou suporte que se apresente (verbal, escrita, físico ou digital), e os Recursos Tecnológicos disponibilizados aos Profissionais do A.C.Camargo são de propriedade da Instituição, tendo natureza exclusiva de ferramentas de trabalho.

(ii) **Confidencialidade:** A Informação deve ser conhecida somente por pessoas autorizadas, que precisem conhecê-la para o desenvolvimento de suas atividades profissionais e nos limites estritamente necessários

ao desempenho de suas respectivas funções, e exclusivamente para o atendimento dos objetivos do negócio da Instituição.

(iii) **Integridade:** A Informação deve ser armazenada de forma a garantir a exatidão, atualização e completude de seu conteúdo.

(iv) **Disponibilidade:** A Informação deve estar disponível para o acesso de pessoas autorizadas, quando necessário ao cumprimento das finalidades de uso das Informações na forma definida pelas políticas e diretrizes da Instituição sobre o tema.

(v) **Monitoramento e Auditoria:** Para garantir a segurança das Informações tratadas pela Instituição, o cumprimento de suas políticas internas e da legislação e regulamentação aplicável, o uso da Informação e dos Recursos Tecnológicos da Instituição estão sujeitos a controle e monitoramento constantes, nos termos desta Política. O resultado do controle e monitoramento pode ser utilizado para auditorias e avaliações visando à constatação de violação desta Política e demais códigos, políticas, processos e procedimentos da Instituição, bem como da legislação e regulamentação aplicáveis, inclusive para a defesa dos direitos e interesses da Instituição e para a aplicação de medidas disciplinares e exercício de direitos em processos administrativos e/ou judiciais, conforme o caso.

(vi) **Garantia da Privacidade e da Proteção dos Dados de Pacientes e de Titulares de Dados Pessoais:** A Instituição e os Profissionais do A.C.Camargo são responsáveis pela segurança de quaisquer Informações e dados por ele administrados, devendo garantir a confidencialidade, integridade e disponibilidade destas Informações, prevenindo assim Incidentes de Segurança de Informação de qualquer natureza envolvendo o tratamento e a proteção de dados, em especial dados relacionados à saúde de pacientes, considerados Dados Pessoais Sensíveis nos termos da legislação vigente. Da mesma forma, projetos de pesquisa devem garantir a privacidade e a proteção dos dados de pacientes, incluindo, mas não se limitando a, dados cadastrais, clínicos, biomoleculares e laudos.

(vii) **Acesso e Guarda de Prontuários:** Os prontuários pertencem exclusivamente aos pacientes. À Instituição, como depositária deste documento, cabe o dever de zelar por sua integridade, confidencialidade, disponibilidade e guarda segura, gerenciando-os de forma a atender integralmente os requisitos da legislação vigente. Os prontuários, sejam eles em versão física ou eletrônica, somente deverão ser disponibilizados aos Profissionais do A.C.Camargo que necessitarem acessar aquelas informações, para finalidades determinadas e justificadas. Sempre que possível, o acesso deve ser modulado, concedendo ao usuário acesso restrito exclusivamente às Informações necessárias. Os prontuários devem ser guardados (i) de forma segura, resguardando a integridade física dos documentos, e sistematizada, possibilitando a localização, armazenamento e recuperação dos documentos; e (ii) pelo tempo que determinar a legislação aplicável.

(viii) **Propriedade Intelectual:** A propriedade sobre o conhecimento, processos, informações, dados, produtos, documentos, livros, relatórios, resultados tangíveis e intangíveis, sistemas, ferramentas, plataformas e tecnologias geradas em projetos de pesquisas será regulamentada por padrões institucionais específicos sobre propriedade intelectual, os quais deverão ser integralmente observados por todos os Profissionais do A.C.Camargo.

6.2. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

O objetivo da gestão de Segurança da Informação da Instituição é garantir a gestão sistemática e efetiva de

todos os aspectos relacionados à Segurança da Informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos na Instituição.

A Instituição está comprometida com uma gestão efetiva de Segurança da Informação, adotando todas as medidas cabíveis para garantir que esta Política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da Instituição.

6.2.1. **Classificação da Informação.**

A classificação da Informação é a atividade que consiste na atribuição de nível de sigilo à Informação, em qualquer forma e suporte que se apresente (verbal ou escrita, física ou digital), de acordo com critérios que consideram a sua importância para o desenvolvimento do negócio da Instituição e a necessidade de proteção. São regras gerais de classificação da Informação, as quais serão operacionalizadas em normativo interno específico:

(i) Toda Informação é atribuída a um Gestor da Informação, que terá a responsabilidade de classificá-la ou designar formalmente um responsável para executar a classificação;

(ii) A Informação deve ser classificada em seu nível adequado de sigilo, em qualquer forma e suporte que se apresente (verbal ou escrita, física ou digital), de acordo com os critérios descritos em normativo específico;

(iii) A Informação deve ser protegida conforme o nível de sigilo classificado, em todas as fases do seu Ciclo de Vida;

(iv) A Informação deve ser reclassificada de acordo com as necessidades do estágio em que se encontra no seu Ciclo de Vida;

(v) A autorização de acesso à Informação deve ser formalmente concedida pelo Gestor da Informação.

6.2.2. **Acesso e Identidades.**

A gestão de acessos e identidades é a atividade que consiste no controle da identificação dos Profissionais do A.C.Camargo que podem ter acesso à Informação e/ou aos Recursos Tecnológicos. São regras gerais de gestão de acessos e identidades:

(i) O acesso à Informação ou aos Recursos Tecnológicos da Instituição deve ser controlado de forma a permitir acesso somente dos Profissionais do A.C.Camargo autorizados pelo respectivo Gestor da Informação, mediante aprovação formal;

(ii) Todo Profissional do A.C.Camargo com acesso aos Recursos Tecnológicos deve ser identificado individualmente, por meio de credencial e senha, de uso pessoal e intransferível;

(iii) A concessão de acesso à Informação para terceiros deve ser precedida de celebração de instrumentos contratuais formais e escritos que imponham a obrigatoriedade de confidencialidade e de atendimento dos controles de Segurança da Informação previstos nesta Política e de observância da Política de Privacidade e demais normativos da Instituição, bem como estabeleçam

responsabilidades no caso de descumprimento.

6.2.3. **E-mail da Instituição.**

A conta de e-mail é uma ferramenta de trabalho disponibilizada a Profissionais do A.C.Camargo, conforme as políticas da Instituição, para fins de comunicação. São regras gerais para o uso adequado do e-mail institucional:

(i) A conta de e-mail é de propriedade da Instituição, sendo disponibilizada aos Profissionais do A.C.Camargo conforme política específica e para fins exclusivamente profissionais;

(ii) O uso da conta de e-mail disponibilizada pela Instituição está sujeito a controle e monitoramento constante por parte da instituição, nos termos desta Política e demais normas da Instituição, bem como da legislação vigente;

(iii) Comunicações eletrônicas são documentos institucionais e devem ser redigidas de acordo com as instruções de trabalho da Instituição;

(iv) É proibido o uso de contas de e-mails pessoais e aplicações de troca de mensagens instantâneas pessoais, ou de terceiros desconhecidos, para comunicação e armazenamento de Informação da Instituição;

(v) É proibido utilizar conta de e-mail institucional para enviar ou receber qualquer material inadequado, ilegal ou em desconformidade com o Código de Conduta, com a presente Política ou outras diretrizes ou normativos da Instituição.

6.2.4. **Internet.**

A Internet é ferramenta de trabalho disponibilizada aos Profissionais do A.C.Camargo como medida de apoio para a execução de suas atividades profissionais. São regras gerais para Internet:

(i) Os recursos que possibilitam o acesso à Internet são de propriedade da Instituição, sendo disponibilizados aos Profissionais do A.C.Camargo conforme política específica e para fins exclusivamente profissionais;

(ii) O uso da internet disponibilizada pela Instituição está sujeito a controle e monitoramento constante por parte da instituição, nos termos desta Política e demais normas da Instituição, bem como da legislação vigente;

(iii) É proibido utilizar a rede de internet corporativa para acessar sites inadequados ou ilegais;

(iv) A divulgação de Informações da Instituição na internet deve ser feita única e exclusivamente por pessoas formalmente autorizadas pela alta direção a falar em nome da Instituição.

6.2.5. **Acesso remoto.**

O acesso remoto consiste na disponibilização aos Profissionais do A.C.Camargo de ferramentas de acesso à Informação como medida de apoio para a execução de suas atividades profissionais. São regras gerais para o acesso remoto:

(i) O acesso remoto é considerado de caráter excepcional e deve ser autorizado formalmente, por período determinado, conforme políticas institucionais;

(ii) O acesso remoto somente poderá ser concedido mediante o uso de ferramentas de proteção do ambiente computacional fornecidas pelo A.C.Camargo, por meio de ferramentas devidamente homologadas pela Instituição;

(iii) É proibido franquear acesso remoto a terceiros não autorizados.

6.2.6. **Dispositivos móveis corporativos.**

Os dispositivos móveis de armazenamento de dados são aqueles que permitem o armazenamento de dados com mobilidade. Para estes casos, são definidas as seguintes regras gerais:

(i) Dispositivos móveis serão disponibilizados aos Profissionais do A.C.Camargo que necessitarem de tais Recursos Tecnológicos para o exercício de suas funções, observando para tanto as políticas institucionais;

(ii) Tais Recursos Tecnológicos devem ser utilizados apenas para a finalidade para o qual foram disponibilizados;

(iii) O Profissional do A.C.Camargo é responsável pela proteção do dispositivo móvel de propriedade da Instituição que esteja em seu poder, mantendo-o sempre em local seguro e protegido;

(iv) É proibido o armazenamento de Informação da Instituição em dispositivos móveis pessoais ou de terceiros.

6.2.7. **Computação na nuvem.**

A computação na nuvem consiste em ferramenta de tecnologia para armazenamento de Informação e/ou sistemas fora do ambiente da Instituição. São regras gerais para computação em nuvem:

(i) A adoção ou contratação de ferramenta de computação em nuvem somente poderá ocorrer mediante análise e aprovação da área de Segurança da Informação e de Tecnologia da Informação, e mediante a estrita avaliação (*due diligence*) do fornecedor quanto a seu nível de conformidade com os requisitos de controles técnicos de Segurança da Informação, em conformidade com esta Política, demais normativos da Instituição e as melhores práticas de Segurança da Informação.

(ii) O armazenamento em nuvem deve ser precedido de celebração de instrumentos contratuais formais e escritos que imponham a obrigatoriedade de confidencialidade e de atendimento dos controles de Segurança da Informação previstos nesta Política e demais normativos da Instituição, bem como estabeleçam responsabilidades no caso de descumprimento; e

(iii) É proibida a utilização de nuvem particular para armazenamento de Informação da Instituição.

6.2.8. **Mesa limpa.**

A mesa limpa consiste na atividade de não deixar à vista na estação de trabalho documentos em suporte físico contendo Informação confidencial. São regras gerais para mesa limpa:

(i) O Profissional do A.C.Camargo deve guardar todos os documentos em sua posse quando não estiver em sua estação de trabalho;

(ii) O Profissional do A.C.Camargo deve recolher imediatamente da impressora os documentos enviados para a impressão.

6.2.9. **Segurança física.**

A Segurança da Informação se faz também com o estabelecimento de mecanismos de proteção física. A criação de barreiras físicas que previnam acessos não autorizados, tais como leitores biométricos, portas de acesso com cartões magnéticos, entre outras medidas, devem ser utilizadas na medida em que forem necessárias para a proteção de Informações e dos Recursos Tecnológicos, em especial aquelas registradas em meio físico.

6.2.10. **Incidentes de Segurança da Informação.**

Cabem, primariamente, à área de Segurança da Informação as ações de prevenção de Incidentes de Segurança da Informação, atuando conforme normativos específicos. Porém, é responsabilidade de todo e cada Profissional do A.C.Camargo atentar para qualquer evento suspeito e comunicar imediatamente à área de Segurança da Informação, para as devidas providências.

6.2.11. **Fornecedores.**

A área de Segurança da Informação deverá implementar manual, diretrizes, normas e procedimentos específicos para avaliação (*due diligence*), contratação e monitoramento constante de fornecedores no que tange a seu nível de conformidade com os requisitos de controles técnicos de Segurança da Informação, em conformidade com esta Política, demais normativos da Instituição e as melhores práticas de Segurança da Informação.

6.2.12. **Segurança da Informação nos processos e projetos de pesquisa.**

Os processos e projetos de Pesquisa envolvem, entre outras pessoas, pesquisadores, equipes clínicas e multiprofissionais, residentes, alunos de pesquisa, empresas e instituições externas. Todos serão corresponsáveis pela segurança e confidencialidade das Informações de seus projetos e processos e deverão observar as diretrizes para garantia da segurança das Informações, privacidade e da proteção de Dados Pessoais e/ou Dados Pessoais Sensíveis aplicados à matéria, de acordo com esta Política de Segurança da Informação, com a Política de Privacidade da Instituição e com procedimentos específicos relacionados à Segurança da Informação na prática científica.

Recursos tecnológicos adquiridos por meio de fundos de apoio à pesquisa devem ter sua especificação obrigatoriamente avaliada e homologada pela área de Tecnologia da Informação antes da aquisição. Estas tecnologias devem ser inventariadas e cumprir com todos os requisitos de segurança praticados pela Instituição, de forma a garantir a segurança dos dados e possibilitar suporte pela área de Tecnologia da Informação, a quem caberá autorizar, de forma prévia, expressa e excepcional, o uso de tecnologias que não atendam aos padrões institucionais, autorização esta que deverá ser obrigatoriamente acompanhada da devida análise de riscos e medidas de mitigação.

6.2.13. **Monitoramento constante e auditoria do ambiente.**

Todo ambiente físico e digital da Instituição é ou poderá ser monitorado, respeitados os limites previstos na legislação vigente, incluindo o acesso, o uso ou o tráfego de Informações em tais ambientes, por qualquer meio (tal qual, por exemplo, e-mail e aplicações utilizadas em dispositivos corporativos) com o objetivo de apurar o cumprimento da legislação aplicável e das políticas institucionais, em especial esta Política de Segurança da Informação.

Neste sentido, a Instituição poderá (e deverá): (i) monitorar todos os servidores, redes, conexões de internet, software, equipamentos e dispositivos corporativos, móveis ou não, conectados à rede corporativa; e (ii) realizar inspeções físicas ou virtuais nos equipamentos e nas estações de trabalho do Profissional do A.C.Camargo, seja em rotina periódica de monitoramento ou sob fundada suspeita de infração às normas internas da Instituição ou à legislação aplicável.

O monitoramento realizado pela Instituição poderá identificar usuários e apresentar dados sobre o seu uso da infraestrutura técnica da Instituição e do material e conteúdo por ele manipulado, sendo certo que todas as Informações coletadas no curso do monitoramento serão armazenadas pela Instituição para fins de auditoria e poderão ser utilizadas como provas de eventual violação das regras e condições estabelecidas pela Instituição ou pela legislação em vigor. Caso solicitado pelas autoridades competentes ou conforme necessário para o exercício de direitos da Instituição em processos de qualquer natureza, as informações oriundas do monitoramento poderão ser divulgadas na medida em que houver razão legal ou determinação judicial para tanto.

O monitoramento é realizado para resguardar a segurança não só dos sistemas da Instituição e das Informações neles tratadas, como também dos próprios Profissionais do A.C.Camargo. Os dados e as Informações monitoradas somente poderão ser acessadas pelos departamentos competentes e para finalidades legítimas, como a apuração de denúncias e condução de investigações corporativas. Todo e qualquer tratamento de dados para estes fins será fundamentado em relatórios de auditoria ou em outro instrumento apropriado para tanto, e cumprirá as normas específicas sobre privacidade e proteção de dados pessoais aplicáveis.

6.3. RESPONSABILIDADES E ATRIBUIÇÕES

Para os fins desta Política, as seguintes atribuições e responsabilidades devem ser consideradas:

6.3.1. Conselho Curador:

(i) Aprovar esta Política e suas eventuais alterações;

(ii) Definir a estratégia geral e as diretrizes de Segurança da Informação para a Instituição;

(iii) Supervisionar, por si e por seus comitês de assessoramento ou consultores especificamente contratados, o nível de segurança da informação e a aderência das práticas e processos da Instituição a esta Política e à Política de Privacidade;

(iv) Garantir a disponibilidade de recursos suficientes para o adequado funcionamento do Sistema de Gerenciamento de Segurança da Informação.

6.3.2. Diretoria Executiva:

(i) Aprovar o plano geral de implementação e as ações estratégicas e operacionais de Segurança da

Informação e as iniciativas em suas diferentes etapas;

(ii) Garantir a implantação de medidas técnicas de segurança da informação e de proteção de dados, de forma a atender a requisitos de sistemas padrões de boas práticas e de governança, alinhada aos termos dessa Política, da Política de Privacidade, normatizações internas de segurança e tecnologia da informação e aos princípios gerais previstos na Legislação de Proteção de Dados;

(iii) Assegurar a provisão orçamentária de recursos suficientes para o adequado funcionamento do Sistema de Gerenciamento de Segurança da Informação;

(iv) Providenciar a instalação e a manutenção de uma estrutura de pessoal para a gestão e coordenação das atividades de Segurança da Informação;

6.3.3. **Área de Segurança da Informação:**

(i) Aplicar a presente Política de forma que a proteção da Informação esteja alinhada com a proteção dos processos estratégicos do negócio;

(ii) Estabelecer, implantar e monitorar o Sistema de Gerenciamento de Segurança da Informação, de acordo com os requisitos da legislação, das normas técnicas aplicáveis e as melhores práticas internacionais;

(iii) Identificar os riscos inerentes à Segurança da Informação da Instituição através do mapeamento das vulnerabilidades, ameaças, impacto e probabilidade de ocorrência, e classificá-los, conforme metodologia institucional de gerenciamento de riscos e com o apoio da área de Gerenciamento de Riscos Corporativos;

(iv) Recomendar e/ou adotar controles que mitiguem os riscos mapeados, inerentes à Segurança da Informação;

(v) Recomendar e/ou adotar mecanismos automatizados para o gerenciamento, prevenção e detecção de eventos de Segurança da Informação;

(vi) Recomendar e/ou implementar processos de autenticação e controle de acesso seguros para os Recursos Tecnológicos;

(vii) Analisar criticamente as ocorrências de Segurança da Informação, considerando a efetividade desta Política frente ao volume e impactos dos eventos, Incidentes de Segurança da Informação detectados e mudanças de tecnologias;

(viii) Estabelecer e divulgar as responsabilidades pelo cumprimento desta Política;

(ix) Informar e orientar os Profissionais do A.C.Camargo sobre a importância da Segurança da Informação e a obrigatoriedade de cumprimento desta Política;

(x) Desenvolver programas de treinamento para os Profissionais do A.C.Camargo de forma a conscientizá-los sobre as responsabilidades de todos relação à Segurança da Informação;

(xi) Realizar auditorias e inspeções periódicas, com o objetivo de avaliar a conformidade com as

definições desta Política;

(xii) Manter atualizado o inventário de Recursos de Tecnologia, com todos os sistemas, aplicativos, softwares, ferramentas de gerenciamento de informações e dados da Instituição;

(xiii) Definir, implementar e testar planos de continuidade de negócios para garantir a disponibilidade dos recursos tecnológicos estratégicos em casos de Incidentes de Segurança da Informação;

(xiv) Em conjunto com o Encarregado e com a área de Privacidade e Proteção de Dados, gerir, analisar e acompanhar os Incidentes de Segurança da Informação e as suspeitas ou casos de violações dessa Política, definindo as ações de remediação conforme as diretrizes e procedimentos estabelecidos pela Instituição e acompanhando sua implementação pelas áreas responsáveis;

(xv) Revisar e propor atualizações à presente Política.

6.3.4. **Área de Privacidade e Proteção de Dados:**

(i) Avaliar os impactos da legislação e da regulamentação relacionada à privacidade e à proteção de dados pessoais às disposições desta Política e trabalhar em conjunto com as áreas de Tecnologia e Segurança da Informação para garantir o cumprimento das normas aplicáveis e implementar melhorias nos procedimentos, controles e medidas de segurança, visando à mitigação de riscos decorrentes do tratamento de Dados Pessoais;

6.3.5. **Área de Recursos Humanos:**

(i) Garantir que, no momento da contratação, o Profissional do A.C.Camargo tenha ciência desta Política e assine os termos de ciência e responsabilidade definidos pela área de Segurança da Informação;

(ii) Implementar os programas de treinamento para os Profissionais do A.C.Camargo, de forma a conscientizá-los sobre as responsabilidades de todos em relação à Segurança da Informação;

(iii) Informar imediatamente para a área de Tecnologia da Informação todas as contratações, transferências, afastamentos, desligamentos, mudanças de funções, licenças e modificações no quadro de colaboradores sob a sua supervisão.

6.3.6. **Gestores da Informação:**

(i) Gerenciar as Informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu Ciclo de Vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela Instituição;

(ii) Identificar, classificar e rotular as Informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela Instituição;

(iii) Revisar periodicamente as Informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;

(iv) Autorizar e revisar os acessos à Informação e sistemas de Informação sob sua responsabilidade;

(v) Aprovar a concessão ou solicitar a revogação de acesso à Informação ou sistemas de informação de acordo com os procedimentos adotados pela Instituição.

6.3.7. **Profissionais do A.C.Camargo:**

(i) Conhecer e cumprir todas as regras definidas nesta Política;

(ii) Adotar a conduta e todos os procedimentos necessários para proteger as Informações da Instituição;

(iii) Evitar discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, entre outros), buscando sempre fazê-lo em ambientes adequados e somente com as pessoas que realmente precisam ser envolvidas;

(iv) Utilizar as Informações e os Recursos Tecnológicos da Instituição exclusivamente para os objetivos da Instituição e para o cumprimento de suas funções, sendo vedado o uso para fins pessoais ou de terceiros;

(v) Solicitar esclarecimentos à Instituição para qualquer dúvida que possa vir a ter quanto ao disposto nesta Política, para que possa cumpri-la, não podendo, em nenhuma hipótese, alegar desconhecimento;

(vi) Relatar para a área de Segurança da Informação eventuais Incidentes de Segurança da Informação ou suspeitas ou violações desta Política das quais venha a tomar conhecimento.

6.4. DISPOSIÇÕES GERAIS

Descumprimento dos padrões institucionais de Segurança da Informação.

O não cumprimento desta Política ou de qualquer dos demais padrões institucionais de Segurança de Informação, comprovado após a devida apuração, serão passíveis de penalidades, tanto na esfera administrativa (advertências, punições administrativas, demissão ou rescisão contratual, entre outras) quanto na esfera legal (reparação dos danos causados à Instituição e às demais pessoas prejudicadas), conforme a gravidade do ato.

Atualização desta Política.

Este documento poderá sofrer alterações em caso de mudanças de processo e/ou alteração de tecnologia, mudanças de diretrizes institucionais ou da legislação vigente, ou ainda por determinação da Instituição.

Política de Segurança da Informação do A.C.Camargo Cancer Center, alterada e consolidada na reunião do Conselho Curador da Instituição realizada em 30 de abril de 2021.