1 – INTRODUÇÃO

A Política de Tecnologia da Informação é o documento que orienta e estabelece as diretrizes corporativas da Fundação Universitária de Cardiologia para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

2 – DOS OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Preservar as informações da FUC quanto à:

• Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
• Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
• Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

• Sigilo: garantia de que a informação fique exclusivamente com quem é de direito e propriedade, não tecendo comentários ou demonstração de documentos de caráter sigiloso.

3 – DA FINALIDADE

Estabelecer o conjunto de controles e responsabilidades que resultem em maior segurança na disponibilização e utilização de recursos de informática (hardwares e softwares) a serem praticados pelos usuários e pela organização, garantindo a manutenção e continuidade do negócio.

4 – DA ÁREA DE APLICAÇÃO

Esta política se aplica a todos os usuários dos recursos de informática – hardwares e softwares, já adquiridos ou que venham a ser adquiridos pela Fundação Universitária de Cardiologia para o desempenho de suas funções.

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

5 – DAS RESPONSABILIDADES

5.1 - Dos Colaboradores em Geral:

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT, estagiários, residentes, jovem aprendiz ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a Fundação Universitária de Cardiologia e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

5.2 - Dos Gestores de Pessoas e/ou Processos:

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da política.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Fundação Universitária de Cardiologia.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Termo de Compromisso dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente.

5.3 - Da Área de Tecnologia da Informação:

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta política;
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente;
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Fundação Universitária de Cardiologia;
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

> os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

> os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

- Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

6 - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta política a Fundação Universitária de Cardiologia poderá:

• implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
• tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação da Direção, Superintendência ou do gerente;
• realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
• instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

6.1 - Correio eletrônico:

É proibido aos colaboradores o uso do correio eletrônico da Fundação Universitária de Cardiologia:
• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Fundação Universitária de Cardiologia vulneráveis a ações civis ou criminais;
• divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
• falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
• apagar mensagens pertinentes de correio eletrônico quando a Fundação Universitária de Cardiologia estiver sujeita a algum tipo de investigação.
• produzir, transmitir ou divulgar mensagem que:
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa; - inclua imagens criptografadas ou de qualquer forma mascaradas;
- tenha conteúdo considerado impróprio, obsceno ou ilegal.

6.2 – Internet:

Todas as regras atuais da Fundação Universitária de Cardiologia visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de

informação. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privados da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

6.3 – Identificação:

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na Fundação Universitária de Cardiologia, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa

física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha. Os sistemas críticos e sensíveis para a

instituição e os logins com privilégios administrativos podem exigir a troca de senhas a cada 180 dias.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for desligado do quadro de pessoal ou terceiro ou solicitar demissão, a Gerência Imediata ou Superintendência, deverá imediatamente comunicar tal fato ao Setor de Informática, a fim de que essa providência seja tomada. Caso o colaborador esqueça sua senha, ele deverá comparecer na informática em horário comercial de posse do seu crachá de identificação da instituição e requisitar pessoalmente a troca de sua senha.

7 – DAS DISPOSIÇÕES GERAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Fundação Universitária de Cardiologia, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição. Há necessidade de revisões periódicas deste documento a fim de mantê-lo atualizado às necessidades institucionais.

8 - PROCEDIMENTOS COM A POLÍTICA IMPLANTADA

Após a política ser implantada ela deverá ser divulgada aos gestores e stakolders, definidos Pela Direção da Fundação Universitária de Cardiologia.

9 - HISTÓRICO DE REVISÃO

Elaborador	**Revisor**	**Aprovador**
Data: 01/04/2025 André Bonczinski **Gerente TI**	**Data: 08/04/2025** Cleber Colpes Lacerda **Superintendente de Apoio** Fabio Etges **Superintendente Financeiro**	**Data: 22/04/2025** Leandro Gomes **Superintendente Executivo**

	Renata Brião **Superintendente Assistencial**	
Versão 1	**Alteração** Elaboração da Politica	**Data:** 01/04/2025