FIOTEC
FIOCRUZ

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

1 Apresentação

Esta política faz parte do Sistema de Informação Documentada da Fundação para o Desenvolvimento Científico e Tecnológico em Saúde (Fiotec).
A Política de Segurança da Informação é o ponto de partida para a gestão da segurança da informação no âmbito da Fiotec e foi elaborada com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2022, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

A segurança da informação é questão estratégica nos negócios da Fiotec, constituindo um dos pilares de sua atuação, buscando garantir a preservação das informações sob sua responsabilidade de forma a construir processos e gerar documentos que promovam a proteção legal da entidade e de seus indivíduos.

Assim, a instituição da Política de Segurança da Informação é uma declaração formal acerca do compromisso com a preservação da confidencialidade, da integridade, da disponibilidade e da privacidade da informação de sua propriedade e/ou sob sua guarda. E visa estabelecer um ambiente seguro, proporcionando melhor qualidade nos processos de gestão e controle dos sistemas de informação da instituição.

2 Finalidade

Estabelecer um conjunto de diretrizes e práticas de segurança da informação que definem como a instituição gerencia e protege seus ativos de informação, visando garantir que as informações confidenciais e críticas da organização sejam protegidas contra ameaças internas e externas, bem como serem mantidas disponíveis para as partes autorizadas.

3 Aplicabilidade

A presente Política se aplica obrigatoriamente a todos os profissionais da Fiotec, sejam conselheiros, diretores, empregados (administrativos ou para projetos), estagiários, bolsistas, jovens aprendizes, autônomos, prestadores de serviços, terceirizados, entendidos neste documento como colaboradores e que formam a comunidade Fiotec.

Seus desdobramentos e aplicação ocorre por meio de normas, procedimentos operacionais, instruções de trabalho e formulários dela derivados, garantindo assim sua perenidade.

4 Princípios

São princípios fundamentais desta política, com base na ISO/IEC 27002:2022:

a) Confidencialidade: Este princípio garante que as informações sejam acessíveis somente por pessoas autorizadas e que os dados não sejam revelados a indivíduos não autorizados.
b) Integridade: Este princípio garante que as informações sejam precisas e completas, não havendo modificação não autorizada ou perda de informações.
c) Disponibilidade: Este princípio garante que as informações estejam sempre disponíveis para as pessoas autorizadas a acessá-las, e que não haja interrupções nos sistemas que afetem a disponibilidade das informações.
d) Privacidade: Este princípio estabelece que as organizações coletem, processem e armazenem as informações pessoais dos indivíduos de forma ética e segura, respeitando suas escolhas e direitos em relação a essas informações.
e) Autenticidade: Este princípio garante que as informações sejam autênticas e provenientes de fontes confiáveis.

f) Conformidade: Este princípio garante que as atividades de segurança da informação estejam em conformidade com as leis e regulamentações aplicáveis.
g) Responsabilidade: Este princípio garante que as pessoas que manipulam as informações assumam responsabilidade pelas ações realizadas.
h) Irretratabilidade (não repúdio): este princípio atua para que um indivíduo ou entidade não negue a autoria de uma ação específica.
i) Aprendizado organizacional: Este princípio enfatiza a importância de aprender com incidentes de segurança e de buscar melhorias contínuas nos processos de segurança da informação.

5 Conteúdo

Este documento estabelece os princípios e diretrizes que norteiam a segurança da informação na Fiotec, sendo aprovado e divulgado por deliberação da Diretoria Executiva e do Conselho Curador, que estabelecem as iniciativas necessárias ao alcance dos objetivos de segurança estabelecidos.

A Política de Segurança da Informação da Fiotec será complementada pelo Código de Segurança da Informação, Normas e Procedimentos, considerados parte integrante deste documento a serem detalhados e divulgados em documentos específicos.

5.1 Diretrizes

A Fiotec deve manter uma estrutura organizacional que possibilite coordenar, orientar e avaliar as atividades relativas à segurança da informação na instituição.

A Fiotec deve instituir um Comitê de Segurança da Informação para acompanhar, avaliar, propor alterações, dirimir eventuais dúvidas e deliberar sobre os assuntos abordados nessa Política e quaisquer outros assuntos encaminhados pela área de

Segurança da Informação da Instituição.

O Comitê de Segurança da Informação deve ser composto obrigatoriamente pelo Diretor Administrativo, Gerente de TI, Gestor de Segurança da Informação e Gerente de Gestão de Pessoas além de outros membros nomeados pelo Diretoria Executiva mediante indicação direta ou por recomendação do próprio Comitê.

A Fiotec deve buscar o contínuo aperfeiçoamento de suas práticas relacionadas com a Gestão de Segurança da Informação.

Com base nos princípios fundamentais desta política, é dever de todos zelar pelas informações da Fiotec que circulam em diferentes formatos e meios de comunicação, dentro e fora da instituição.

A Fiotec deve definir a classificação da informação, seu grau de importância e criticidade e os dados devem ser protegidos e tratados conforme essa classificação. Cabe ao usuário identificar a classificação atribuída a um dado, e aplicar as restrições de acesso e divulgação associados.

É responsabilidade e compromisso dos diretores e empregados da Fiotec, trabalhar para:

a) Garantir a integridade, confidencialidade, disponibilidade e privacidade da informação, seja em meio físico ou digital;
b) Evitar a revelação de informações sensíveis, que ponham em risco as atividades da Instituição ou de seus parceiros;
c) Proteger o seu patrimônio, em especial os dispositivos que suportam ou permitem o trânsito da informação;
d) Garantir que as informações e os processos de trabalho estejam em conformidade com a legislação, a Política de Privacidade e o Código de Conduta Ética da Fiotec;

e) Não permitir que seus ativos sejam utilizados para atividades ilegais, sejam elas de qualquer natureza;

f) Atuar de maneira prioritariamente preventiva em relação à segurança da informação, minimizando os riscos de forma equilibrada; e

g) Atuar de maneira corretiva e transparente, sempre que acontecerem incidentes que possam comprometer a segurança da informação.

5.2 Matriz de Responsabilidades

Responsável	Atividade
BÁSICO	
Todos os Colaboradores da Fiotec	• Conhecer e cumprir as diretrizes desta Política, assim como comunicar qualquer violação ou suspeita, por meio dos canais disponibilizados pela Fiotec; • Atuar na primeira linha de defesa da Fiotec, identificando, atuando e comunicando potenciais riscos e não conformidades identificadas.
Gestores da Fiotec	• Garantir na sua equipe a leitura e a aplicação do conteúdo desta Política; • Assegurar que os princípios e diretrizes orientem permanentemente as decisões de suas equipes.
Diretoria Executiva	• Aprovar o conteúdo dessa Política; • Garantir a aplicação desta Política.
Conselho Curador	• Aprovar o conteúdo dessa Política;
ESPECÍFICA	
Coordenação de Segurança da Informação	• Promover a cultura de Segurança da Informação na Instituição;

	• Prover recursos técnicos para execução dessa Política; • Revisão periódica desta Política; • Tratar incidentes que violem esta Política.
Comitê de Segurança da Informação	• Aprovar o conteúdo e garantir a aplicação dessa Política; • Acompanhar, avaliar, propor alterações, dirimir eventuais dúvidas e deliberar sobre os assuntos abordados nessa Política. • Apoiar na implementação das ações de Segurança da Informação
Assessoria de Planejamento e Qualidade	• Revisar este documento.

6 Disposições Gerais

O não cumprimento das diretrizes descritas nesta Política, constitui falta grave, estando sujeito as penalidades administrativas e/ou contratuais.

Situações não previstas e sugestões devem ser encaminhadas para a Coordenação da Segurança da Informação, via canais institucionais.

Este documento será atualizado periodicamente e/ou de acordo com a necessidade.

7 Referências Normativas

Norma NBR ISO/IEC 27002:2022 – Código de Práticas para a Gestão da Segurança da Informação.
Política de Privacidade da Fiotec

Código de Conduta Ética da Fiotec

Política de Riscos da Fiotec

8 Controle de Revisões

Revisão	Data	Resumo da Alteração
0	18/12/2017	Versão inicial aprovada pelo Diretoria e Conselho Curador.
1	30/06/2022	Primeira revisão formulada pelo Comitê de Segurança da Informação e aprovada pela Diretoria.
2	25/06/2025	Adequação dos itens da Política, conforme o Procedimento de Informação Documentada; Inclusão da Matriz de Responsabilidades, item 5.2, e bem como atualização nos demais itens.

9 Termos e definições

Não se aplica

10 Anexos

Não se aplica