

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



Sumário

1	Apresentação.....	3
2	Finalidade.....	3
3	Aplicabilidade.....	3
4	Princípios.....	4
5	Conteúdo.....	5
5.1	Diretrizes gerais.....	5
5.2	Matriz de Responsabilidades.....	6
5.3	Diretrizes específicas.....	12
6	Disposições Gerais.....	15
7	Referências Normativas.....	15
8	Controle de Revisões.....	16
9	Termos e definições.....	16
10	Anexos.....	17



Este documento pertence à Fiotec. As informações nele contidas possuem todos os direitos reservados. Nenhuma parte deste material deverá ser reproduzida, armazenada em cópias de segurança, transmitida sob qualquer forma ou por qualquer meio de impressão, seja ele físico ou eletrônico, sem autorização prévia e expressa da Fiotec.



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 pelas normas ABNT NBR ISO/IEC 27001 - Sistema de Gestão da Segurança da Informação – Requisitos e ABNT NBR ISO/IEC 27002 - Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de 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 27001:

- 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 colem, 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

Esta Política apresenta as diretrizes estratégicas que orientam a proteção das informações da Fiotec. As seções seguintes estabelecem os requisitos gerais a serem observados por todos os colaboradores, complementados, quando necessário, por documentos específicos do Sistema de Gestão da Segurança da Informação (SGSI).

5.1 Diretrizes gerais

A Fiotec mantém uma estrutura organizacional que possibilita coordenar, orientar e avaliar as atividades relativas à segurança da informação na instituição, esta estrutura é denominada Coordenação Estratégica de Segurança da Informação (CSI).

A Fiotec instituiu um Comitê de Segurança da Informação para acompanhar, com a missão de avaliar, propor alterações, dirimir eventuais dúvidas e deliberar sobre os assuntos abordados nessa Política e quaisquer outros assuntos encaminhados pela Coordenação de Segurança da Informação.

A Fiotec busca 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 definiu critérios para a classificação das informações, considerando seu



grau de importância, criticidade e sensibilidade, de forma a estabelecer os níveis de proteção aplicáveis. Cabe ao usuário identificar a classificação atribuída à informação, e observar as restrições de acesso, uso, armazenamento, compartilhamento e divulgação correspondentes.

É responsabilidade e compromisso 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
Básicas	
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. • Zelar pela confidencialidade, integridade e disponibilidade das informações sob sua responsabilidade, utilizando os recursos da Fiotec de uma forma segura e em conformidade com esta Política.
Gestores da Fiotec	• Garantir na sua equipe a leitura e a aplicação do conteúdo desta Política; • Assegurar que os princípios e diretrizes desta política orientem permanentemente as decisões de suas equipes. • Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os profissionais sob a sua gestão (liderança e comprometimento); • Informar à Coordenação de Segurança da Informação o desligamento de prestadores de serviço, incluindo terceiros em formato de “Pessoa Jurídica”; • Comunicar imediatamente à Coordenação de Segurança da Informação qualquer descumprimento ou violação das diretrizes, Procedimentos e/ou de suas Instruções de trabalho. • Assegurar que os riscos de segurança da informação relacionados aos processos sob



	sua responsabilidade sejam identificados, comunicados e tratados quando aplicável. • Garantir que os acessos concedidos aos colaboradores sob sua gestão sejam compatíveis com suas atribuições, comunicando admissões, movimentações e desligamentos às áreas competentes.
Diretoria Executiva	• Demonstrar comprometimento com o Sistema de Gestão da Segurança da Informação (SGSI), assegurando recursos necessários para sua implementação e melhoria contínua; • Aprovar o conteúdo dessa Política; • Garantir a aplicação desta Política.
Conselho Curador	• Aprovar o conteúdo dessa Política;
ESPECÍFICAS	
Coordenação de Segurança da Informação	• Deve estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação, incluindo os processos necessários e suas interações; • Promover a cultura de Segurança da Informação na Instituição; • Prover recursos técnicos para execução dessa Política; • Revisão periódica desta Política; • Planejar e se preparar para gerenciar incidentes da segurança da informação, definindo, estabelecendo e comunicando processos, papéis



	e responsabilidades de gestão de incidentes da segurança da informação. • Administrar o Sistema de Gestão de Segurança da Informação. • Propor e apoiar iniciativas que visem a segurança dos ativos de informação da instituição, de acordo com as recomendações dos órgãos reguladores; • Promover as versões da Política de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação; • Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços; • Analisar em conjunto com a área de Tecnologia da Informação e/ou Gerências envolvidas nos incidentes de segurança da informação, e propor as ações para o tratamento das vulnerabilidades, conforme a análise dos riscos; • Manter comunicação efetiva com o Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do comitê ou de membros da diretoria; • Auditar rotineiramente os controles de segurança da informação; • Apoiar as auditorias internas e/ou externas, e realizar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
--	--



	• Identificar preventivamente e mitigar riscos que comprometem a segurança da informação e de serviços em ambiente corporativo; • Executar ações de controle e gestão de mecanismo/ferramentas de segurança cibernética; • Realizar gestão de vulnerabilidade em sistemas, dispositivos e infraestrutura disponibilizados na rede interna e externa e adequar os serviços que necessitam de controles de segurança.
Comitê de Segurança da Informação	• Aprovar o conteúdo e garantir a aplicação desta Política; • Acompanhar, avaliar, propor alterações e deliberar sobre os assuntos abordados nesta Política. • Apoiar na implementação das ações de Segurança da Informação. • Atuar de acordo com o estabelecido no Regimento Interno do Comitê de Segurança da Informação. • Avaliar material disponibilizado mensalmente pelo analista de Segurança da Informação; • Acompanhar informações consolidadas sobre riscos, incidentes e vulnerabilidades relevantes, avaliar impactos para o SGSI e recomendar prioridades, recursos ou ações de tratamento às instâncias competentes; • Acompanhar informações consolidadas sobre riscos, incidentes e vulnerabilidades relevantes, avaliar impactos para o SGSI e recomendar prioridades, recursos ou ações de tratamento às instâncias competentes;



	• Sempre que for necessário, discutir sobre algum incidente grave ou relevante para a instituição e fazer recomendações ao Diretor Executivo; • O comitê de Segurança da Informação poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.
Assessoria de Planejamento e Qualidade	• Apoio operacional a revisão e publicação desta política. • Apoiar auditorias. • Apoiar na gestão da informação documentada do SGSI.
Tecnologia da Informação	• Garantir a recuperação dos dados corporativos, além de administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes; • Gerar e manter as trilhas para auditoria de acordo com as especificações estabelecidas para rastrear possíveis falhas e fraudes nos sistemas críticos do Plano de Continuidade dos Sistemas de Informação; • Configurar os equipamentos e sistemas concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança da informação corporativa; • O processo de aquisição e desenvolvimento de sistemas e acesso em produção deve atender requisitos de segurança previsto nas especificações de segurança da Fiotec.



5.3 Diretrizes específicas

As diretrizes específicas de Segurança da Informação foram definidas como desdobramento das diretrizes gerais, no que tange à implementação dos controles aplicáveis de segurança da informação:

5.3.1 Tratamento da Informação: A Fiotec deve criar, gerir e avaliar critérios de tratamento e classificação das informações que lhe pertencem, ou estejam sob sua responsabilidade, de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor e demais normas aplicáveis.

5.3.2 Gestão de Incidentes: Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, de forma a impedir a interrupção das atividades da instituição e não afetar negativamente o alcance dos seus objetivos estratégicos.

5.3.3 Gestão de Riscos: Foi estabelecido um processo de Gestão de Riscos de Segurança da Informação, com a finalidade de minimizar possíveis impactos associados aos ativos, possibilitando a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

5.3.4 Gestão de Continuidade: A Gestão de Continuidade de Negócio foi estabelecida no âmbito da Fiotec, visando reduzir assegurar a continuidade das operações críticas por meio da prevenção, resposta e recuperação frente a eventos que possam comprometer pessoas, processos, informações, instalações ou recursos tecnológicos..

5.3.5 Controle de Acessos Lógicos: Foram formalizadas regras que estabeleçam procedimentos, garantam o controle de acesso às informações, instalações e sistemas de informação, fazendo uso de mecanismos apropriados e MFA (múltiplo fator de autenticação), quando aplicável.

5.3.6 Controle de Acessos Físicos, Segurança Física e Segurança do Ambiente: Os ativos da instituição são protegidos contra acesso físico de pessoas não autorizadas, bem como contra danos, perdas, furto e



interferências internas e externas. As proteções estão alinhadas aos riscos identificados relacionados ao ativo.

5.3.7 Armazenamento, Descarte e Transporte Seguros da Informação: Foram estabelecidos procedimentos seguros, com os mecanismos apropriados, que garantem a segurança das informações tratadas pela **Fiotec**, sejam elas físicas ou digitais, garantindo a segurança e inviolabilidade de seu conteúdo, evitando que pessoas não autorizadas tenham acesso às mesmas.

5.3.8 Classificação da Informação: Foi estabelecida uma classificação sistemática e objetiva para qualificar as informações que circulem no âmbito da **Fiotec**, considerando a sua importância para o desenvolvimento das atividades da instituição, a necessidade de proteção à privacidade das pessoas às quais os dados se referem, a criticidade, a sensibilidade e relevância da informação.

5.3.9 Bring Your Own Device (BYOD): As informações da instituição não devem ser acessadas através de dispositivos que não são de propriedade da Fiotec, exceto sob autorização expressa da Coordenação de Segurança da Informação ou fornecimento de meio de acesso controlado pela instituição. No caso da utilização de dispositivos pertencentes à Fiotec, estes serão monitorados e as informações pertencentes à instituição serão preservadas. A Fiotec se reserva ao direito de deletar as informações de sua propriedade em dispositivos perdidos ou de profissionais que não tenham mais vínculo com a instituição.

5.3.10 O Código de Conduta: O Código de Conduta ética é obrigatoriamente a todos os profissionais da Fiotec, sejam conselheiros, diretores, empregados (administrativos ou para projetos), estagiários, bolsistas, jovens aprendizes, prestadores de serviços, terceirizados, contratados via RPA, que formam a comunidade Fiotec. Todos os profissionais da Fiotec assinam o Código de Conduta.

5.3.11 Orientação para Autenticação: A instituição estabelece diretrizes para autenticação segura, incluindo uso de senhas robustas e autenticação multifator quando aplicável."



5.3.12 Gestão de Backups: Para assegurar o bom funcionamento da gestão de backups, a Fiotec estabelece diretrizes para realização, monitoramento e testes periódicos, visando assegurar a disponibilidade e recuperação das informações.

5.3.13 Gestão de Mudanças Tecnológicas: A gestão de mudanças no âmbito da TI é necessária para garantir que os métodos e procedimentos padronizados mais adequados sejam utilizados para o manuseio eficiente de todas as alterações ocorridas no ambiente organizacional da **Fiotec**. Toda mudança relevante em ativos de informação deve seguir processo formal de avaliação, aprovação, implementação e registro.

5.3.14 Homologação de Aplicações: Para garantir a segurança e bom funcionamento dos ativos de informação da **Fiotec**, somente aplicações e softwares aceitos pela instituição poderão ser instalados e executados nos notebooks, AVDs e outros sistemas de uso dos profissionais. Quaisquer outros softwares serão, a princípio, bloqueados, mas sua execução ou instalação pode ser aceita mediante solicitação via ferramenta de abertura de chamados.

5.3.15 Homologação de Serviços em Nuvem: Para garantir a homologação correta e funcional dos serviços em nuvem, somente serviços aceitos pela instituição poderão ser utilizados pelos profissionais. O uso de outros serviços será, a princípio, negado, considerando que os ambientes dispõem de dados que são frequentemente consultados ou atualizados e têm altos requisitos de tempo de resposta de acesso e a preservação destes é necessária.

5.3.16 Trabalho remoto: O trabalho remoto, quando autorizado, só é permitido com a utilização de dispositivos de propriedade da Fiotec. Estes serão monitorados e as informações pertencentes à instituição serão preservadas. Os profissionais em trabalho remoto devem usar o seu login corporativo para acessar os sistemas necessários para o desenvolvimento do seu trabalho, não sendo permitido o uso de login anônimo. O login é pessoal e intransferível, não podendo ser compartilhado com outros usuários ou revelado a qualquer pessoa, de maneira que todas as atividades realizadas



possam ser rastreadas e identificadas, a fim de serem imputadas ao usuário, conforme esta Política de Segurança da Informação. O desenvolvimento das atividades em trabalho remoto deve ter a mesma diligência e seguir as mesmas regras de segurança aplicadas no trabalho presencial. Os cuidados em relação à exposição indevida de informações, principalmente em relação às mais sensíveis, devem ser realizados da mesma forma que são realizados no trabalho presencial. A informação não deve ficar exposta em cima de mesas ou ser armazenada em locais inseguros e sem vigilância. O equipamento/dispositivo fornecido pela Fiotec deverá sempre ser bloqueado na ausência temporária do profissional, bem como desligado ao final da jornada de trabalho.

5.3.17 Conscientização e Capacitação: A Fiotec promove ações contínuas de capacitação e conscientização em segurança da informação, garantindo que todos compreendam suas responsabilidades e contribuam para a proteção dos ativos de informação.

6 Disposições Gerais

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

Este documento deve ser interpretado em conjunto com outras políticas corporativas, normas e procedimentos relevantes adotados pela Fiotec.

Em situações não previstas por esta política, as decisões serão tomadas pelo Diretor Executivo ou por um membro da Diretoria Colegiada designado por ele, que poderá buscar o apoio na Coordenação da Segurança da Informação.

7 Referências Normativas

ABNT NBR ISO/IEC 27001:2022 Sistema de Gestão da Segurança da Informação - Requisitos.





ABNT NBR ISO/IEC 27002:2022 Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação.

Política de Privacidade da Fiotec.

Código de Conduta Ética da Fiotec.

Política de Riscos da Fiotec.

Regimento Interno do Comitê de Segurança da Informação.

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.
3	14/09/2026	Adequação a Norma ISO 27001, seguindo os preceitos de preparação do SGSI (sistema de gestão de segurança da informação) conforme projeto de preparação da certificação ISO 27001. Aprovação do documento, conforme Ata de Reunião 147ª do Conselho Curador.

9 Termos e definições

Os termos utilizados nesta Política seguem as definições estabelecidas no Manual do SGSI, bem como nas normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022, quando aplicável.



10 Anexos

Não se aplica

