CÓDIGO

DE SEGURANÇA DA INFORMAÇÃO

COD_FIOTEC_002_00

FUNDAÇÃO PARA O DESENVOLVIMENTO
CIENTÍFICO E TECNOLÓGICO EM SAÚDE

Histórico de Alterações				
Revisão	**Referências**	**Autor**	**Data de Execução**	**Resumo da Alteração**
	Política de Segurança da Informação	Evandro Maroni	02/01/2018	Primeira Versão
1ª				
2ª				
3ª				
4ª				
5ª				
6ª				
7ª				
8ª				
9ª				
10ª				
11ª				
12ª				
13ª				
14ª				
15ª				
16ª				
17ª				
18ª				
19ª				
20ª				

Sumário

LISTA DE SIGLAS E ABREVIATURAS

- ABNT – Associação Brasileira de Normas Técnicas
- CLT – Consolidação das Leis do Trabalho
- CONARQ – Conselho Nacional de Arquivos
- CTDE – Câmara Técnica de Documentos Eletrônicos
- ISO – *International Organization for Standardization*
- PSIF – Política de Segurança da Informação da Fiotec
- RH – Recursos Humanos
- TI – Tecnologia da Informação

OBJETIVO

Este Código tem como objetivo normatizar diversos aspectos relacionados à segurança da informação, em conformidade com a Política de Segurança da Informação da Fiotec (PSIF).

Por meio da orientação e do estabelecimento das diretrizes da instituição para proteger seus ativos de informação, a PSIF visa determinar os padrões de comportamentos relacionados à segurança da informação adequados às necessidades do negócio e também os de proteção legal da entidade e de seus indivíduos.

Os riscos típicos que a aplicação deste Código pretende evitar são:

- Revelação de informações sensíveis;
- Modificações indevidas de dados e programas;
- Perda de dados e programas;
- Destruição ou perda de recursos e instalações;
- Interdições ou interrupções de serviços essenciais;
- Roubo de propriedades.

Esses riscos ocorrem pelos seguintes motivos:

- Negligência – atos não intencionais de usuários;
- Subversão – ataques disfarçados praticados por usuários;
- Acidente – ocorrências acidentais e por fatores alheios;
- Ataque furtivo – ataques praticados por pessoas estranhas;
- Ataque forçado – ataques às claras praticados por usuários ou estranhos.

APLICAÇÃO

As regras, recomendações e conceitos deste Código são aplicáveis a todos os empregados, estagiários e aprendizes da Fiotec, à sua Diretoria, aos seus prestadores de serviços e aos eventuais visitantes que tenham acesso a quaisquer informações da instituição. Todos esses grupos são denominados “usuários” sempre que tratados de forma indistinta neste documento.

Empregados, estagiários e prestadores de serviços da Fiotec que trabalham na área de Tecnologia da Informação distinguem-se dos demais usuários pelo fato de possuírem direitos e privilégios diferenciados para a necessária administração do ambiente computacional e de rede. Neste documento, esses colaboradores são denominados “equipe de TI”.

Todos, indistintamente, são responsáveis pela observação e cumprimento da PSIF bem como deste Código de Segurança da Informação.

Neste documento, a menção a uma determinada gerência refere-se à área como um todo, representada pelo seu respectivo gerente, mas não limitada a ele. Consequentemente, a menção à responsabilidade de uma determinada gerência em fazer alguma coisa não implica que o próprio gerente deve executar a tarefa, mas sim que ele é responsável pela correta execução da tarefa, mesmo quando a delega.

As gerências de Tecnologia da Informação e de Recursos Humanos são referenciadas neste Código como gerência de TI e gerência de RH, respectivamente, utilizando seus acrônimos mais conhecidos.

A PSIF é o ponto de partida para a gestão da segurança da informação no âmbito da Fiotec e sua aplicação ocorre por meio de normas, procedimentos operacionais, instruções de trabalho e formulários dela derivados, garantindo assim sua perenidade.

REFERÊNCIAS

- ABNT NBR ISO IEC 27001 – Código de práticas para a gestão da segurança da informação.

- ABNT NBR ISO IEC 27002 – Código de práticas para controles de segurança da informação.

- Consumerization of IT: Risk Mitigation Strategies – 2012 - European Network and Information Security Agency.

- Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018 v.1.0 – 2015 – Presidência da República.

- Fundamentos do Direito para Atuação Judicial e Extrajudicial – 1ª edição (2015). Ministério Público Federal.

- Glossário – Documentos Arquivísticos Digitais – 7ª versão (2016). CONARQ e CTDE.

- Security Framework for Governmental Clouds – 2015 - European Network and Information Security Agency.

1 DEFINIÇÕES

No contexto deste Código, são adotadas as definições a seguir.

1.1 Informação

Resultado da produção, manipulação, organização ou processamento de dados que represente uma modificação no conhecimento do sistema que a recebe.
Um dado não é considerado informação quando, sem o devido processamento, for insuficiente para conferir sentido ou significado a uma determinada matéria.
Porém, será considerado como informação o dado que, mesmo não processado, for suficiente para produzir modificações no conhecimento de sistemas humanizados ou informatizados.

1.2 Equipamento

Todo dispositivo utilizado para processamento, produção, transformação, manipulação, organização ou transmissão de informações no ambiente da Fiotec ou que seja de sua propriedade. Essa denominação engloba computadores, impressoras, scanners, smartphones, roteadores, switches, servidores, centrais telefônicas, aparelhos telefônicos, câmeras, monitores, dentre outros. No contexto deste Código, os equipamentos podem ser referenciados como hardware.

1.3 Aplicativo

Qualquer programa ou grupo de programas que instrui o hardware sobre a execução de uma tarefa. No contexto deste Código, os aplicativos podem ser referenciados como **sistema, aplicativo interno** ou ***software***, e podem estar instalados localmente ou disponibilizados na internet.

1.4 Aplicativo Externo

Programas, serviços, assinaturas ou contratos disponibilizados por outra instituição de forma eletrônica, seja por meio de aplicativos ou de sítios virtuais.

1.5 Recurso de TI ou Ativo de TI

Refere-se genericamente aos equipamentos e aplicativos, internos e externos.

1.6 Empregado

Denominação dada à pessoa contratada cujo vínculo de cunho empregatício é regido pela CLT - Consolidação das Leis do Trabalho.

1.7 Prestador de Serviço ou Terceiro

Parte contratada pela Fiotec que tem acesso às instalações, recursos e informações necessárias para o cumprimento de suas obrigações profissionais. Fazem parte dessa categoria: autônomos, terceiros, contratados diretos, *part time*, cooperativas, pessoa jurídica ou pessoa física, subcontratado, terceirizado e quarteirizado.

1.8 Ambiente da Fiotec

Refere-se ao ambiente físico – instalações e área ao seu redor – e também ao ambiente denominado virtual, que compreende os servidores, rede e serviços tecnológicos ofertados pela instituição, que podem estar hospedados localmente ou remotamente, em *datacenter* ou em serviço de nuvem.

1.9 Identidade Lógica

Conjunto de informações que caracterizam o usuário no contexto dos sistemas de informação. Cada usuário na Fiotec possui uma identidade lógica que, na medida do possível, é única e dá-lhe acesso aos sistemas e recursos inerentes a sua atuação.

2 REGRAS GERAIS

Para o perfeito entendimento e aplicação deste Código, são estabelecidas as seguintes regras gerais.

2.1 Informação na Fiotec

Toda e qualquer ação em relação à informação na Fiotec deve ser orientada explicitamente por este Código, resguardados os direitos e penalidades conforme legislação vigente.

2.2 Política de Segurança da Informação e Outras Normas Vigentes

Todas as regras, recomendações e quaisquer outras ações contidas neste Código buscam materializar a Política de Segurança da Informação da Fiotec e não podem sobrepor a legislação vigente ou regras contidas no Código de Ética da Fiotec.

2.3 Termo de Ciência, Responsabilidade e Compromisso

A Assessoria Jurídica, em conjunto com a Gerência de Tecnologia da Informação, deve elaborar o Termo de Ciência, Responsabilidade e Compromisso, instrumento de concordância que trata das obrigações relativas à confidencialidade das informações, uso de equipamentos e compromisso com as determinações da Política de Segurança da Informação e Código de Segurança da Informação.
Todos os usuários devem ter acesso a este Código e atestar o seu conhecimento por meio de assinatura no Termo de Ciência, Responsabilidade e Compromisso.

2.3.1 Termo de Ciência, Responsabilidade e Compromisso Para Usuários Internos

É o instrumento a ser assinado individualmente por cada usuário, atestando e acatando este Código.

2.3.2 Termo de Ciência, Responsabilidade e Compromisso Para Empresas Contratadas

Deve ser elaborado um modelo específico de Termo para ser assinado pelos responsáveis legais por empresas contratadas para prestação de serviços no ambiente da Fiotec ou que precisem ter acesso a informações internas ou confidenciais.

2.4 Do uso de Equipamentos e Aplicativos da Fiotec

Equipamentos e aplicativos são fornecidos pela Fiotec para que seus usuários os utilizem no desempenho de suas atividades profissionais, sendo que o uso para fins particulares é entendido e aceitado, desde que sejam respeitados os limites da razoabilidade.

2.5 Circulação de Informação na Fiotec

A informação deve circular livremente dentro do ambiente da Fiotec, desde que sejam observadas as regras específicas para cada tipo de informação, conforme a classificação da informação detalhada no capítulo 9 deste Código.

2.6 Materiais de Terceiros Protegidos por *Copyright*

Os computadores e sistemas da Fiotec não podem ser utilizados para baixar, copiar, modificar, enviar, encaminhar ou receber materiais protegidos por *copyright*, segredo industrial, sigilo financeiro ou quaisquer outros dispositivos a estes assemelhados, sem a autorização prévia e expressa do titular de direito.

Sob nenhuma circunstância os equipamentos e sistemas da Fiotec podem ser utilizados para a troca direta de arquivos de material não licenciado, incluindo arquivos de áudio e vídeo.

Nos casos de dúvida sobre direitos de proteção de qualquer material ou conteúdo, ou se o mesmo é adequado para transferência, deve-se, sempre, decidir pelo não envio e consultar a chefia imediata ou a Assessoria Jurídica da Fiotec.

2.7 Envio de Material ao Público Externo

Qualquer material ou conteúdo aprovado pela Fiotec para envio ao público externo, seja por meio dos equipamentos ou dos sistemas da instituição, deve estar acompanhado do devido aviso referente à proteção e confidencialidade das informações.

2.8 Manipulação de Material Impróprio ou Proibido

É proibida a utilização dos recursos da Fiotec para distribuição, arquivamento, publicação, veiculação ou execução de material com teor pornográfico, homofóbico, de pedofilia, de cunho racista ou qualquer outro teor proibido pelas leis brasileiras.

2.9 Marca, Nome e Logo da Fiotec

A marca, o nome e o logo da Fiotec só podem ser utilizados para fins relacionados às atividades da instituição e conforme regras contidas em seu Manual de Identidade Visual.

O uso da marca, do nome e do logo da Fiotec em outros contextos, que não os relacionados às atividades da instituição, só é permitido se expressamente autorizado pela área responsável pela comunicação institucional.

2.10 Alçada da TI para Preservação de Provas e Eliminação de Conteúdo Não Permitido

Independentemente de autorização ou prévio aviso, a equipe de TI deve tomar os procedimentos previamente definidos pelo Comitê de Segurança da Informação para preservação de provas de acesso a conteúdos não permitidos e eliminação de quaisquer arquivos encontrados nos equipamentos da Fiotec que não sejam permitidos conforme as diretrizes deste Código.

2.11 Comitê de Segurança da Informação

Deve ser instituído um Comitê para tratar de assuntos referentes à segurança da informação, doravante denominado Comitê de Segurança da Informação, que deve ser composto obrigatoriamente pelo Gerente Geral, Gerente de TI, Gerente de RH e Gerente da Assessoria Jurídica além de outros membros nomeados pela Direção Executiva mediante indicação direta ou por recomendação do próprio Comitê.
As atividades necessárias para instalação do Comitê de Segurança da Informação são de responsabilidade da Gerência de TI, inicialmente, mas o próprio Comitê se encarregará de definir suas normas de funcionamento, em conformidade com este Código.

2.12 Obrigatoriedade de Elaboração de Mapa de Risco para Projetos Internos da Fiotec

Todo projeto interno da Fiotec, que implique em mudança ou implantação de um processo, informatizado ou não, deverá gerar um mapa de risco em relação à segurança da informação. Esse mapa será analisado pelo Comitê de Segurança da Informação, que deverá emitir parecer em relação ao mapa e ao projeto, autorizando a continuidade do projeto ou recomendando alterações. Fica a critério do Comitê de Segurança da Informação a dispensa de mapa de risco para projetos de menor dimensão.

2.13 Responsabilidade Pelo Cumprimento da PSIF

Todos os usuários são responsáveis pelo cumprimento das disposições da Política de Segurança da Informação da Fiotec materializada através deste Código de Segurança da Informação.

2.14 Prazo Para Implantação de Controles, Processos, Procedimentos e do Comitê de Segurança da Informação

Todos os controles, processos, procedimentos e o próprio Comitê de Segurança da Informação deverão estar implantados em até 180 (cento e oitenta) dias após a entrada em vigor deste Código.
O Comitê de Segurança da Informação será considerado implantado a partir da sua entrada em atividade, portanto, poderá ser acionado em ocorrências ainda não contempladas no prazo de 180 dias.

2.15 Cláusula de Confidencialidade em Contratos de Trabalho

É obrigatória a presença de cláusula de confidencialidade em todos os contratos de trabalho para que possa ser concedido o acesso do usuário aos ativos de informação disponibilizados pela instituição.

3 DISPONIBILIZAÇÃO E RESPONSABILIDADE SOBRE EQUIPAMENTOS

Todos os equipamentos da Fiotec são de uso exclusivo para o alcance dos objetivos da instituição e disponibilizados de acordo com as necessidades específicas dos usuários para o desempenho de suas atribuições.

3.1 Responsabilidade Sobre Equipamentos Recebidos

Os usuários são responsáveis pela segurança dos equipamentos recebidos e devem ser responsabilizados caso haja caracterização de mau uso.

3.1.1 Perda de Equipamento de Propriedade da Fiotec

Quando um equipamento de propriedade da Fiotec for subtraído ou perdido, o usuário deve comunicar imediatamente o fato à gerência de TI, que dará ciência ao Comitê de Segurança da Informação.
Nos casos de furto ou roubo de equipamentos da Fiotec, o usuário que dele tinha a posse deverá registrar boletim de ocorrência policial e apresentar imediatamente à gerência de TI e de Recursos Humanos da Fiotec. O Boletim de Ocorrência deverá ser anexado ao dossiê profissional, se a vítima for empregado, estagiário ou aprendiz.

3.1.2 Caracterização de Mau Uso

A caracterização de mau uso se dá mediante reconhecimento do próprio usuário ou, no caso de constatação pela equipe de TI, por meio de análise e decisão do Comitê de Segurança da Informação.

3.1.3 Custos com Reparos e Reposições de Equipamentos Danificados ou Perdidos

Nos casos de mau uso, o usuário deverá assumir os custos de reparo ou, na impossibilidade de conserto, de nova aquisição de equipamento de mesma marca e modelo.
No caso de perda, o usuário deverá assumir os custos de nova aquisição de equipamento de mesma marca e modelo.
Caso o equipamento perdido ou danificado de forma irreparável não seja mais fabricado, deverá ser utilizado como referência outro equipamento similar, preferencialmente do mesmo fabricante.
As regras de ressarcimento de custos para reparo ou aquisição de novo equipamento não são aplicáveis nos casos de roubo desde que o usuário apresente o boletim de ocorrência policial.

3.2 Troca de Senha do Usuário

Mediante a comunicação de perda, extravio, furto ou roubo, a equipe de TI deverá trocar as senhas do usuário que utilizava o equipamento.

4 ADESÃO E UTILIZAÇÃO DE APLICATIVOS EXTERNOS

Todos os aplicativos externos utilizados pelos usuários para consecução de suas atividades são de responsabilidade da Fiotec e devem ser mantidos pela instituição e não pelos usuários.

4.1 Termos de Licenças

Os usuários não podem concordar com termos de licenças sem a anuência prévia da gerência de TI.

4.2 Adesões aos Aplicativos Externos

Todas as adesões aos aplicativos externos devem ser feitas em nome da Fiotec, não sendo permitida a utilização de nomes de pessoas físicas, empregados, estagiários, aprendizes ou terceirizados, a não ser na qualidade de representante técnico ou funcional, quando solicitado pelo fornecedor.

Os procedimentos para adesões a aplicativos pagos devem ser solicitados à TI que dará início ao processo internamente demandando às demais áreas envolvidas nos procedimentos de compra.

Para adesão a aplicativos não pagos, os chamados free, o usuário deve solicitar à TI que deverá fazer a adesão. Enquadram-se nesta categoria não só os aplicativos de mercado, mas também aqueles fornecidos sem custos por fornecedores ou financiadores, por exemplo.

Nos casos de aplicações governamentais, os responsáveis legais devem fazer a adesão sem a interferência da TI.

O endereço eletrônico institucional de referência fiotecTI@fiotec.fiocruz.br deve ser usado em qualquer condição de aquisição ou adesão a aplicativos externos.

4.3 Senhas de Acesso aos Aplicativos Externos

Todas as senhas de acesso devem ser informadas à gerência de TI que se responsabiliza pelo armazenamento em local seguro, com a identificação dos usuários autorizados a utilizá-las.

5 SEGURANÇA E MONITORAMENTO DA INFORMAÇÃO

Visando garantir a segurança das suas informações, a Fiotec pode estabelecer procedimentos de inspeção e monitoração de seus sistemas e equipamentos. Os procedimentos de inspeção e monitoramento devem abranger todos os usuários, inclusive os alocados na equipe de TI. Para isso, uma auditoria técnica anual deverá ser realizada ou quando o Comitê de Segurança da Informação julgar necessária.

5.1 O Papel da TI nas Ações de Monitoramento de Sistemas e Equipamentos

A equipe de TI é responsável pela realização de monitoramentos gerais, que não dependem de solicitação, para detectar eventuais desvios na utilização dos recursos, sendo que tais desvios devem ser reportados ao Comitê de Segurança da Informação.
A execução das ações de monitoramento é feita exclusivamente pela equipe de TI.

5.2 Formas de Monitoramento de Sistemas e Equipamentos

A Fiotec, através de sua área de Tecnologia da Informação, poderá exercer o monitoramento de seus sistemas e equipamentos sem necessitar de prévio aviso ou permissão do usuário.
Os procedimentos para garantir a segurança da informação, podem incluir ações de diferentes tipos.

5.2.1 Instalação de Dispositivos ou Sistemas de Monitoramentos

A Fiotec poderá instalar dispositivos ou sistemas de monitoramentos em quaisquer equipamentos, sistemas, serviços ou dispositivos de rede e utilizar as informações geradas por estes dispositivos ou sistemas para identificar os usuários e seus respectivos acessos efetuados, bem como os materiais manipulados.

5.2.2 Inspeção Física nos Equipamentos

A qualquer tempo, a Fiotec poderá executar a inspeção física nos equipamentos de sua propriedade.

5.2.3 Utilização de Informações Obtidas em Procedimentos Disciplinares

A Fiotec poderá utilizar as informações obtidas pelos sistemas de monitoramento e auditoria para embasar as medidas disciplinares previstas neste Código.

6 ACESSO AOS SISTEMAS E EQUIPAMENTOS

Todos os acessos dos usuários aos sistemas utilizados pela Fiotec devem estar atrelados a perfis específicos condizentes com sua função e cargo, no caso de empregados, estagiários e aprendizes, ou ao uso específico, no caso de terceiros, sendo proibido o acúmulo de perfis.

6.1 Perfil de Acesso

Os perfis de acesso aos sistemas são criados pela gerência de TI e englobam todos os sistemas em uso.

6.2 O Comitê de Segurança da Informação e a Criação e Cancelamento de Perfis

O Comitê de Segurança da Informação é responsável pela aprovação para criação e cancelamento de perfis.

6.3 Restrição de Acesso do Usuário

Sem necessidade de prévia autorização, a equipe de TI pode restringir o acesso dos usuários que forem detectados exaurindo ou prejudicando algum recurso tecnológico.
A restrição imposta ao usuário deve ser comunicada formalmente à gerência de TI, que se encarregará de informar aos demais componentes do Comitê de Segurança da Informação.
O Comitê de Segurança da Informação decide sobre a manutenção ou retirada da restrição e suas possíveis consequências, com base nas informações fornecidas pela equipe de TI.

7 RESPONSABILIDADE SOBRE EQUIPAMENTOS PESSOAIS

Os equipamentos pessoais trazidos e/ ou mantidos nas dependências da Fiotec são de responsabilidade exclusiva do proprietário ou usuário.

7.1 Perda ou Furto de Equipamentos Pessoais

Eventuais perdas ou furtos de equipamentos pessoais são de responsabilidade exclusiva dos usuários, não cabendo à Fiotec qualquer obrigação de reposição ou indenização em eventuais casos de sinistros dessas naturezas. O Comitê de Segurança da Informação deverá elaborar os procedimentos para a entrada e saída de equipamentos pessoais eventualmente utilizados em trabalhos que envolvam informação.

7.2 Instalação de Sistemas e Serviços da Fiotec em Equipamentos Pessoais

Os sistemas e serviços de TI da Fiotec não podem ser utilizados em equipamentos pessoais, exceto se autorizado pela gerência de TI ou se estiverem liberados para uso público.

7.2.1 Segurança da Informação na Utilização de Sistemas e Serviços da Fiotec em Equipamentos Pessoais

Caso haja liberação para uso de aplicativos internos ou externos em algum equipamento pessoal, a equipe de TI deverá verificar se tal equipamento possui a proteção apropriada para o uso autorizado.

8 IDENTIFICAÇÃO DE PESSOAS E ACESSO ÀS INFORMAÇÕES

Todos os dispositivos de reconhecimento de pessoas utilizados na Fiotec, como o número de registro do empregado, do crachá, das identificações de acessos aos sistemas, dos certificados, das assinaturas digitais e dos dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

8.2 Uso Compartilhado de Identificação

Excepcionalmente e em decorrência da garantia da economicidade, da eficiência das equipes de trabalho, da natureza do trabalho a ser executado e da definição dos perfis, poderá ser autorizada a utilização de senhas de uso comum. Esta excepcionalidade em hipótese alguma se confunde com o compartilhamento de senhas pessoais, prática

expressamente proibida por este Código e deve ser autorizado previamente pelo Comitê de Segurança da Informação.

8.3 Criação e Controle das Identidades Lógicas e Certificações Digitais

A gerência de TI é responsável pela criação e controle das certificações digitais e identidades lógicas dos diretores, empregados, estagiários, aprendizes e prestadores de serviço na instituição.

8.4 Desligamento ou Remanejamento de Empregados, estagiários e aprendizes da Fiotec

Nos casos de desligamento ou remanejamento de empregado da Fiotec, a gerência de RH deverá comunicar o fato imediatamente à gerência de TI.

8.5 Desligamento de Prestador de Serviço

Nos casos de desligamento de prestador de serviço, o gestor da área tomadora do serviço deverá comunicar o fato imediatamente à gerência de TI.

8.6 Bloqueio de Acesso do Usuário nos Casos de Desligamento

Quando algum usuário se desligar da Fiotec, a equipe de TI deverá bloquear imediatamente o acesso aos sistemas e equipamentos aos quais ele tinha acesso.

9 CLASSIFICAÇÃO DA INFORMAÇÃO

Todos os usuários são responsáveis pelas informações da Fiotec que circulam em diferentes formatos e meios de comunicação, dentro e fora da instituição.
Toda informação deve ser protegida e mantida sob sigilo conforme a sua importância e criticidade para a Fiotec.
Quanto mais crítica ou sigilosa, maiores cuidados devem ser dedicados ao manuseio, arquivamento e eventual descarte.

9.1 Informação em Documentos Físicos Eletrônicos

A Fiotec trabalha com documentos físicos e eletrônicos criados internamente ou recebidos de terceiros. Todos os documentos são de propriedade da Fiotec e, portanto, devem ser protegidos, pois podem conter informações corporativas críticas.

9.2 Processo de Classificação da Informação

O diretor executivo da Fiotec é o responsável pela classificação dos tipos de documento, podendo delegar essa função total ou parcialmente por meio de instrumento formal.
O processo de classificação da informação consiste em identificar quais são os níveis de proteção requeridos, bem como estabelecer classes e formas de identifica-las, além de determinar os controles de proteção necessários a cada uma delas. O sistema de classificação de informação da Fiotec obedece a seguinte estrutura de acordo com a sua criticidade.

9.2.1 Informação Confidencial

É a informação da Fiotec e/ ou de seus clientes e parceiros com o mais alto grau de confidencialidade e restrição e que, se for divulgada sem autorização, pode causar danos materiais significativos ou até mesmo colocar em risco a viabilidade do negócio da Fiotec. São limitadas a um número reduzido de pessoas, pois exigem medidas especiais de controle e proteção contra acessos ou cópias não autorizadas.

9.2.2 Informação Interna

É toda informação cujo conhecimento é limitado ao ambiente interno e aos propósitos da Fiotec. Apenas os empregados, estagiários ou aprendizes e prestadores de serviços podem ter acesso a essas informações e sua revelação ao público em geral só poderá ocorrer se explicitamente autorizada pela instituição.

9.2.3 Informação Pública

É a informação para uso interno e/ ou externo com controles mínimos cuja divulgação pública não causa impacto à Fiotec. É colocada à disposição do empregado ou prestador de serviço e pode ser revelada ao público externo.

9.2.4 Informação não Classificada

Toda informação não classificada deve ser considerada como INTERNA.

10 PROTEÇÃO CONTRA AMEAÇAS DIGITAIS

Os hábitos seguros contra ameaças digitais são de responsabilidade de todos os usuários, que devem seguir as recomendações da equipe de TI divulgadas pelos instrumentos de comunicação disponíveis na Fiotec.

10.1 Dispositivo de Acesso Externo

É proibido o uso de quaisquer dispositivos externos de acesso à rede que ultrapassem ou anulem intencionalmente os controles de segurança da Fiotec.

10.2 Proteção Contra Aplicativos Mal-Intencionados

A proteção contra aplicativos mal-intencionados deve ser realizada por meio de ações conjuntas dos profissionais de TI, sistemas de proteção, procedimentos de segurança e comportamento dos usuários.

10.3 Aquisição e Instalação de Sistemas ou Equipamento de Prevenção

A aquisição e instalação de sistemas ou equipamentos de prevenção contra ameaças digitais são de responsabilidade exclusiva da equipe de TI.

10.4 Instalações de Aplicativos

Todo e qualquer aplicativo deve ser instalado exclusivamente pela equipe de TI.

10.5 Aplicativos Ilegais ou não Homologados

Não são permitidas instalações de aplicativos ilegais ou não homologados pela gerência de TI nos equipamentos da Fiotec.

10.6 Lista dos Aplicativos Homologados

A gerência de TI deve elaborar lista com todos os aplicativos homologados e disponibilizá-la através dos instrumentos de comunicação disponíveis na Fiotec.

11 TRATAMENTO DE INCIDENTES

Ao tomar conhecimento de uma brecha, incidente e/ ou violação deste Código, o usuário não deverá fazer nenhum teste para checar possíveis falhas na segurança.
A efetivação de testes de vulnerabilidade ou tentativa para solucionar possíveis brechas pode ser interpretada como tentativa de violação da segurança e o usuário que assim proceder poderá ser responsabilizado legalmente.

11.1 Comunicação de Incidentes de Segurança da Informação

Ao perceber uma possível brecha, incidente ou violação da PSIF, o usuário deverá comunicar o fato à gerência de TI.

11.2 Documentação de Incidentes de Segurança da Informação

A equipe de TI deve documentar todas as ocorrências de brechas ou incidentes de segurança e colher todas as evidências possíveis quando identificar violações intencionais, inclusive usando as atas notariais, quando necessário.

12 MEDIDAS DISCIPLINARES POR VIOLAÇÃO DA PSIF

Os usuários que cometerem excessos ao utilizar os recursos disponibilizados pela Fiotec podem ter seus privilégios cancelados.

12.1 Ação Disciplinar

A violação das normas estabelecidas neste Código de Segurança da Informação ou das suas alterações ou normas complementares é considerada infração, cuja natureza e gravidade implicam na utilização de medidas disciplinares ao usuário que assim proceder.

12.2 Notificação da Violação da PSIF ao Comitê de Segurança da Informação

Quando houver alguma violação deste Código ou dos instrumentos de proteção e controle, a gerência de TI deve notificar o fato ao Comitê de Segurança da Informação.
A notificação emitida pela gerência de TI deve indicar o tipo de violação e se houve reincidência por parte do usuário.

12.3 Medidas Disciplinares Cabíveis

O Comitê de segurança da Informação decide sobre a aplicação das medidas disciplinares cabíveis, conforme a gravidade e em conformidade com a legislação em vigor.

12.4 Níveis de Gravidade de Eventual Violação da PSIF

De acordo com a gravidade da infração eventualmente cometida, os impactos e eventuais prejuízos causados por ela, a Fiotec poderá aplicar sanções cabíveis e proporcionais conforme previsto na legislação em vigor e no Código de Ética da Fiotec.
A gravidade da infração deve ser explicitada, levando-se em consideração os riscos aos quais a Fiotec foi exposta e os prejuízos causados.
A gravidade das violações da PSIF é classificada como:

12.4.1 Violação de Baixa Gravidade

Violação que não gera consequências imediatas e pode ser sanada imediatamente.

12.4.2 Violação de Média Gravidade

Violação que pode gerar ou não prejuízo, porém requer tempo e esforço considerável para corrigi-la.

12.4.3 Violação de Alta Gravidade

Violação que gera consequências imediatas, trazendo prejuízos para a imagem da Fiotec e para a continuidade do negócio ou financeira.

12.5 Violações Cometidas Por Profissionais da Equipe de TI

Todas as violações da PSIF, quando cometidas por profissionais da equipe de TI, devem ser notificadas ao Comitê de Segurança da Informação e automaticamente posicionadas um nível acima no grau de gravidade avaliado. Desta forma uma violação classificada como “baixa”, se cometida por um profissional de TI, será automaticamente alçada à condição de “média”, e assim sucessivamente.

12.6 Casos Omissos

Os casos omissos, não previstos neste Código, devem ser avaliados e tratados pelo Comitê de Segurança da Informação.

13 PRESTADORES DE SERVIÇOS

Os prestadores de serviços contratados pela Fiotec devem estar atentos à prevenção de riscos e impactos a confidencialidade, proteção e segurança da informação da Fiotec, comunicando os casos de incidentes e/ ou violações da PSIF ao responsável pela contratação.

13.1 Violações Cometidas por Prestadores de Serviço

Caso o usuário em questão seja um prestador de serviço, a Fiotec poderá aplicar sanções cabíveis e proporcionais conforme previsto na legislação em vigor.

13.2 Violações Cometidas por Empregados de Empresas Prestadoras de Serviços

Havendo violação da PSIF ou deste Código por empregado de empresa prestadora de serviço, a Fiotec deverá notificar a infração à empresa contratada que deverá tomar as medidas cabíveis.

13.3 Cláusulas Obrigatórias em Contratos com Prestadores de Serviços

Para garantir o cumprimento da Política de Segurança da Informação da Fiotec, os contratos firmados com prestadores de serviços devem conter cláusulas específicas.

13.3.1 Cláusula de Confidencialidade

É obrigatória a presença de cláusula de confidencialidade em todos os contratos de prestação de serviço para que possa ser concedido o acesso do usuário aos ativos de informação disponibilizados pela instituição.

13.3.2 Cláusula de Conhecimento e Cumprimento da PSIF e do Código de Segurança da Informação

Todos os contratos assinados com prestadores de serviços que atuem dentro do ambiente da Fiotec, devem conter cláusula que especifique o compromisso em seguir as regras deste Código.

13.3.3 Confidencialidade Após Término da Prestação do Serviço

O direito autoral e a confidencialidade das informações da Fiotec ou dos seus parceiros devem ser preservados em todos os trabalhos realizados em nome da Fiotec, mesmo após o término do referido trabalho, por tempo indeterminado ou formalmente expresso pela Fiotec.

13.5 Utilização de Equipamentos Próprios por Prestadores de Serviços

Prestadores de serviços que necessitem utilizar equipamentos próprios para o desempenho de suas atribuições também estão sujeitos às diretrizes da PSIF e deste Código.

13.6 Acesso de Prestadores de Serviços ao Ambiente Tecnológico da Fiotec a Partir de Equipamentos Próprios

Os equipamentos dos prestadores de serviços que necessitem de acesso ao ambiente tecnológico da Fiotec devem ser configurados pela equipe de TI da Fiotec e os privilégios dados ao usuário e ao equipamento devem ser limitados ao mínimo necessário para a execução das tarefas estabelecidas no contrato.

13.7 Encerramento das Atividades de Prestadores de Serviços

O encerramento das atividades dos prestadores de serviços deve ser comunicado imediatamente pelo gerente de área responsável pelas atividades à gerência de TI.

13.8 Devolução de Recursos Disponibilizados pela Fiotec

Todos os prestadores de serviço, no encerramento de suas atividades, devem devolver integralmente os recursos disponibilizados pela Fiotec ou que vieram a ter acesso em decorrência da sua contratação e que estejam sob sua posse ou responsabilidade.

13.9 Cancelamento de Acessos ao Fim das Atividades, Contratos ou Acordos

Todos os acessos concedidos aos prestadores de serviços devem ser cancelados pela equipe de TI após o encerramento das atividades, contratos ou acordos.

14 COMPETÊNCIA E RESPONSABILIDADES

Todos os usuários são responsáveis pelo cumprimento das determinações deste Código.

14.1 Responsabilidades Gerais de Todos os Empregados da Fiotec

a. Cumprir as normas estabelecidas por este Código, bem como manter-se informado sobre suas atualizações e das normas dele derivadas;
b. Comunicar ao Comitê de Segurança da Informação com cópia aos superiores imediatos quaisquer atos ou situações que, segundo sua percepção ou avaliação, coloquem em risco a segurança da informação;
c. Ter comportamento idôneo com relação à utilização dos recursos de TI;
d. Ser ético na aquisição, tratamento e utilização da informação corporativa;
e. Praticar atos pautados nas regras e orientações contidas neste código.

14.2 Responsabilidades Específicas dos Diretores, Gerentes e Supervisores

a. Adequar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender à PSIF e o CSIF;

b. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os membros de suas respectivas equipes;
c. Apresentar e informar aos futuros usuários, em fase de contratação e formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a exigibilidade de cumprimento deste Código;
d. Providenciar para que os membros de suas respectivas equipes leiam e assinem o Termo de Compromisso e Ciência, assumindo o dever de cumprirem as normas estabelecidas, bem como se comprometendo a manterem sigilo e confidencialidade sobre todos os ativos de informações da Fiotec, mesmo quando desligados;
e. Providenciar para que os prestadores de serviços e outros usuários que não estejam cobertos por um contrato assinem o Termo de Compromisso e Ciência antes de receberem acesso às informações em formato físico ou digital da instituição;
f. Comunicar às suas equipes as atualizações deste Código.

14.3 Responsabilidades Específicas da equipe de TI

a. Pela característica de seus privilégios, manter sigilo sobre as informações e dados da Fiotec e dos usuários, restringindo-se a acessá-los somente quando forem necessários para a execução das atividades operacionais sob sua responsabilidade;
b. Segregar as funções administrativas, operacionais e educacionais nos sistemas a fim de restringir ao mínimo necessário os poderes de cada usuário e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
c. Testar a eficácia dos controles e ferramentas de segurança utilizadas e informar aos gestores das demais áreas e ao Comitê de Segurança da Informação sobre os riscos residuais;
d. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
e. Realizar auditorias periódicas de configurações técnicas e análise de riscos para subsidiar as decisões do Comitê de Segurança da Informação;

f. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Fiotec;
g. Proteger continuamente todos os sistemas e equipamentos da instituição contra códigos maliciosos e garantir que os novos sistemas e equipamentos só entrem para o ambiente de produção após estarem livres de códigos maliciosos e/ ou indesejados;
h. Monitorar o ambiente de TI, gerar indicadores e históricos de todos os fatos relevantes que possam impactar na segurança da informação;
i. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela equipe de TI nos ambientes totalmente controlados por ela;
j. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;
k. Configurar os equipamentos, ferramentas e sistemas concedidos aos usuários com todos os controles necessários, para cumprir os requerimentos de segurança estabelecidos por este Código;
l. Manter os sistemas atualizados em suas versões mais recentes, bem como os equipamentos que necessitam de atualizações de *firmware*;
m. Acompanhar a evolução tecnológica e propor novas soluções para garantir que o ambiente tecnológico da Fiotec se mantenha seguro;
n. Definir as regras formais para instalação de software e hardware em ambiente de produção institucional, exigindo o seu cumprimento dentro da instituição;
o. Garantir segurança especial para sistemas com acesso público, procurando fazê-lo guardar as evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
p. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da Fiotec operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro;
q. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Fiotec em processo de mudança, sendo ideal a

auditoria de código e a proteção contratual para controle e atribuição de responsabilidade no caso de uso de terceiros;

r. Garantir que as informações de um usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário, quando ocorrer movimentação interna dos ativos de TI;
s. Garantir, no menor prazo possível, o bloqueio de acesso de usuários por motivo de desligamento da instituição, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Fiotec;
t. Promover a conscientização dos usuários em relação à relevância da segurança da informação para o negócio da Fiotec, mediante campanhas, palestras, treinamentos e outros meios de endomarketing;
u. Apoiar as avaliações e as adequações de controles específicos de segurança da informação para novos sistemas ou serviços;
v. Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação;
w. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Fiotec;
x. Disponibilizar os indicadores de segurança gerados, bem como as principais ocorrências, para a Diretoria e Gerentes da Fiotec. A disponibilização deve ser periódica, e os prazos acordados entre as partes;
y. Garantir o sigilo sobre as senhas de acesso aos sistemas e equipamentos, não as fornecendo em hipótese algum a usuários;
z. Garantir o controle de acessos aos ambientes de processamento e armazenamento das informações da Fiotec por meio de estabelecimento de perímetros de segurança;
aa. Planejar e aplicar proteções físicas contra fenômenos naturais bem como contra incêndio, infiltrações e outros sinistros que possam trazer danos aos equipamentos de processamento e armazenamento das informações.

CONTROLES E REGISTROS DA QUALIDADE

Os controles e registros da Qualidade que evidenciam a correta aplicação da PSIF estão relacionados a seguir:

a. Mapa de riscos de segurança da informação;
b. Relatório de registros de incidentes de segurança da informação;
c. Mapa de controle de acessos;
d. Relatório de registro de backups realizados;
e. Planejamento de exercícios de recuperações de registros;
f. Execução de exercícios de recuperações de registros;
g. Controle de assinantes dos Termos de Compromisso e Ciência;
h. Mapa de estrutura de prevenções contra-ataques externos;
i. Registros de atualizações de defesas individuais (antivírus, *antispyware*, etc.);
j. Atas das reuniões do Comitê de Segurança da Informação;
k. Relatório de níveis de serviços dos recursos disponíveis (principalmente servidores);
l. Planejamentos e evidências de testes dos sistemas implantados ou customizados.

MATRIZ DE RESPONSABILIDADE PARA ELABORAÇÃO DO CÓDIGO DE SEGURANÇA DA INFORMAÇÃO

ATIVIDADE	RESPONSABILIDADE
Elaboração do Código de Segurança da Informação	TI
1ª Aprovação – Formatação e Revisão de Conteúdo	Gestão da Qualidade
2ª Aprovação – Responsabilidade Direta	RH/ Logística
3ª Aprovação – Legalidade	Assessoria Jurídica
4ª Aprovação – Ratificação do Projeto	Gerência Geral/ Direção
5ª Aprovação – Ratificação do Projeto	Conselho Curador
Revisão Textual	Comunicação
Revisão Geral, Codificação e Controle	Gestão da Qualidade
6ª Aprovação – Homologação de Atendimento a Requisitos	TI
Divulgação	Comunicação

GLOSSÁRIO

Ameaças: situações que exploram uma vulnerabilidade. Exemplo: vírus, *spam*, acesso indevido, *hackers* etc.

Aplicativos mal-intencionados: são programas de computador desenvolvidos para causar algum tipo de dano aos arquivos, aos sistemas ou às redes de computadores, bem como para capturar informações ou utilizar seu equipamento para ações danosas a outras máquinas ou redes. Podem ser introduzidas por meio de arquivos anexos aos e-mails, mídias removíveis contaminadas, configuração inadequada no sistema operacional de seu equipamento ou, ainda, arquivos obtidos na Internet.

Arquivo: em qualquer sistema de computador, arquivo é um conjunto de dados disponível aos usuários (inclusive o próprio sistema e os programas aplicativos), capaz de ser manipulado (por exemplo: movido, copiado, apagado etc.).

Ata notarial: trata-se de uma das espécies do gênero instrumento público notarial, por cujo meio o tabelião de notas acolhe e relata, na forma legal adequada, fato ou fatos jurídicos que ele vê e ouve com seus próprios sentidos, quer sejam fatos naturais quer sejam fatos humanos, esses últimos desde que não constituam negócio jurídico.

Backup: cópia de segurança dos dados originais ou conjunto de dados mantidos por questão de segurança, a fim de garantir sua disponibilidade.

Computação em grade: ou *grid computing*, é um modelo computacional capaz de alcançar altas taxas de velocidade de processamento dividindo as tarefas em diversas máquinas, que formam uma máquina virtual.

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Controle de acesso: controle efetuado sobre um hardware ou software para prevenir ou detectar o acesso não autorizado a sistemas, informações, equipamentos, instalações, entre outros, inclusive o perímetro de segurança de equipamentos e áreas de processamento e armazenamento de informações.

Copyright: direito autoral, propriedade literária ou artística.

Datacenter: é um ambiente projetado para abrigar servidores e outros componentes como sistemas de armazenamento de dados (*storages*) e ativos de rede (*switches*, roteadores). Em geral um datacenter deve prover ambiente de rede, segurança física, sistema de combate e prevenção a incêndios, refrigeração e energia.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Documento: é toda unidade de registro de informações, qualquer que seja o suporte ou formato. Em outras palavras, a informação pode estar registrada em papel, em arquivo eletrônico, em uma placa de identificação ou em qualquer outro tipo de suporte.

E-mail (Correio eletrônico): correspondência eletrônica trocada entre partes distintas.

Empregado: denominação dada à pessoa contratada cujo vínculo de cunho empregatício é regido pela CLT - Consolidação das Leis do Trabalho.

Firmware: conjunto de instruções operacionais programadas diretamente no hardware de um equipamento eletrônico.

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.

Internet: acrônimo de Interconnected Networks. Rede global e descentralizada de computadores, interconectados pelo uso de protocolos comuns de comunicação.

Intranet: rede privada utilizada por uma organização.

***Malware* (aplicativo mal-intencionado):** software criado para infectar computadores privados e cometer crimes como fraude e roubo de identidade. Esses programas são criados especificamente para roubo de dados.

Mídia: meio de transmissão e/ou armazenamento de dados.

Parceiro: empresa que participa com a Fiotec no desenvolvimento de determinados projetos.

Perímetro de segurança: área física ou virtual que circunda determinado ambiente, garantindo a sua impenetrabilidade em relação a eventuais ameaças.

Redes Sociais: são as páginas da Internet pelas quais os usuários se conectam para se comunicar, trocar experiências e compartilhar conhecimentos. As redes sociais podem proporcionar diferentes meios de interação entre seus membros: sociais (Exemplos: *Facebook*, *Orkut*, *MySpace*, *Twitter*, *Instagram*), ou profissionais (Exemplo: *Linkedin*).

Senhas: dispositivos de verificação de identidade. Não podem ser compartilhadas com outras pessoas em nenhuma hipótese, pois o uso de senhas de outra pessoa constitui crime tipificado no Código Penal Brasileiro (Art. 307 – Falsa identidade).

Serviço de nuvem: também referenciado como computação em nuvem, refere-se à utilização de memória, capacidade de armazenamento e processamento utilizando computadores interligados e seguindo o princípio da computação em grade (*grid computing*).

Servidor: termo genérico que designa o computador considerado central em algum processo. Assim, existem servidores de impressão (gerenciam impressões em cada rede), de arquivos (armazenam os arquivos criados pelos usuários) e de mensagem (gerenciam as mensagens enviadas e recebidas por componentes da rede), entre outros.

Sítio virtual: página ou conjunto de páginas na Internet.

Transferência de arquivos: processo de envio de dados entre duas ou mais fontes.

FOLHA DE APROVAÇÃO

Este Código de Segurança da Informação foi elaborado pelo Gestor da área de Tecnologia da Informação e sua concepção determinada conforme previsto na Política de Segurança da Informação aprovada na 85ª Reunião do Conselho Curador realizada em 18 de dezembro de 2017 e instituída pela Portaria N.001 – Fiotec/2018 de 02 de janeiro de 2018.

O Códido de Segurança da Informação da Fiotec entra em vigor a partir da data de sua publicação.