Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Número	
069/2011-PR	
Folha 01	De 07
Entrada em vigor	

Portaria da Presidência

O Presidente da Fundação Oswaldo Cruz, no uso das atribuições que lhe são conferidas pelo Decreto de 29 de dezembro de 2008

RESOLVE:

1.0 – PROPÓSITO

Instituir a Política de Segurança da Informação e Comunicações (POSIC), visando assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações da Fiocruz.

2.0 – OBJETIVO

Estabelecer e difundir as Diretrizes da Política de Segurança da Informação e Comunicações no âmbito da Fiocruz, inclusive em seus Institutos, visando à orientação quanto ao uso adequado das informações e dos recursos de tecnologia da informação que as suportam, evitando impactos prejudiciais às atividades finalísticas e à Gestão da Instituição.

3.0 – CONCEITOS E DEFINIÇÕES

Agente público: todo aquele que, por força de lei, contrato ou de qualquer ato jurídico, preste serviços de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, desde que ligado direta ou indiretamente à Fiocruz;

Ativo de informação: qualquer pessoa, tecnologia, processo ou ambiente que processe, armazene, transporte ou descarte informação institucional;

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Comitê de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da Fiocruz.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

Cancela	Altera	Distribuição	Data
		Geral	21/02/2011

Diretriz: conjunto de instruções ou indicações que orientam o que deve ser feito para se alcançar os objetivos estabelecidos na política;

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

Incidente de segurança: qualquer evento indesejado ou inesperado, que comprometa as operações ou ameace a segurança da informação;

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

Gestão de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do órgão;

Metodologia de Desenvolvimento de Sistemas: conjunto de práticas que define o processo de desenvolvimento de sistemas de informação;

Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficiente à implementação da segurança da informação e comunicações;

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Severidade: índice ou grau que se refere à medição do impacto de um evento ou incidente de segurança da informação.

4.0 – REFERÊNCIAS LEGAIS E NORMATIVAS

- Decreto nº 1.171, de 22 de junho de 1994, que dispõe sobre o Código de Ética do Servidor Público Civil do Poder Executivo Federal;
- Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados e informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado;
- Instrução Normativa nº 01/IN01/DSIC/GSIPR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;
- Norma Complementar nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008, que estabelece a metodologia de Gestão de Segurança da Informação e Comunicações;
- Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta;
- Norma Complementar nº 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações nos órgãos ou entidades da Administração Pública Federal, direta e indireta;
- Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que regulamenta a criação de equipes de tratamento e resposta a incidentes em redes computacionais.

▪ Norma Complementar nº 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009, que regulamenta a Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações;

▪ NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos;

▪ NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.

5.0 – PRINCÍPIOS

As ações de Segurança da Informação e Comunicações na Fiocruz são norteadas pelos seguintes princípios (sem prejuízo aos princípios da Administração Pública Federal, definidos no art. 37 da Constituição Federal):

Alinhamento estratégico: deve haver um alinhamento entre a Política de Segurança da Informação e Comunicações com a missão institucional e seu planejamento estratégico;

Diversidade organizacional: a elaboração da Política de Segurança da Informação e Comunicações deve levar em consideração a diversidade das atividades da Fiocruz, respeitando a natureza e finalidade de cada Unidade da Instituição;

Propriedade da informação: toda informação produzida ou armazenada na Fiocruz é de sua propriedade e não de seu colaborador, exceto nos casos onde a Instituição atua como custodiante dessa informação.

6.0 – DIRETRIZES GERAIS

Para fins desta Portaria ficam estabelecidas as seguintes diretrizes gerais:

Tratamento das informações: **a)** Os ativos de informação da instituição devem ser identificados, classificados de acordo com seu grau de severidade e documentados. **b)** Todo ativo de informação deve possuir um responsável explicitamente identificado;

Tratamento de incidentes de redes: **a)** Os incidentes de segurança da informação devem ser registrados e gerenciados. **b)** Deve ser definida uma equipe para tratamento e resposta aos incidentes em redes computacionais, segundo critérios a serem definidos pela área de Segurança da Informação da CGTI, a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes computacionais no órgão;

Gestão de risco: Deve ser adotada a gestão de riscos de segurança da informação, segundo critérios a serem definidos pela área de Segurança da Informação da CGTI, para a identificação e implementação das medidas de proteção necessárias para a mitigação ou eliminação dos riscos;

Gestão de continuidade: Deve ser adotada a gestão de continuidade de negócios em segurança da informação, segundo critérios a serem definidos pela área de Segurança da Informação da CGTI, visando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, através de ações de prevenção, resposta e recuperação dos ativos que sustentam os processos críticos da Instituição;

Auditoria e Conformidade: Deve-se manter a conformidade com as legislações vigentes;

Controles de acesso: **a)** Todo acesso à informação sigilosa se dará através de mecanismos de identificação e controle de acesso. **b)** Qualquer mudança funcional implicará na revisão dos direitos de acesso à informação;

Segurança de recursos humanos: Todo agente público deve ter pleno conhecimento das diretrizes, responsabilidades, limitações e penalidades relacionadas à utilização dos recursos de informação, inclusive por ocasião da mudança de atividades;

Segurança física e do ambiente: Todo ambiente que contenha ativos de informação deve ser protegido de acordo com sua severidade;

Gerenciamento de operações e comunicações: Deve-se garantir a operação segura e correta dos recursos de processamento da informação;

Aquisição, desenvolvimento e manutenção de sistemas: **a)** Todos os sistemas de informação adquiridos ou desenvolvidos para uso da Instituição devem ter sua continuidade garantida, independentemente de eventuais mudanças na relação Fiocruz – fornecedor. **b)** Todo desenvolvimento de sistemas de informação para a Fiocruz deve ser realizado com base em uma Metodologia de Desenvolvimento de Sistemas publicada.

7.0 – PENALIDADES

A violação de um ou mais itens da Política de Segurança da Informação e Comunicações ou quebra de segurança estará sujeita a sanções da esfera administrativa, civil ou penal.

8.0 – COMPETÊNCIAS E RESPONSABILIDADES

Instituir, no âmbito da Fiocruz, a seguinte estrutura para Gestão da Segurança da Informação e Comunicações:

a) O Gestor de Segurança da Informação e Comunicações, que será exercido pelo Gerente de Segurança da Informação da Coordenação de Gestão de Tecnologia da Informação – CGTI;

b) O Comitê de Segurança da Informação e Comunicações, cuja composição será definida em norma específica;

c) Equipe de Tratamento de Incidentes de Rede, que funcionará em conformidade com norma específica.

São competências do Gestor de Segurança da Informação e Comunicações:

a) Promover cultura de segurança da informação e comunicações;

b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) Propor recursos necessários às ações de segurança da informação e comunicações;

d) Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

f) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;

g) Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito da Fiocruz.

São competências do Comitê de Segurança da Informação e Comunicações:

a) Assessorar na implementação das ações de segurança da informação e comunicações;

b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

c) Propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

9.0 – ATUALIZAÇÃO

A Política de Segurança da Informação e Comunicações, bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de dois anos.

10.0– VIGÊNCIA

A presente Portaria entra em vigor na data de sua publicação.

Dr. PAULO GADELHA