POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC)

MUNDO
VIRTUAL,
SEGURANÇA
REAL.

Este documento visa 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.

Versão 1.11

ATENÇÃO

Esta é uma versão compilada da Política de Segurança da Informação e Comunicações e suas normas complementares. Os textos aqui apresentados não substituem os originais. Em caso de dúvidas consulte a versão original dos documentos:

- Política de Segurança da Informação e Comunicações
- Norma complementar 01 – Responsabilidades do Usuário
- Norma complementar 02 – Uso da Internet
- Norma complementar 03 – Uso do E-mail
- Norma complementar 04 – Segurança Física em Data Center
- Norma complementar 05 – Cópias de Segurança
- Norma complementar 06 – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
- Norma complementar 07 – Acesso Remoto
- Norma complementar 08 – Uso de Redes Sociais
- Norma Complementar 09 – Dispositivos Móveis
- Norma Complementar 10 – Credenciamento de Usuários
- Norma Complementar 11 – Classificação e tratamento de informações quanto ao grau de sigilo

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

1.0 PROPÓSITO

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

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;

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 medias 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: é 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 suficientes 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 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 os 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

- Os ativos de informação da instituição devem ser identificados, classificados de acordo com seu grau de severidade e documentados.
- Todo ativo de informação deve possuir um responsável explicitamente identificado.

Tratamento de incidentes de redes

- Os incidentes de segurança da informação devem ser registrados e gerenciados.
- 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

- Todo acesso à informação sigilosa se dará através de mecanismos de identificação e controle de acesso.

- 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

- 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.

- 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:

I. 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;

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

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

São competências do Gestor de Segurança da Informação e Comunicações:

I. Promover cultura de segurança da informação e comunicações;

II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. Propor recursos necessários às ações de segurança da informação e comunicações;

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

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

VI. 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;

VII. 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:

I. Assessorar na implementação das ações de segurança da informação e comunicações;

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

III. 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.

Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE RESPONSABILIDADES DO USUÁRIO

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE RESPONSABILIDADES DO USUÁRIO

1. OBJETIVO

Este documento dispõe sobre as responsabilidades do usuário quanto ao uso de senhas e equipamentos, mesa limpa e tela limpa.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se a todos os agentes públicos da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Área de TI correlata: área de tecnologia da informação da unidade do usuário de rede.

Armazenamento local: ato de manter um arquivo armazenado no próprio dispositivo (estação de trabalho, notebook, etc.).

Rede local: rede de dados disponibilizada por uma Unidade da Fiocruz.

Servidor de arquivo: servidor de rede disponibilizado especificamente para o armazenamento de arquivos dos usuários.

TI: Tecnologia da Informação.

Usuário: servidores, terceirizados, colaboradores, consultores, auditores, estagiários, prestadores de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- Cartilha de segurança para a Internet, versão 3.1 do Cert.br – http://cartilha.cert.br

5. REGRAS

5.1. Disposições gerais

5.1.1 Todo usuário deve conhecer e cumprir a Política de Segurança da Informação e Comunicações (POSIC) e as legislações em vigor referenciadas nesta norma.

5.1.2 A Fiocruz deve estabelecer um processo de divulgação permanente da sua POSIC, para a conscientização de todos os usuários.

5.2. Uso de recursos de TI

5.2.1 Os usuários devem proteger os recursos de TI da Fiocruz contra acesso, modificação, destruição ou divulgação não autorizada.

5.2.2 Utilizar os recursos de TI colocados à sua disposição somente para os fins institucionais aos quais se destinam.

5.2.3 Não abrir o gabinete das estações de trabalho ou computador portátil, nem modificar qualquer configuração, seja de *hardware* ou *software*. Essas configurações são padronizadas, conforme definições da área de TI correlata. Havendo a necessidade de alteração destas configurações, a solicitação deve ser encaminhada à área de TI correlata para análise.

5.2.4 Não instalar ou executar *software* de sua propriedade ou de terceiros sem prévia homologação e autorização da área de TI correlata.

5.2.5 Desligar a estação de trabalho ou computador portátil corretamente e diariamente ao final do expediente, seguindo os procedimentos do sistema operacional.

5.2.6 As estações de trabalho ou computadores portáteis da Fiocruz devem ser ligadas somente em pontos elétricos estabilizados, evitando-se que sejam ligados em conjunto com outros equipamentos elétricos que não sejam recursos de TI.

5.2.7 Devem-se armazenar os arquivos com informações institucionais nos servidores de arquivos disponibilizados na rede local da Unidade. Deve-se evitar o armazenamento nas estações de trabalho.

5.2.8 Evitar realizar conversas em locais públicos ou sem a reserva adequada sobre assuntos sensíveis da Instituição, restringindo-se a tratá-los somente em locais que ofereçam a proteção adequada.

5.2.9 Colaborar ativamente na solução de problemas e no aprimoramento dos processos de segurança da informação da Fiocruz.

5.3. Uso de dispositivos portáteis

5.3.1 Os dispositivos portáteis da Fiocruz, sempre que não estiverem sendo utilizados, devem ser guardados em local seguro, onde o responsável, por estes, possa garantir que os mesmos não serão utilizados por outras pessoas.

5.3.2 O uso de dispositivos portáteis pessoais deve ser avaliado pela área de TI correlata.

5.4. Uso da identificação e senhas de acesso

5.4.1 O Usuário somente terá acesso às informações e aos recursos de TI após a conclusão do processo de credenciamento/concessão de acesso, que se dará através de solicitação formal da chefia imediata do usuário à área de Recursos Humanos da Unidade, que por sua vez fará o encaminhamento à área de TI correlata.

5.4.2 A cada usuário deve ser disponibilizada apenas uma identificação de acesso aos recursos de TI. Essa identificação deve ser única, pessoal e intransferível.

5.4.3 A senha de acesso ao recurso de TI qualifica o usuário como responsável por todos os acessos realizados. A definição e a utilização de senhas estão condicionadas às regras definidas pela área de TI correlata.

5.4.4 Os direitos e perfis de acesso seguem as definições do responsável pelo usuário em concordância com os padrões estabelecidos pela área de TI correlata.

5.4.5 O usuário não deve compartilhar sua senha de acesso com outras pessoas.

5.4.6 O usuário deve trocar sua senha de acesso aos recursos de TI periodicamente, seguindo as orientações da área de TI correlata.

5.5. Política de mesa e tela limpa

5.5.1 Os documentos impressos devem ser classificados em conformidade com a legislação vigente.

5.5.2 Os documentos sigilosos não devem ser deixados sobre as mesas na ausência do usuário e devem ser guardados em local seguro e com controle de acesso.

5.5.3 Bloquear o acesso à estação de trabalho ou computador portátil que lhe foi confiado sempre que dele se ausentar.

5.6. Descarte de informações

5.6.1 Os ativos não mais utilizados pelos usuários, em meio eletrônico ou não, devem ser apagados ou destruídos conforme regras da legislação vigente.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações da CGTI.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

6.3. Os incidentes de segurança, quebra de segurança e denúncias de descumprimento à Política de Segurança da Informação e Comunicações e suas normas podem ser encaminhadas através do e-mail seguranca@fiocruz.br.

6.4. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

Nº da Norma	Revisão	Emissão	Folha
SIC-002/CGTI/VPGDI	00	17/04/2012	1

NORMA INSTITUCIONAL DE USO DA INTERNET

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

1. OBJETIVO

Este documento dispõe sobre as regras de segurança relativas ao uso do serviço da Internet.

2. PÚBLICO ALVO

Esta norma operacional aplica-se a todos os agentes públicos da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Área de TI correlata: área de tecnologia da informação da unidade do usuário de rede.

Certificado digital: é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade.

Código malicioso: também conhecido como *Malware*, é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador (vírus, worms, cavalos de tróia, keyloggers, etc.).

Proxy: um computador intermediário, que fica entre o computador do usuário e a Internet, que pode ser utilizado para registrar o uso da Internet ou ainda bloquear o acesso a um site.

Rede corporativa: qualquer rede de dados na Fiocruz.

Rede de dados móvel: rede de dados que permite conexão com a Internet a partir de qualquer lugar com cobertura de sinal.

Rede local: rede de dados disponibilizada por uma Unidade da Fiocruz.

Usuário: servidores, terceirizados, colaboradores, consultores, auditores, estagiários, prestadores de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- Cartilha de segurança para a Internet, versão 3.1 do cert.br – http://cartilha.cert.br

5. REGRAS

5.1. Disposições gerais

5.1.1 O acesso à Internet disponibilizado aos usuários de rede pela Fiocruz deve ser realizado somente para os interesses de negócio da Instituição.

5.1.2 A Fiocruz permite o uso parcimonioso da Internet para interesses particulares dos usuários da rede, desde que este uso não exceda os limites da ética, bom senso e razoabilidade, bem como não contenha, receba ou transmita informações institucionais.

5.1.3 É atribuição exclusiva da área de TI correlata definir os softwares para uso da Internet na Unidade.

5.1.4 O uso dos recursos computacionais da Fiocruz para acesso à Internet nas instalações da Instituição, somente será permitido quando realizado através de redes de dados homologadas pelas áreas de TI correlatas.

5.1.5 O acesso à Internet por meio da rede local não pode ser realizado se utilizando mais de um meio de comunicação simultaneamente.

5.1.6 O acesso à Internet por meio da rede local não pode ser realizado por equipamentos particulares, tais como laptops, smartphones, etc. Casos excepcionais devem ser tratados pela área de TI correlata.

5.1.7 É recomendado que quando o acesso à Internet for realizado por meio de dispositivos móveis da Fiocruz fora de suas dependências, este seja feito por meio de uma rede de dados móvel fornecida pela própria Instituição.

5.2. Permissão de acesso

5.2.1 A todo usuário da rede local da Fiocruz é facultado o acesso a Internet em conformidade com os termos estabelecidos nesta norma.

5.2.2 O acesso à Internet dependerá do processo de credenciamento do usuário junto à área de recursos humanos da Unidade.

5.3. Cancelamento e bloqueio do acesso à Internet

5.3.1 O acesso à Internet pelo usuário da rede será obrigatoriamente desativado quando ocorrer o desligamento do usuário.

5.4. Uso da Internet

5.4.1 O acesso à Internet concedido ao usuário de rede da Fiocruz é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos causados à Instituição por meio de seu uso.

5.4.2 O uso da Internet através da rede corporativa não poderá ser feito via *proxies* externos.

5.4.3 O usuário da rede deverá utilizar a Internet de forma a não causar tráfego desnecessário na rede corporativa e demais redes de outras Instituições.

5.4.4 Todo serviço disponibilizado na Internet, antes de ser implantado na rede corporativa, deve ser avaliado pela área de TI correlata através de avaliação e relatório técnico, considerando os aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

5.4.5 A Coordenação de Gestão de Tecnologia da Informação, através de sua área de Infraestrutura como gestora dos recursos tecnológicos, deverá publicar na Intranet, de forma consolidada, relatórios que demonstrem o uso da Internet no ambiente da Fiocruz, ficando vedada a divulgação de dados de acesso individualizados.

5.4.6 É vedada a utilização da Internet para:

- Acessar sites com códigos maliciosos;
- Acessar sites com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;
- Acessar sites ou arquivos que contenham conteúdo criminoso ou ilegal, ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares;
- Acessar sites ou arquivos com conteúdo de incitação à violência, que não respeitem os direitos autorais ou com objetivos comerciais particulares;
- Realizar download de arquivos que não estejam relacionados às necessidades de trabalho da Fiocruz;
- Realizar atividades relacionadas a jogos eletrônicos pela Internet;
- Escutar música ou assistir programas de TV, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho na Fiocruz;
- Acessar sites para transferência de arquivos, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho da Fiocruz;
- Utilizar serviços de compartilhamento de arquivos online, salvo aqueles homologados pela área de TI correlata.

5.4.7 O usuário deve sempre se certificar da procedência do site, verificando, quando cabível, o certificado digital do mesmo, principalmente para realizar transações eletrônicas via internet, digitando o endereço do site diretamente no navegador.

5.4.8 É vedado aos usuários disponibilizar informações de propriedade da Fiocruz em sites da Internet sem observar sua classificação e o público a que se destina.

5.4.9 A utilização de equipamentos pessoais no ambiente da Fiocruz não poderá ser realizada por meio da rede corporativa, salvo quando a Unidade dispuser de uma rede isolada específica para este fim e mediante a concordância do termo de responsabilidade pelo usuário.

5.5. Monitoramento

5.5.1 O acesso à Internet é monitorado e pode ser restringido pela área de TI correlata quanto a endereço de sites, quantidade de acessos, horário, tempo de permanência, tipo de conteúdo e volume de informações trafegadas, desde que estes controles sejam feitos por parâmetros gerais.

5.5.2 A área de recursos humanos ou chefias hierarquicamente superiores podem solicitar formalmente um relatório com as informações de acesso à Internet de um de seus usuários da rede, para si ou para outros, nas seguintes situações:

- Suspeita de infração à Política de Segurança da Informação e Comunicações;
- Necessidade de visualizar os sites acessados e o tempo gasto nos mesmos por seus usuários de rede.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações da CGTI.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

6.3. As notificações ao Serviço de Segurança da Informação e Comunicações devem ser feitas através do e-mail seguranca@fiocruz.br.

6.4. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

Nº da Norma	Revisão	Emissão	Folha
SIC-003/CGTI/VPGDI	00	17/04/2012	1

NORMA INSTITUCIONAL DE USO DO E-MAIL

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

1. OBJETIVO

Este documento dispõe sobre as regras de segurança relativas ao uso do serviço de correio eletrônico.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se a todos os agentes públicos da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Área de TI correlata: área de tecnologia da informação da unidade do usuário de rede.

Caixa postal: conjunto de elementos necessários para o funcionamento do correio eletrônico, tais como pastas (caixa de entrada, itens enviados, rascunhos, etc.) e as próprias mensagens.

Cavalo de Tróia: programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Conta de correio eletrônico: identificação do proprietário de uma caixa postal.

Correio eletrônico institucional: conta de correio eletrônico mantido por uma das unidades da Fiocruz.

Correio eletrônico particular: conta de correio eletrônico mantido por terceiros (Gmail, Hotmail, Yahoo, etc.).

Correntes: é considerado um tipo de spam. Geralmente é apresentado em um texto que pede para que o usuário (destinatário) repasse a mensagem um determinado número de vezes ou, ainda, "para todos os amigos" ou "para todos que ama". O texto pode contar uma história antiga, descrever uma simpatia (superstição) ou, simplesmente, desejar sorte.

Lista de discussão: uso de um e-mail como ferramenta que permite a troca de mensagens entre os membros de um grupo.

Lista de distribuição: uso de um e-mail para o envio de mensagens (unidirecional) aos membros de um grupo. Ao contrário da lista, não permite o envio de mensagens entre os membros do grupo.

Provedor de e-mail externo: fornecedor de serviços de e-mail provido por terceiros (Gmail, Yahoo, Hotmail, etc.).

Spam: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Spyware: termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros, geralmente utilizadas de forma não autorizada e maliciosa.

Usuário: servidores, terceirizados, colaboradores, consultores, auditores, estagiários, prestadores de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz.

Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- Cartilha de segurança para a Internet, versão 3.1 do cert.br – http://cartilha.cert.br

5. REGRAS

5.1. Disposições iniciais

5.1.1 A conta de correio eletrônico institucional, disponibilizada aos usuários da rede de dados pela Fiocruz, deve ser utilizada somente para os interesses de trabalho.

5.1.2 A conta de correio eletrônico institucional disponibilizada ao usuário da rede de dados pela Fiocruz é pessoal e intransferível, sendo seu titular o único e total responsável pelo seu uso e suas consequências.

5.1.3 É atribuição exclusiva da área de TI correlata definir os softwares homologados para o uso do correio eletrônico institucional.

5.1.4 É atribuição exclusiva da área de TI correlata normatizar o uso do correio eletrônico particular.

5.1.5 Quando a área de TI correlata permitir o uso do correio particular, o usuário não deverá exceder os limites da ética, bom senso e razoabilidade, sendo o responsável pelo conteúdo trafegado e seus eventuais riscos.

5.1.6 É proibido o uso de provedores de e-mail externos para o encaminhamento das mensagens de uma caixa postal da Fiocruz.

5.2. Permissão de acesso e criação de contas

5.2.1 O usuário terá direito a uma única conta de e-mail que o identificará univocamente em toda Fiocruz.

5.2.2 O responsável pelo usuário da rede de dados da Unidade deve avaliar a necessidade de utilização do correio eletrônico institucional, indicando tal necessidade quando da solicitação da criação da conta de acesso aos recursos de TI.

5.2.3 A conta de correio eletrônico institucional deve ser revalidada anualmente. A não revalidação implicará no cancelamento da conta.

5.2.4 A caixa postal compartilhada ou lista de discussão deve ter um responsável e um substituto formalizados.

5.3. Cancelamento, bloqueio, suspensão ou desbloqueio do correio eletrônico.

5.3.1 Cabe à área de Recursos Humanos de cada unidade comunicar à área de TI correlata o cancelamento, bloqueio, suspensão ou desbloqueio da conta de correio do usuário.

5.3.2 O do correio eletrônico institucional é uma concessão da Fiocruz e será desativado:

a) Em até dois anos no caso de aposentadoria do servidor público;
b) Imediatamente ao desligamento, nos demais casos.

5.3.3 No caso de afastamento do usuário, o acesso à sua caixa de correio eletrônico respeitará as normas estipuladas pela Diretoria de Recursos Humanos.

5.4. Uso do correio eletrônico

5.4.1 As caixas postais do correio eletrônico institucional possuem tamanho limitado, conforme a capacidade e disponibilidade de área de armazenamento, ficando a cargo da área de TI provedora do serviço definir esses limites.

5.4.2 Os arquivos a serem anexados às mensagens no correio eletrônico institucional não poderão ultrapassar o limite de tamanho estabelecido pela área de TI provedora do serviço.

5.4.3 É vedada a utilização do correio eletrônico institucional para:

- Realizar Spam;
- Contribuir com a continuidade de correntes de mensagens eletrônicas;
- Utilizá-lo com objetivos político-partidários, religiosos, entre outros;
- Receber de forma consentida, armazenar ou enviar mensagens com:

a) Vírus de computador, cavalo de Tróia, Spyware e outros códigos maliciosos;

b) Material pornográfico, atentatório à moral e aos bons costumes ou ofensivos;
c) Conteúdo criminoso, ilegal, ou que façam sua apologia;
d) Conteúdo discriminatório (racial, religioso, etc.) ou de incitação à violência;
e) Conteúdo que desrespeitem os direitos autorais.

5.4.4 De forma a preservar o funcionamento do serviço de correio eletrônico institucional, o Usuário da rede de dados deve:

- Eliminar, periodicamente, as mensagens desnecessárias de sua caixa postal, inclusive as existentes nas pastas personalizadas, na lixeira, rascunho e enviados, de forma a não exceder o limite de tamanho da caixa postal;
- Evitar clicar em links de acesso a páginas de Internet existentes em mensagens de correio eletrônico recebidas de origem desconhecida, pois esses podem iniciar a instalação de softwares maliciosos ou direcionar o usuário da rede de dados para um site falso, possibilitando a captura de informações;
- Evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico, sem antes verificá-los quanto à sua procedência. No caso de suspeita de irregularidade na mensagem, o usuário deve solicitar ajuda a área de TI correlata;

5.4.5 Todo usuário da rede de dados da Fiocruz, antes de enviar mensagens pelo correio eletrônico institucional, deve levar em conta a classificação da informação, conforme legislação vigente.

5.4.6 O uso da conta de correio eletrônico institucional em listas de discussão ou distribuição deve se limitar aos casos de necessidade do trabalho ou atividade desempenhada na Fiocruz.

5.4.7 O correio eletrônico particular não deve ser utilizado para o envio ou recebimento de informações da Fiocruz.

5.4.8 O correio eletrônico institucional não deve ser utilizado para fim particular, como cadastro de comércio eletrônico, por exemplo.

5.4.9 A Fiocruz não se responsabiliza em fornecer suporte técnico ao correio eletrônico particular.

5.5. Monitoramento

5.5.1 O correio eletrônico institucional pode ser monitorado e restringido pela área de TI correlata, quanto à origem, destino, quantidade, tipo de conteúdo, tipo de anexo e volume das informações, desde que esses controles sejam feitos por parâmetros gerais (não personalizados).

5.5.2 Nos casos de suspeita de infração à Política de Segurança da Informação e Comunicações, a área de TI correlata poderá acessar a caixa postal institucional do respectivo usuário através de ato administrativo ou judicial;

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações da CGTI.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

6.3. As notificações ao Serviço de Segurança da Informação e Comunicações devem ser feitas através do e-mail seguranca@fiocruz.br.

6.4. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE SEGURANÇA FÍSICA EM DATA CENTER

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE SEGURANÇA FÍSICA EM DATA CENTER

1. OBJETIVO

Este documento dispõe sobre as regras para prevenção de acesso não autorizado, dano ou interferência às informações, recursos tecnológicos e instalações físicas em Data Centers na Fiocruz.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se a todos os agentes públicos da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Data Center: ambiente físico desenvolvido ou adaptado exclusivamente para hospedar os sistemas de informação ou equipamentos de TI.

Identificação física: crachá, credencial de acesso, etc.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- ISO/IEC 73:2005 – Gestão de riscos – Vocabulário
- ISO/IEC 51:1999 – Safety aspects – Guidelines for their inclusion in standards

5. REGRAS

5.1. Disposições Gerais

5.1.1 O acesso ao Data Center é permitido aos agentes públicos credenciados e portadores da identificação física.

5.1.2 A identificação física dos agentes públicos lotados no Data Center deve ser distinta dos demais;

5.1.3 Os agentes públicos devem utilizar a identificação física em local de fácil visualização;

5.1.4 Os agentes públicos devem comunicar imediatamente a perda, furto ou desaparecimento da sua identificação física à área de segurança da informação;

5.1.5 A entrada de visitantes no Data Center só será permitida mediante autorização e acompanhamento por um agente público lotado nessa área, sendo obrigatório o registro do nome completo, RG, CPF, data e hora de entrada e saída.

5.2. Áreas de segurança do Data Center

5.2.1 Todas as instalações de processamento ou armazenamento de informações sensíveis devem ser mantidas em áreas de segurança do Data Center;

5.2.2 As permissões de acesso físico às áreas de segurança do Data Center devem ser mensalmente revisadas.

5.2.3 As áreas de segurança do Data Center devem ser claramente definidas com a utilização de barreiras de segurança e mecanismos de controle de acesso, de forma a impedir o acesso não autorizado;

5.2.4 Deve ser evitada a utilização de informações visuais que identifiquem as áreas de atividade de processamento e guarda das informações;

5.2.5 As portas das áreas de segurança do Data Center devem possuir mecanismos para fechamento automático.

5.3. Segurança ambiental

5.3.1 A localização do Data Center deve ser ocultada às pessoas que transitam em áreas públicas;

5.3.2 O Data Center deve estar situado, preferencialmente, em local de baixa frequência de desastres naturais ou causados por pessoas, e distante de áreas vizinhas perigosas;

5.3.3 O Data Center deve estar posicionado em local seguro, protegido por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso de acordo com criticidade associada aos seus ativos e informações;

5.3.4 As barreiras físicas a ser implementado para proteção do Data Center devem, caso necessário, ser estendidas da laje do piso até a laje superior, para prevenir acessos não autorizados ou contaminação ambiental, como as causadas por fogo ou inundação;

5.3.5 A edificação do Data Center deve ser protegida contra descargas elétricas atmosféricas;

5.3.6 A edificação do Data Center deve ser livre de sistemas de tubulação de drenagem pluvial, tubulação pressurizada de gases, exceto para a finalidade de combate a incêndio;

5.3.7 As portas e janelas do Data Center devem ser mantidas fechadas;

5.3.8 Todas as portas e janelas acessíveis ao público devem possuir sistemas de detecção de intrusos, periodicamente testados;

5.3.9 Áreas não ocupadas ou que possuam pouca movimentação de pessoal devem possuir sistemas de alarme de presença permanentemente ativo;

5.3.10 Os sistemas de alarme devem cobrir também as salas dos equipamentos de comunicação e voz;

5.3.11 Materiais combustíveis ou perigosos devem ser guardados de forma segura, a uma distancia apropriada das áreas de trabalho e áreas de segurança;

5.3.12 Suprimentos e materiais de escritório não devem ser armazenados em áreas de segurança, a menos que requeridos;

5.3.13 Equipamentos de contingência e mídias com cópias de segurança devem ser armazenados a uma distância segura da instalação principal;

5.3.14 Todo trabalho realizado por terceiros no Data Center deve ser registrado e supervisionado;

5.3.15 As instalações elétricas, de cabeamento lógico e dos equipamentos de detecção e combate a incêndio devem ser feitas de acordo com o especificado nas normas da ABNT;

5.3.16 É proibido o manuseio de alimentos, bebidas e cigarros, bem como o consumo no Data Center.

5.4. Instalação e proteção dos equipamentos

5.4.1 É proibida a ligação de mais de um equipamento em uma mesma tomada;

5.4.2 Os equipamentos de TI do Data Center devem ser instalados em *racks*, sempre que possível;

5.4.3 Todos os *racks* do Data Center devem ser seguros, possuírem portas dotadas de chaves em todos os seus lados e permitirem trancamentos, de maneira que as tomadas de energia permaneçam no seu interior e os fios e cabos sejam acondicionados sem contato com a parte externa, diretamente do piso para o interior do rack;

5.4.4 Os equipamentos cuja dimensão impeça a instalação dentro de racks devem ter seus botões de ligar/desligar devidamente protegidos contra acessos ou internamente desconectados, de forma a evitar seu acionamento local;

5.4.5 As chaves dos *racks* e dos quadros de força devem receber identificação e serem guardadas em um claviculário em local adequado, protegido contra acesso indevido;

5.4.6 Deve ser designado um responsável pela chave do claviculário, que deverá registrar todas as retiradas e devoluções de chaves;

5.4.7 A identificação adotada deve ser de difícil dedução para pessoas estranhas ao ambiente;

5.5. Segurança do cabeamento

5.5.1 Todos os cabos existentes no Data Center devem ser identificados;

5.5.2 Os pontos de rede excedentes devem ficar inativos;

5.5.3 O cabeamento deve ser implementado de acordo com a ABNT NBR 14.565:2007 - Cabeamento de telecomunicações para edifícios comerciais;

5.5.4 Os cabos de dados devem ser lançados em bandejas ou dutos rígidos, separados dos cabos e fios elétricos, de forma a evitar interferências eletromagnéticas;

5.5.5 Deve ser adotado piso elevado no Data Center de forma a facilitar futuras manutenções;

5.5.6 A estrutura do Data Center deve prover mecanismos de proteção, impermeáveis e à prova de fogo, em todas as suas dimensões, tais como, parede e piso, prevendo a passagem de cabos elétricos.

5.6. Sistema de combate a incêndio

5.6.1 Levar ao conhecimento da brigada de incêndio da Fiocruz a relevância do serviços contido no Data Center.

5.6.2 Realizar, em parceria com a brigada de incêndio da Fiocruz, ações de conscientização e capacitação dos agentes públicos quanto às ações a serem adotadas em situações de emergência, bem como montar e divulgar as rotas de fuga.

5.6.3 Instalar no Data Center, exceto sala cofre, extintores portáteis compatíveis com os tipos de materiais existentes (classe de fogo a ser combatido).

5.6.4 É proibido manter materiais inflamáveis (diesel, álcool, etc.) no Data Center.

5.6.5 É proibido o uso de chuveiros automáticos para extinção de incêndio (*Sprinkler*) no Data Center.

5.6.6 Devem ser instalados sistemas para detecção de fogo e fumaça como meio de alerta de incêndio.

5.6.7 Devem ser elaborados planos de teste dos detectores de fogo e fumaça, sendo executados mensalmente variando o local de procedência e a intensidade da fumaça.

5.6.8 Os detectores também devem monitorar a área abaixo do piso elevado e acima do rebaixamento do teto.

5.6.9 O sistema de alarme de incêndio deve possuir som distinto em tonalidade e altura dos demais dispositivos acústicos do Data Center.

5.6.10 Os equipamentos de combate a incêndio devem ser periodicamente inspecionados e testados por empresa tecnicamente qualificada, registrando-se a revisão.

5.6.11 Todos os agentes públicos que trabalham no Data Center devem ser capacitados para a utilização dos componentes do sistema de combate a incêndio, bem como saber interpretar os tipos de alarmes existentes.

5.6.12 Deve ser instalada uma rede de gás pressurizado, com tubos identificados e pontos de distribuição dimensionados especificamente para o Data Center, como meio de extinção de incêndio.

5.6.13 Os gases utilizados para extinção de incêndio devem ser inofensivos aos equipamentos, pessoas e meio ambiente.

5.7. Fornecimento de energia

5.7.1 Os circuitos específicos (elétrico, telefônico, sinalização, controle, sonorização e dados) devem ser identificados e instalados em eletrodutos ou bandejas separados dos demais circuitos de fornecimento de energia.

5.7.2 O circuito de energia que alimenta os recursos de tecnologia no interior do Data Center, deve ser estabilizado e separado dos demais circuitos.

5.7.3 Devem ser implementados estabilizadores centrais ou individuais equipados com filtros contra variação de tensão e com monitoramento por voltímetro.

5.7.4 As tomadas de energia localizadas no piso do Data Center devem possuir caixa protetora, garantindo seu fechamento quando não estiverem sendo utilizadas e evitando que objetos possam ser inseridos ocasionando curtos-circuitos.

5.7.5 Nobreaks e geradores de energia devem ser instalados, a fim de garantir a continuidade no fornecimento de energia aos equipamentos críticos para os serviços alocados no Data Center.

5.7.6 Os circuitos elétricos devem ser divididos e protegidos por disjuntores, dimensionados de acordo com normas específicas.

5.7.7 Os disjuntores dos quadros de distribuição de energia devem identificar claramente cada circuito elétrico.

5.7.8 O quadro de distribuição de energia, painéis de controle e caixas de passagem do cabeamento lógico devem ser protegidos contra acesso indevido.

5.7.9 Deve-se realizar mensalmente a verificação da voltagem e amperagem de energia de entrada no Data Center, mantendo-se o registro dos valores aferidos.

5.7.10 Somente circuitos de alimentação e controle relativos ao Data Center devem ser dispostos em seu interior.

5.7.11 A fonte de energia do sistema de controle de acesso deve ser contingenciado, evitando que, na ocorrência de falha, a entrada de pessoas não autorizadas seja permitida.

5.8. Controles de segurança do Data Center

5.8.1 Devem ser realizadas rondas de segurança em regime 24 X 7 no perímetro do Data Center.

5.8.2 Os acessos ao Data Center devem ser monitorados por circuito fechado de TV (CFTV). Câmeras de monitoramento devem ser instaladas em locais estratégicos do ambiente, seja ele interno ou externo.

5.8.3 Os circuitos das câmeras de monitoramento devem ser protegidos por conduítes de metal e ficar fora do alcance manual, evitando-se desativação intencional ou acidental.

5.8.4 As imagens captadas pelas câmeras do circuito interno de TV devem ser gravadas de forma contínua, visando embasar futuras investigações em caso de suspeitas ou incidentes de segurança.

5.8.5 Os arquivos das imagens gravadas devem ser guardados pelo período mínimo de um ano, sendo tratados com os mesmos critérios das mídias de cópia de segurança.

5.8.6 O sistema de circuito fechado de TV deve ser diariamente inspecionado, de forma a garantir a efetiva gravação das imagens.

5.8.7 As imagens gravadas pelo circuito interno de TV devem ser periodicamente analisadas, a fim de identificar possíveis eventos que contrariem a Política de Segurança.

5.8.8 O sistema de circuito fechado de TV deve ser monitorado, alertando a equipe em caso de indisponibilidade no funcionamento.

5.8.9 As portas de acesso ao Data Center devem possuir mecanismos de fechamento automático.

5.8.10 Alarmes de intrusão devem ser instalados nas portas e janelas do Data Center.

5.8.11 As portas de acesso devem possuir dispositivo de controle de acesso, tais como crachá por aproximação e solicitação de senha.

5.8.12 A entrada no Data Center deve ser condicionada a pessoas portando a identificação física (crachá) em local visível.

5.8.13 Após o horário normal de trabalho, o acesso para qualquer pessoa que não esteja envolvida na administração, gerenciamento ou operação do Data Center, será permitido somente através de autorização emitida pela chefia área de TI correlata.

5.8.14 É de responsabilidade dos agentes públicos lotados no Data Center, registrar e acompanhar os prestadores de serviço e visitantes, sendo responsáveis pelas ações destes enquanto permanecerem no ambiente.

5.8.15 A coleta de lixo e limpeza do Data Center deve ser realizada por pessoas instruídas quanto os cuidados necessários para tal serviço, devendo sempre ser autorizadas, registradas e acompanhadas por agente público lotado no ambiente.

5.8.16 Devem-se definir os dias e horários destinados à limpeza do Data Center, de forma a não comprometer a prestação dos serviços disponibilizados pela área.

5.8.17 A entrada e saída de qualquer ativo devem ser registradas.

5.8.18 É proibida a entrada de equipamentos de fotografia, vídeo e áudio.

5.8.19 É proibido comer, fumar ou beber no interior do Data Center.

5.8.20 Os ramais telefônicos devem ser restritos a chamadas internas.

5.8.21 Somente pessoas autorizadas podem portar equipamentos eletrônicos portáteis (celular, pen drive, palms, etc.) no interior do Data Center.

5.9. Sistema de ar condicionado

5.9.1 O sistema de ar-condicionado deve ser redundante.

5.9.2 O sistema de ar-condicionado deve ser, preferencialmente, do tipo *fan coil* e rede de dutos, utilizando caminhos redundantes e independentes entre si, através do teto rebaixo ou piso elevado.

5.9.3 Devem ser instalados filtros de limpeza no sistema de ar-condicionado para tratamento do ar circulante.

5.9.4 Os equipamentos externos de suprimento do ar-condicionado devem ser protegidos de ações ambientais ou humanas.

5.9.5 O fornecimento de energia elétrica do sistema de suprimento do ar-condicionado deve ser contínuo.

5.9.6 Os dutos de ar-condicionado devem ser revestidos por material térmico e não combustível.

5.9.7 O sistema de água do circuito de refrigeração deve ser protegido contra corrosão.

5.9.8 O termostato para controle de temperatura deve ser exclusivo para o Data Center.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações da CGTI.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

6.3. As notificações ao Serviço de Segurança da Informação e Comunicações devem ser feitas através do e-mail seguranca@fiocruz.br.

6.4. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

Nº da Norma	Revisão	Emissão	Folha
SIC-005/CGTI/VPGDI	00	15/FEV/2013	1

NORMA INSTITUCIONAL PARA CÓPIAS DE SEGURANÇA

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

1. OBJETIVO

Este documento estabelece as diretrizes para a geração de cópias de segurança das informações e sua recuperação em um tempo aceitável.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se a todos os agentes públicos da Fiocruz

3. DEFINIÇÕES E TERMINOLOGIAS

Ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

Cópia de segurança: cópia das informações e *softwares*, que permita a recuperação após um desastre ou falha de uma mídia.

Diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas.

Usuário: servidores, terceirizados, colaboradores, consultores, auditores, estagiários ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz.

Segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Salvaguarda: Responsabilidade concedida por uma autoridade a um indivíduo ou coletividade para proteger/preservar um ativo de informação.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- Norma Complementar nº 07 IN01/DSIC/GSI/PR, de 6 de maio de 2010, que estabelece as diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações.

5. REGRAS

5.1. Disposições Gerais

5.1.1 Convém que as cópias de segurança das informações e de *software* sejam efetuadas e testadas regularmente pela área de TI correlata.

5.1.2 Convém que a infraestrutura para a geração de cópias de segurança seja adequada para garantir que toda informação essencial possa ser recuperada.

5.1.3 Convém que informações sensíveis sejam salvaguardadas criptografadas nas cópias de segurança.

5.2. Cópias de segurança da informação

5.2.1 A área de TI correlata é a responsável pelo processo de cópias de segurança no âmbito das Unidades da Fiocruz.

5.2.2 Os equipamentos envolvidos no processo de cópias de segurança devem garantir que os dados selecionados sejam gravados na sua totalidade.

5.2.3 As cópias de segurança devem ser realizadas em horário de baixa utilização das informações, preferencialmente fora do horário de expediente.

5.2.4 Sendo inevitável a realização de cópias de segurança no horário do expediente deverá ser justificado antecipadamente caso haja necessidade de parada do serviço ou queda no desempenho dos recursos de TI.

5.2.5 Cada área de TI correlata deve definir e regulamentar os critérios necessários das cópias de segurança, a frequência, a extensão (completa, diferencial e incremental) e o seu período de retenção.

5.2.6 Cabe à área de TI correlata definir procedimentos para a geração e restauração das cópias de segurança, mantendo os registros completos e fidedignos das cópias de segurança.

5.2.7 Deve ser implementado um controle de acesso físico e lógico para as informações das cópias de segurança.

5.2.8 As cópias de segurança devem ser testadas regularmente e os registros das evidências dos testes devem ser devidamente documentados.

5.2.9 Os mecanismos de cópias de segurança devem ser automatizados, a fim de facilitar os processos de geração e recuperação.

5.3. Armazenamento de mídias

5.3.1 As mídias devem ser armazenadas em local distinto da área de TI correlata, a uma distância suficiente para preservá-las de possíveis ameaças, respeitando as recomendações dos fabricantes.

5.3.2 As mídias devem ser armazenadas em local seguro com acesso restrito e controlado somente a usuários autorizados.

5.3.3 As mídias devem ser devidamente identificadas de forma a permitir sua rápida localização e recuperação.

5.3.4 As mídias devem ser transportadas por um colaborador autorizado pela área de TI correlata, para um local seguro, dentro de embalagem lacrada que proteja adequadamente o seu conteúdo.

5.4. Descarte / substituição de mídias

5.4.1 Para cada tipo de mídia devem ser observados os critérios do fabricante quanto aos seus requisitos de utilização.

5.4.2 No caso de mudança de infraestrutura tecnológica, as mídias com informações que ainda não expiraram devem ser transferidas para as novas mídias.

5.4.3 Devem-se adotar mecanismos seguros para o descarte de mídias (incineração, trituração, etc.) a fim de garantir que informações armazenadas e sem uso sejam irrecuperáveis, observando as legislações pertinentes.

5.4.4 Mídias a serem descartadas devem ser registradas e suas informações de identificação devem ser removidas.

5.5. Restauração de cópias de segurança

5.5.1 A área de TI correlata deve realizar regularmente testes de restauração das cópias de segurança em ambiente distinto ao de produção e suas evidências dos testes devem ser devidamente documentados.

5.5.2 O usuário deve solicitar formalmente a restauração de uma cópia de segurança, de acordo com procedimento definido pela área de TI correlata.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações da CGTI.

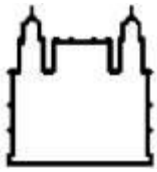
6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

6.3. As notificações ao Serviço de Segurança da Informação e Comunicações devem ser feitas através do e-mail seguranca@fiocruz.br.

6.4. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.



Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

1. OBJETIVO

Este documento estabelece as diretrizes de segurança para aquisição, desenvolvimento e manutenção de sistemas da informação no âmbito da Fiocruz.

2. PÚBLICO-ALVO

Esta norma aplica-se a todos que executam atividades profissionais que envolvem aquisição, desenvolvimento e manutenção de sistemas de informação no âmbito da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação.

Ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Controle: Medidas de proteção utilizada para redução do risco.

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

Requisitos: condição ou capacidade com a qual o sistema deve estar de acordo.

Usuário: servidores, terceirizados, colaboradores, consultores, auditores, estagiários, prestadores de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos
- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- ISO/IEC 15408-1:2009 – *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*
- ISO/IEC 15408-2:2008 – *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.*

- Norma Complementar nº 07 IN01/DSIC/GSI/PR, de 6 de maio de 2010, que estabelece as diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações.
- Boas Práticas em Segurança da Informação – Tribunal de Contas da União – 3ª edição.

5. REGRAS

5.1. Disposições gerais

5.1.1 Todos os requisitos de segurança devem ser identificados e justificados na fase de definição de requisitos de um projeto, acordados e documentados.

5.1.2 Todo projeto de sistema de informação antes da sua concepção, inclusive aquele desenvolvido pelo usuário, deve ser submetido à área de TI correlata para avaliação/homologação dos aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

5.1.3 Esta norma não substitui o documento de metodologia de desenvolvimento de sistemas adotado pelas Unidades da Fiocruz, mas o complementa quanto aos aspectos de segurança da informação e comunicações.

5.1.4 Os sistemas de informação classificados como críticos deverão ser desenvolvidos levando em consideração requisitos para sua contingência.

5.1.5 Todos os usuários que utilizarão um sistema devem ser treinados e capacitados para exercer suas atividades.

5.2. Requisitos de segurança de sistemas de informação

5.2.1 Devem ser considerados requisitos de segurança na definição dos novos sistemas.

5.2.2 Devem ser considerados requisitos de segurança na aquisição de novos sistemas.

5.2.3 Devem ser considerados requisitos de segurança em todas as fases de criação dos sistemas, ou seja, definição, projeto, desenvolvimento, implantação e manutenção.

5.3. Processamento correto nas aplicações

5.3.1 Devem ser incorporados controles apropriados em projetos de aplicações para assegurar o processamento correto.

5.3.2 Os controles devem incluir os dados de entrada, o processamento interno e os dados de saída.

5.3.3 Controles adicionais para sistemas que processem informações sensíveis, valiosas ou críticas ou que nessas exerçam algum impacto devem ser determinados com base em requisitos de segurança e análise/avaliação de riscos.

5.3.4 Os dados de entrada de aplicações devem ser validados para garantir que são corretos e apropriados.

5.3.5 Devem ser incorporadas nas aplicações checagens de validação com o objetivo de detectar qualquer corrupção de informações por erros ou por ações deliberadas.

5.3.6 Devem ser identificados e implementados requisitos e controles apropriados para garantir a autenticidade e proteger a integridade das mensagens em aplicações.

5.3.7 Devem ser validados os dados de saída das aplicações para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.

5.3.8 A utilização dos recursos e as projeções feitas para a necessidade de capacidade futura devem ser monitoradas de modo a garantir o desempenho requerido do sistema de informação.

5.4. Controles criptográficos

5.4.1 Devem ser elaboradas e implementadas políticas de uso de criptografia nos sistemas.

5.4.2 Devem ser armazenadas em servidores de rede com nível de segurança elevado as chaves utilizadas nas soluções de criptografia.

5.5. Segurança dos arquivos do sistema

5.5.1 Devem ser documentos os procedimentos para a instalação e atualização de softwares.

5.5.2 A massa de dados utilizados nos testes da fábrica de software deve ser diferente da utilizada no ambiente de produção.

5.5.3 O acesso aos códigos fontes dos sistemas deve ser controlado e autorizado pela área de TI correlata.

5.6. Segurança em processo de desenvolvimento e de suporte

5.6.1 Deve ser documentado e implementado um processo de gestão de mudanças.

5.6.2 A área de TI correlata deve supervisionar o processo desde o seu planejamento até a implementação no caso de desenvolvimento de softwares por terceiros.

5.6.3 Deve ser implementado controle de versão para garantir a gestão dos códigos fontes.

5.6.4 Deve ser realizada a análises de riscos a fim de detectar falhas nos sistema que possam comprometer a segurança da informação.

5.6.5 O suporte dos sistemas somente poderá ser realizado após abertura de chamado (para registro dos eventos).

5.6.6 Devem ser protegidas as informações envolvidas em transações *online*, a fim de prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.

5.7. Gestão de Vulnerabilidades técnicas

5.7.1 Devem ser investigado e tratado de forma contínua as vulnerabilidades técnicas dos sistemas de informação em uso.

5.7.2 Devem ser avaliada e implementada medidas apropriadas para lidar com os riscos associados a uma eventual vulnerabilidade.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações da CGTI.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

6.3. As notificações ao Serviço de Segurança da Informação e Comunicações devem ser feitas através do e-mail seguranca@fiocruz.br.

6.4. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

Nº da Norma	Revisão	Emissão	Folha
SIC-007/CGTI/VPGDI	00	23/SET/2013	1

NORMA INSTITUCIONAL DE ACESSO REMOTO

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

1. OBJETIVO

Este documento estabelece as diretrizes para a realização de acesso à rede de dados da Fiocruz a partir de um local externo.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se a todos os usuários da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação.

Acesso remoto: conexão entre uma rede de dados externa com a rede de dados da instituição.

Área de TI correlata: área de tecnologia da informação da unidade do usuário de rede.

Usuário: servidores, terceirizados, colaboradores, consultores, auditores, estagiários, prestadores de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz, formalizada por meio da assinatura do Termo de Responsabilidade.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

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

5. REGRAS

5.1. Disposições gerais

5.1.1 O acesso remoto a uma rede de dados da Fiocruz será permitido em caráter excepcional e somente para fins de trabalho.

5.1.2 Deve ser formalizado junto à área de TI correlata o pedido de acesso remoto, justificando a necessidade de acesso e período de uso.

5.1.3 A área de TI correlata deve registrar e monitorar o acesso remoto do usuário.

5.1.4 O acesso remoto deve ser concedido por um período de tempo pré-definido.

5.2. Do Acesso

5.2.1 O acesso remoto a uma rede de dados da Fiocruz deve ser realizado por meio de canal criptografado e solicitação de autenticação do Usuário.

5.2.2 A área de TI correlata deve informar aos usuários os requisitos mínimos de segurança estabelecidos para realização de acesso remoto.

5.2.3 Os recursos de Tecnologia da Informação – TI utilizados no ambiente de trabalho remoto, tal como residências, devem conter mecanismos de proteção contra vírus, software malicioso e controle de acesso.

5.2.4 O acesso a uma rede de dados da Fiocruz deve ser permitido somente a partir de recursos de TI que foram previamente cadastrados e homologados pela área de TI correlata.

5.2.5 Quando os recursos de informática forem de propriedade de terceiros, a área de TI correlata deve solicitar a estes que os referidos recursos atendam aos requisitos mínimos de segurança estipulados.

5.2.6 A área de TI correlata deve garantir aos Usuários que fazem uso do acesso remoto a uma rede de dados da Fiocruz a capacitação quanto à utilização da solução de acesso.

5.3. Responsabilidades

5.3.1 A área de TI correlata deve prover mecanismos de proteção adequados às redes de dados sob responsabilidade de sua Unidade, bem como aos serviços a elas conectados.

5.3.2 O usuário é responsável por toda e qualquer operação (acesso, processamento, comunicação, etc.) realizada através de um acesso remoto.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma à área de TI correlata.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente acionado pela área de TI correlata para adotar as providências necessárias.

6.3. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

Nº da Norma	Revisão	Emissão	Folha
SIC-008/CGTI/VPGDI	00	23/SET/2013	1

NORMA INSTITUCIONAL DE USO DE REDES SOCIAIS

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

1. OBJETIVO

Este documento estabelece diretrizes para o uso das redes sociais nos aspectos relativos à Segurança da Informação e Comunicações no âmbito da Fiocruz.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se a todos os colaboradores da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

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 e Comunicações: 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 a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

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

Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da Fiocruz.

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

Link encurtado: serviços que encurta endereços (url) longos de forma que eles sejam curtos o suficiente para serem enviados por e-mail, Twitter, etc. Estes serviços são representados por sites como bit.ly (j.mp), TinyURL e Migre.me, entre outros.

Perfil institucional: cadastro do órgão/unidade como usuário em redes sociais, alinhado ao planejamento estratégico e à Política de Segurança da Informação e Comunicações (POSIC) da instituição, com observância de sua correlata atribuição e competência.

Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pelo Presidente da Fiocruz, com o objetivo de fornecer diretrizes, critérios e suporte administrativo à implementação da segurança da informação e comunicações.

Redes sociais: estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

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

Usuários: servidores, terceirizados, colaboradores, consultores, auditores, estagiários, prestadores de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz;

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação;
- Norma Complementar nº 15 IN01/DSIC/GSI/PR, de 11 de junho de 2012, que estabelece diretrizes para o uso seguro das redes sociais na Administração Pública Federal.

5. REGRAS

5.1. Disposições gerais

5.1.1 Entende-se como redes sociais as estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns;

5.1.2 As redes sociais na Fiocruz podem ser utilizadas para a comunicação institucional entre pessoas, empresas, órgãos e entidades públicas e privadas, desde que seu uso não comprometa a disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação da instituição;

5.2. Diretrizes

5.2.1 As redes sociais ao serem utilizadas na Fiocruz por suas unidades devem ter como finalidade a aproximação da instituição com o cidadão, sendo entendidas como

ferramentas para a prestação de serviços públicos de forma ágil e transparente, em consonância com os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e eficiência;

5.2.2 O uso das redes sociais deve respeitar a legislação vigente, a Política de Segurança da Informação e Comunicações (POSIC) da Fiocruz e quaisquer outros atos normativos complementares;

5.3. Critérios

5.3.1 As áreas de comunicação devem designar um servidor público, ocupante de cargo efetivo, para responder por um ou mais perfis institucionais nas redes sociais e ser responsável pela equipe e sua coordenação. As equipes devem ser compostas exclusivamente por profissionais ocupantes de cargo efetivo da Fiocruz. No entanto, caso não seja possível, admite-se uma equipe mista;

5.3.2 É vedada a terceirização da administração e gestão dos perfis institucionais da Fiocruz nas redes sociais;

5.3.3 A área responsável por uma conta com perfil institucional em uma rede social deve utilizar o e-mail institucional (Ex: @fiocruz.br) da área responsável;

5.3.4 As contas com perfil institucional devem ser associadas ao e-mail da área responsável pela conta em detrimento ao e-mail pessoal;

5.3.5 É vedada a utilização de e-mail institucional em redes sociais por usuários que não tenham o papel de produzir ou disseminar conteúdo de caráter institucional;

5.4. Limitações

5.4.1 A Fiocruz permite o uso parcimonioso das redes sociais a partir das suas infraestruturas de redes, desde que este uso não exceda os limites da ética, bom senso e razoabilidade;

5.4.2 O acesso às redes sociais pode ser monitorado pela área de TI correlata quanto a endereço, quantidade de acessos, horário, tempo de permanência, tipo de conteúdo e volume de informações trafegadas, desde que o monitoramento seja feito por parâmetros gerais;

5.4.3 O monitoramento servirá para eventuais adequações de uso que se fizerem necessárias, a fim de assegurar a melhor utilização dos recursos de TI.

5.5. Responsabilidades

5.5.1 Todo usuário deve conhecer e cumprir as recomendações do Manual de Mídias Sociais elaborado pela Coordenadoria de Comunicação Social – CCS, que traz orientações quanto ao uso responsável das principais redes sociais;

5.5.2 Todo usuário, além do Manual de Mídias Sociais, deve observar a legislação vigente, a Política de Segurança da Informação e Comunicações (POSIC) da Fiocruz e quaisquer outros atos normativos complementares a fim de que não comprometa a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações;

5.5.3 Todo usuário ao acessar uma rede social (independentemente de seu perfil de acesso) é responsável pelas informações veiculadas ou que de alguma forma tenham relação com a instituição;

5.5.4 O usuário deve se certificar sobre a autenticidade de uma informação antes de divulgá-la em uma rede social;

5.5.5 O usuário responsável por uma conta institucional em uma rede social deve adotar comportamentos que protejam esta conta. Alguns exemplos são:

a) Criar senhas fortes;
b) Manter a senha em sigilo;
c) Trocar a senha periodicamente;
d) Não salvar senhas no navegador;
e) Não deixar o computador desbloqueado quando se afastar dele;
f) Manter antivírus instalado e atualizado;
g) Sair do serviço usando o link "*logout*" (ou similar), etc.
h) Tomar as devidas precauções ao acessar um link encurtado;

5.5.6 O Serviço de Segurança da Informação e Comunicações da CGTI deve acompanhar e analisar de forma contínua o uso das redes segundo os critérios estabelecidos nesta norma a fim de manter seu uso em níveis seguros.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Serviço de Segurança da Informação e Comunicações da CGTI.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

6.3. As notificações ao Serviço de Segurança da Informação e Comunicações devem ser feitas através do e-mail seguranca@fiocruz.br.

6.4. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

NORMA INSTITUCIONAL DE DISPOSITIVOS MÓVEIS

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

APROVAÇÃO

NORMA INSTITUCIONAL DE DISPOSITIVOS MÓVEIS

1. OBJETIVO

Este documento estabelece as diretrizes e fornece orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações no âmbito da Fiocruz.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se a todos os usuários da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Dispositivo móvel: qualquer equipamento portátil, tais como: notebooks, netbooks, tablets, smartphones, etc.;

Usuário: servidores, terceirizados, colaboradores, consultores, auditores, estagiários, prestadores de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz;

Usuários com dispositivos móveis corporativos: usuários que utilizam dispositivos móveis de computação de propriedade da Fiocruz;

Usuários com dispositivos móveis particulares: usuários que utilizam dispositivos móveis de computação de sua propriedade.

Usuários visitantes com dispositivos móveis: todos os usuários que utilizam dispositivos móveis de sua propriedade, ou do órgão/entidade a que pertencem, dentro dos ambientes físicos e virtuais de outros órgãos/entidades, dos quais não fazem parte. Exemplos: fornecedores, visitantes, servidores fora da sua unidade de origem, etc.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação;
- Norma Complementar nº 12 IN01/DSIC/GSI/PR, de 30 de janeiro de 2012, que estabelece diretrizes para o uso de dispositivos móveis nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal.

5. REGRAS

5.1. Disposições gerais

5.1.1 O uso de dispositivos móveis na Fiocruz deve ser pautado na necessidade e interesse da Instituição;

5.1.2 O usuário deve ser orientado a respeito dos procedimentos de segurança e a responsabilidade que o mesmo passa a assumir acerca do uso dos dispositivos móveis, mediante assinatura de um termo de uso e responsabilidade, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido;

5.1.3 Os dispositivos móveis devem ser utilizados somente pelos usuários que assumiram formalmente a responsabilidade pelo seu uso;

5.2. Uso dos dispositivos móveis corporativos

5.2.1 Os dispositivos móveis corporativos devem ser inventariados;

5.2.2 Os dispositivos móveis devem possuir somente os softwares homologados e instalados pela área de TI correlata;

5.2.3 O Usuário não deve instalar ou desinstalar qualquer tipo de software nos dispositivos móveis;

5.2.4 Os dispositivos móveis devem ser registrados como membros de um domínio de rede, sempre que tecnicamente possível;

5.2.5 Os dispositivos devem oferecer mecanismos que garantam o controle de acesso e sigilo das informações neles armazenada. (Exemplo: senhas, usuários e senhas, tokens, criptografia dos dados, etc.)

5.2.6 É necessária a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário e/ou dispositivo, às conexões de rede e recursos disponíveis;

5.2.7 A área de TI correlata deve adotar mecanismos que garantam a proteção e sigilo dos dados armazenados nos dispositivos em casos de extravio;

5.2.8 É de uso exclusivo da área de TI correlata o uso da conta “Administrativa”. O uso dessa conta é restrito às atividades de manutenção do equipamento;

5.2.9 A utilização de contas com perfil de “Administrativo” nos dispositivos móveis só será autorizada quando devidamente formalizada e justificada à área de TI correlata;

5.3. Uso dos dispositivos móveis particulares

5.3.1 É vedado o uso de dispositivos móveis particulares para fins de trabalho.

5.4. Uso dos dispositivos móveis por visitantes

5.4.1 Devem ser estabelecidos procedimentos de controle e concessão de acesso a visitantes que, durante sua permanência, na instituição necessitem conectar seus dispositivos móveis à rede da Fiocruz;

5.4.2 A concessão de acesso ao visitante deve estar vinculada à conscientização do usuário sobre as normas internas de uso da rede;

5.4.3 A utilização de equipamentos de visitantes no ambiente da Fiocruz não poderá ser realizada por meio da rede corporativa, salvo quando a Unidade dispuser de uma rede isolada específica para este fim e mediante a concordância do termo de responsabilidade pelo usuário.

5.5. Considerações finais

5.5.1 O Usuário deve bloquear seu dispositivo móvel ao se afastar do mesmo, evitando que outras pessoas tenham acesso às informações armazenadas;

5.5.2 No caso de equipamentos que não são de uso contínuo, quando fora de uso, devem ser desligados e guardados em local que somente o seu responsável tenha acesso;

5.5.3 O usuário deve realizar uma varredura com o software antivírus disponível antes de gravar no equipamento portátil de TI qualquer informação que receba por e-mail ou mídias de armazenamento removíveis;

5.5.4 O usuário deve proteger o equipamento portátil de TI e os dados nele contidos contra situações de risco. Tais proteções incluem: não deixá-lo sozinho, não permitir que outra pessoa tenha acesso às informações nele armazenadas, etc.

5.5.5 O Usuário deve providenciar a transferência das informações institucionais manipuladas no equipamento portátil de TI para os servidores de rede da Fiocruz, quando do seu retorno à unidade;

5.5.6 A área de TI correlata não se responsabilizará por informações armazenadas nos dispositivos móveis;

5.5.7 As unidades devem observar os requisitos de segurança descritos nesta norma ao adquirir dispositivos móveis corporativos, independentemente de serem consignados ou não.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma à área de TI correlata.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente acionado pela área de TI correlata para adotar as providências necessárias.

6.3. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE CREDENCIAMENTO DE USUÁRIOS

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

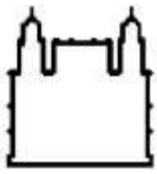
CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.



Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE CREDENCIAMENTO DE USUÁRIOS

1. OBJETIVO

Este documento estabelece as diretrizes para o processo de credenciamento para acesso aos ativos de informação no âmbito da Fiocruz.

2. PÚBLICO-ALVO

Esta norma operacional aplica-se as áreas responsáveis por vínculos de usuários nas unidades da Fiocruz e áreas de tecnologia da informação, aos gestores e aos usuários no âmbito da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação.

Área responsável: instância responsável pelo vínculo de um usuário em uma unidade da Fiocruz. São entendidos como 'área responsável' a área de recursos humanos' das unidades em relação aos servidores e colaboradores nela localizados, as 'secretarias acadêmicas' em relação aos seus estudantes, ou qualquer outra instância responsável pelo vínculo de um usuário dentro da unidade.

Ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso.

Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

Credenciamento ou concessão de acesso: processo pelo qual o usuário recebe credenciais que lhe concederão o acesso em função de autorização prévia e da necessidade de conhecer.

Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

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

Responsável pelo usuário: gestor ao qual o usuário está subordinando, independentemente de seu vínculo.

Revogação de acesso: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso.

Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

Usuário: servidores, terceirizados, colaboradores, consultores, auditores, estagiários, prestadores de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Fiocruz, formalizada por meio da assinatura do Termo de Responsabilidade.

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- Norma Complementar nº 07 IN01/DSIC/GSI/PR, de 6 de maio de 2010, que estabelece as diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.
- Portaria nº 70, de 25 de fevereiro de 2011, que institui o Modelo de Gestão do Sistema de Segurança da Informação e Comunicações da Fiocruz.
- Boas Práticas em Segurança da Informação – Tribunal de Contas da União – 3ª edição.

5. REGRAS

5.1. Disposições gerais

5.1.1 A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso na Fiocruz.

5.1.2 A concessão de acesso ocorrerá somente após o processo de credenciamento do usuário pela área responsável.

5.2. Papéis e responsabilidades

5.2.1 A área responsável deve realizar o credenciamento do usuário, bem como registrar e solicitar a concessão, alteração ou revogação das permissões de acesso junto à área de TI.

5.2.2 Cabe ao responsável pelo usuário avaliar e, quando pertinente, solicitar a concessão de acesso do usuário.

5.2.3 A equipe de TI somente concederá ou modificará as permissões de acesso mediante procedimento formal da área responsável.

5.2.4 O usuário é responsável por todo e qualquer acesso realizado através de sua credencial, sendo seu uso indevido passível de apuração de responsabilidade nas esferas administrativa, civil e penal.

5.3. Credenciamento de usuários

5.3.1 A área de TI da Unidade ao realizar o processo de credenciamento deve utilizar um identificador único para acesso, que deve ser pessoal e intransferível (exceto os casos onde o usuário exerça função de administração da rede local).

5.3.2 O usuário deve receber da área responsável um aviso formal sobre seus acessos concedidos.

5.3.3 A área responsável deve conceder credenciais de acesso a partir da data entrada em exercício do usuário.

5.3.4 Para o credenciamento é necessário que o usuário conheça e assine o termo de responsabilidade (conforme anexo A desta norma), independente do seu vínculo.

5.3.5 As áreas responsáveis e a TI da unidade, devem verificar anualmente o cadastro dos usuários e promover a correção de eventuais inconsistências.

5.4. Gerenciamento do credenciamento do usuário

5.4.1 A área responsável deve manter o registro de todos os usuários com suas respectivas permissões de acessos e eventuais alterações.

5.4.2 Respeitar o princípio do “menor privilégio” ao conceder as credenciais e/ou contas de acesso dos usuários aos ativos de informação.

5.4.3 A área de TI correlata deve registrar os acessos à rede corporativa de forma a permitir a rastreabilidade e identificação do usuário por um período mínimo de 60 meses.

5.4.4 Deve-se implementar, sempre que possível, mecanismos adicionais de autenticação da identidade do usuário tais como: biometria, tokens, smart cards, etc.

5.4.5 É considerado indevido e passível de imediato bloqueio de acesso o uso dos ativos de informação que não guardem relação com o exercício do cargo, função, emprego ou atividade.

5.5. Revogação ou bloqueio de acesso do usuário

5.5.1 A área responsável deve comunicar imediatamente a equipe de TI a mudança de cargo ou função que requeira alteração nas permissões de acesso do usuário, ou ainda o seu desligamento.

5.5.2 A equipe de TI deve adequar imediatamente os acessos do usuário que deixar a Fiocruz, após ser notificado pela área responsável.

5.5.3 O usuário deve devolver suas credenciais de acesso (crachá, cartões, *tokens*, etc.), quando do encerramento de suas atividades.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma à área de TI correlata.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente acionado pela área de TI correlata para adotar as providências necessárias.

6.3. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário

Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÃO CLASSIFICADA

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- 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.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

1. OBJETIVO

Este documento estabelece as diretrizes para classificação e tratamento das informações quanto ao seu grau de sigilo nos aspectos referentes à segurança da informação e comunicações no âmbito da Fiocruz.

2. PÚBLICO-ALVO

Esta norma aplica-se a todos que manipulam informações institucionais e pessoais no âmbito da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

- Algoritmo de Estado: função matemática utilizada na cifração e na decifração, Desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável;
- Autenticidade - qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
- Chave Criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;
- Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis por pessoas não autorizadas a conhecê-la;
- Credencial de Segurança: certificado que autoriza pessoa para o tratamento de informação classificada;
- Dados processados - dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;
- Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;
- Disponibilidade - qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
- Documento - unidade de registro de informações, qualquer que seja o suporte ou formato;
- Informação - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

- Informação Classificada: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada;
- Informação pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;
- Informação sigilosa - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;
- Integridade - qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
- Tratamento da informação - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- Lei nº 12.527, de 18 de novembro de 2011
- Decreto nº 7.724, de 16 de maio de 2012
- Decreto nº 7.845, de 14 de novembro de 2012
- Norma Complementar 09/IN01/DSIC/GSIPR, de 15 de fevereiro de 2013
- Instrução Normativa 02 GSIPR, de 5 de fevereiro de 2013
- Norma Complementar 01/IN02/DSIC/GSIPR, de 27 de junho de 2013
- ISO/IEC 27001/2008

5. REGRAS

5.1. Disposições gerais

5.1.1 Deve-se classificar a informação em termos de seu valor, requisitos legais, sensibilidade e criticidade para a Fiocruz.

5.1.2 O nível de proteção deve ser avaliado analisando a confidencialidade, a integridade e a disponibilidade da informação.

5.1.3 Os procedimentos de rotulação da informação precisam abranger tanto os ativos de informação no formato eletrônico quanto no formato físico.

5.1.4 O disposto nesta norma não exclui as demais hipóteses legais de sigilo e de segredo de justiça, nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

5.2. Classificação da informação quanto ao grau de sigilo

5.2.1 Deve-se classificar toda informação que possa vir a colocar em risco a segurança do estado ou da sociedade, como por exemplo:

5.2.1.1 Pôr em risco a vida, a segurança ou a saúde da população;

5.2.1.2 Oferecer elevado risco à estabilidade financeira do país, econômica ou monetária do país;

5.2.1.3 Prejudicar ou causar riscos a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;

5.2.1.4 Pôr em risco a segurança das instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares.

5.2.2 Observando-se o teor e em razão a imprescindibilidade à segurança da sociedade ou do Estado, a informação poderá ser classificada como ultrassecreta, secreta e reservada.

5.2.3 Os prazos máximos de restrição de acesso à informação vigoram a partir da sua data de produção e são os seguintes:

5.2.3.1 A informação classificada como ultrassecreta terá o prazo de restrição de 25 (vinte e cinco) anos e sua classificação será de competência das seguintes autoridades: Presidente da República, Vice-presidente da República, Ministros de Estado e autoridades com as mesmas prerrogativas (Comandantes da Marinha, Comandantes do Exército, Comandantes da Aeronáutica, Chefes de Missões Diplomáticas e Consulares permanentes no exterior).

5.2.3.2 A informação classificada como secreta terá o prazo de restrição de 15 (quinze) anos e sua classificação será de competência das autoridades supracitadas no item "a" e: titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista.

5.2.3.3 A informação classificada como reservada terá o prazo de restrição de 5 (cinco) anos e sua classificação será de competência das autoridades supracitadas nos itens "a" e "b" e: autoridades que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou

superior, do Grupo-Direção e Assessoramento Superiores, ou hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade;

5.2.4 Transcorrido o prazo de classificação ou consumado algum evento que defina o seu termo final, a informação torna-se automaticamente de acesso público.

5.2.5 Para a classificação da informação em determinado grau de sigilo, deve ser observado o interesse público das informações e utilizado o critério menos restritivo possível.

5.2.6 A informação classificada deve ser formalizada e conter minimamente o assunto sobre o qual versa a informação, fundamento da classificação, indicação do prazo de sigilo, identificação da autoridade que a classificou.

5.3. Da proteção e do controle de informações sigilosas

5.3.1 É dever da Fiocruz assegurar a proteção e controlar o acesso e a divulgação de informações sigilosas produzidas por suas unidades.

5.3.2 Entidades públicas ou privadas que tiverem algum vínculo com a Fiocruz para o tratamento ou o uso de informações sigilosas deverão observar as regulamentações das leis vigentes, inclusive instruir seus empregados, prepostos ou representantes a observarem as medidas e procedimentos de segurança das informações classificadas quanto ao seu grau de sigilo.

5.3.3 Aquele que tiver acesso à informação classificada cria a obrigação de resguardar o sigilo.

5.3.4 O acesso, a divulgação e o tratamento de informações classificadas como sigilosas ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma das regulamentações das leis vigentes.

5.4. Tratamento das Informações Pessoais

5.4.1 O tratamento das informações pessoais deve respeitar à intimidade, a honra, a vida privada e a imagem das pessoas.

5.4.2 As informações pessoais terão seu acesso restrito, independente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos, a contar da sua data de produção.

5.4.3 Terceiros poderão ter acessos às informações pessoais mediante previsão legal ou consentimento expresso da pessoa a que se refere às informações.

5.4.4 Não haverá a necessidade de consentimento da pessoa nos casos que a informação for necessária para:

5.4.4.1 A prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico.

5.4.4.2 Realização de pesquisas e estatísticas cientificas de evidente interesse público ou geral, previsto em lei, sendo vedada a identificação da pessoa a que as informações se referirem.

5.4.4.3 Ao cumprimento de ordem judicial, à defesa de direitos humanos, ou à proteção do interesse público e geral preponderante, requisição de autoridade policial no exercício da investigação policial com fim de apuração de infrações penais, aos membros do Ministério Público no exercício de suas atividades para a instrução do Inquérito civil e procedimentos administrativos.

5.5. Dos sistemas de informação

5.5.1 Devem ser utilizados sistemas de informação e canais de comunicação seguros.

5.5.2 As informações, classificadas em qualquer grau de sigilo, contidas em sistemas de informação, devem ser transmitidas através da rede corporativa por meio de um canal seguro.

5.5.3 De forma a garantir a autenticidade, a identidade do usuário da rede deve ser garantida minimamente pelo uso de certificado digital.

5.5.4 Os sistemas de informação devem prever níveis de controle de acesso e recursos criptográficos adequados aos graus de sigilo.

5.5.5 Os sistemas de informação devem manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por um prazo igual ou superior ao de restrição da informação.

5.5.6 Os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar isolados ou ligados a canais de comunicação seguros, que estejam fisicamente ou logicamente isolados de qualquer outro, e que possuam recursos criptográficos e de segurança adequados à sua proteção.

5.5.7 Toda a informação, classificada em qualquer grau de sigilo, produzida, armazenada ou transmitida, em parte ou totalmente, por qualquer meio eletrônico, deve ser protegida com recurso criptográfico baseado em algoritmo de Estado.

5.5.8 A cifração e decifração de informações classificadas, em qualquer grau de sigilo, utilizará exclusivamente recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros e padrões mínimos conforme as legislações vigentes.

5.5.9 Todo recurso criptográfico constitui material de acesso restrito e requer procedimentos especiais para sua criação, controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação vigente.

5.5.10 O recurso criptográfico, baseado em algoritmo de Estado, deve ser de desenvolvimento próprio ou por órgãos e entidades da APF, direta ou indireta, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos à APF, para tal finalidade.

5.5.11 Com anuência da Alta Administração do órgão ou entidade, o previsto no item 5.5.10 poderá ser terceirizado, desde que sejam atendidas obrigatoriamente as seguintes condições:

5.5.11.1 Seja realizado exclusivamente por meio de contrato sigiloso, conforme as legislações vigentes.

5.5.11.2 Seja previsto em contrato que fica vedado ao contratado os direitos de propriedade e exploração comercial do recurso criptográfico com algoritmo de estado.

5.6. Das áreas, instalações e materiais

5.6.1 As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito.

5.6.2 Devem ser adotadas medidas para definição, demarcação, sinalização, segurança e autorização de acessos às áreas restritas.

5.6.3 Qualquer matéria, produto, substância ou sistema que contenha, utilize e veicule conhecimento ou informação classificada em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica, cuja divulgação implique em risco ou danos aos interesses da sociedade e do estado, como por exemplo: recursos criptográficos, equipamentos, máquinas, protótipos, sistemas, entre outros, devem receber o devido tratamento.

5.6.4 O meio de transporte utilizado para deslocamento de material de acesso restrito é de responsabilidade do custodiante e deve considerar o grau de sigilo das informações.

5.6.5 O material de acesso restrito poderá ser transportado por empresas contratadas, desde que sejam adotadas as medidas necessárias à manutenção do sigilo das informações. Tais medidas de manutenção de sigilo devem ser estabelecidas em contratos.

5.7. Da celebração de contratos sigilosos

5.7.1 A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada em qualquer grau de sigilo, ou cuja execução envolva informação classificada, é condicionada à assinatura do Termo de

Compromisso de Manutenção de Sigilo (TCMS) e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:

5.7.1.1 Obrigação de manter sigilo relativo ao objeto e a sua execução;

5.7.1.2 Possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;

5.7.1.3 Obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;

5.7.1.4 Identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso a informação classificada em qualquer grau de sigilo e material de acesso restrito;

5.7.1.5 Obrigação de receber inspeções para habilitação de segurança e sua manutenção; e

5.7.1.6 Responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.

5.8. Dos procedimentos para classificação de informação

5.8.1 A Comissão Permanente de Acesso à Informação da Fiocruz (CPAI) definirá metodologia de trabalho e estabelecerá critérios para a classificação, desclassificação ou reavaliação de documentos, dados e informações sigilosas no âmbito da instituição.

5.8.2 A informação que for classificada em qualquer grau de sigilo deve ser formalizada no Termo de Classificação de Informação (TCI).

5.8.3 O TCI deve conter as seguintes informações: código de indexação do documento, grau de sigilo, categoria na qual se enquadra a informação, tipo de documento, data da produção do documento, indicação de dispositivo legal que fundamenta a classificação, razões da classificação, indicação do prazo de sigilo, data da classificação e identificação da autoridade que classificou a informação.

5.8.4 A informação classificada no grau ultrassecreto ou secreto deve encaminhar cópia do TCI à Comissão Mista de Reavaliação de Informações no prazo de trinta dias, contado da decisão de classificação ou de ratificação.

5.8.5 Documento que contenha informações classificadas em diferentes graus de sigilo, será atribuído ao documento tratamento do grau de sigilo mais elevado, ficando assegurado o acesso às partes não classificadas por meio de certidão, extrato ou cópia, com ocultação da parte sob sigilo.

5.9. Da Desclassificação e Reavaliação da Informação Classificada em Grau de Sigilo

5.9.1 A classificação das informações será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, para desclassificação ou redução do prazo de sigilo.

5.9.2 Para toda informação classificada que sofrer desclassificação ou reavaliação devem ser observados:

5.9.2.1 O prazo máximo de restrição de acesso à informação;

5.9.2.2 O prazo máximo de quatro anos para revisão de ofício das informações classificadas no grau ultrassecreto ou secreto;

5.9.2.3 A permanência das razões da classificação;

5.9.2.4 A possibilidade de danos ou riscos decorrentes da divulgação ou acesso irrestrito da informação; e

5.9.2.5 A peculiaridade das informações produzidas no exterior por autoridades ou agentes públicos.

5.9.3 O pedido de desclassificação e reavaliação das informações classificadas será endereçado a autoridade classificadora, que decidirá no prazo de trinta dias.

5.9.4 Negado o pedido de desclassificação ou de reavaliação pela autoridade classificadora, o requerente poderá apresentar recurso no prazo de dez dias, contando da ciência negativa, ao Ministro de Estado ou à autoridade com as mesmas prerrogativas, que decidirá no prazo de trinta dias.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma à área de TI correlata.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente acionado pela área de TI correlata para adotar as providências necessárias.

6.3. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.