



Ministério da Saúde
FIOCRUZ - Fundação Oswaldo Cruz
Vice-Presidência de Gestão e Desenvolvimento Institucional
Coordenação de Gestão de Tecnologia da Informação

Nº da Norma	Revisão	Emissão	Folha
SIC-001/CGTI/VPDI	00	17/04/2012	1/4

NORMA INSTITUCIONAL DE RESPONSABILIDADES DO USUÁRIO

ORIGEM

VPDI/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

1. OBJETIVO.....	2
2. PÚBLICO-ALVO	2
3. DEFINIÇÕES E TERMINOLOGIAS	2
4. DOCUMENTOS DE REFERÊNCIA DA NORMA.....	2
5. REGRAS	2
6. DISPOSIÇÕES FINAIS.....	4
7. VIGÊNCIA E ATUALIZAÇÃO	4

INFORMAÇÕES ADICIONAIS

Não se aplica.

APROVAÇÃO

APROVADA PELA PORTARIA 345/2012-PR

Nº da Norma	Revisão	Emissão	Folha
SIC-001/CGTI/VPDI	00	17/04/2012	2/4

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.

Nº da Norma	Revisão	Emissão	Folha
SIC-001/CGTI/VPDI	00	17/04/2012	3/4

- 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.

Nº da Norma	Revisão	Emissão	Folha
SIC-001/CGTI/VPDGI	00	17/04/2012	4/4

- 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.