Nº da Norma	Revisão	Emissão	Folha
SIC-008/CGTI/VPGDI	00	23/SET/2013	1/5

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.

APROVAÇÃO

APROVADA PELA PORTARIA 18/2013-VPGDI

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.