PORTARIA Nº 433, DE 15 DE MAIO DE 2012

O Presidente da Fundação Oswaldo Cruz, no Uso de suas atribuições e da competência que lhe foi delegada pela Portaria do MS/nº 938, de 22.07.99, resolve:

Instituir Norma Complementar nº 003: sobre o uso do Email, que trata da Política de Segurança da Informação e Comunicação no âmbito da Fiocruz.

ORIGEM: NORMA Nº 003 - 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

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.

PAULO ERNANI GADELHA VIEIRA