Nº da Norma	Revisão	Emissão	Folha
SIC-005/CGTI/VPGDI	00	15/FEV/2013	1/4

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.

APROVAÇÃO

APROVADA PELA PORTARIA 153/2013-PR

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.