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.

APROVAÇÃO

APROVADA PELA PORTARIA 153/2013-PR

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.