Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Número	
003/2013-VPGDI	
Folha 01	De 05
Entrada em vigor 11/03/2013	

Portaria da Presidência

O Vice Presidente de Gestão e Desenvolvimento Institucional, no uso de suas atribuições,

RESOLVE:

1.0 - PROPÓSITO

Instituir o Modelo de Gestão de Incidentes de Segurança da Informação e Comunicações da Fiocruz.

2.0 - OBJETIVO

Estabelecer e difundir os procedimentos de notificação, registro e tratamento dos incidentes de segurança da informação e comunicações no âmbito da Fiocruz, de forma a permitir a geração de estatísticas, análise de tendências, proposição de soluções integradas, etc.

3.0 - CONCEITOS E DEFINIÇÕES

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por determinado sistema, órgão ou entidade;
Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à 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;
ETIR-Fiocruz: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;
Incidente de Segurança: qualquer evento indesejado ou inesperado, que comprometa as operações ou ameace a segurança da informação;
Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;
Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, confidencialidade e autenticidade das informações.

4.0 - REFERÊNCIAS LEGAIS E NORMATIVAS

- NBR 15999-1: 2007 – Gestão de Continuidade de Negócios – Código de Boas Praticas;

Cancela	Altera	Distribuição	Data
		Geral	11.03.2013

- NBR 15999-2: 2007 – Gestão de Continuidade de Negócios – Requisitos;
- Norma Complementar nº 06/IN01/DSIC/GSIPR, de 09 de Novembro de 2009, que estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal;
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.
- Boas Práticas em Segurança da Informação – Tribunal de Contas da União – 3ª edição

5.0 - INTRODUÇÃO

É possível observar nos últimos anos a crescente demanda pelos recursos de TI, em especial o uso intenso das redes locais de computadores bem como as informações que nelas circulam. Da mesma forma, observa-se o número cada vez mais crescente de eventos indesejados ou inesperados, que comprometem as operações ou ainda ameaçam a segurança da informação, a que chamamos de incidente de segurança.

Diante do desafio de viabilizar e assegurar a segurança da informação e comunicações na Fiocruz a Coordenação de Gestão de Tecnologia da Informação – CGTI, estruturou em seu Serviço de Segurança da Informação e Comunicações uma equipe para tratamento e resposta aos incidentes em redes computacionais na Fiocruz (ETIR-Fiocruz), que tem como atribuição receber, analisar e responder as notificações e atividades relacionadas aos incidentes de segurança no âmbito da Instituição. Também é atribuição da ETIR-Fiocruz orientar as equipes de TI nas Unidades e notificar os incidentes de segurança ao Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov que faz parte do Departamento de Segurança da Informação e Comunicações – DSIC, subordinado ao Gabinete de Segurança Institucional da Presidência da República - GSIPR.

6.0 - RESPONSABILIDADE

Para a operacionalização do processo de gestão de incidentes de segurança são necessários diversos atores, cada qual com atribuições distintas. A tabela a seguir apresenta as principais responsabilidades:

Responsável	Atividades
TI da Unidade	• Notificar os incidentes de segurança ocorridos no âmbito da unidade à ETIR-Fiocruz; • Implementar ações de segurança para o adequado tratamento de incidentes no âmbito de sua Unidade.
ETIR-Fiocruz (CGTI)	• Receber, analisar e responder as notificações e atividades relacionadas aos incidentes de segurança no âmbito da Instituição; • Notificar CTIR Gov sobre incidentes de segurança ocorrido no âmbito da Fiocruz; • Dar suporte às Unidades da Fiocruz através da recomendação de estratégias de contenção e recuperação; • Difundir alertas, recomendações e estatísticas de incidentes, a partir de informações coletadas na Fiocruz ou oriundas do CTIR Gov.

7.0 - PROCEDIMENTOS

a) A comunicação entre a Unidade e a ETIR-Fiocruz (localizada no Serviço de Segurança da Informação e Comunicações da CGTI) deve ocorrer de forma centralizada pela TI da unidade, preferencialmente através de um e-mail institucional da TI da Unidade;
b) Os incidentes de segurança devem ser notificados através do e-mail abuse@fiocruz.br;
c) O campo assunto da mensagem deve conter o nome da Unidade e o tipo de incidente. Exemplo: Presidência – Phishing;
d) O corpo da mensagem deve conter uma descrição sucinta do incidente ocorrido. Quando possível, deve-se anexar evidências;

e) A seguir são listados alguns tipos de incidentes. No entanto, a Unidade poderá notificar outros tipos que possam não estar listados.

1) Desfiguração de sites (pichação, etc.);
2) Uso abusivo de servidores de e-mail (envio de spam, phishing, etc);
3) Redirecionamento ou hospedagem de artefatos ou código malicioso (phishing, malware, etc.);
4) Ataques de negação de serviço (DoS, DDos);
5) Uso ou acesso não autorizado a sistemas ou dados (invasão, controle de acesso inadequado, etc);
6) Comprometimento de computadores ou redes (DNS aberto, bonet, etc);
7) Desrespeito à POSIC ou uso inadequado dos recursos TI;
8) Ataques de engenharia social;
9) Cópia e/ou distribuição não autorizada de material protegido por direitos autorais
10) Uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes;
11) Indisponibilidade de serviços, sites, sistemas, etc.

f) Questões gerenciais ou dúvidas poderão ser encaminhadas ao e-mail seguranca@fiocruz.br;
g) Toda notificação recebida pela ETIR-Fiocruz passa por uma análise. Caso seja confirmado o incidente de segurança, este será registrado em sistema próprio e gerado um código que permitirá ao interessado acompanhar todo o processo de gestão do incidente (recebimento, análise, resposta e tratamento do incidente);
h) A ETIR-Fiocruz poderá recomendar ações de tratamento do incidente à TI da Unidade, que após a implementação das ações de tratamento deverá informar à ETIR-Fiocruz se as ações propostas foram suficientes para conter/recuperar os serviços afetados;
i) O Serviço de Segurança da Informação e Comunicações da CGTI poderá limitar o acesso a parte ou todo um serviço de TI da unidade nos seguintes casos:

I. Três notificações seguidas sem que a unidade tenha apresentado indícios de tratamento suficientes para contenção/tratamento do incidente;
II. Não tratamento dos incidentes dentro do prazo estabelecido;
III. O incidente apresente emitente risco de segurança para a própria unidade ou ainda para a instituição;
IV. Notificação reincidente através de instâncias externas (CTIR Gov, CERT.br, etc.)

8.0 - DISPOSIÇÕES FINAIS

Todos os eventos devem ser reportados à ETIR-Fiocruz, inclusive aqueles que possam parecer simplórios ou que já tenham sido tratados no âmbito da unidade ou ainda estejam sobre controle. A notificação dos eventos à ETIR-Fiocruz, possibilita ao Serviço de Segurança da Informação e Comunicações da CGTI propor investimentos, recursos e soluções tecnológicas integradas, adequadamente dimensionadas às necessidades de segurança de toda a instituição.

O Serviço de Segurança da Informação e Comunicações da CGTI mantém contato permanente com o Departamento de Segurança da Informação e Comunicações, sendo a única instância na Fiocruz credenciada a reportar os eventos ao CTIR Gov.

9.0 – VIGÊNCIA

A presente Portaria tem vigência a partir da data da sua divulgação.

Pedro Ribeiro Barbosa
Vice Presidente de Gestão e
Desenvolvimento Institucional