Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Número	
007/2013-VPGDI	
Folha	De
01	07
Entrada em vigor	
12/abril/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 Continuidade de Negócios de Tecnologia da Informação da Fiocruz.

2.0 - OBJETIVO

Difundir o Modelo de Gestão de Continuidade de Negócios de Tecnologia da Informação no âmbito da Fiocruz, visando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

3.0 - CONCEITOS E DEFINIÇÕES

Atividade: Processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem/suportem um ou mais produtos/serviços.

Atividades Críticas: Atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

Análise de Impacto nos Negócios de Tecnologia da Informação (AIN): Visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da Administração Pública Federal, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio de tecnologia da informação, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

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.

Continuidade de Negócios de Tecnologia da Informação: Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios de tecnologia da informação, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

Desastre: Evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.

Estratégia de Continuidade de Negócios de Tecnologia da Informação: Abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior.

Gestão de Continuidade: Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio de tecnologia da informação, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

Incidente: evento que tenha causado algum dano, colocado em risco, algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

Plano de Continuidade de Negócios de Tecnologia da Informação: Documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.

Plano de Gerenciamento de Incidentes: Plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

Plano de Recuperação de Negócios de Tecnologia da Informação: Documentação dos procedimentos e informações necessárias para que o órgão ou entidade da Administração Pública Federal operacionalize o retorno das atividades críticas a normalidade.

Programa de Gestão da Continuidade de Negócios de Tecnologia da Informação: Processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção.

Tempo Objetivo de Recuperação: É o tempo pré-definido no qual uma atividade deverá estar disponível, após uma interrupção ou incidente.

Resiliência: Poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

4.0 - REFERÊNCIAS LEGAIS E NORMATIVAS

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

Diante de um incidente de segurança cabe a ETIR recomendar os procedimentos a serem executados ou medidas de recuperação (em caso de ataques), ao Gestor de Segurança, que será o responsável por discutir as ações a serem tomadas e suas repercussões (caso as recomendações não sejam seguidas) com os demais membros do processo decisório.

A autonomia da ETIR será compartilhada, ou seja, o processo decisório (para ações de alto impacto) será compartilhado entre: o Gestor de Segurança da Informação e Comunicações, o Coordenador da CGTI e o Vice Presidente de Gestão e Desenvolvimento Institucional.

Em casos de extrema urgência e na impossibilidade de contato com todos os membros, a decisão poderá ser pactuada por apenas dois membros do processo decisório.

5.0 - SERVIÇOS

Os serviços a serem prestados pela ETIR serão definidos com base no histórico de incidentes de segurança reportados e que necessitam de apoio/orientação para o tratamento. Inicialmente serão oferecidos os seguintes serviços (sem prejuízos a serviços futuros):

6.0 - INTRODUÇÃO

A Gestão da Continuidade de Negócio de Tecnologia da Informação (GCN) visa minimizar impactos negativos decorrentes de falhas, desastres ou indisponibilidades nos recursos tecnológicos, de modo a garantir a continuidade das atividades institucionais em níveis aceitáveis.

7.0 – RESPONSABILIDADE

Responsável	Atividades
Alta direção	• Aprovar as diretrizes estratégicas que norteiam a elaboração do Programa de Gestão de Continuidade de Negócios de Tecnologia da Informação; • Avaliar a relação custo / benefício das estratégias de continuidade propostas e dos Planos que compõem o Programa de Gestão da Continuidade de Negócios de Tecnologia da Informação e decida sobre sua implementação; • Garantir os recursos necessários para estabelecer, implementar, operar e manter o Programa de Gestão da Continuidade de Negócios de Tecnologia da Informação.
Gestor de Continuidade de Negócios de Tecnologia da Informação ou Gestor de Segurança da Informação e Comunicações	• Propor as diretrizes estratégicas do Programa de Gestão da Continuidade de Negócios de Tecnologia da Informação; • Avaliar o plano de tratamento de riscos; • Realizar, periodicamente, a Análise de Impacto nos Negócios de Tecnologia da Informação (AIN); • Propor melhorias na implantação de novos controles relativos ao Programa de Gestão de Continuidade de Negócios de Tecnologia da Informação; • Supervisionar a elaboração, implementação , testes e atualização dos Planos; • Desenvolver a cultura de Gestão de Continuidade de Negócios de Tecnologia da Informação.
Responsáveis pelos setores ou processos onde foram identificadas atividades críticas	• Elaborar os Planos previstos no Programa de Gestão da Continuidade de Negócios de Tecnologia da Informação relacionados às atividades críticas; • Realizar os testes e exercícios dos Planos; • Avaliar e aprimorar os Planos a partir dos resultados dos testes e exercícios; • Administrar a contingência quando da interrupção de atividades, com base nos Planos desenvolvidos;

8.0 - PROCEDIMENTOS

O processo de gestão de continuidade de negócios de tecnologia da informação deve fornecer resiliência organizacional para que seja possível responder de forma efetiva as necessidades das partes interessadas, a reputação e marca da organização, além de garantir a continuidade das atividades críticas. Para isso, deve ser desenvolvido um Programa de Gestão de Continuidade de Negócios de Tecnologia da Informação – PGCN, que deve estar em conformidade com os requisitos de segurança da informação, necessários à proteção dos ativos de informação críticos da Unidade, incluindo pessoas, processos, ativos tecnológicos, fornecedores e ambientes. O PGCN deve conter minimamente:

- Diretrizes do programa de continuidade;
- Identificação das atividades críticas da Unidade;
- Avalição dos riscos a que estão expostos às atividades críticas;
- Definição das estratégias de continuidade para as atividades críticas;
- Elaboração de planos para respostas tempestivas a interrupções;
- Estratégias para exercícios, testes e manutenção periódica dos planos (a fim de promover as correções necessárias);
- Estratégias para o desenvolvimento da cultura de continuidade de negócios de tecnologia da informação no órgão/entidade.

Recomenda-se que o PGCN contenha os seguintes planos:

- Plano de Gerenciamento de Incidentes de Segurança da Informação – PGI;
- Plano de Recuperação de Negócios de Tecnologia da Informação – PRN;
- Plano de Continuidade de Negócios de Tecnologia da Informação – PCN.

Os planos devem ser concisos e acessíveis àqueles que possuam alguma responsabilidade na sua execução. Recomenda-se que cada plano contemple minimamente os seguintes conteúdos:

Conteúdo	Plano de Gerenciamento de Incidentes de Segurança da Informação – PGI	Plano de Recuperação de Negócios de Tecnologia da Informação – PRN	Plano de Continuidade de Negócios de Tecnologia da Informação – PCN
Objetivo e escopo	X	X	X
Papéis e responsabilidades	X	X	X
Condições para ativação do plano	X		
Autoridade responsável	X	X	X
Detalhes de contato	X	X	X
Lista de tarefas	X	X	X
Atividades das pessoas	X		
Comunicação à mídia	X		
Localização para o gerenciamento de incidentes	X		
Recursos necessários		X	X

Portaria da Presidência

Objetivo e escopo: breve descrição do objetivo e escopo do plano. Deve conter ainda o objetivo priorizado em termos de:

a) Atividades críticas que necessitam de recuperação;
b) Escala de tempo em que a recuperação deve ocorrer;
c) Níveis de recuperação necessários para cada atividade;
d) Situação em que cada plano pode ser utilizado.

Papéis e responsabilidades: devem ser descritos os papéis e responsabilidades das pessoas e equipes que façam parte de um plano.

Condições para ativação do plano: a ativação de um plano compreende a mobilização imediata de recursos organizacionais. Assim, deve estar claro e preciso os mecanismos para:
a) Mobilizar equipes;
b) Pontos de encontro;

Autoridade responsável: a unidade deve definir um responsável pela correção e atualização do plano. O responsável deve manter o controle de versões do plano, notificando e distribuindo a todos os envolvidos a versão atual.

Detalhes de contato: os planos devem conter referências detalhadas das principais partes interessadas.

Lista de tarefas: lista de tarefas e ações a serem executadas a fim de administrar as consequências imediatas de uma interrupção.

Atividades das pessoas: definir responsável pelo bem estar daqueles que de alguma forma possa ser impactado após um acidente. Levar em consideração questões como evacuação do local, mobilização de equipes de segurança, primeiros socorros, etc.

Comunicação à mídia: devem ser definidas estratégias de comunicação de incidentes, interface com a mídia escolhida, porta-vozes, local para realização de contato com a mídia, etc.

Localização para o gerenciamento de incidentes: local, sala ou espaço onde um incidente será gerenciado.

Recursos necessários: todos os recursos necessários para a execução de um plano.

Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Número	
007/2013-VPGDI	
Folha 07	De 07
Entrada em vigor 12/abril/2013	

Portaria da Presidência

9.0 - CONSIDERAÇÕES FINAIS

Os planos desenvolvidos no Programa de Gestão de Continuidade de Negócios de Tecnologia da Informação devem ser continuamente revisados, exercitados e testados, onde os resultados devem ser documentados para análise crítica e melhoria contínua.

Os contratos firmados com empresas que suportem atividades críticas devem conter cláusula que obriguem a empresa a manter planos de continuidade de negócio de tecnologia da informação e comprovação de testes realizados.

10.0 - VIGÊNCIA

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

Pedro Ribeiro Barbosa
Vice Presidente de Gestão e
Desenvolvimento Institucional

Cancela:	Altera	Distribuição	Data
		Geral	12.04.2013