PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

Art. 6º da Lei nº 10.683, de 28 de maio de 2003.
Art. 8º do Anexo I do Decreto nº 6.931, de 11 de agosto de 2009.
Decreto nº 3.505, de 13 de junho de 2000.
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
NBR 15999-1: 2007 – Gestão de Continuidade de Negócios.
NBR ISO/IEC 27002 (17799:2005)
Cobit 4.1 DS4 *Ensure Continuous Service*

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

1. Objetivo
2. Considerações Iniciais
3. Fundamento Legal da Norma Complementar
4. Conceitos e Definições
5. Procedimentos
6. Responsabilidades
7. Vigência

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Estabelecer diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

2 CONSIDERAÇÕES INICIAIS

A implantação do processo de Gestão de Continuidade de Negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

A Gestão de Continuidade de Negócios pode envolver ações mais abrangentes do que as definidas no âmbito da Gestão de Segurança da Informação e Comunicações, especialmente devido aos requisitos estratégicos de continuidade relativos às pessoas, à infraestrutura, aos processos e às atividades operacionais.

A Gestão de Continuidade de Negócios, objeto desta norma complementar, está limitada ao escopo das ações de Segurança da Informação e Comunicações implementadas nos órgãos ou entidades da APF.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações – DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar, aplicam-se os seguintes conceitos e definições:

4.1 **Atividade:** processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

4.2 **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.

4.3 **Análise de Impacto nos Negócios (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 APF, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, 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

4.4 **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;

4.5 **Continuidade de Negócios**: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, 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;

4.6 **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;

4.7 **Estratégia de Continuidade de Negócios:** 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;

4.8 **Gestão de Continuidade**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, 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;

4.9 **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;

4.10 **Plano de Continuidade de Negócios:** documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

4.11 **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;

4.12 **Plano de Recuperação de Negócios:** documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade;

4.13 **Programa de Gestão da Continuidade de Negócios:** 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 análises críticas, testes, treinamentos e manutenção;

4.14 **Tempo Objetivo de Recuperação:** é o tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente;

4.15 **Resiliência:** poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

5 PROCEDIMENTOS

5.1 A elaboração do Programa de Gestão da Continuidade de Negócios envolve os seguintes procedimentos:

5.1.1 desenvolver documento com as diretrizes do Programa de Continuidade;

5.1.2 definir as atividades críticas do órgão ou entidade;

5.1.3 avaliar os riscos a que estas atividades críticas estão expostas;

5.1.4 definir as estratégias de continuidade para as atividades críticas;

5.1.5 desenvolver e implementar os Planos previstos no Programa de Gestão da Continuidade de Negócios para respostas tempestivas a interrupções;

5.1.6 realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias;

5.1.7 desenvolver a cultura de continuidade de negócios no órgão ou entidade;

5.2 Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios são executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação e comunicações;

5.3 Recomenda-se que o Programa de Gestão de Continuidade de Negócios de um órgão ou entidade da APF seja composto, no mínimo, pelos seguintes Planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:

5.3.1 Plano de Gerenciamento de Incidentes - PGI;

5.3.2 Plano de Continuidade de Negócios - PCN;
5.3.3 Plano de Recuperação de Negócios - PRN.

5.4 Cada um dos Planos contém, no mínimo:

5.4.1 Plano de Gerenciamento de Incidentes:
a) Objetivo e escopo;
b) Papéis e responsabilidades;
c) Condições para a ativação de Planos;
d) Autoridade responsável;
e) Detalhes de contato;
f) Lista de tarefas e ações;
g) Atividades das pessoas;
h) Comunicação à mídia;
i) Localização para o gerenciamento de incidentes.

5.4.2 Plano de Continuidade de Negócios:
a) Objetivo e escopo;
b) Papéis e responsabilidades;
c) Autoridade responsável;
d) Detalhes de contato;
e) Lista de tarefas;
f) Recursos necessários.

5.4.3 Plano de Recuperação de Negócios:
a) Objetivo e escopo;
b) Papéis e responsabilidades;
c) Autoridade responsável;
d) Detalhes de contato;
e) Lista de tarefas;
f) Recursos necessários.

5.5 Os Planos são exercitados e testados periodicamente, bem assim os resultados documentados de forma a garantir a sua efetividade.

5.6 A revisão dos Planos é realizada nas seguintes situações:

5.6.1 No mínimo, uma vez por ano;

5.6.2 Em função dos resultados dos testes realizados; ou

5.6.3 Após alguma mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

5.7 Sugere-se que os contratos firmados com empresas terceirizadas que suportem atividades críticas contenham cláusula segundo a qual as referidas empresas possuam Planos de Continuidade dos seus Negócios, bem como as evidências dos testes realizados.

6 RESPONSABILIDADES

6.1 Para a Alta Administração do órgão ou entidade da APF, no âmbito de suas atribuições, recomenda-se que sejam adotadas as seguintes responsabilidades:

6.1.1 aprovar as diretrizes estratégicas que norteiam a elaboração do Programa de Gestão de Continuidade de Negócios;

6.1.2 avaliar a relação custo / benefício das estratégias de continuidade propostas e dos Planos que compõem o Programa de Gestão da Continuidade de Negócios e decida sobre sua implementação;

6.1.3 garantir os recursos necessários para estabelecer, implementar, operar e manter o Programa de Gestão da Continuidade de Negócios.

6.2 As seguintes atribuições devem ser conferidas ao responsável pela Gestão da Continuidade de Negócios, ou ao Gestor de Segurança da Informação e Comunicações, no caso do órgão ou entidade não possuir o Gestor de Continuidade de Negócios;

6.2.1 Propor as diretrizes estratégicas do Programa de Gestão da Continuidade de Negócios;

6.2.2 Avaliar o plano de tratamento de riscos;

6.2.3 Realizar, periodicamente, a Análise de Impacto nos Negócios (AIN);

6.2.4 Propor melhorias na implantação de novos controles relativos ao Programa de Gestão de Continuidade de Negócios;

6.2.5 Supervisionar a elaboração, implementação, testes e atualização dos Planos;

6.2.6 Desenvolver a cultura de Gestão de Continuidade de Negócios.

6.3 As seguintes atribuições devem ser conferidas aos responsáveis pelos setores ou processos onde foram identificadas atividades críticas para o órgão ou entidade da APF:

6.3.1 Elaborar os Planos previstos no Programa de Gestão da Continuidade de Negócios relacionados às atividades críticas;

6.3.2 Realizar os testes e exercícios dos Planos;

6.3.3 Avaliar e aprimorar os Planos a partir dos resultados dos testes e exercícios;

6.3.4 Administrar a contingência quando da interrupção de atividades, com base nos Planos desenvolvidos;

6.3.5 Propor os recursos necessários para a implantação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes e dos exercícios dos Planos.

7 **VIGÊNCIA**

Esta Norma entra em vigor na data de sua publicação, gerando seus efeitos a partir de 17 de maio de 2010.