PODER JUDICIÁRIO

JUSTIÇA FEDERAL

CONSELHO DA JUSTIÇA FEDERAL

PORTARIA Nº CJF-POR-2014/00413 de 30 de setembro de 2014

Dispõe sobre a aprovação do Documento Acessório Diferenciado "Política de Gestão de Continuidade de Negócios em Segurança da Informação", de que trata a Resolução n. 006, de 2008.

O PRESIDENTE DO CONSELHO DA JUSTIÇA FEDERAL, usando de suas atribuições legais, tendo em vista o decidido no Processo n. CF-ADM-2012/00494 e considerando os termos da Resolução n. 6, de 07 de abril de 2008, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal, e da Portaria da Presidência n. 45, de 09 de julho de 2010, que criou a Comissão Local de Segurança da Informação,

RESOLVE:

Art. 1º Aprovar o Documento Acessório Diferenciado "Política de Gestão de Continuidade de Negócios em Segurança da Informação" do Conselho da Justiça Federal, na forma do anexo.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

MINISTRO FRANCISCO FALCÃO

Anexo

"Política de Gestão de Continuidade de Negócios em Segurança da Informação"

1 Apresentação

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 Conselho da Justiça Federal - CJF, além de recuperar perdas de ativos de informação em 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, 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 política, está limitada ao escopo das ações de Segurança da Informação implementadas no órgão.

A elaboração e a atualização deste documento são de responsabilidade da Comissão Local de Segurança da Informação, criada pela Portaria de Presidência n. 45/2010, conforme estabelecido no item 9.3.4 do Anexo I da Resolução n. 6/2008, que dispõe sobre a Política de Segurança da Informação do Conselho da Justiça Federal e da Justiça Federal, para permitir melhorias, adequações e atualizações progressivas e independentes.

2 Escopo

Este documento define as diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação do CJF, consoante o item 9.3.4 da Política de Segurança da Informação da Justiça Federal.

3 Público-alvo

As regras aqui dispostas aplicam-se a todos os agentes públicos lotados ou não no CJF e a quaisquer pessoas ou entidades que interajam com a rede do CJF ou utilize os serviços de TI nela disponíveis.

4 Conceituação

A este documento aplicam-se as seguintes conceituações:

Agente público – magistrados, servidores, estagiários e prestadores de serviço que estejam exercendo atividades neste Conselho.

Alta Administração – Presidente e Vice-Presidente do Conselho da Justiça Federal, Corregedor-Geral da Justiça Federal, Secretário-Geral e titulares das unidades.

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 do órgão. Almeja ainda estabelecer 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.

Atividade – processo ou conjunto de processos executado(s) pelo órgão, ou em seu nome, que produza(m) ou suporte(m) um ou mais produtos ou serviços.

Atividades críticas – atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

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.

CLSI – Comissão Local de Segurança da Informação: com atribuições definidas pela Resolução CJF n. 6/2008, criada pela Portaria da Presidência n. 45/2010.

CLRI – Comissão Local de Resposta a Incidentes: com atribuições definidas pela Resolução CJF n. 6/2008, criada pela Portaria da Presidência n. 43 de 9 de julho de 2010.

CSI-JUS – Comitê de Segurança da Informação da Justiça Federal: com atribuições definidas pela Resolução CJF n. 6/2008, criado pela Portaria da Presidência n. 44/2010.

CRI-JUS – Comitê de Resposta a Incidentes da Justiça Federal: com atribuições definidas pela Resolução CJF n. 6/2008, criado pela Portaria da Presidência n. 42/2010.

Continuidade de Negócios – capacidade estratégica e tática do órgão 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.

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 – abordagem do órgão 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 determinada organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece estrutura para que se desenvolva resiliência organizacional, que seja capaz de responder efetivamente e salvaguardar os interesses das partes, 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 – documentação dos procedimentos e informações necessárias para que o órgão mantenha seus ativos de informação

críticos e a continuidade de suas atividades críticas em local alternativo em nível previamente definido, em casos de incidentes.

Plano de gerenciamento de incidentes – plano de ação claramente definido e documentado, para ser usado quando ocorrer 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 – documentação dos procedimentos e informações necessárias para que o órgão operacionalize o retorno das atividades críticas à normalidade.

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 de análises críticas, testes, treinamentos e manutenção.

Resiliência – poder de recuperação ou capacidade de determinada organização resistir aos efeitos de um desastre.

Sistema de informação – aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, com o fim de otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação.

Tempo objetivo de recuperação – é o tempo predefinido no qual uma atividade deverá estar disponível após interrupção ou incidente.

Titular da Unidade – secretários, assessores chefe e chefe de gabinete da Secretaria-Geral ou seus substitutos.

5 Objetivos

Definir diretrizes para a implantação da Gestão de Continuidade de Negócios no âmbito do Conselho da Justiça Federal.

6 Documentos de Referência

Resolução CJF n. 6, de 7 de abril de 2008.

Documentos normativos complementares à Resolução CJF n. 6/2008.

Norma Complementar 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009, do Departamento de Segurança da Informação e das Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC, *GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.*

NBR ISO 15999-1: 2007 – Gestão de Continuidade de Negócios.

Cobit 4.1 DS4 Ensure Continuous Service

7 Procedimentos

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

7.1.1 Documentar as diretrizes do Programa de Continuidade;

7.1.2 Definir as atividades críticas do CJF;

7.1.3 Avaliar os riscos a que estas atividades críticas estão expostas;

7.1.4 Definir as estratégias de continuidade para as atividades críticas;

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

7.1.6 Realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias;

7.1.7 Desenvolver a cultura de continuidade de negócios no órgão.

7.2 Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios são executados em conformidade com os requisitos de segurança da informação 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.

7.3 O Programa de Gestão de Continuidade de Negócios do CJF será composto pelos seguintes Planos, a fim de assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:

7.3.1 Plano de Gerenciamento de Incidentes - PGI;

7.3.2 Plano de Continuidade de Negócios - PCN;

7.3.3 Plano de Recuperação de Negócios - PRN.

7.4 Cada um dos Planos contém, no mínimo:

7.4.1 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.

7.4.2 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.

7.4.3 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.

7.5 Os Planos são exercitados e testados periodicamente, bem assim os resultados documentados, para garantir a sua efetividade.

7.6 A revisão dos Planos é realizada nas seguintes situações:

7.6.1 No mínimo, uma vez por ano;

7.6.2 Em função dos resultados dos testes realizados; ou

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

7.7 Os contratos firmados com empresas terceirizadas que suportem atividades críticas devem conter cláusula segundo a qual as referidas empresas possuam Planos de Continuidade dos seus Negócios, bem como as evidências dos testes realizados.

8 Responsabilidades

8.1 São responsabilidades da alta administração do órgão, no âmbito de suas atribuições:

8.1.1 Nomear o gestor responsável pelo Programa de Gestão da continuidade de negócio;

8.1.2 Aprovar as diretrizes estratégicas que norteiam a elaboração do Programa de Gestão de Continuidade de Negócios;

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

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

8.2 São atribuições do gestor responsável pelo Programa de Gestão da Continuidade de Negócios:

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

8.2.2 Avaliar o plano de tratamento de riscos;

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

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

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

8.2.6 Desenvolver a cultura de Gestão de Continuidade de Negócios.

8.3 São atribuições dos responsáveis pelos setores ou processos onde foram identificadas atividades críticas para o CJF:

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

8.3.2 Realizar os testes e exercícios dos Planos;

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

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

8.3.5 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.

9 Disposições Gerais

Esta política será atualizada sempre que necessário, de modo a refletir as necessidades do CJF.

9.1 As alterações nesta política poderão ser feitas por determinação da CLSI-CJF ou por recomendação do CSI-Jus.

10 Disposições Finais

10.1 Este documento e seus anexos devem ser amplamente divulgados entre os magistrados, servidores, prestadores de serviço e estagiários que atuem no Conselho da Justiça Federal.

10.2 Este documento deverá estar disponível, para acesso ou *download*, a qualquer tempo.