

PORTARIA N.º 1.109/2017-TJ, DE 17 DE JULHO DE 2017

Regulamenta a Política de Gestão de Continuidade de Negócio do Poder Judiciário do Estado do Rio Grande do Norte - PJRN.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO NORTE, no uso das suas atribuições legais e,

CONSIDERANDO que todos têm o direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado, nos termos do inciso XXXIII do art. 5º da Constituição Federal;

CONSIDERANDO que é dever de todo servidor público prestar as informações requeridas pelo público em geral, ressalvadas as protegidas por sigilo, bem como guardar sigilo sobre assuntos institucionais, nos termos do art. 116 da Lei nº 8.112, de 11 de dezembro de 1990;

CONSIDERANDO, finalmente, a legislação pertinente à matéria, notadamente o Decreto nº 7.845/2012, a Instrução Normativa GSI nº 1/2008, a Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, a Norma Complementar nº 05/IN01/DSIC/GSICPR, de 14 de agosto de 2009, a Norma Complementar nº 06/IN01/DSIC/GSICPR, de 11 de novembro de 2009, e Normas ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27031 e Normas ABNT NBR ISO/IEC 22313, que instituem os códigos de melhores práticas para Gestão de Sistemas de Continuidade de Negócio e a Resolução CNJ nº 182 de 17 de outubro de 2013 e Resolução CNJ nº 211 de 15 de dezembro de 2015;

RESOLVE:

Art. 1º A presente Portaria rege a Política de Gestão de Continuidade de Negócio do Poder Judiciário do Estado do Rio Grande do Norte (PJRN) que descreve as diretrizes, os processos, as responsabilidades e a estrutura para o sistema de continuidade de negócio, através do uso dos serviços de Tecnologia da Informação.

Parágrafo único. Essa política deve ser divulgada e adotada por todas as unidades do PJRN em todos os níveis aplicáveis de processos, estratégias, táticas e de operações.

Art. 2º Para fins desta Política consideram-se:

I - Agente público: magistrados, servidores, estagiários e prestadores de serviço que estejam exercendo atividades no PJRN;

II - Análise de Impacto nos Negócios: processo para estimar os impactos ocasionados por eventual interrupção de serviços críticos de Tecnologia da Informação e Comunicação (TIC), inclusive cenários de desastre que venham a prejudicar ou interromper total ou parcialmente os serviços fins prestados pelo PJRN;

III - Atividades Críticas de TIC: conjunto de serviços de TIC, sejam eles fornecidos pela Setic/TJRN ou prestados por terceiros, indispensáveis para a consecução adequada dos serviços do PJRN;

IV - Ativos de informação: qualquer meio de armazenamento, transmissão ou processamento de dados, os sistemas de informação, bem como os locais onde se encontram e as pessoas que a eles possuem acesso;

V - Continuidade de Negócio: planejamento e resposta a eventos que representem ameaças potenciais ou reais de interrupções do negócio visando reduzir ou eliminar a ocorrência de incidentes ou, quando inevitável, minimizar o impacto deles decorrentes, preservando ao máximo a continuidade das atividades finalísticas do PJRN;

VI - Desastre: evento repentino que causa perda da capacidade de entregar serviços essenciais ou críticos ao PJRN por um período de tempo;

VII - Incidente: evento que não faz parte da operação normal de um serviço e que comprometa a confidencialidade, integridade ou disponibilidade de informações críticas ao PJRN, inclusive nas situações em que o desempenho do serviço afetado inviabilize o desempenho das atividades laborais dos usuários dele dependentes;

VIII - Plano de Continuidade de Negócio: conjunto de ações que tem por objetivo primordial a manutenção do funcionamento da organização, em um nível aceitável, face à ocorrência de eventos que representem risco à integridade das informações institucionais;

IX - Plano de Gerenciamento de Incidentes: processo de prevenção e tratamento de incidentes, por meio

da definição e utilização de recursos organizacionais correlatos;
X - Plano de Recuperação de Negócios: documentação dos procedimentos e informações necessárias para que o PJRN operacionalize o retorno das atividades críticas;
XI - Programa de Gestão de Continuidade de Negócio: processo contínuo de gestão para garantir que as diretrizes dos Planos de Continuidade de Negócio, Gerenciamento de Incidentes e Recuperação de Negócios sejam executadas corretamente, revisadas através de análise crítica e testadas periodicamente.

Art. 3º Essa Política tem como objetivos específicos:

- I - Guiar a implantação do Programa de Gestão de Continuidade de Negócios bem como os Planos de Continuidade de Negócio, Gerenciamento de Incidentes e Recuperação de Negócios;
- II - Minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do PJRN;
- III - Definir diretrizes para a tomada de ações preventivas, de resposta ou recuperação face ao desastre.

Art. 4º São responsabilidades do Comitê de Segurança da Informação (CSInfo), no âmbito das suas atribuições:

- I - Aprovar as diretrizes estratégicas para elaboração do Programa de Gestão e Continuidade de Negócios;
- II - Analisar e aprovar Estratégias de Continuidade propostas e dos Planos que compõem o Programa de Gestão de Continuidade de Negócios;
- III - Garantir que os recursos necessários sejam disponibilizados para estabelecer, implementar, operar e manter o Programa de Gestão de Continuidade de Negócios;
- IV - Analisar e propor diretrizes Estratégicas do Programa de Gestão da Continuidade de Negócios;
- V - Avaliar o plano de tratamento de riscos;
- VI - Realizar, periodicamente, a Análise de Impacto nos Negócios, criticando os procedimentos e buscando a melhoria do Programa de Gestão e Continuidade de Negócios;
- VII - Propor melhorias da implantação de novos controles relativos ao Programa de Gestão de Continuidade de Negócios;
- VIII - Supervisionar a elaboração, implementação, testes e atualização dos Planos;
- IX - Desenvolver e divulgar a cultura de Gestão de Continuidade de Negócios.

Art. 5º São atribuições dos gestores dos diversos setores onde forem identificadas atividades críticas para o PJRN:

- I - Elaborar Planos previstos no Programa de Gestão da Continuidade de Negócios relacionados às atividades críticas;
- II - Executar, periodicamente, os testes e exercícios dos Planos;
- III - Avaliar e aprimorar os Planos a partir dos resultados dos testes;
- IV - Administrar a contingência em caso de interrupção de atividades descritas nos Planos;
- V - Realizar testes e exercícios dos Planos periodicamente.

Art. 6º As ações dessa Política são delimitadas ao escopo das diretrizes definidas pela Política de Segurança da Informação (PSI) vigente para o PJRN.

Art. 7º A Política de Continuidade de Negócio é de responsabilidade do CSInfo e deve ser revisada anualmente.

Art. 8º A elaboração do Programa de Gestão de Continuidade de Negócios, pelos gestores da área de negócio, envolve os seguintes procedimentos:

- I - Documentar as diretrizes do Programa de Continuidade;
- II - Definir as atividades críticas do PJRN;
- III - Avaliar os riscos a que estas atividades críticas estão expostas;
- IV - Definir estratégias de continuidade para as atividades críticas;
- V - Desenvolver e implementar os planos previstos no Programa de Gestão de Continuidade de Negócios para respostas tempestivas a interrupções;
- VI - Realizar exercícios, testes e manutenção periódica dos planos, promovendo as revisões necessárias;
- VII - Desenvolver a cultura de continuidade de negócios no PJRN.

Art. 9º Todos os procedimentos previstos no Programa de Gestão da Continuidade de Negócios são

executados em conformidade com as diretrizes definidas na Política de Segurança da Informação (PSI) vigente.

Art. 10. O Programa de Gestão de Continuidade de Negócio do PJRN define quais planos serão utilizados para assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas.

§ 1º Os planos que constituem o Programa de Gestão de Continuidade de Negócio são:

- I - Plano de Gerenciamento de Incidentes - PGI;
- II - Plano de Continuidade de Negócios - PCN;
- III - Plano de Recuperação de Negócios - PRN.

§ 2º Os planos devem ser testados e avaliados em períodos não maiores do que um ano ou após qualquer mudança significativa nos ativos de informação ou atividades.

§ 3º Cada plano deve abranger pelo menos as seguintes diretrizes:

I - 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.

II - 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.

III - Plano de Recuperação

- a) objetivo e escopo;
- b) papéis e responsabilidades;
- c) autoridade responsável;
- d) detalhes de contato;
- e) lista de tarefas;
- f) recursos necessários.

Art. 11. Contratos com empresas terceirizadas que deem suporte a sistemas de informação críticos do PJRN devem conter cláusula garantindo que as empresas contratadas possuam Planos de Continuidade de Negócios devidamente testados e revisados periodicamente.

Art. 12. Essa política deve ser amplamente divulgada para todos os agentes públicos em todos os níveis de todas as unidades do PJRN.

Art. 13. Esta Portaria entra em vigor na data de sua publicação.

Desembargador EXPEDITO FERREIRA
Presidente