TRIBUNAL SUPERIOR DO TRABALHO
PRESIDÊNCIA

ATO Nº 117/SETIN.SEGP.GP, DE 17 DE MARÇO DE 2017

Estabelece diretrizes para o processo de Gestão de Continuidade de Serviços de Tecnologia da Informação e Comunicação no âmbito do Tribunal Superior do Trabalho (TST).

O **PRESIDENTE DO TRIBUNAL SUPERIOR DO TRABALHO**, no uso de suas atribuições legais e regimentais,

Considerando a importância da padronização de processos de trabalho para o estabelecimento de indicadores e metas, com vistas ao aprimoramento contínuo e sistemático da gestão de serviços de Tecnologia da Informação e Comunicação, em benefício do Tribunal Superior do Trabalho;

Considerando a importância de estabelecer processos de trabalho, responsabilidades e práticas compatíveis com os modelos de excelência reconhecidos mundialmente, como COBIT e ITIL;

Considerando o Decreto nº 3.505, de 13 de junho de 2000, que "Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal";

Considerando o Ato nº 764/GDGSET.GP, de 27 de novembro de 2012, que "Estabelece as diretrizes de segurança da informação no âmbito do Tribunal Superior do Trabalho";

Considerando o art. 10 da Resolução nº 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, que estabelece: "A estrutura organizacional, o quadro permanente de servidores, a gestão de ativos e os processos de gestão de trabalho da área de TIC de cada órgão, deverão estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as atividades consideradas como estratégicas";

Considerando a Instrução Normativa nº 1 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que "Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências";

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 10, 17 mar. 2017, p. 28-31.

Considerando a Norma ABNT NBR ISO/IEC 27002:2013, Código de prática para controles de segurança da informação, que "fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização";

Considerando a Norma ABNT NBR ISO/IEC 27031:2015, Diretrizes para a prontidão para a continuidade dos negócios da Tecnologia da Informação e Comunicação, que "descreve os conceitos e princípios da prontidão esperada para a Tecnologia da Informação e Comunicação e fornece uma estrutura de métodos e processos para identificar e especificar todos os aspectos";

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES

Art. 1º Este Ato estabelece a Política de Gestão de Continuidade de Serviços de Tecnologia da Informação e Comunicação – TIC, que objetiva minimizar os impactos sobre as atividades do Tribunal Superior do Trabalho decorrentes de desastres relacionados a serviços de TIC.

Art. 2º Para os fins deste Ato, são considerados:

I – 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;

II – Serviços de TIC: conjunto de ativos de informação que, por meio de integração e orquestração, entregam valor aos usuários e ao órgão, mediante recursos de TIC empregados;

III – Desastre: acontecimento que afeta um sistema ou serviço de TIC e que exige considerável esforço para restauração ao nível de desempenho original;

IV – Continuidade de Serviços de TIC: conjunto de práticas, procedimentos, processos, planos e ferramentas de trabalho que maximizam a possibilidade de que o órgão, dispondo de um sistema de gestão de continuidade documentado, mantenha o fornecimento dos serviços de TIC após a ocorrência de determinados cenários de desastre;

V – Escritório de Gestão de Continuidade de Serviços de TIC: arranjo organizacional que propõe fundamentos e colabora na concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de continuidade de serviços de TIC, composto por integrantes das unidades responsáveis pela segurança da informação, infraestrutura tecnológica, desenvolvimento de software, suporte e demais áreas relevantes para a prestação dos serviços de TIC;

VI – Gestão de Segurança da Informação: objetiva a proteção da informação, a fim de garantir a continuidade do negócio e a minimização dos riscos que possam comprometê-la.

Art. 3º O escopo do processo de Gestão de Continuidade de Serviços de TIC abrange o conjunto de serviços de TIC classificados com relevância "muito alta" na

relação de serviços críticos aprovada pelo Comitê Gestor de Tecnologia da Informação.

Art. 4º O processo de Gestão de Continuidade de Serviços de TIC considerará, no mínimo, cenários de desastre dos seguintes ativos de informação:

I – rede interna de comunicação de dados;

II – acesso à internet;

III – banco de dados;

IV – servidor de aplicação; e

V – equipamentos do datacenter.

Art. 5º O processo de Gestão de Continuidade de Serviços de TIC é contínuo e aplicado na implementação e operação dos serviços de TIC no âmbito da Secretaria de Tecnologia da Informação – SETIN.

Parágrafo único. São macroatividades do processo de Gestão de Continuidade de Serviços de TIC:

I – elaboração e manutenção de planos de continuidade de serviços de TIC ao longo dos respectivos ciclos de vida;

II – ativação de plano de continuidade para contingenciamento de serviços de TIC em cenários específicos de desastre;

III – interrupção de contingenciamento de serviços de TIC e sua recondução à normalidade operacional.

CAPÍTULO II
DAS RESPONSABILIDADES

Art. 6º Cabe ao Comitê Gestor de Tecnologia da Informação aprovar a classificação de relevância dos serviços críticos de TIC, ouvidos os Comitês Gestores de Sistemas Judiciais, de Sistemas Administrativos e de Segurança da Informação.

Parágrafo único. A classificação da relevância dos serviços de que trata o caput será revisada anualmente ou quando oportuno.

Art. 7º Cabe ao Comitê Gestor de Segurança da Informação propor revisões da Política de Gestão de Continuidade de Serviços de TIC, observada, dentre normas e procedimentos internos, a Política de Segurança da Informação do TST.

Art. 8º Cabe ao Secretário de Tecnologia da Informação do TST:

I – aprovar o processo de Gestão de Continuidade de Serviços de TIC;

II – propor à Presidência do TST a composição do Escritório de Gestão de Continuidade de Serviços de TIC;

III – aprovar os planos de continuidade de serviços de TIC e os respectivos planos de testes, comunicando-os ao Comitê Gestor de Segurança da Informação, bem como os resultados aferidos após os testes de simulação de desastres;

IV – autorizar a ativação e a respectiva interrupção de plano de continuidade de serviço de TIC, comunicando a decisão à Presidência e ao Coordenador do Comitê Gestor de Segurança da Informação.

Art. 9º Cabe ao Escritório de Gestão de Continuidade de Serviços de TIC:

I – propor os planos de continuidade de serviços de TIC e os respectivos planos de testes;

II – acompanhar, validar e informar sobre a execução dos testes dos planos de continuidade de serviços de TIC;

III – realizar o monitoramento e a análise crítica do processo de Gestão de Continuidade de Serviços de TIC;

IV – fornecer consultoria às unidades da SETIN responsáveis pela execução dos planos de continuidade de serviços de TIC.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 10. A SETIN editará normativo alinhado às diretrizes da Política de Gestão de Continuidade de Serviços de TIC, objetivando detalhar os aspectos táticos e operacionais do processo de Gestão de Continuidade de Serviços de TIC.

Art. 11. O prazo para a consecução do estabelecido nos incisos I e II do art. 8º e no art. 10 é de 180 dias a contar da publicação deste Ato.

Art. 12. Os planos de continuidade de serviços de TIC e os respectivos planos de testes, estabelecidos no inciso III do art. 8º, poderão constar dos Planos Diretores de Tecnologia da Informação e Comunicação, considerando as limitações de recursos humanos, orçamentários e técnicos da SETIN.

Art. 13. Este Ato entra em vigor na data de sua publicação.

Ministro IVES GANDRA DA SILVA MARTINS FILHO

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 10, 17 mar. 2017, p. 28-31.