PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 23/2020

Altera o Ato TRT7.GP nº 02/2017, que aprova a Norma Complementar com as diretrizes para o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a solicitação de alteração da Norma Complementar nº 07/NC/STI/SESTI, requerida pelo Secretário de Tecnologia da Informação e Comunicação, mediante Ofício nº 43/2019/ SETIC/TRT7, de 17 de dezembro de 2019, (Proad 8353/2019),

RESOLVE:

Art. 1º O Anexo do Ato TRT7.GP nº 02/2017 passa a vigorar na forma do anexo único do presente ato.

Art. 2º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 28 de fevereiro de 2020.
PLAUTO CARNEIRO PORTO
Presidente do Tribunal

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2926, 04 mar. 2020. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

Gestão de Continuidade de TIC

Número	Revisão
07/NC/SETIC	02

1 - Objetivo

Estabelecer as diretrizes e definir o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações, aplicáveis ao ambiente tecnológico deste Tribunal.

2 - Motivações

2.1 - Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2 - Correto direcionamento e dimensionamento de recursos tecnológicos para prover a Gestão de Continuidade de TIC.

2.2 - Aumentar o nível de resiliência dos serviços e sistemas de TIC frente a eventos que possam causar sua interrupção, contribuindo para contínua melhoria da prestação jurisdicional.

2.4 - Estabelecer procedimentos de gestão para assegurar a continuidade das operações de TIC.

3 - Referências normativas

3.1 - Norma Complementar nº 06/IN01/DSIC/GSIPR, de 11.11.2009, 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 (APF), direta e indireta.

3.2 - Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.3 - Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação.

3.4 - Norma Técnica ABNT NBR ISO/IEC 22301:2013, que normatiza o sistema de gestão de continuidade de negócios e especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem.

4 - Conceitos e Definições

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

4.1 - Atividades Críticas: atividades que devem ser executadas de forma a garantir a consecução

dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo.

4.2 - Análise de Impacto nos Negócios (AIN): estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar a prestação jurisdicional do Tribunal, bem como técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, prioridades, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

4.3 - Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções dos 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.

4.4 - Desastre: incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização.

4.5 - Estratégia de continuidade: 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.

4.6 - 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, a marca da organização e suas atividades de valor agregado.

4.7 - Plano de Continuidade: nome que se dá à documentação que abrange os procedimentos referentes à continuidade dos serviços de TIC e é composta por Plano de Continuidade Operacional e Plano de Recuperação de Desastres.

4.8 - Plano de Continuidade Operacional (PCO): documento que descreve procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para manutenção dos serviços, ainda que em um nível mínimo de operacionalidade.

4.9 - Plano de Recuperação de Desastres (PRD): documento que descreve procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TIC, visando o retorno à normalidade.

4.10 - Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos

de um desastre.

4.11 - RPO (*Recovery Point Objective*) - Tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após a ocorrência de um desastre.

4.12 - RTO (*Recovery Time Objective*) - Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

5 - Diretrizes

5.1 - A gestão de continuidade de TIC visa a:

5.1.1 - Reduzir o risco e minimizar o impacto de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas do TRT7.

5.1.2 - Manter os sistemas e serviços críticos de TIC em um nível minimamente operável e aceitável durante a ocorrência de um desastre, de forma a não interromper a prestação jurisdicional do TRT7.

5.1.3 - Definir procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne à normalidade.

5.2 - A gestão de continuidade de TIC deve observar o resultado das análises de riscos de TIC e da análise de impacto de negócio realizadas, de forma a nortear as estratégias de continuidade.

5.3 - Será elaborado Plano de Continuidade de TIC, com vistas a documentar os procedimentos necessários à operação em nível de contingência e comunicações necessárias, bem como o retorno à normalidade, quando da ocorrência de interrupções dos serviços e sistemas de TIC.

5.4 - Devem ser fornecidos recursos humanos, tecnológicos e financeiros para a manutenção e melhoria contínua da gestão de continuidade de TIC.

6 - Processo de Gestão de Continuidade de TIC

6.1 - O processo de Gestão de Continuidade de TIC é composto pelas seguintes etapas:

6.1.1 - Planejamento - compreende a análise dos processos críticos para o negócio, a fim de estabelecer quais atividades da SETIC são essenciais para prestação jurisdicional, quais deverão ser tratadas na Continuidade de TIC e quais estratégias serão utilizadas durante a ocorrência de

um incidente. Compreende também a avaliação da necessidade de revisão dos planos já instituídos, seja em virtude do tempo decorrido desde sua aprovação, seja em razão de mudanças na infraestrutura, procedimentos ou testes realizados.

6.1.2 - Execução - abrange a elaboração ou revisão dos planos pelas equipes técnicas, com a descrição dos cenários de falhas e os procedimentos técnicos para lidar com os problemas, a realização de testes (execução parcial ou integral dos procedimentos), a aprovação dos planos, seu armazenamento e divulgação.

6.1.3 - Verificação - abrange a realização de testes periódicos dos Planos desenvolvidos e a análise dos incidentes críticos ocorridos (desastres) a fim de subsidiar a etapa de Melhoria.

6.1.4 - Melhoria - compreende a identificação das oportunidades de melhoria e seu encaminhamento à consideração superior, com vistas a dar início a novo ciclo do processo.

6.2 - O desenho do processo de Gestão de Continuidade de TIC, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos e indicadores definidos para o processo serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

6.2.1 - O processo será revisto periodicamente e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior.

7 - Plano de Continuidade de TIC

7.1 - O Plano de Continuidade de TIC é composto pelos Planos de Continuidade Operacional e Planos de Recuperação de Desastres.

7.2 - O Plano de Continuidade de TIC deve ser periodicamente testado, de forma a garantir sua efetividade.

7.3 - O Plano de Continuidade de TIC deve ser revisado no mínimo uma vez por ano ou, ainda, em função dos resultados de testes realizados ou após mudança significativa nos ativos de informação (infraestrutura tecnológica, processo, atividades etc).

7.4 - O Plano de Continuidade de TIC será acionado quando verificadas interrupções parciais ou totais que impactem nas atividades críticas do TRT.

7.4.1 - Ocorrido o incidente, considerados os serviços, sistemas ou ativos afetados e a criticidade, as equipes técnicas responsáveis acionarão os Planos de Continuidade Operacional para a manutenção da continuidade das atividades, ainda que de forma contingencial, e os Planos de Recuperação de Desastre para retorno das atividades à normalidade.

7.4.2 - A comunicação às partes interessadas observará as orientações contidas nos Planos de Continuidade Operacional.

7.4.3 - Os ativos e serviços afetados pelo incidente serão monitorados pelas equipes responsáveis, a fim de subsidiar o fornecimento de informações à autoridade superior.

7.4.4 - Considerando as atuais capacidades operacionais instaladas no ambiente de TIC do TRT7, a tolerância a perda de dados e o tempo de recuperação por conjunto de dados são os seguintes:

CONJUNTO DE DADOS	**Tolerância a perda de dados (recovery point objective - RPO)**	**Meta de prazo para disponibilizar o conjunto de dados em caso de perda do ambiente de produção (recovery time objective - RTO)**
Arquivos de usuários armazenados na rede corporativa - SEDE E FÓRUM AUTRAN NUNES	24 horas	36 horas
Arquivos de usuários armazenados na rede corporativa - INTERIOR	24 horas	48 horas
Bancos de dados ORACLE (PROAD, SIGEP, etc)	24 horas	36 horas
Bancos de dados MYSQL e OUTROS (site institucional, intranet, outros)	24 horas	36 horas
Arquivos de usuários armazenados em nuvem contratada, tais como documentos de texto, planilhas eletrônicas e	-Não aplicável o conceito de RPO. Os dados devem ser persistidos com	-Não aplicável o conceito de RTO. -Deve ser exigido da contratada disponibilidade mensal mínima de

arquivos pdf´s	redundância, garantindo no mínimo 5 9's de durabilidade dos dados em um ano (99,999% de durabilidade no ano).	99.5%
E-mails armazenados na solução de correio eletrônico	-Não aplicável o conceito de RPO. Os dados devem ser persistidos com redundância, garantindo no mínimo 5 9's de durabilidade dos dados em um ano (99,999% de durabilidade no ano).	-Não aplicável o conceito de RTO. -Deve ser exigido da contratada disponibilidade mensal mínima de 99.5%
Bancos de dados POSTGRESQL (PJe, outros) - CENÁRIO DE CONTINGÊNCIA - USO DE RÉPLICA	15 minutos	8 horas
Bancos de dados POSTGRESQL (PJe, outros) - CENÁRIO DE CONTINGÊNCIA - USO DE BACKUP ON-SITE	24 horas	72 horas
CENÁRIO DE DESASTRE - USO DE BACKUP OFF-SITE, PARA QUALQUER CONJUNTO DE DADOS	48 horas	96 horas

7.4.5 - A ativação do Plano de Continuidade de TIC será encerrada quando da comunicação de retorno à normalidade dos serviços, sistemas ou ativos afetados.

8 - Atualização da Norma

As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Continuidade de TIC, observada a periodicidade prevista para a Política de Segurança da Informação.