ANEXO VIII
Gestão de Continuidade de TIC

1. Objetivos

1.1. 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.

2.3. Manutenção de um nível adequado de resiliência dos serviços e sistemas de TIC críticos 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. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

3.2. Norma ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão da Segurança da Informação;

3.3. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles genéricos de segurança da informação;

3.4. Norma Técnica ABNT NBR ISO/IEC 22301:2020, 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.

3.5. Resolução CNJ nº 396, de 07 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

4. 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 de um órgão ou entidade de, quando ocorrer algum incidente de interrupção, manter suas operações em um nível aceitável, previamente definido, minimizando os impactos e recuperando perdas de ativos da informação das atividades críticas.

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: conjunto de procedimento documentados que orientam a organização, após a interrupção, em como responder, recuperar, retomar e restaurar para um nível predefinido de operação, composto 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*): ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada.

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

4.13. Sistema de Gestão de Segurança da Informação (SGSI) - processo que representa a gestão do Macroprocesso de Gestão de Segurança da Informação, englobando todas as atividades realizadas pela Coordenadoria de Segurança da Informação e Proteção de Dados para um biênio.

5. Diretrizes

5.1. A gestão de continuidade de TIC visa a:

5.1.1. Reduzir o risco de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas do TRT4, minimizando o impacto decorrente de tais eventos adversos.

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 TRT4.

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, de forma a nortear as estratégias de continuidade.

5.3. Será elaborado o Plano de Continuidade de TIC, com vistas a documentar os procedimentos necessários à operação em nível de contingência e as 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.

5.5. Em decorrência de um desastre poderá ser acionado o Protocolo de Gerenciamento de Crises Cibernéticas do TRT4.

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 avaliação da necessidade de criação, exclusão ou revisão dos planos já instituídos, seja em virtude do tempo decorrido desde sua aprovação, seja em razão de mudanças no ambiente tecnológico, 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 aprovação dos planos, seu armazenamento e divulgação; além da realização de testes dos Planos.

6.1.3. Encerramento - compreende a análise dos incidentes críticos ocorridos (desastres), a identificação das oportunidades de melhoria e seu encaminhamento à consideração superior, via SGSI, 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.

6.3. O processo será revisto anualmente ou em menor prazo, quando necessário, 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 máximo a cada 2 anos, conforme escopo definido no processos de Gestão de Continuidade de TIC 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.

7.5. 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.

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

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

7.8. 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

8.1. 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.