ANEXO À PORTARIA Nº 1.796/STI, DE 11 DE JUNHO DE 2019.

NORMA COMPLEMENTAR Nº 1

GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

CAPÍTULO I
DAS DEFINIÇÕES

Art. 1º Para os fins desta Portaria, consideram-se:

I - Análise de Impacto nos Negócios (AIN): análise que visa a estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho da ANAC, bem como as técnicas para quantificar e qualificar esses impactos, possibilitando, também, a definição da criticidade dos processos de negócio suportados pelos serviços de TI, 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.

II - Atividades Críticas: atividades que devem ser executadas de forma a garantir a entrega dos produtos e consecução dos serviços fundamentais da ANAC, de tal forma que permitam atingir os seus objetivos.

III - Ativo Crítico de Tecnologia da Informação e Comunicações: é todo aquele relacionado aos objetivos estratégicos da ANAC e que afeta a missão da Agência se for revelado, modificado, destruído ou mal-usado, ou seja, é o ativo requerido para executar as atividades-fim e de suporte da Instituição, bem como para desempenhar outras atividades essenciais para o alcance da sua missão.

IV - Ativos de Tecnologia da Informação e Comunicações: constituem os meios de armazenamento, transmissão e processamento, os sistemas de informação e os locais onde se encontram esses meios, bem como as pessoas que a eles têm acesso;

V - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI - Gestão de Continuidade de Serviços de TI: processo de gestão global que identifica as potenciais ameaças para os sistemas e serviços de Tecnologia da Informação e os impactos nas operações que essas ameaças, se concretizadas, poderiam causar, fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;

VII - Gestão de Risco: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

VIII - Gestores de Soluções de Tecnologia da Informação e Comunicação: representantes das unidades organizacionais formalmente designados como responsáveis pela gestão das soluções de TIC da ANAC;

IX - Incidente de Segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

X - Plano de Continuidade de Serviços de TI – PCSTI: documentação dos procedimentos e informações necessárias para que a ANAC mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, num nível mínimo previamente definido, em casos de incidentes;

XI - Plano de Gerenciamento de Incidentes – PGI: plano de ação definido e documentado para ser usado quando ocorrer um incidente. O Plano deve abordar os meios "pessoas, recursos, serviços e outras ações" que sejam necessários para implementar o processo de gerenciamento de incidentes;

XII - Plano de Recuperação de Serviços de TI – PRSTI: documentação dos procedimentos e informações necessárias para que a ANAC operacionalize o retorno das atividades críticas à normalidade;

XIII - Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

XIV - RTO (*Recovery Time Objective*): tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre;

XV - Solução de TIC: conjunto de sistemas, bens e serviços de TIC e automação que, com sua construção ou contratação, se integram para o alcance das necessidades da ANAC; e

XVI - Tratamento de Incidentes de Segurança em Redes Computacionais: consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e, também, identificar tendências.

CAPÍTULO II
DAS COMPETÊNCIAS

Art. 2º Constituem objetivos desta Norma:

I - estabelecer as diretrizes para garantir a disponibilidade necessária aos processos de negócios e recursos tecnológicos e humanos, de forma ordenada, assegurando a continuidade dos negócios e serviços de TI essenciais da ANAC;

II - definir orientações para a implementação de controles para a recuperação de ativos de TI, por intermédio de ações de prevenção, resposta e recuperação, de forma ordenada, assegurando a continuidade dos serviços de TI essenciais da ANAC; e

III - atribuir papéis e responsabilidades aos envolvidos nas ações necessárias para minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas nos serviços de TI.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 3º Constituem princípios do Processo de Gestão de Continuidade de Serviços de TI da ANAC:

I - implementar uma estrutura documental definida para a capacidade contínua da Gestão de Continuidade de Serviços de TI;

II - assegurar-se de que as atividades destinadas à Gestão de Continuidade de Serviços de TI sejam implementadas e conduzidas de modo controlado e conforme o planejado;

III - alcançar a resiliência necessária à continuidade de negócios que seja apropriada ao seu tamanho, à sua complexidade e à sua natureza; e

IV - atender às expectativas dos seus usuários e demais partes interessadas, demonstrando a capacidade para administrar uma interrupção no negócio e proteger a imagem da Agência.

CAPÍTULO IV
DA ESTRUTURA DOCUMENTAL

Art. 4º A estrutura documental para a Gestão de Continuidade de Serviços de TI será organizada pelos seguintes Planos:

I - Plano de Continuidade de Serviços de TI;

II - Plano de Gerenciamento de Incidentes; e

III - Plano de Recuperação de Serviços de TI.

Parágrafo único. Os documentos que compõem a Gestão de Continuidade de Serviços de TI devem ser revistos sempre que houver mudança significativa nos ativos críticos da ANAC.

CAPÍTULO V
DAS DIRETRIZES

Art. 5º A Gestão da Continuidade de Serviços de TI obedecerá às seguintes diretrizes:

I - as ações relativas à Gestão de Continuidade de Serviços de TI devem estar em conformidade com a Política de Backup e Política de Gestão de Riscos da ANAC, e com toda a legislação aplicável à Administração Pública Federal.

II - deverão ser adotados planos proativos, de forma a viabilizar que os sistemas de informação que sustentam as atividades críticas da ANAC sejam recuperados e tenham sua continuidade assegurada, por meio da manutenção de estratégias e planos de recuperação viáveis;

III - devem ser previstos e destinados o tempo, o capital e os recursos necessários para assegurar que a cultura de Continuidade de Serviços de TI seja disseminada e compreendida por toda a Agência, por meio de campanhas de conscientização que envolvam os executores de todos os processos que são suportados pela Gestão da Continuidade de Serviços de TI da ANAC;

IV - devem-se realizar exercícios e testes periódicos na execução dos Planos de Continuidade de Serviços de TI, de Gerenciamento de Incidentes e de Recuperação de Serviços de TI, com o levantamento das dificuldades e das necessidades de ajuste;

V - as atividades de Gestão de Continuidade de Serviços de TI devem ser monitoradas regularmente e o progresso no desenvolvimento da cultura e das estratégias de continuidade de negócios em toda a Agência deve ser avaliado como base para a melhoria contínua da Governança de Tecnologia da Informação e Comunicação;

VI - periodicamente, deve-se realizar a manutenção dos Planos, promovendo as revisões consideradas necessárias por ocasião dos testes realizados e da avaliação do progresso das estratégias e da cultura;

VII - a gestão dos processos, das atividades e dos produtos relativos à Gestão de Continuidade de Serviços de TI deve ser realizada com foco na melhoria contínua;

VIII - deve-se promover a gestão dos ativos de informação críticos que compõem a Gestão de Continuidade de Serviços de TI, o que inclui as pessoas, os processos, a tecnologia e o ambiente interno e externo à ANAC;

IX - deve-se realizar o gerenciamento dos Riscos à Continuidade de Serviços de TI de maneira aderente à Política de Gestão de Riscos da ANAC;

X - deve-se realizar a Análise de Impacto nos Negócios da ANAC suportados pelos Serviços de TI;

XI - deve-se realizar nova AIN sempre que houver atualização desta norma ou quando se julgar necessário;

XII - a Gestão de Continuidade de Serviços de TI deve observar o resultado da Análise de Riscos de Serviços de TI e da Análise de Impacto de Negócio realizadas, de forma a nortear as estratégias de continuidade;

XIII - os incidentes devem ser contidos ou solucionados dentro de prazos estabelecidos, minimizando os impactos e buscando assegurar que o nível de serviço prestado pela ANAC junto ao seu público externo e interno seja percebido como aceitável; e

XIV - os contratos firmados com empresas terceirizadas que suportem atividades críticas devem conter cláusula que prevejam que as referidas empresas possuam Planos de Continuidade dos seus Negócios.

CAPÍTULO VI
DO PROCESSO DE GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TI

Art. 6º O processo de Gestão de Continuidade de Serviços de TI da ANAC é composto pelas seguintes etapas:

I - Planejamento - compreende a análise dos processos críticos para o negócio, a fim de estabelecer quais atividades da Superintendência de Tecnologia de Informação são essenciais para o negócio, quais deverão ser tratadas na Continuidade de Serviços de TI e quais estratégias serão utilizadas durante a ocorrência de um incidente, podendo compreender também a avaliação da necessidade de revisão dos planos já instituídos, seja em virtude do tempo decorrido desde a sua aprovação, seja em razão de mudanças nos ativos de informação, procedimentos ou testes realizados;

II - Execução - abrange a elaboração ou revisão dos planos, 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 planos), a aprovação dos planos, seu armazenamento e divulgação;

III - Verificação - abrange a realização de testes periódicos dos Planos desenvolvidos e a análise dos incidentes críticos ocorridos (desastres), a fim de prover as informações necessárias na etapa de Melhoria; e

IV - Melhoria - compreende a identificação das oportunidades de melhoria com vistas a dar início a um novo ciclo do processo e consequente atualização dos planos.

Art. 7º O Processo de Gestão de Continuidade de Serviços de TI será acionado quando verificadas interrupções parciais ou totais que impactem as atividades críticas da ANAC, previstos nos incisos seguintes:

I - Ocorrido o incidente, considerados os serviços, sistemas ou ativos de TIC afetados e a criticidade, a Superintendência de Tecnologia da Informação acionará os Plano de Continuidade de Serviços de TI para a manutenção da continuidade das atividades, ainda que de forma contingencial e, se for o caso, os Plano de Recuperação de Serviços de TI para retorno das atividades à normalidade e o Plano de Gerenciamento de Incidentes para a execução do plano de ação;

II - A comunicação às partes interessadas observará as orientações contidas no Plano de Gerenciamento de Incidentes de TI;

III - Os ativos e serviços de tecnologia da informação e comunicações afetados pelo incidente serão monitorados pela ETIR, a fim de subsidiar o fornecimento de informações ao Superintendente de Tecnologia da Informação; e

IV - A execução do Plano de Continuidade de Serviços de TI será encerrada quando da comunicação de retorno à normalidade dos serviços, sistemas ou ativos críticos afetados.

CAPÍTULO VII
DAS RESPONSABILIDADES

Art. 8º A Superintendência de Tecnologia da Informação terá as seguintes responsabilidades:

I - elaborar e revisar o Plano de Continuidade de Serviços de TI;

II - elaborar e revisar o Plano de Gerenciamento de Incidentes;

III - elaborar e revisar o Plano de Recuperação de Serviços de TI;

IV - propor alterações nesta Norma Complementar;

V - realizar a avaliação dos riscos de TI;

VI - realizar, periodicamente, a Análise de Impacto nos Negócios;

VII - propor melhorias na implantação de novos controles relativos à Gestão de Continuidade de Serviços de TI;

VIII - supervisionar a elaboração, implementação, testes e atualização dos planos;

IX - desenvolver a cultura de Gestão de Continuidade de Serviços de TI; e

X - acionar o Plano de Gerenciamento de Incidentes, o Plano de Continuidade de Serviços de TI e o Plano de Recuperação de Serviços de TI.

Art. 9º Os gestores de soluções de Tecnologia da Informação e Comunicação da ANAC terão as seguintes responsabilidades:

I - contribuir para a elaboração do Plano de Continuidade de Serviços de TI, em seus aspectos não tecnológicos;

II - contribuir para a elaboração do Plano de Gerenciamento de Incidentes, em seus aspectos não tecnológicos;

III - contribuir para a elaboração do Plano de Recuperação de Serviços de TI, em seus aspectos não tecnológicos;

IV - classificar o nível minimamente operável e aceitável de cada aplicação; e

V - definir o tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre (RTO).

Art. 10. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da ANAC terá as seguintes responsabilidades:

I - contribuir para a elaboração do Plano de Gerenciamento de Incidentes, do Plano de Continuidade de Serviços de TI e do Plano de Recuperação de Serviços de TI; e

II- receber, analisar, tratar e responder às notificações relacionadas a incidentes de segurança em redes de computadores.

CAPÍTULO VIII
DAS ATUALIZAÇÕES

Art. 11. Esta Norma deve ser revisada e atualizada periodicamente, no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 12. Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e Comunicações da ANAC apoiado pelo Comitê de Tecnologia da Informação e Comunicações quando for necessário.