PORTARIA Nº 3.654/STI, DE 26 DE NOVEMBRO DE 2019.

Institui a Norma Complementar nº 6, que dispõe sobre a Gestão de Riscos de Tecnologia da Informação e Comunicações da ANAC.

O SUPERINTENDENTE DE TECNOLOGIA DA INFORMAÇÃO, considerando a deliberação da 4ª Reunião Ordinária do Comitê de Segurança da Informação e Comunicações da ANAC realizada em 9 de dezembro de 2019, e

Considerando as obrigações estabelecidas no Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

Considerando as orientações para Gestão de Segurança da Informação e Comunicações, que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta, contidas na Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008, e em suas Normas Complementares;

Considerando as recomendações constantes nas normas técnicas NBR ISO/IEC 27001:2006 – Sistema de Gestão de segurança da informação e NBR ISO/IEC 27002:2005 - Código de Práticas para a Gestão da Segurança da Informação;

Considerando as Instruções Normativas nº 114, de 9 de maio de 2017, que institui a Política de Gestão de Riscos Corporativos da ANAC, nº 120, de 22 de fevereiro de 2018, que institui a Política de Governança de Tecnologia da Informação e Comunicação – PGTIC da ANAC, e nº 128, de 6 de novembro de 2018, que institui a Política de Segurança da Informação e Comunicações da Agência Nacional de Aviação Civil - PoSIC/ANAC; e

Considerando o que consta do processo nº 00058.044684/2019-12,

RESOLVE:

Art. 1º Instituir a Norma Complementar que disciplina a Gestão de Riscos de Tecnologia da Informação e Comunicações da Agência Nacional de Aviação Civil – GRTIC/ANAC, nos termos do anexo.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

GUSTAVO SANCHES

Publicado no Boletim de Pessoal e Serviço - BPS v.14, nº 50, de 13 de dezembro de 2019.

ANEXO À PORTARIA Nº 3.654/STI, DE 26 DE NOVEMBRO DE 2019.

NORMA COMPLEMENTAR Nº 6

GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES

CAPÍTULO I
DAS DEFINIÇÕES

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

I - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

II - Apetite ao risco: nível de risco que a ANAC está disposta a aceitar na busca de seus objetivos e para agregar valor aos serviços prestados;

III - Ativo Crítico de Informação: 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 - PDCA: do inglês (Plan-Do-Check-Act), consiste em um método interativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos;

V - Proprietário do ativo de informação: refere-se a parte interessada da ANAC, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

VI - Riscos de Segurança de Tecnologia da Informação e Comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de tecnologia da informação e comunicações ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização; e

VII - Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO II
DOS OBJETIVOS E DOS PRINCÍPIOS

Art. 2º Constituem objetivos e princípios do Processo de Gestão de Riscos de Tecnologia da Informação e Comunicações da ANAC:

I - estabelecer as diretrizes para que os processos de tomada de decisão da Superintendência de Tecnologia da Informação - STI - sejam suportados por abordagens sistemáticas de identificação, avaliação e tratamento de riscos, em conformidade com os requisitos legais e do negócio; e

II - proporcionar o entendimento comum, consistente e inequívoco dos Riscos de TIC, aperfeiçoando a atuação da STI com base na identificação de oportunidades e de ameaças relacionadas aos objetivos da Agência.

Publicado no Boletim de Pessoal e Serviço - BPS v.14, nº 50, de 13 de dezembro de 2019.

III - considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura da ANAC, estando alinhadas à sua Política de Segurança da Informação e Comunicações e à sua Política de Gestão de Riscos Corporativos;

IV - assegurar-se de que as atividades destinadas à GRTIC sejam implementadas e conduzidas de modo controlado e conforme o planejado;

V - produzir subsídios para a Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Serviços de TIC, nos aspectos relacionados à SIC da ANAC;

VI - estar alinhado ao modelo PDCA e modo a fomentar a sua melhoria contínua; e

VII - 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
DAS DIRETRIZES

Art. 3º A Gestão de Riscos de Tecnologia da Informação e Comunicações obedecerá às seguintes diretrizes:

I - as ações relativas à GRTIC/ANAC devem estar em conformidade com a Política de Gestão de Continuidade de Serviços de TIC e a Política de Gestão de Riscos Corporativos da ANAC, e com toda a legislação aplicável à Administração Pública Federal;

II - deve-se considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura da ANAC;

III - deverá ser contínua, tendo como principal objetivo a manutenção da segurança dos Ativos Críticos de Informação da ANAC;

IV - deverá subsidiar propostas de novos investimentos na área de SIC;

V - deverá ser interativa e evolutiva, devendo observar, para sua consecução, a capacidade operacional da infraestrutura de Gestão da Segurança da Informação da ANAC e dos seus demais recursos operacionais; e

VI - a gestão dos processos, das atividades e dos produtos relativos à GRTIC deve ser realizada com foco na melhoria contínua;

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

CAPÍTULO V
DO PROCESSO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 4º O processo de Gestão de Riscos de Tecnologia da Informação e Comunicações da ANAC é composto pelas seguintes etapas:

I - Definições Preliminares;

II - Análise/Avaliação dos Riscos de TIC;

III - Plano de Tratamento dos Riscos de TIC;

IV - Aceitação de Risco de TIC;

V - Implementação do Plano de Tratamento dos Riscos de TIC;

VI - Monitoração e Análise Crítica;

VII - Melhoria do Processo de GRTIC; e

VIII - Comunicação do Risco de TIC.

Art. 5º Na fase de Definições preliminares, deve-se realizar uma análise da Agência, visando estruturar o processo de GRTIC, sendo consideradas as características da ANAC e as restrições a que está sujeita.

I - Poderão fazer parte desta etapa:

a) definir o escopo de aplicação da GRTIC. Esse escopo pode abranger a STI como um todo, uma gerência, um processo, um sistema, um recurso ou um ativo de informação;

b) adotar uma metodologia de GRTIC que atenda aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e de aceitação do risco.

Art. 6º Na fase de Análise/avaliação dos riscos de TIC, serão identificados os riscos iniciais, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados

I - Poderão fazer parte desta etapa:

a) Realizar inventário e mapeamento dos ativos de informação, no âmbito do escopo estabelecido, conforme Norma Complementar de Mapeamento e Inventário de Ativos de Informação da ANAC;

b) Identificar os riscos associados ao escopo definido;

c) Estimar os riscos levantados, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados;

d) Avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento;

e) Relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos pela STI.

Art. 7º Na fase de Plano de Tratamento dos Riscos de TIC, deve-se determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou reter o risco, observando:

I - o alinhamento com as ações de SIC já existentes;

II - as restrições organizacionais, técnicas e estruturais da ANAC;

III - requisitos legais; e

IV - a análise custo/ benefício.

Parágrafo Único: Ao final desta etapa, deve-se formular um plano para o tratamento dos riscos, relacionando, as ações de SIC, os responsáveis, as prioridades e os prazos de execução necessários à sua implantação.

Art. 8º Na fase de Aceitação de Risco de TIC, deve-se verificar os resultados do processo executado, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.

Art. 9º Na fase de Implementação do Plano de Tratamento dos Riscos de TIC, deve-se executar as ações de SIC incluídas no Plano de Tratamento dos Riscos aprovado.

Art. 10. Na fase de Monitoração e análise crítica, tem-se como objetivo detectar possíveis falhas nos resultados, monitorar os riscos, as ações de SIC e verificar a eficácia do processo de GRTIC.

I - deve-se manter os riscos monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:

a) nos critérios de avaliação e aceitação dos riscos;

b) no ambiente;

c) nos ativos de informação;

d) nas ações de SIC; e

e) nos fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).

Art. 11. A fase de Melhoria do Processo de GRTIC tem os seguintes objetivos:

I - propor à autoridade decisória da ANAC a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica.

II - executar as ações corretivas ou preventivas aprovadas; e

III - assegurar que as melhorias atinjam os objetivos pretendidos.

Art. 12. Na etapa de Comunicação do Risco de TIC, deve-se manter as instâncias superiores informadas a respeito de todas as fases da GRTIC, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas.

CAPÍTULO VI
DA ESTRUTURA PROCESSUAL

Art. 13. A abordagem sistemática do processo de Gestão de Riscos de Tecnologia da Informação e Comunicações deverá ser composta por 4 (quatro) fases:

I - planejamento: Nesta fase, estão inclusas as atividades de Definições Preliminares, Análise e avaliação dos Riscos, Plano de Tratamento dos Riscos e Aceitação dos Riscos;

II - execução: Esta fase é composta pela atividade de Implementação do Plano de Tratamento dos Riscos de TIC;

III - checagem: Esta fase é composta pela atividade de Monitoração e Análise crítica; e

IV - ação: Esta fase é composta pela atividade de Melhoria do Processo de GRTIC.

Parágrafo Único. A atividade de Comunicação é transversal a todas as fases do modelo PDCA aplicado ao processo de GRTIC/ANAC.

CAPÍTULO VII
DAS RESPONSABILIDADES

Art. 14. O Comitê de Segurança da Informação e Comunicações da ANAC terá a seguinte responsabilidade:

I - aprovar as diretrizes gerais para o Processo de GRTIC observada, dentre outros, a Política de Segurança da Informação e Comunicações e a Gestão de Riscos Corporativos da ANAC, bem como a sua missão e os seus objetivos estratégicos.

Art. 15. A Superintendência de Tecnologia da Informação terá as seguintes responsabilidades:

I - coordenar o processo de GRTIC/ANAC;

II - realizar análise/avaliação e tratamento dos riscos de tecnologia da informação;

III - desenvolver a cultura de GRTIC;

IV - analisar os resultados obtidos de controle dos níveis de SIC de cada risco de tecnologia da informação;

V - propor ajustes e de medidas preventivas e proativas ao órgão;

VI - definir o escopo do processo de Riscos de Tecnologia da Informação e Comunicações para cada ciclo de execução;

VII - propor alterações nesta Norma Complementar;

VIII - realizar, periodicamente, a Análise de Impacto nos Negócios; e

IX - propor melhorias na implantação de novos controles relativos à GRTIC.

CAPÍTULO VIII
DAS ATUALIZAÇÕES

Art. 16. 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. 17. Os casos omissos serão resolvidos pelo Comitê de Tecnologia da Informação e Comunicações apoiado pelo Comitê de Segurança da Informação e Comunicações da ANAC quando for necessário.