PORTARIA Nº 2.111/STI, DE 11 DE JULHO DE 2019.

Institui a Norma Complementar nº 3, que dispõe sobre a Gestão de Inventário e Mapeamento de Ativos de Informação da ANAC.

O SUPERINTENDENTE DE TECNOLOGIA DA INFORMAÇÃO, considerando a deliberação da 1ª Reunião Extraordinária do Comitê de Segurança da Informação e Comunicações da ANAC realizada em 4 de outubro 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 00058.025766/2019-50,

RESOLVE:

Art. 1º Instituir a Norma Complementar que disciplina a Gestão de Inventário e Mapeamento de Ativos de Informação da Agência Nacional de Aviação Civil - 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 47, de 22 de novembro de 2019.

ANEXO À PORTARIA Nº 2.111/STI, DE 11 DE JULHO DE 2019.

NORMA COMPLEMENTAR Nº 3.

GESTÃO DE INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

CAPÍTULO I
DAS DEFINIÇÕES

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

I - ativos de informação - 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;

II - 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;

III - contêineres dos ativos de informação - o contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado;

IV - custodiante do ativo de informação - refere-se a qualquer indivíduo ou estrutura da ANAC que tenha a responsabilidade formal de proteger um ou mais ativos de informação,como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação;

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; e

VI - valor do ativo de informação - valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos da ANAC, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado.

CAPÍTULO II
DOS OBJETIVOS

Art. 2º Constituem princípios do Processo de Gestão de Inventário e Mapeamento de Ativos de Informação da ANAC:

I - estabelecer as diretrizes para subsidiar a ANAC a conhecer, valorizar, proteger e manter seus ativos de informação, em conformidade com os requisitos legais e do negócio; e

III - proporcionar o entendimento comum, consistente e inequívoco dos ativos de informação, da identificação clara de seus responsáveis, de um conjunto completo de informações básicas sobre os requisitos de SIC de cada ativo de informação e da identificação do valor que o ativo de informação representa para a ANAC, nos aspectos relativos à segurança da informação.

CAPÍTULO III
DOS PRINCÍPIOS

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

I - 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;

II - assegurar-se de que as atividades destinadas à Gestão de Inventário e Mapeamento de Ativos de Informação sejam implementadas e conduzidas de modo controlado e conforme o planejado;

III - produzir subsídios para a Gestão de Segurança da Informação e Comunicações, a Gestão de Riscos de Segurança da Informação e Comunicações, e a Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações da ANAC;

IV - produzir subsídios para os procedimentos de avaliação da conformidade, de melhorias contínuas, auditoria e, principalmente, de estruturação e geração de base de dados sobre os ativos de informação;

V - 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 PROCESSUAL

Art. 4º A abordagem sistemática do processo de Gestão de Inventário e Mapeamento de Ativos de Informação deverá ser composta por 4 (quatro) subprocessos:

I - identificação de ativos de informação;

II - classificação da informação;

III - identificação de potenciais ameaças e vulnerabilidades; e

IV - avaliação de riscos associados aos ativos.

Parágrafo único. O subprocesso I será tratado nesta norma; os subprocessos "II" "III" e "IV" são objetos tratados por meio de normas específicas, abordando a Classificação da Informação e a Gestão de Riscos.

CAPÍTULO V
DAS DIRETRIZES

Art. 5º A Gestão de Inventário e Mapeamento de Ativos de Informação obedecerá às seguintes diretrizes:

I - as ações relativas à Gestão de Inventário e Mapeamento de Ativos de Informação devem estar em conformidade com a Política de Gestão de Continuidade de Serviços de TI e a Política de Gestão de Riscos 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 contínuo, tendo como principal objetivo a manutenção da segurança das Infraestruturas Críticas de Informação da ANAC;

IV - deverá subsidiar propostas de novos investimentos na área de Segurança da Informação e Comunicações;

V - deverá ser dinâmico, periódico, e estruturado, para manter a base de dados de ativos de informação atualizada e consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações;

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

VII - a gestão dos processos, das atividades e dos produtos relativos à Gestão de Inventário e Mapeamento de Ativos de Informação deve ser realizada com foco na melhoria contínua; e

VIII - deve-se promover a gestão dos ativos de informação críticos, o que inclui as pessoas, os processos, a tecnologia e o ambiente interno e externo à ANAC.

CAPÍTULO VI
DO PROCESSO DE GESTÃO DE INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 6º O processo de Gestão de Inventário e Mapeamento de Ativos de Informação da ANAC é composto pelas seguintes etapas:

I - coleta de informações gerais dos ativos de informação;

II - detalhamento dos ativos de informação;

III - caracterização dos contêineres dos ativos de informação;

IV - identificação do(s) responsável(is) - proprietário(s) e custodiante(s) de cada ativo de informação;

V - Definição dos requisitos de segurança da informação e comunicações; e

VI - Estabelecimento do valor do ativo de informação.

Art. 7º Coleta de Informações Gerais dos Ativos de Informação:

I - esta etapa consiste na definição dos responsáveis pela coleta e na utilização de um conjunto essencial de informações para cada ativo de informação.

II - poderão fazer parte do escopo do inventário os ativos de informação da ANAC relacionados a:

a) Tecnologia da Informação (equipamentos, sistemas, aplicativos, serviços e comunicação de dados);

b) Documentos Físicos e Digitais (ostensivos, sigilosos e classificados);

c) Processos de Negócio e seus Viabilizadores (recursos tangíveis e intangíveis);

Art. 8º Detalhamento dos ativos de informação:

I - o detalhamento do ativo deve contemplar informações que:

a) determinem com clareza e objetividade o conteúdo do ativo de informação;

b) identifiquem o(s) responsável(is) - proprietário(s) e custodiante(s) - de cada ativo de informação;

c) identifiquem o valor de cada ativo de informação;

d) identifiquem os respectivos requisitos de segurança da informação e comunicações dos ativos de informação.

Art. 9º Caracterização dos contêineres dos ativos de informação:

I - o contêiner deve ser caracterizado, no mínimo, com a lista de todos os recipientes em que um ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes.

II - devem ser definidos os limites do ambiente que deve ser examinado;

III - devem ser descritos os relacionamentos que necessitam ser compreendidos para atendimento das exigências de segurança da informação e comunicações.

Art. 10. Identificação do(s) responsável(is) - proprietário(s) e custodiante(s) de cada ativo de informação

I - o proprietário do ativo de informação é 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.

Art. 11. Definição dos requisitos de segurança da informação e comunicações:

I - os requisitos de segurança da informação e comunicações devem ser definidos por meio de critérios que atendam a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

II - os critérios devem ser categorizados, no mínimo, em 5 categorias de controle:

a) tratamento da informação;

b) controles de acesso físico e lógico;

c) gestão de risco de segurança da informação e comunicações;

d) tratamento e respostas a incidentes em redes computacionais; e

e) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação e comunicações.

Art. 12. Estabelecimento do valor do ativo de informação:

I - O(s) proprietário(s) do ativo da informação deve(m) indicar o valor do ativo, o qual deve refletir o quão cada ativo de informação é importante para a que organização alcance seus objetivos estratégicos, e o quão o ativo de informação é imprescindível aos interesses da sociedade e do Estado.

II - Cabe ao(s) proprietário(s) dos ativos de informação indicar o valor do ativo para o negócio da Agência, considerando fatores do(s) risco(s) aos quais os ativos possam estar expostos, como ameaça, vulnerabilidade e impacto.

CAPÍTULO VII
DAS RESPONSABILIDADES

Art. 13. O Comitê de Segurança da Informação e Comunicações da ANAC terá a seguinte responsabilidade:

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

Art. 14. O Agente Responsável terá as seguintes responsabilidades:

I - executar o processo de identificação e classificação de ativos de informação;

II - monitorar os níveis de segurança dos ativos de informação junto aos proprietários dos ativos de informação.

III - coordenar o Processo de Inventário e Mapeamento de Ativos de Informação custodiados na STI;

IV - analisar os resultados obtidos de controle dos níveis de segurança da informação e comunicações de cada ativo de informação;

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

VI - definir o escopo do inventário para cada ciclo de execução.

Art. 15. O Proprietário do Ativo de Informação terá as seguintes responsabilidades:

I - descrever o ativo de informação;

II - definir as exigências e os riscos de segurança da informação e comunicações do ativo de informação, respeitados os parâmetros técnicos estabelecidos pelo custodiante; e

III - monitorar o cumprimento das exigências de SIC.

Art. 16. O Custodiante terá as seguintes responsabilidades:

I - proteger os ativos de informação, isto é, como o ativo é armazenado, transportado e processado, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;

II - proteger os contêineres dos ativos de informação, e, consequentemente, aplicar os níveis de controles de segurança conforme as exigências de segurança da informação e comunicações, comunicadas pelo(s) proprietário(s) do(s) ativo(s) de informação; e

III - estabelecer diretrizes e parâmetros técnicos de forma a subsidiar o proprietário dos ativos de informação na definição das exigências de SIC.

CAPÍTULO VIII
DAS ATUALIZAÇÕES

Art. 17. 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. 18. 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.