PORTARIA Nº 3.646/STI, DE 25 DE NOVEMBRO DE 2019.

Institui a Norma Complementar nº 5, que dispõe sobre a Gestão de Incidentes de Segurança em Redes de Computadores 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 11 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 00058.044536/2019-90,

RESOLVE:

Art. 1º Instituir a Norma Complementar que disciplina a Gestão de Incidentes de Segurança em Redes de Computadores 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 50, de 13 de dezembro de 2019.

ANEXO À PORTARIA Nº 3.646/STI, DE 25 DE NOVEMBRO DE 2019.

NORMA COMPLEMENTAR Nº 5.

GESTÃO DE INCIDENTES DE SEGURANÇA EM REDES DE COMPUTADORES

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 - Artefato Malicioso - Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - Incidente de Segurança em redes computacionais - Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IV - 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

Art. 2º Constituem objetivos desta Norma:

I - estabelecer as diretrizes referentes à gestão de incidentes em redes de computadores da ANAC, a fim de minimizar o impacto no âmbito da segurança da informação, em conformidade com os requisitos legais e do negócio; e

II - disciplinar os processos e responsabilidades a serem observados no gerenciamento de incidentes de Segurança em Redes de Computadores realizado pela Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR da ANAC, em complemento ao disposto na Política de Segurança da Informação e Comunicações - POSIC - da Agência.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 3º Constituem princípios do Processo de Gestão de Incidentes de Segurança em Redes de Computadores da ANAC:

I - considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura da ANAC, estando alinhados à sua Política de Segurança da Informação e Comunicações;

II - assegurar de que as atividades destinadas à Gestão de Incidentes de Segurança em Redes de Computadores sejam implementadas e conduzidas de modo controlado e conforme o planejado;

III - produzir subsídios para os procedimentos de avaliação da conformidade, de melhorias contínuas, auditoria e, principalmente, gerenciamento e tratamento de Incidentes de Segurança em Redes de Computadores; e

IV - atender às expectativas dos seus usuários e demais partes interessadas, demonstrando a capacidade para administrar e/ou mitigar uma interrupção dos serviços que sustentam o negócio e proteger a imagem da Agência.

CAPÍTULO IV
DA ESTRUTURA ORGANIZACIONAL

Art. 4º A composição da ETIR/ANAC respeitará o disposto na Portaria que designa o agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR/ANAC e a sua composição, conforme normativo interno.

CAPÍTULO V
DAS DIRETRIZES

Art. 5º A Gestão de Incidentes de Segurança em Redes de Computadores obedecerá às seguintes diretrizes:

I - as ações relativas à Incidentes de Segurança em Redes de Computadores devem estar em conformidade com a Norma Complementar de Gestão de Continuidade de Serviços de TIC e a Norma Complementar de Gestão de Riscos de TIC da ANAC, e com toda a legislação aplicável à Administração Pública Federal;

II - deverá 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 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; e

VI - a gestão dos processos, das atividades e dos produtos relativos à Gestão de Incidentes de Segurança em Redes de Computadores deve ser realizada com foco na melhoria contínua.

CAPÍTULO VI
DO PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA EM REDES DE COMPUTADORES

Art. 6º O processo de Gestão de Incidentes de Segurança em Redes de Computadores da ANAC é composto pelas seguintes etapas: Preparação, Proteção e Prevenção, Detecção, Triagem e Resposta.

Art. 7º A etapa de Preparação consiste na fase inicial para a implementação de um programa de resposta a incidente de segurança de redes de computadores.

I - Poderão fazer parte do escopo desta etapa:

a) Definição de políticas de segurança, procedimentos, categorias e listas de severidade;

b) Instituição da ETIR e definição da sua composição;

c) Identificação dos papéis e responsabilidades dos envolvidos no processo; e

d) Implementação da infraestrutura de suporte, tais como sistema de registro de incidentes, ferramentas de análise de ativos de informação, canais de comunicação e demais infraestruturas necessárias.

Art. 8º A etapa de Proteção e Prevenção envolve ações para conter e evitar incidentes, realizando mudanças na infraestrutura após a detecção e durante a resposta, incluindo atividades de filtragem, bloqueio e erradicação. Esta etapa também inclui a implementação de mudanças baseadas em incidentes anteriores, reportes técnicos ou na experiência dos analistas.

I - Poderão fazer parte do escopo desta etapa:

a) varredura de vulnerabilidades;

b) implementação de recomendações da indústria e implementação de melhoras práticas de mercado; e

c) atualização das proteções de segurança nos equipamentos e softwares instalados na rede de computadores da ANAC (IDS/IPS, Firewall, Antivírus).

Art. 9º A etapa de Detecção consiste na identificação de atividades anômalas na rede, por elementos internos ou externos, que podem comprometer a disponibilidade, a integridade ou a confidencialidade das informações ou sistemas da ANAC.

I - Um evento de detecção pode ser proativo ou reativo.

Art. 10. A etapa de Triagem consiste em coletar as informações disponíveis, a fim de determinar o escopo de um incidente, seu impacto e quais ativos estão sendo afetados.

I - Poderão fazer parte do escopo desta etapa, as seguintes atividades:

a) Categorizar;

b) Priorizar;

c) Atribuir; e

d) Correlacionar o incidente com outros eventos.

Art. 11. A etapa de Resposta envolve as ações necessárias para sanar ou mitigar um incidente, analisando, coordenando e distribuindo as informações.

I - Poderão fazer parte do escopo desta etapa as respostas de cunho técnico, gerencial e legal.

CAPÍTULO VII
DAS RESPONSABILIDADES

Art. 12. O Comitê de Segurança da Informação e Comunicações da ANAC terá a seguinte responsabilidade:

I - Aprovar as diretrizes gerais para o Processo de Gestão de Incidentes de Segurança em Redes de Computadores, observada dentre outros, a Política de Segurança da Informação e Comunicações da ANAC - PoSIC/ANAC;

II - Acompanhar as investigações e as avaliações dos danos decorrentes de Incidentes de Segurança em Redes de Computadores, e em casos específicos, relatar à Diretoria da ANAC.

Art. 13. O Agente Responsável pela ETIR, em complemento ao disposto na PoSIC, terá as seguintes responsabilidades:

I - Coordenar a instituição, implementação e manutenção da infraestrutura necessária para a execução das atividades desempenhadas pela ETIR;

II - Garantir que os incidentes em Redes Computacionais da Rede de Computadores da ANAC sejam monitorados;

III - Coordenar o processo de comunicação entre a ETIR e o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov, conforme estabelece a norma complementar nº 08/IN01/DSIC/GSIPR, emitida em 9 de agosto de 2010;

IV - Adotar procedimentos de feedback para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações sejam informados dos procedimentos adotados;

V - Propor ajustes e medidas preventivas e proativas à ANAC sobre assuntos afetos a incidentes em Redes Computacionais da Rede de Computadores da Agência;

VI - Apoiar e prover os meios necessários para a capacitação e treinamentos relacionados à Segurança da Informação e Comunicação para os membros da ETIR; e

VII - Apoiar, quando demandado, no acionamento de autoridades policiais competentes para a adoção dos procedimentos legais, em casos que exijam, conforme previsto na norma complementar nº 08/IN01/DSIC/GSIPR, emitida em 9 de agosto de 2010.

Art. 14. A ETIR, em complemento ao disposto na PoSIC, terá as seguintes responsabilidades:

I - Executar as atividades de tratamento e resposta a incidentes nos sistemas informacionais e na rede de computadores da ANAC;

II - Executar, quando possível, o tratamento de artefatos maliciosos e vulnerabilidades;

III - Executar a emissão de alertas e advertências relacionadas a incidentes de SIC no âmbito da TI;

IV - Apresentar, trimestralmente, para o STI, de forma proativa, vulnerabilidades e incidentes críticos de segurança em redes de computadores;

V - Efetuar, de acordo com a maturidade da equipe, análises da infraestrutura de segurança em redes de computadores da organização com base nas necessidades da Agência e nas melhores práticas do mercado;

VI - Executar tarefas que viabilizem ou facilitem a detecção e prevenção de intrusão;

VII - Disseminar informações relacionadas à segurança, que sejam ostensivas, e que facilitem a pesquisa e utilização por todos os membros da ETIR;

VIII - Observar os procedimentos de forense digital para registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes; e

IX - Apoiar tecnicamente na elaboração de políticas, normas, notas técnicas e procedimentos direcionados à segurança da informação e comunicações no âmbito da ANAC.

Art. 15. As Unidades Organizacionais terão as seguintes responsabilidades:

I - informar imediatamente à Superintendência de Tecnologia da Informação todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes na rede de computadores da ANAC, sobre os quais venham a tomar conhecimento; e

II - definir seus procedimentos internos em observância à esta Norma Complementar.

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.