INSTRUÇÃO NORMATIVA Nº 128, DE 6 DE NOVEMBRO DE 2018.

Aprova a Política de Segurança da Informação e Comunicações - PoSIC no âmbito da Agência Nacional de Aviação Civil - ANAC.

A DIRETORIA DA AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL - ANAC, no exercício das competências que lhe foram outorgadas pelo arts. 11, inciso IX, da Lei nº 11.182, de 27 de setembro de 2005, e 24 do Anexo I do Decreto nº 5.731, de 20 de março de 2006, e

Considerando o disposto no Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

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 GSI/PR nº 01, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, e em suas Normas Complementares;

Considerando a previsão constante no art. 37 da Instrução Normativa nº 80, de 26 de novembro de 2014, de revisão periódica da Política de Segurança da Informação e Comunicações; e

Considerando o que consta do processo nº 00058.014301/2018-92, deliberado e aprovado na 3ª Reunião Administrativa Extraordinária da Diretoria, realizada em 6 de novembro de 2018,

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicações da Agência Nacional de Aviação Civil - PoSIC/ANAC.

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os fins desta Instrução Normativa, considera-se:

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

II - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

IV - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

V - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade autorizada;

VI - gestão de continuidade de negócio: sistema de gestão que objetiva responder eficazmente a ocorrências que possam interromper o funcionamento normal de uma organização;

VII - Gestão de Segurança da Informação e Comunicações - GSIC: sistema de gestão corporativo voltado para a Segurança da Informação e Comunicações - SIC, que inclui toda a abordagem organizacional usada para proteger os sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como a abordagem destinada a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

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

IX - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

X - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XI - não-repúdio: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;

XII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XIII - recursos computacionais: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, computadores, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura; e

XIV - 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 ação interna de segurança da informação.

CAPÍTULO II
DOS OBJETIVOS, DA ABRANGÊNCIA E DA APLICABILIDADE

Art. 3º São objetivos da PoSIC/ANAC:

I - preservar a disponibilidade, integridade, confidencialidade e autenticidade das informações mantidas e tratadas pela ANAC;

II - dotar a ANAC de instrumentos jurídicos, normativos e organizacionais que a capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

IV - estabelecer normas e procedimentos necessários à efetiva implementação da segurança da informação; e

V - promover as ações necessárias à implementação e manutenção da segurança da informação.

Art. 4º A PoSIC/ANAC aplica-se no âmbito da Agência, englobando todos os servidores, colaboradores, fornecedores, prestadores de serviços e estagiários que, oficialmente, executem atividades vinculadas à atuação institucional e, no que couber, ao relacionamento da Agência com agentes credenciados, órgãos e entidades públicos ou privados.

CAPÍTULO III
DA ESTRUTURA NORMATIVA

Art. 5º A estrutura normativa que norteará a Gestão de Segurança da Informação e Comunicações da Política de Segurança da Informação e Comunicações da ANAC - GSIC/ANAC será organizada da seguinte forma:

I - Política de Segurança da Informação e Comunicações - PoSIC: define as regras e diretrizes de alto nível, que representam os princípios básicos incorporados pela ANAC à sua gestão, de acordo com sua visão estratégica, servindo como base para que as normas complementares e os procedimentos internos sejam criados e detalhados;

II - normas complementares de SIC: contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas na PoSIC/ANAC, apresentando os controles que deverão ser implementados para alcançar a estratégia estabelecida; e

III - procedimentos internos de SIC: instrumentalizam o disposto na PoSIC/ANAC e nas normas complementares, viabilizando sua aplicação imediata nas tarefas operacionais da Agência.

CAPÍTULO IV
DAS DIRETRIZES

Art. 6º A GSIC/ANAC observará às seguintes diretrizes gerais:

I - estabelecer e promover ações para garantir a confidencialidade, integridade, autenticidade, não-repúdio e disponibilidade das informações da ANAC, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado;

II - mitigar os riscos associados aos ativos da informação utilizados pelos servidores, colaboradores, estagiários e público externo da ANAC;

III - prever a aplicação de penalidades em caso de descumprimento dos dispositivos definidos nesta PoSIC e nas Normas Complementares; e

IV - definir as atribuições e responsabilidades relativas ao processo de promoção e aplicação da PoSIC/ANAC.

Art. 7º Deverão ser publicadas, por meio de portaria, normas complementares que obedeçam às diretrizes específicas abaixo, organizadas pelos seguintes pilares de ativo da informação:

I - tecnologia: versará, no mínimo, sobre os seguintes temas:

a) cópias de segurança: diretrizes para a realização de cópia de segurança (Backup) e de restauração dos dados (Restore) corporativos ou que são custodiados pela ANAC, visando assegurar a segurança das informações, conforme as propriedades de confidencialidade, integridade e disponibilidade dos ativos de informação, definindo estratégias e orientações para a implementação de controles relativos ao tema e atribuindo papéis e responsabilidades aos envolvidos nas ações de cópia e restauração de dados;

b) computação em nuvem: diretrizes para utilização de serviço de computação em nuvem, considerando a legislação e as boas práticas vigentes, o processo de tratamento da informação, os controles de acesso, físicos e lógicos, a localização geográfica e o modelo de serviço e de implementação de computação em nuvem a serem adotados pela ANAC;

c) criptografia: diretrizes para o uso de recursos criptográficos para as informações que tenham sido classificadas em qualquer grau de sigilo; e

d) desenvolvimento e obtenção de software seguro: o processo de desenvolvimento de software deverá conter regras que permitam a segurança das aplicações no que diz respeito aos acordos de licenciamento, propriedade dos códigos e direitos de propriedade intelectual, bem como os requisitos de documentação específicos de segurança para as aplicações a serem adquiridas ou desenvolvidas interna ou externamente.

II - pessoas: versará, no mínimo, sobre os seguintes temas:

a) uso de dispositivos móveis: deverão ser adotados controles para o uso adequado de dispositivos móveis corporativos ou particulares por servidores, colaboradores e visitantes da ANAC;

b) acesso à internet: o acesso à internet deverá englobar a esfera profissional com conteúdo relacionado às atividades da ANAC, observando-se sempre a conduta compatível com os princípios definidos nesta PoSIC. Para tanto a ANAC deverá estabelecer controles de acesso à Internet, com o objetivo de evitar que os recursos computacionais sejam utilizados em desrespeito às leis, aos costumes e à dignidade da pessoa humana;

c) uso de e-mail: deverão ser definidas regras claras e precisas de uso do e-mail institucional, com o objetivo de evitar o seu mau uso ou violação à imagem da ANAC;

d) segurança em recursos humanos: a segurança dos recursos humanos deverá ser consolidada por meio de ações que promovam a cultura, sensibilização, conscientização, educação e treinamento em SIC no âmbito da ANAC;

e) uso de redes sociais: o uso seguro das redes sociais deverá ter como referência os objetivos estratégicos da ANAC, os critérios, as limitações e a estratégia de comunicação social, o processo de gestão de conteúdo e as responsabilidades na gestão de seu uso; e

f) controle de acesso: os computadores e sistemas da ANAC deverão possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação deverá ser claramente definido e registrado.

III - processos: versará, no mínimo, sobre os seguintes temas:

a) gestão de mudanças: terá como base a metodologia de gestão de processos da ANAC e deverá garantir que as mudanças na organização, nos processos de negócio, nos recursos de processamento da informação e nos sistemas não afetem a segurança da informação da ANAC;

b) gestão de riscos: orientar na formulação das ações de mitigação de riscos, com o objetivo de reduzir as vulnerabilidades, evitar ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos de informação da ANAC, observada a Política de Gestão de Riscos da ANAC;

c) gestão de continuidade de negócios: orientar na formulação das ações de gestão de continuidade, com o objetivo de identificar ameaças e possíveis impactos na continuidade dos processos e serviços essenciais para o funcionamento da ANAC;

d) registro de eventos e trilhas de auditoria: implementar mecanismos de registro de eventos e auditoria, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação;

e) conformidade legal: estabelecer mecanismos para avaliação de conformidade nos aspectos relativos às normas de Segurança da Informação e Comunicações em vigor, com o objetivo de identificar, organizar e armazenar a legislação, regulamentação e contratos relevantes aos processos de trabalho da ANAC, bem como preservar a conformidade contratual, o direito autoral e a propriedade intelectual das informações e recursos utilizados nestes processos de trabalho;

f) tratamento de incidentes de rede: a ANAC deverá manter equipe de tratamento e resposta a incidentes em redes computacionais, com objetivo de registrar, analisar e tratar incidentes de SIC por meio da coleta de evidências, investigação de ataques, provimento de assistência local e remota e intermediação da comunicação entre as partes envolvidas;

g) tratamento da informação: a informação utilizada pela ANAC deverá ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade e autenticidade. A ANAC deverá estabelecer medidas e procedimentos de tratamento e classificação da informação, respeitando a legislação vigente; e

h) gestão de ativos da informação: o processo de Inventário e Mapeamento de Ativos de Informação deverá considerar, prioritariamente, os objetivos estratégicos da ANAC, os processos e os requisitos legais, a fim de 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.

IV - ambiente: versará, no mínimo, sobre os seguintes temas:

a) segurança física e do ambiente: as instalações de processamento das informações críticas ou sensíveis deverão ser prevenidas contra acesso não autorizado e mantidas em áreas seguras, protegidas por perímetros de segurança, conter barreiras de segurança e controles de acesso apropriados; e

b) controles de acesso: deverão ser adotados controles de entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança e habilitando o acesso apenas de pessoal autorizado. No caso de sistemas críticos, convém que sejam criados ambientes reservados, de uso exclusivo, para abrigá-los.

CAPÍTULO V
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º Compete à Diretoria:

I - aprovar alterações na PoSIC; e

II - estabelecer diretrizes, prioridades e ações específicas de SIC.

Art. 9º O Comitê de Segurança da Informação e Comunicações - CSIC/ANAC será composto pelos seguintes membros:

I - Superintendente de Administração e Finanças;

II - Superintendente de Tecnologia da Informação;

III - Superintendente de Planejamento Institucional;

IV - Superintendente de Gestão de Pessoas; e

V - Superintendente de Ação Fiscal.

Art. 10. Compete ao CSIC/ANAC:

I - orientar as Unidades Organizacionais quanto à implementação das ações de SIC;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

III - propor alterações na PoSIC/ANAC;

IV - aprovar normas complementares relativas à SIC, em conformidade com os normativos existentes;

V - promover cultura de SIC;

VI - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

VII - propor recursos necessários às ações de SIC;

VIII - solicitar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na SIC;

IX - convidar para participar das reuniões do Comitê, representantes de outras Unidades Organizacionais; e

X - definir, por meio de portaria, as regras de funcionamento e demais questões de ordem operacional relativos ao CSIC/ANAC.

§ 1º A propositura das normas complementares de que trata o inciso I do art. 7º desta Instrução Normativa referentes ao pilar de Tecnologia e o acompanhamento das atividades da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR/ANAC, ficarão sob a responsabilidade do Comitê de Tecnologia da Informação - CTI/ANAC.

§ 2º O CSIC/ANAC e o CTI/ANAC deverão manter contato permanente, a fim de assegurar o alinhamento de suas diretrizes e ações.

§ 3º O CSIC/ANAC apresentará anualmente à Diretoria um Plano de Ações de SIC, incluindo cronograma e entregas a serem realizadas no ano seguinte à sua publicação.

§4º O Plano de Ações de SIC conterá a relação das normas complementares de SIC a serem atualizadas ou publicadas, quando couber, as atividades relacionadas a SIC a serem desenvolvidas, bem como relatório de execução do plano anterior.

§5º Quando necessário, caberá ao Gestor de Segurança da Informação e Comunicações da ANAC viabilizar a inclusão das atividades necessárias ao cumprimento do Plano de Ações de SIC nos planos específicos da ANAC.

Art. 11. As Unidades Organizacionais terão as seguintes responsabilidades:

I - definir seus procedimentos internos em observância à PoSIC e suas normas complementares; e

II - cumprir a PoSIC, as normas complementares e os procedimentos internos de SIC da ANAC.

Art. 12. O Gestor de Segurança da Informação e Comunicações terá as seguintes responsabilidades:

I - presidir o CSIC/ANAC;

II - manter contato permanente com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para tratar de assuntos relativos à segurança da informação e comunicações; e

III - reportar à Diretoria, nos casos em que entender necessário, as principais ocorrências relacionadas à SIC.

IV - manter a PoSIC e suas normas complementares disponíveis na página da intranet da ANAC, respeitadas a classificação de níveis de acesso.

Parágrafo único. O Diretor-Presidente da ANAC designará, por meio de portaria, o Gestor de Segurança da Informação e Comunicações da ANAC.

Art. 13. A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR/ANAC terá as seguintes responsabilidades:

I - receber, analisar e responder às notificações relacionadas a incidentes de segurança em redes de computadores;

II - recolher provas imediatamente após a ocorrência de um incidente de SIC;

III - executar análise crítica sobre os registros de falha para assegurar que foram satisfatoriamente resolvidas;

IV - investigar as causas dos incidentes de SIC;

V - implementar mecanismos para permitir a quantificação e o monitoramento dos tipos, volumes e custos de incidentes e falhas de funcionamento;

VI - indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes; e

VII - apresentar trimestralmente ao CTI/ANAC, bem como ao CSIC/ANAC, quando solicitado, relatório de suas atividades.

§ 1º Caberá ao presidente do CTI/ANAC designar o agente responsável pela ETIR/ANAC e a sua composição.

§ 2º O agente responsável pela ETIR/ANAC definirá, em ato próprio, o funcionamento da ETIR/ANAC.

§3º Em casos de ameaças, incidentes ou quebra de segurança que exponham a riscos os sistemas e serviços da ANAC, o agente responsável pelo ETIR/ANAC poderá convocar, em caráter emergencial, servidores da Agência que tenham conhecimento para atuar.

CAPÍTULO VI
DAS PENALIDADES

Art. 14. O descumprimento das disposições constantes nesta Política e nas normas complementares sobre segurança da informação e comunicações caracteriza violação de dever funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades civil e penal.

CAPÍTULO VII
DAS ATUALIZAÇÕES

Art. 15. Esta Política deve ser revisada e atualizada periodicamente, no máximo a cada 3 (três) anos.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 16. A PoSIC, bem como as normas complementares dela decorrentes, deverão estar alinhadas à Política de Gestão de Riscos Corporativos da ANAC.

Art. 17. Os casos omissos serão resolvidos pela Diretoria.

Art. 18. Fica revogada a Instrução Normativa nº 80, de 26 de novembro de 2014, publicada no Boletim de Pessoal e Serviço - BPS v.9, nº 48, de 28 de novembro de 2014.

Art. 19. Esta Instrução Normativa entra em vigor na data de sua publicação.

JOSÉ RICARDO PATARO BOTELHO DE QUEIROZ
Diretor-Presidente

Publicado no Boletim de Pessoal e Serviço - BPS v.13, nº 45, de 9 de novembro de 2018.