INSTRUÇÃO NORMATIVA Nº 80, DE 26 DE NOVEMBRO DE 2014.

Institui 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 da competência que lhe foi outorgada pelo art. 11, inciso IX, da Lei nº 11.182, de 27 de setembro de 2005, tendo em vista o disposto no art. 5º, inciso VII, da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e considerando o que consta do processo nº 00058.015036/2012-74, deliberado e aprovado na Reunião Administrativa de Diretoria realizada em 26 de novembro de 2014,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação e Comunicações - PoSIC, que estabelece as diretrizes para o tratamento a ser dado às informações produzidas, processadas, transmitidas ou armazenadas no âmbito da Agência Nacional de Aviação Civil - ANAC.

CAPÍTULO I
DOS CONCEITOS

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

I - agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: servidor público ocupante de cargo efetivo incumbido de chefiar e gerenciar a ETIR;

II - ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III - ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - atributos básicos de segurança da informação e comunicações: disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade (não-repúdio), privacidade e primariedade da informação;

V - autenticidade: qualidade da informação quanto à certeza de que tenha sido produzida, expedida, recebida ou modificada por fonte anunciada;

VI - capacitação em SIC: habilitação no conhecimento de segurança da informação e comunicações que permite a um indivíduo aplicá-lo na rotina pessoal e profissional, atuar como multiplicador do tema e utilizar seus conceitos e procedimentos na organização;

VII - Comitê de Segurança da Informação e Comunicações - CSIC: grupo de servidores responsável pela proposição de normas e supervisão da segurança da informação e comunicações;

VIII - confidencialidade: princípio no qual somente pessoas devidamente autorizadas devem ter acesso à informação;

IX - conscientização em SIC: habilitação no conhecimento de segurança da informação e comunicações que permite a um indivíduo aplicá-lo na rotina pessoal e profissional e atuar como multiplicador do tema;

X - controle: qualquer ação tomada pela organização para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados;

XI - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XII - CTIR.GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSI/PR;

XIII - disponibilidade: qualidade que garante que a informação esteja sempre disponível para ser utilizada por indivíduos, equipamentos ou sistemas autorizados;

XIV - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: grupo de servidores responsável por receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito da ANAC;

XV - especialização em SIC: habilitação no conhecimento de segurança da informação e comunicações que permite a um indivíduo aplicá-lo na rotina pessoal e profissional, atuar como multiplicador do tema, utilizar seus conceitos e procedimentos na organização como gestor de SIC e tornar-se referência na pesquisa e aplicação de SIC;

XVI - gestão da informação: processo que consiste na aplicação de técnicas e conhecimentos em atividades de busca, identificação, classificação, processamento, armazenamento e disseminação de informações, independentemente do formato ou meio em que se encontra, com o objetivo de subsidiar o processo de tomada de decisões, observando os atributos básicos de segurança na manutenção de níveis mínimos de confiabilidade;

XVII - gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção dos controles desses ativos;

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

XIX - gestão de operações e comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporta, satisfazendo aos requisitos mínimos de qualidade;

XX - gestão de riscos de segurança da informação e comunicações - GRSIC: 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;

XXI - Gestão de Segurança da Informação e Comunicações - GSIC: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

XXII - Gestor de SIC: servidor designado pelo Diretor-Presidente como responsável pela gestão de segurança da informação e comunicações no âmbito da ANAC;

XXIII - incidente de SIC: evento simples ou série de eventos indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

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

XXV - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

XXVI - infraestrutura de TI: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XXVII - integridade: qualidade da informação quanto à garantia de não ter sido alterada de forma não autorizada ou indevida;

XXVIII - irretratabilidade ou não-repúdio: suficiente evidência a respeito da origem, submissão, entrega e integridade da informação, fornecendo garantia que possa ser verificado por quaisquer terceiros interessados, a qualquer tempo e que não podem ser subsequentemente refutados;

XXIX - Órgãos Governantes Superiores - OGS: são aqueles que têm a responsabilidade por normatizar e fiscalizar o uso e a gestão de TI em seus respectivos segmentos da Administração Pública Federal;

XXX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações;

XXXI - privacidade: informação que deve ser acessada somente pelo seu dono;

XXXII - proteção da informação: atribuição de níveis de segurança a dado, informação, documento, material, área ou instalação, de forma a assegurar o nível adequado de proteção, em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização;

XXXIII - recursos criptográficos: sistemas, programas, processos e equipamentos que utilizam função matemática para realizar a cifração de conteúdo, tornando-o ininteligível, e a decifração (reversão do processo de cifração);

XXXIV - risco de SIC: evento que pode gerar impacto negativo no negócio da organização, associado ao seu potencial de ocorrência;

XXXV - segurança da informação: modelo de conceitos e procedimentos relacionados à proteção da informação no sentido de preservar o valor que possui para um indivíduo ou uma organização e garantir a continuidade do negócio;

XXXVI - segurança física e do ambiente: conjunto de aspectos de segurança que trata da proteção dos ativos físicos da instituição, englobando instalações físicas de acesso restrito ou público em todas as localidades em que a organização está presente;

XXXVII - sensibilização em SIC: habilitação no conhecimento de segurança da informação e comunicações que permite a um indivíduo aplicá-lo na rotina pessoal e profissional;

XXXVIII - tratamento de incidentes: metodologia organizada para gerir consequências de uma violação de segurança da informação;

XXXIX - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, armazenamento, eliminação, avaliação, destinação ou controle da informação, inclusive as sigilosas; e

XL - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO II
DOS OBJETIVOS

Art. 3º A PoSIC objetiva garantir a disponibilidade, integridade, confidencialidade e autenticidade - DICA das informações produzidas, transmitidas ou custodiadas pela ANAC.

Parágrafo único. Para alcance desses objetivos, deverão ser observados os demais atributos básicos de segurança da informação e comunicações.

Art. 4º A PoSIC visa estabelecer as diretrizes a serem seguidas na abordagem de segurança da informação e comunicações na ANAC, orientando e esclarecendo os seus princípios e controles, no que concerne à sua regulamentação e conscientização na Agência.

Art. 5º As diretrizes, normas complementares, manuais e procedimentos decorrentes da PoSIC aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a esta Agência.

Art. 6º Esta PoSIC se aplica, no que couber, ao relacionamento da ANAC com órgãos e entidades públicos ou privados.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Art. 7º As diretrizes de Segurança da Informação e Comunicações - SIC devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura da ANAC.

Art. 8º Cabe à ANAC fazer a gestão do conhecimento em SIC, instituindo programas permanentes e regulares de conscientização, sensibilização e capacitação, buscando parcerias com outros órgãos e entidades e zelando pela preservação e agregação do conhecimento.

Art. 9º A ANAC deve observar as diretrizes emanadas pelos Órgãos Governantes Superiores - OGS e suas normas complementares como modelos de referência em SIC.

Art. 10. A estrutura de suporte à Gestão de Segurança da Informação e Comunicações - GSIC será composta pelo Gestor de SIC, pelo Comitê de Segurança da Informação e Comunicações - CSIC e pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR.

Parágrafo único. Cabe ao Gestor de SIC, com o apoio da área responsável pela gestão da informação da ANAC, a gestão e a coordenação das atividades da GSIC.

Art. 11. A GSIC deve auxiliar a administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da Agência e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Seção I
Da Gestão da Informação

Art. 12. A gestão da informação é essencial para a eficiência dos processos de SIC e deve ser implementada por meio de uma estrutura apropriada de planejamento integrado, de desenvolvimento de procedimentos, de implantação e utilização de tecnologia e recursos.

CAPÍTULO IV
DAS DIRETRIZES ESPECÍFICAS

Art. 13. A aplicação de cada uma das diretrizes constantes das seções deste capítulo deverá ser realizada após a elaboração e publicação de normas, manuais e procedimentos.

Parágrafo único. A implementação do disposto neste capítulo é um processo contínuo e estratégico visando à melhoria da SIC.

Seção I
Da Gestão de Ativos de Informação

Art. 14. Os ativos de informação devem ser protegidos contra ameaças e vulnerabilidades de acordo com sua relevância, criticidade e sensibilidade, considerando os atributos básicos de segurança da informação.

Seção II
Da Proteção da Informação

Art. 15. A informação, independente do seu formato, deverá ser protegida contra utilização ou divulgação indevidas.

Art. 16. A informação sigilosa será classificada de acordo com a legislação em vigor.

Art. 17. Deverão ser definidos níveis de proteção e controles a serem implementados durante o ciclo de vida da informação contemplando manuseio, armazenamento, transporte e descarte.

Seção III
Da Gestão de Riscos

Art. 18. Os riscos relativos à informação devem ser gerenciados de modo a reduzir vulnerabilidades e impactos referentes aos ativos de informação.

Art. 19. A gestão de riscos corporativa deve ser implementada por meio de planejamento de segurança fundamentado em desenvolvimento de cultura corporativa para riscos, qualificação de pessoas, desenvolvimento de procedimentos e implantação de tecnologia e recursos.

Seção IV
Da Segurança Física e do Ambiente

Art. 20. As instalações físicas e as áreas de processamento de informações críticas ou sensíveis devem ser protegidas contra acesso indevido, danos e interferências.

Seção V
Da Segurança em Recursos Humanos

Art. 21. Todos os usuários devem adotar comportamento seguro e consistente com o objetivo de proteção das informações da Agência, bem como difundir e exigir o cumprimento da PoSIC, das normas de segurança e da legislação vigente acerca do tema.

Art. 22. Devem ser promovidos continuamente o treinamento, a capacitação, a reciclagem e o aperfeiçoamento de todos os usuários da Agência, de acordo com suas competências funcionais.

Seção VI
Da Gestão de Operações e Comunicações

Art. 23. Os procedimentos e os parâmetros adequados para a disponibilização de informações, sistemas, serviços e infraestrutura serão estabelecidos de forma a atender aos requisitos mínimos de qualidade e a refletir as necessidades operacionais da Agência.

Seção VII
Dos Controles de Acessos

Art. 24. O acesso às instalações, às informações e aos recursos computacionais da Agência ou sob sua guarda deve ser autorizado e controlado de forma a assegurar o seu uso adequado e evitar o uso indevido ou abusivo.

Parágrafo único. O acesso aos ativos de informação e sua utilização, quando autorizados, pode ser condicionado ao aceite a termo de sigilo e responsabilidade.

Seção VIII
Da Criptografia

Art. 25. Deve ser implementado, quando necessário, o uso de recursos criptográficos nas informações sensíveis produzidas e custodiadas a fim de assegurar sua inviolabilidade.

Seção IX
Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas

Art. 26. As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação devem observar critérios e controles de segurança a fim de garantir o respeito aos atributos básicos de segurança da informação.

Seção X
Do Tratamento de Incidentes

Art. 27. Os incidentes de segurança da informação devem ser conhecidos, analisados e gerenciados para tratamento e reação tempestivos.

Seção XI
Da Gestão de Continuidade

Art. 28. A continuidade do negócio deve ser assegurada por meio de planejamento de contingência contra a ocorrência de situações fortuitas e ação de recuperação de incidentes que comprometam as atividades da Agência.

Seção XII
Da Conformidade

Art. 29. Deve ser realizada, periodicamente, verificação de conformidade das práticas de SIC da Agência e de suas unidades administrativas com esta PoSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC.

Seção XIII
Do Plano de Investimentos em SIC

Art. 30. Os investimentos em SIC serão realizados de forma planejada e consolidados em um Plano de Investimentos e, no que couber, no Plano Diretor de Tecnologia da Informação - PDTI.

Art. 31. O Plano de Investimentos deverá ser reavaliado quando houver revisão orçamentária ou revisão de prioridades das ações de SIC.

Seção XIV
Da Propriedade Intelectual

Art. 32. As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual da Agência e não cabe a seus criadores qualquer forma de direito autoral.

Art. 33. É vedada a utilização de informações produzidas por terceiros em quaisquer projetos ou atividades de uso diverso do estabelecido pela Agência, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pela Diretoria, nos demais casos.

Seção XV
Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 34. Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC.

Art. 35. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PoSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades vinculadas à Agência.

Capítulo V
DAS PENALIDADES

Art. 36. Ações que violem a PoSIC, suas diretrizes e normas ou os controles de SIC, serão devidamente apuradas e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor.

Capítulo VI
DA ATUALIZAÇÃO

Art. 37. Esta PoSIC, bem como os documentos gerados a partir dela, deverão ser avaliados periodicamente, em intervalos não superiores a 3 (três) anos, para elaboração, se necessário, de proposta de revisão.

Capítulo VII
DAS DISPOSIÇÕES FINAIS

Art. 38. Casos omissos serão analisados pelo Gestor de SIC, com o auxílio da área responsável pela gestão da informação e do CSIC, e encaminhados para deliberação da Diretoria Colegiada.

Art. 39. Esta Instrução Normativa entra em vigor na data de sua publicação.

MARCELO PACHECO DOS GUARANYS
Diretor-Presidente