POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA AEB

2017 - 2018

Versão 1.0

AEB
AGÊNCIA ESPACIAL BRASILEIRA

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA,
INOVAÇÕES E COMUNICAÇÕES

BRASIL
GOVERNO FEDERAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA AEB

Ministério da Ciência, Tecnologia, Inovações e Comunicações

Agência Espacial Brasileira

José Raimundo Braga Coelho
Presidente da AEB

Grupo de Trabalho da POSIC

Paulo Henrique da Silva Junior
Presidente do Grupo de Trabalho da POSIC

Fabiano de Avelar Apoliano
Secretário do Grupo de Trabalho da POSIC

João Valentim Bin
Fernanda Lins Leal Uchôa de Lima
Representantes da Diretoria de Política Espacial e Investimentos Estratégicos – DPEI

Gabriel Figueiró de Oliveira
Rodrigo Leonardi
Representantes da Diretoria de Satélites, Aplicações e Desenvolvimento – DSAD

Marcio Akira Harada
Amélia Naomi Onohara
Representantes da Diretoria de Transporte Espacial e Licenciamento – DTEL

Arthur Pullen Sousa
Priscila Hardman Rodrigues de Oliveira
Representantes da Diretoria de Planejamento, Orçamento e Administração – DPOA

Henrique Fernandes Nascimento
Simonny Valéria Soares
Representantes do Núcleo da Presidência

Jean Carlos Borges Brito
Juliano Raphael Simões de Souza
Representantes da Divisão de Informática - DINF

Setembro de 2017

Sumário

1. Introdução

Segurança da Informação (SI) é a disciplina dedicada à proteção da informação para garantir a continuidade dos negócios, minimizar os danos, maximizar o retorno dos investimentos e promover as oportunidades de atuação de uma instituição. A SI é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e *funções de software e hardware*. Para compreensão de termos técnicos da área de segurança da informação é disponibilizado um glossário ao final deste documento.

A Política de Segurança da Informação e Comunicações (POSIC) orienta e estabelece as diretrizes institucionais para a proteção dos ativos de informação e a gestão da segurança da informação.

Esta política considera as recomendações e práticas propostas pelo Decreto n° 3.505/2000, pela IN GSI/PR n° 01/2008, pela norma internacional *ABNT NBR ISO/IEC 27002:2013* e se alinha, ainda, às demais leis e normas vigentes sobre esta temática, elencadas no Anexo 1.

O Decreto n° 3.505/2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal estabelece, em seu artigo 3º, os seguintes objetivos:

I. Dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os 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.

II. Eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação.

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

IV. Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação.

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

VI. Promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação.

VII. Promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação. e

VIII. Assegurar a interoperabilidade entre os sistemas de segurança da informação.

2. Diretrizes Gerais de Segurança da Informação

São diretrizes gerais desta política de segurança da informação:

a) Preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação da AEB.

b) **Garantia do acesso, proteção e guarda da informação:** o acesso à informação deve ser regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela AEB é considerada seu patrimônio e deve ser protegida, esteja ela em meio físico ou digital.

c) **Utilização dos recursos de informação**: os recursos disponibilizados são fornecidos com o propósito único de garantir o desempenho das atividades da AEB. O acesso e o uso da informação e dos recursos de tecnologia da informação e comunicações devem ser controlados e limitados ao necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de acesso ou uso necessitará de prévia autorização do gestor do ativo de informação e da chefia imediata do usuário, observando-se a legislação em vigor. O controle operacional de uma atividade crítica, todavia, não pode ser atribuição exclusiva de uma única pessoa a não ser em casos justificados.

d) **Classificação das informações**: para que o nível adequado de proteção para a informação seja estabelecido é conveniente que as informações, existentes e futuras, tenham seu grau de sigilo estabelecido.

e) **Complementariedade:** poderão ser estabelecidas normas específicas da AEB para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação, que serão definidas de acordo com o grau de sigilo da informação, sem prejuízo de outros cuidados que poderão ser especificados pela AEB.

f) **Gestão de incidentes**: processo contínuo que visa mitigar riscos que resultem na interrupção não planejada de um serviço, uma redução na qualidade do serviço ou um evento que ainda não impactou o serviço do cliente. Será definido, no mínimo, um responsável para receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como identificar tendências tecnológicas e comportamentais.

g) **Gestão de risco**: processo contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação - SGSI, produzindo subsídios para a Gestão de Continuidade dos Negócios. Nesse contexto, devem ser estabelecidos, através de uma política do SGSI, objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e a melhoria da segurança da informação. Após a elaboração da política, a mesma deve ser implementada e operada, produzindo insumos que sejam possíveis de medir e avaliar, a fim de relatar os resultados para a gerência. Caso necessário, serão tomadas ações corretivas e preventivas para alcançar a melhoria contínua do SGSI. O processo de Gestão de Risco abordado neste documento deve estar alinhado à Política de Gestão de Riscos e Controles Internos da Gestão – POLIGRI desta AEB.

h) **Plano de continuidade**: processo de medidas, regras e procedimentos definidos, que serão adotados para assegurar que as funções ou atividades críticas da AEB possam ser mantidas ou recuperadas, após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações.

i) **Auditoria e conformidade**: deverão ser levantados, regularmente, os aspectos legais de segurança aos quais as atividades da AEB estão submetidas, e o seu cumprimento, de forma a evitar responsabilizações decorrentes da não observância de tais aspectos por desconhecimento ou omissão.

j) **Segurança física**: controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos da AEB e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo-se a entrada e saída de visitantes, pessoal interno, equipamentos e mídias e estabelecendo-se perímetros de segurança.

k) **Capacitação e aperfeiçoamento**: os colaboradores deverão se capacitar continuamente para o desenvolvimento de competências em Segurança da Informação e Comunicações. A AEB deve dispor de condições para que isso seja alcançado.

l) **Patrimônio intelectual**: as informações, os sistemas e os métodos criados pelos servidores da AEB, no exercício de suas funções, são patrimônios intelectuais da AEB, não

cabendo a seus criadores qualquer forma de direito autoral, ressalvado o disposto na Lei nº 10.973/2004.

m) **Termo de Compromisso de Manutenção de Sigilo - TCMS:** documento oficial que estabelece o compromisso dos colaboradores com a Política de Segurança da AEB. Os requisitos de segurança da informação devem estar explicitamente citados nos termos de compromisso celebrados entre a AEB e terceiros nos casos pertinentes.

n) **Economicidade da proteção dos ativos de informação**: as medidas de proteção e as despesas na aplicação de controles devem ser planejadas e compatibilizadas com o valor do ativo a ser protegido.

o) **Pessoalidade do acesso:** o acesso às informações, sistemas e instalações depende da apresentação de credencial ou TCMS, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

p) **Responsabilização do usuário pelos atos que comprometam a segurança do Sistema de Informação**: o usuário é responsável por todos os atos praticados com suas identificações, dentre as quais se destacam: nome do usuário na rede, carimbo, crachá, endereço de correio eletrônico e assinatura digital. O usuário responderá pela segurança dos ativos. dos processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento do usuário.

q) **Revisão dos direitos de acesso e uso dos ativos**: quando do afastamento, mudança de responsabilidade, atribuições ou lotações dentro da organização, faz-se necessária a revisão imediata dos direitos de acesso e uso dos ativos. Quando da efetivação do desligamento de usuário, cabe a CRH/DPOA/AEB comunicar **imediatamente** a DINF/DPOA/AEB para as adoções das medidas cabíveis relativas aos direitos de acesso e de uso dos ativos a ele atribuídos. Todo ativo produzido pelo usuário desligado deverá ser mantido pela AEB, por no mínimo doze meses, garantindo o reconhecimento e o esclarecimento da propriedade do acervo.

3. Princípios e Objetivos

3.1 São princípios da POSIC:

a) A informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence à AEB. As exceções devem ser explicitadas e formalizadas entre as partes.

b) O uso de ativos de informação da AEB deve ser consciente e responsável. Os recursos de tecnologia da informação e comunicação da AEB devem ser utilizados para a consecução de seus objetivos.

c) Deverão ser criados, quando possível, controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário, com vista à redução dos riscos dos seus ativos de informação.

d) Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais de usuário (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários, desde que justificado e demandado pela chefia imediata do colaborador supervisionado. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade.

e) Os acessos às redes e sistemas da AEB deverão ser feitos, preferencialmente, por meio de credencial única, pessoal e intransferível.

f) A AEB pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informações alocadas na infraestrutura provida pela AEB.

g) O usuário é responsável pela segurança das informações que estão sob sua responsabilidade, dentro e fora da AEB.

h) Com o objetivo de reduzir o risco de descontinuidade das atividades da AEB e de perda de sigilo, integridade e disponibilidade dos ativos de informação, deverão ser implantados planos de contingência e de continuidade para os principais serviços e sistemas e serem revisados e testados periodicamente.

i) Os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante sua fase de execução.

j) Deverá constar em todos os contratos da AEB, quando o objeto for pertinente, cláusula de sigilo e de obediência à Política de Segurança da Informação e Comunicações e suas Normas Complementares.

k) Os colaboradores que desempenharem suas atividades na AEB, inclusive provenientes de cooperações internacionais, que tiverem necessidade de conhecer informações classificadas em função de suas atividades, deverão ser credenciados ou assinar o Termo de Compromisso de Manutenção de Sigilo, sem prejuízo das atribuições dos agentes públicos autorizados na legislação, em relação ao conhecimento da POSIC e de suas normas complementares vigentes, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela AEB (Ref.: Decreto nº 7.845/2012, art. 18).

l) Esta POSIC será implementada, na AEB, por meio de normas complementares e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço. Os casos excepcionais serão resolvidos pelo Gestor de Segurança da Informação e Comunicações da AEB.

3.2 Objetivos:

A POSIC tem por objetivo geral preservar os ativos de informação e comunicações, tangíveis e intangíveis, quanto ao sigilo, integridade, disponibilidade e autenticidade. Nestes termos, são estabelecidos os seguintes objetivos específicos:

a) Estabelecer diretrizes para a disponibilização e utilização de ativos de informação, serviços de redes de dados, estações de trabalho, *internet*, telecomunicações e correio eletrônico institucional.

b) Designar, definir ou alterar categorias e responsabilidades do grupo responsável pela Segurança da Informação.

c) Possibilitar a implantação de iniciativas relativas à Segurança da Informação.

d) Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo para a minimização dos riscos associados.

4. Abrangência de Aplicação

Esta Política, bem como suas Normas Complementares, se aplicam a todos os colaboradores que executem atividades vinculadas à atuação institucional da AEB e, quando necessário, aos contratos, convênios,

acordos e outros instrumentos congêneres celebrados pela AEB, sob pena de responsabilidade na forma de Lei.

Esta Política, dentre outras diretrizes, dá ciência a cada colaborador de que os ambientes, sistemas, recursos computacionais e redes informacionais do órgão poderão ser monitorados e gravados conforme previsto na legislação brasileira.

4.1 Responsabilidades

Compete a todos os colaboradores que executem atividades vinculadas à atuação institucional da AEB o cumprimento desta POSIC e de suas Normas Complementares e:

a) A promoção da segurança de sua credencial de acesso, departamental ou de rede, bem como de seus respectivos dados.

b) A adoção das orientações fornecidas pelos setores competentes, em relação ao uso dos ativos de informação da AEB.

c) A utilização, de forma ética, legal e consciente, dos ativos de informação da AEB.

d) A atualização em relação a esta POSIC e às normas e procedimentos relacionados, buscando informação junto ao Gestor de Segurança da Informação e Comunicações da AEB sempre que não estiver absolutamente seguro quanto ao acesso, uso e/ou descarte de informações.

5. Grupo de Trabalho da POSIC

A elaboração da POSIC e suas atualizações serão realizadas pelo Grupo de Trabalho da POSIC, formalizado na portaria da AEB nº 102, de 19 de junho de 2017, a qual definiu sua abrangência representativa e será presidido pelo Gestor de Segurança da Informação e Comunicações, conforme IN GSI Nº 1 de 13 de maio de 2008. Após a confecção da POSIC e a aprovação pelo Grupo de Trabalho, será encaminhada para o Comitê de Tecnologia da Informação, constituído conforme a Portaria da AEB nº 97, de 14 de maio de 2017, o qual está incumbido de atuar como Comitê de Segurança da Informação e Comunicação - CSIC, previsto na NC03/IN01/DSIC/GSIPR/2009, deliberando sobre os assuntos tratados no grupo de trabalho da POSIC. Por sua vez, o CSIC é o grupo de pessoas com a responsabilidade de assessorar a implementação das ações de Segurança da Informação e Comunicações no âmbito da AEB (Ref: NC 03/IN01/DSIC/GSIPR/2009)

5.1 Competências do GT

a) Manifestar-se às instâncias ordenadoras de recursos da AEB relativamente a provisão de recursos necessários para a implementação e gestão da POSIC da AEB.

b) Assessorar a implementação das ações de segurança da informação e comunicações.

c) Planejar, coordenar, supervisionar e orientar a execução das atividades da Equipe de Tratamento de Incidentes de Rede - ETIR.

d) Propor alterações na POSIC.

e) Propor normas relativas à segurança da informação e comunicações.

f) Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações.

g) Definir estratégias para a implantação da POSIC.

h) Auxiliar na elaboração de Normas Complementares e Procedimentos de Segurança da Informação e Comunicações, cabendo ao Comitê de Tecnologia da Informação recomendar alterações normativas.

i) Apoiar a implementação de programas destinados à conscientização e capacitação de recursos humanos em segurança da informação e comunicações.

5.2 Competências do Gestor de Segurança da Informação e Comunicações da AEB

a) Promover cultura de segurança da informação e comunicações.

b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança.

c) Propor recursos necessários às ações de segurança da informação e comunicações.

d) Levar ao Comitê de Tecnologia da Informação os casos omissos e excepcionais.

e) Coordenar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

i. A coordenação do Comitê de Segurança da Informação e Comunicações – CSIC fica transferida para o presidente do Comitê de Tecnologia da Informação – CTI, instituído pela portaria de nº 97 AEB, de 14 de maio de 2017.

f) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

g) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações.

h) Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

5.3 Competências e responsabilidades do Comitê de Segurança da Informação e Comunicações - CSIC

a) Assessorar na implementação das ações de segurança da informação e comunicações na AEB.
b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações.
c) Propor alterações na Política de Segurança da Informação e Comunicações;

d) Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

6 Responsabilidades Específicas

6.1 Dos Colaboradores

Todo prejuízo ou dano que a AEB vier a sofrer, em decorrência da não obediência às diretrizes referidas nesta POSIC, nas Normas Complementares e procedimentos específicos delas decorrentes, poderá ser de responsabilidade dos usuários (internos ou externos), cabendo ampla defesa e o contraditório.

Os colaboradores devem conhecer os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes desta Agência. A AEB poderá, a qualquer tempo, revogar credenciais de acesso e/ou TCMS concedidos a usuários, em virtude do descumprimento da POSIC ou das normas e procedimentos específicos dela decorrentes.

Além disso, cabe aos colaboradores da AEB:

a) Cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações da AEB.

b) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação, ou ainda do Gestor de Segurança da Informação e Comunicações da AEB.

c) Assinar Termo de Sigilo e/ou Termo de Responsabilidade, que formalizará a ciência e o aceite da POSIC da AEB, bem como estabelecerá responsabilidade pessoal por seu cumprimento.

d) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela AEB.

e) Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela AEB. e

f) Comunicar imediatamente, ao Gestor de Segurança da Informação e Comunicações, qualquer descumprimento ou violação desta Política e/ou de seus documentos complementares que vier a ter conhecimento.

7. Penalidades

a) O descumprimento das disposições constantes nesta Política e nas Normas Complementares sobre segurança da informação e comunicações caracteriza infração funcional, a ser apurada em Processo Administrativo Disciplinar, sem prejuízo das responsabilidades penal e civil.

b) O usuário que fizer uso de forma indevida ou não autorizada dos ativos de informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei nº 8.112/90 e na legislação pertinente, garantidos a ampla defesa e o contraditório.

8. Da Revisão e Vigência

a) Esta POSIC deverá ser revisada, no mínimo, a cada 2 (dois) anos e, no máximo, a cada 3 anos.

b) Esta POSIC entrará em vigor na data de sua publicação.

Brasília, ____/____/_____

_____

JOSÉ RAIMUNDO BRAGA COELHO

Presidente da Agência Espacial Brasileira

Glossário (Conceitos e Definições)

Para efeito desta POSIC entende-se por:

I. **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. (Ref.: NC07/IN01/DSIC/GSIPR/2010).

II. **Agente público**: todo aquele que exerce cargo, emprego ou função na AEB, ainda que transitoriamente ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, militares, servidores temporários regidos pela Lei nº 8.745/1993 e empregados públicos regidos pela Lei nº 9.962/2000, e colaboradores).

III. **Algoritmo de Estado**: função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado para uso exclusivo em interesse do serviço de órgãos ou entidades da Administração Pública Federal, direta e indireta, não comercializável (Ref.: NC 09/IN01/DSIC/GSIPR/2013).

IV. **Ameaça**: conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização (Ref.: NC 04/IN01/DSIC/GSIPR/2013).

V. **Assinatura Eletrônica**: geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser um laço legalmente equivalente à assinatura manual do indivíduo.

VI. **Ativo classificado**: ativo de informação com informação classificada ou sigilosa.

VII. **Ativo de informação**: meio 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 (Ref.: NC04/IN01/DSIC/GSIPR/2013).

VIII. **Ativo sob restrição de acesso**: ativo de informação com informação institucional não pública ou com informação de acesso transitoriamente restrito.

IX. **Auditabilidade**: atributo que garante garanta a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa.

X. **Auditoria**: atividade que englobe o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões.

XI. **Autenticidade:** qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema (Ref.: Lei nº 12.527/2011).

XII. **Capacitação e aperfeiçoamento**: Capacitação continua de servidores para o desenvolvimento de competências em Segurança da Informação.

XIII. **Colaborador**: pessoa jurídica ou pessoa física que desempenhe atividade de interesse da AEB, realize estágio ou preste serviço, em caráter permanente ou eventual.

XIV. **Complementariedade**: Normas para operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação de acordo com a sua classificação.

XV. **Continuidade de negócios**: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido. (Ref.: NC06/IN01/DSIC/GSIPR/2009).

XVI. **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

XVII. **Desastre**: evento repentino e não planejado que causa perda para toda ou parte da AEB e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação (Ref.: NC06/IN01/DSIC/GSIPR/2009).

XVIII. **Disponibilidade**: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados (Ref.: Lei nº 12.527/2011).

XIX. **Documento classificado**: documento com informação classificada ou sigilosa.

XX. **Documento**: unidade de registro de informações, qualquer que seja o suporte ou formato (Ref.: Lei nº 12.527/2011).

XXI. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)**: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas aos incidentes de segurança em computadores. (Ref.: NC03/IN01/DSIC/GSIPR/2009).

XXII. **Gestão de Incidentes**: processo contínuo que visa mitigar riscos que resultem na interrupção não planejada de um serviço, uma redução na qualidade do serviço ou um evento que ainda não impactou o serviço do cliente (Ref.: ISO/IEC 20000-1/2011, adaptada).

XXIII. **Gestão de riscos**: É um processo continuo e aplicado na implementação e operação do SGI, produzindo subsídios para a gestão de continuidade dos negócios. Os riscos devem ser monitorados e analisados periodicamente a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos no ambiente, nos ativos de informação e em fatores de risco como ameaça, vulnerabilidade, probabilidade e impacto.

XXIV. **Gestão de Segurança da Informação e Comunicações**: ações e métodos que visem 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. (Ref.: IN GSI/PR 01/2008).

XXV. **Gestor de Segurança da Informação e Comunicações**: responsável pelas ações de segurança da informação e comunicação no âmbito da AEB.

XXVI. **Gestor do ativo de informação**: autoridade legal responsável pela concessão de acesso a terceiros (pode ser a autoridade marcadora, a autoridade classificadora ou a autoridade instituidora do processo).

XXVII. **Informação sob restrição de acesso**: informação institucional não pública ou informação de acesso transitoriamente restrito.

XXVIII. **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (Ref.: Lei nº 12.527/2011).

XXIX. **Informações institucionais não públicas**: informações geradas ou custodiadas pela AEB ou por seus colaboradores, no exercício de suas funções, sujeitas a restrição de acesso. Dividem-se em:

a. **De acesso ostensivo:** aquelas que não estão sujeitas a nenhuma restrição de acesso.

b. **De acesso transitoriamente restrito:** aquelas referentes aos documentos utilizados como fundamento de decisões e atos administrativos, as quais o acesso será franqueado após a edição do correspondente ato decisório, conforme previsto no § 3º do artigo 7º da Lei nº 12.527/2011 – Lei de Acesso a Informação – LAI, salvo se forem, posteriormente objeto de classificação como sigilosas.

c. **Informações sujeitas a outros tipos de sigilo**: aquelas sob segredo de justiça ou protegidas pelo sigilo comercial, bancário, fiscal, industrial, "Pesquisa e desenvolvimento científicos e tecnológicos imprescindíveis à segurança do Estado", ou outros, na forma da legislação vigente conforme o disposto nos artigos 7º e 22 da Lei nº 12.527/11 e no artigo 45 do Decreto nº 7.845/12. ou outros, na forma da legislação vigente.

d. **Informação classificada**: informação sigilosa em poder de órgãos e entidades públicos, observado o seu teor, e, em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada.

e. **Registros**: informações contidas em anotações, levantamentos e análises preliminares, ou seja, aquelas de produção e guarda dos agentes públicos no exercício de suas funções e que não integrem processo ou expediente que subsidie decisão administrativa editada.

XXX. **Informações Institucionais Públicas**: informações geradas ou custodiadas pela AEB ou por seus colaboradores, no exercício de suas funções, as quais o acesso será permitido, observando-se eventual restrição temporária. Dividem-se em:

XXXI. **Integridade**: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino (Ref.: Lei nº 12/527/2011).

XXXII. **Legalidade**: atributo que garanta a legalidade jurídica da informação, assegurando que todos os seus dados estão de acordo com as cláusulas contratuais pactuadas ou com a legislação nacional ou internacional vigente.

XXXIII. **Não repúdio**: propriedade de que a informação não possa ter seu envio ou conteúdo contestados, rejeitados ou repudiados por seu emissor ou por seu receptor.

XXXIV. **Patrimônio intelectual**: Informações, sistemas e métodos criados pelos colaboradores da AEB, no exercício de suas funções, são patrimônios intelectuais da AEB, não cabendo a seus criadores qualquer forma de direito autoral, ressalvado o disposto na Lei nº 10.973/2004.

XXXV. **Plano de continuidade**: Processo de medidas, regras e procedimentos definidos, que serão adotados para assegurar que as funções ou atividades críticas da AEB possam ser mantidas ou recuperadas após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações.

XXXVI. **Política de Segurança da Informação e Comunicações (POSIC)**: documento aprovado pela autoridade responsável pela AEB, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações (ref.: IN GSI/PR 01/2008).

XXXVII. **Princípios**: são ideias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional.

XXXVIII. **Privacidade**: propriedade de que a informação privada só possa ser acessada por terceiros com conhecimento e autorização prévios das pessoas de que ela trata.

XXXIX. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações (Ref.: IN GSI/PR 01/2008).

XL. **Recurso criptográfico**: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração (ref.: IN GSI/PR 03/2013).

XLI. **Recurso de tecnologia da informação**: servidor de rede, estação de trabalho, equipamentos de conectividade, todo e qualquer hardware e software que compõem soluções e aplicações de TI.

XLII. **Segurança da Informação e Comunicações (SIC)**: ações que objetivem viabilizar e assegurar a disponibilidade, a integridade, o sigilo e a autenticidade das informações (Ref.: IN GSI/PR 01/2008).

XLIII. **Segurança física**: controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos da AEB, e que garantam a proteção dos Recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo-se a entrada e saída de visitante, pessoal interno, equipamentos e mídias, e estabelecendo-se perímetros de segurança.

XLIV. **Termo de responsabilidade e sigilo**: Documento oficial, assinado pelos usuários que utilizem a infraestrutura e os serviços da AEB, se comprometendo com o conhecimento da Política de Segurança da Informação e Comunicações da AEB e com o sigilo das informações.

XLV. **Tratamento da informação**: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação (Ref.: Lei nº 12.527/2011).

XLVI. **Usuário**: agente público, auditor e quaisquer outros entes que podem acessar ativos de informação da AEB mediante autorização de gestores de ativos. (Ref.: NC07/IN01/DSIC/GSIPR/2010).

XLVII. **Vulnerabilidade**: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização e pode ser evitado por uma ação interna de segurança da informação. (Ref.: NC04/IN01/DSIC/GSIPR/2013).

Anexo 1 – Referências Legais e Normativos

Esta Política de Segurança da Informação e Comunicações observa a legislação e normas específicas, destacando-se:

A. Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para uso da internet no Brasil.

B. Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos e altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal.

C. Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso a Informação (LAI).

D. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto Lei nº 2848/40 – Código Penal acerca da tipificação de crimes por computador contra a Previdência Social e a Administração Pública.

E. Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais.

F. Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

G. Decreto nº 8.100, de 04 de setembro de 2013, que em seu Anexo I, art. 6º, determina a competência do Departamento de Segurança da Informação e Comunicações.

H. Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

I. Decreto nº 7.724 de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, a qual dispõe sobre o acesso a informações.

J. Decreto nº 3.505, de 13 de junto de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

K. Decreto nº 1.171, de 24 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

L. Instrução Normativa GSI nº 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal.

M. Instrução Normativa GSI nº 02, de 05 de fevereiro de 2013, que dispõe sobre o Credenciamento de Segurança para o Tratamento de Informação Classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

N. Norma Complementar nº 01/IN01/CSIC/GSIPR, que regulamenta a Atividade de Normatização.

O. Norma Complementar nº02/IN01/CSIC/GSIPR, que regulamenta a Metodologia de Gestão de Segurança da Informação e Comunicações.

P. Norma Complementar nº 03/IN01/CSIC/GSIPR, que estabelece diretrizes para a elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

Q. Norma Complementar nº 04/IN01/CSIC/GSIPR, e seu anexo, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos e entidades da Administração Pública Federal.

R. Norma Complementar nº 05/IN01/CSIC/GSIPR, e seu anexo, que disciplina a criação de Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal.

S. Norma Complementar nº 06/IN01/CSIC/GSIPR, que estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

T. Norma Complementar nº 07/IN01/CSIC/GSIPR, que estabelece diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

U. Norma Complementar nº 08/IN01/CSIC/GSIPR, que estabelece diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

V. Norma Complementar nº 09/IN01/CSIC/GSIPR, que estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta.

W. Norma Complementar nº 10/IN01/CSIC/GSIPR, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

X. Norma Complementar nº 11/IN01/CSIC/GSIPR, que estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF.

Y. Norma Complementar nº 12/IN01/CSIC/GSIPR, que estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

Z. Norma Complementar nº 13/IN01/CSIC/GSIPR, que estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).

AA. Norma Complementar nº 14/IN01/CSIC/GSIPR, que estabelece diretrizes para utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

BB. Norma Complementar nº 15/IN01/CSIC/GSIPR, que estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

CC. Norma Complementar nº 16/IN01/CSIC/GSIPR, que estabelece diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos órgãos e Entidades da Administração Pública Federal, direta e indireta.

DD. Norma Complementar nº 17/IN01/CSIC/GSIPR, que estabelece diretrizes nos contextos de atuação e adequações para profissionais da Área de Segurança da Informação e Comunicações (SIC) nos órgãos e Entidades da Administração Pública Federal (APF).

EE. Norma Complementar nº 18/IN01/CSIC/GSIPR, que estabelece diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos órgãos e Entidades da Administração Pública Federal (APF).

FF. Norma Complementar nº 19/IN01/CSIC/GSIPR, que estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta.

GG. Norma Complementar nº 20/IN01/CSIC/GSIPR (Revisão 01), que estabelece diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos Órgãos e Entidades da Administração Pública Federal (APF), direta e indireta.

HH. Norma Complementar nº 21/IN01/CSIC/GSIPR, que estabelece diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

II. Norma Complementar nº 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B), que disciplina o Credenciamento de Segurança de Pessoas Naturais, órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas.

JJ. ISO/IEC Guide 73:2009, que disciplina a Gestão de Riscos/Vocabulário e apresenta recomendações para uso em normas.

KK. Norma NBR/ISO/IEC 27.005:2011, que estabelece diretrizes para o gerenciamento dos riscos de Segurança da Informação (SI).

LL. Norma ABNT/NBR/ISO/IEC 27.001:2013, que estabelece requisitos para o sistema de gestão de segurança da informação.

MM. Norma ABNT/NBR/ISO/IEC 27.002:2013, que institui o código de prática para controles de segurança da informação.

Anexo 2 – Normas Complementares/Específicas

Esta POSIC/AEB está estruturada, detalhadamente, nas Normas Complementares, contidas nesse anexo, as quais tratam, especificamente, da gestão dos recursos de tecnologia da informação e do tratamento das informações, em conformidade com a Norma Complementar 03/IN01/DSIC/GSIPR.

.

A. **NC-AEB 01** – Tratamento da Informação – estabelece as diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação na AEB.

B. **NC-AEB 02** – Tratamento de Incidentes de Rede – estabelece as diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes na AEB.

C. **NC-AEB 03** – Gestão de Risco – estabelece diretrizes para o processo de gestão de riscos de segurança da informação e comunicações na AEB.

D. **NC-AEB 04** – Gestão de Continuidade – estabelece diretrizes para gestão de continuidade de negócios na AEB.

E. **NC-AEB 05** – Auditoria e Conformidade – estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações na AEB.

F. **NC-AEB 06** – Controles de Acesso – estabelece as diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações na AEB.

G. **NC-AEB 07** – Uso de e-mail – estabelece diretrizes para implementação de rotinas e regras relativas ao uso de e-mail na AEB.

H. **NC-AEB 08** – Acesso à Internet – estabelece diretrizes para a implementação de controles de uso da internet no âmbito da AEB.