EMPRESA BRASILEIRA DE INFRAESTRUTURA AEROPORTUÁRIA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC

Aprovada pela Diretoria Executiva
em reunião realizada em 3 de setembro de 2019

Aprovada pelo Conselho de Administração
em reunião realizada em 27 de setembro de 2019

Setembro/2019

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC

CAPÍTULO I

DO ESCOPO E ABRANGÊNCIA

Art. 1º A presente Política de Segurança da Informação e Comunicações - POSIC tem por finalidade estabelecer diretrizes, objetivos, competências e responsabilidades para o manuseio, tratamento, controle e proteção dos dados, informações e conhecimentos custodiados ou de propriedade da Infraero, de forma a viabilizar e assegurar sua disponibilidade, integridade, confidencialidade e autenticidade.

Art. 2º Esta Política abrange os empregados do quadro regular, comissionados, cedidos, requisitados e terceirizados, os estagiários, os colaboradores, os fornecedores e os prestadores de serviços que executem atividades nas instalações da Infraero.

CAPÍTULO II

DA FUNDAMENTAÇÃO LEGAL E NORMATIVA

Art. 3º A presente Política está fundamentada nos seguintes instrumentos legais e normativos:

I - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

II - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

III - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, **caput**, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

IV - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do **caput** do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

V - 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;

VI - Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

VII - Instrução Normativa GSI/PR nº 2, de 5 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;

VIII - Instrução Normativa GSI/PR nº 3, de 6 de março de 2013, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal;

IX - Norma Complementar nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008, que dispõe sobre a metodologia de gestão de segurança da informação e comunicações;

X - Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

XI - Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;

XII - Norma Complementar nº 14/IN01/DSIC/GSIPR, de 19 de março de 2018, que estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

XIII - ABNT NBR ISO/IEC 27001:2013, que dispõe sobre os sistemas de gestão da segurança da informação - requisitos; e

XIV - ABNT NBR ISO/IEC 27002:2013, que dispõe sobre o código de prática para controles de segurança da informação.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para os efeitos desta Política, são adotados os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como de possibilitar o uso dos ativos de informação da Infraero;

II - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para a Infraero;

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

IV - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por pessoa física específica e identificada, equipamento ou sistema;

V - classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

VI - Comitê de Gestão de Segurança da Informação e Comunicações - CGSIC: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da Infraero;

VII - computação em nuvem: modelo computacional que permite acesso por demanda, independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação, tais como rede de computadores, servidores, armazenamento, aplicativos e serviços, provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

VIII - confidencialidade: qualidade atribuída à informação que não deve estar disponível ou ser revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

IX - continuidade de negócios: capacidade estratégica e tática da Infraero de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

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

XI - disponibilidade: qualidade atribuída à informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

XII - 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 a incidentes de segurança em computadores;

XIII - integridade: qualidade atribuída à informação não modificada, inclusive quanto à origem, trânsito e destino;

XIV - gestão de continuidade de negócios: processo de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem, e que fornece estrutura para que se desenvolva resiliência organizacional, capaz de responder eficazmente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

XV - gestão de riscos de segurança da informação e comunicações: conjunto de processos que permitem identificar, analisar, avaliar e implementar as medidas necessárias para o tratamento de riscos e equilibrá-los com os custos operacionais e financeiros envolvidos;

XVI - gestão de segurança da informação e comunicações: ações e métodos que visam a integração das atividades de análise de riscos, gestão de continuidade do negócio, tratamento de incidentes, classificação e tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança de recursos humanos e segurança

documental aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

XVII - gestor de segurança da informação e comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da Infraero;

XVIII - Plano de Continuidade de Negócio - PCN: procedimentos documentados que orientam as organizações a responder, recuperar, retornar e restaurar, após a interrupção, para um nível predefinido de operação, sendo composto pelo Plano de Contingência Operacional - PCO e Plano de Recuperação de Desastres - PRD;

XIX - Plano de Resposta a Incidentes: documento contendo um conjunto de procedimentos ou instruções predeterminadas, com a finalidade de detectar, responder e limitar consequências de ciberataques maliciosos;

XX - segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações; e

XXI - vulnerabilidades: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para a Infraero, os quais podem ser evitados por ação interna de segurança da informação.

CAPÍTULO IV

DOS PRINCÍPIOS, DIRETRIZES E OBJETIVOS

Art. 5º Constituem princípios norteadores desta Política a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Art. 6º Constituem diretrizes da presente Política:

I - integração aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional da Infraero;

II - submissão às regras de conformidades legal e normativa dos procedimentos relacionados à segurança da informação e das comunicações;

III - proteção adequada do ativo de informação, independentemente da forma ou do meio pelo qual a informação seja apresentada ou compartilhada; e

IV - utilização dos recursos de tecnologia da informação e comunicação estritamente para seu propósito institucional.

Art. 7º Constituem objetivos da presente Política:

I - estabelecer diretrizes gerais para a efetiva implementação da segurança da informação e comunicações na Infraero;

II - orientar e subsidiar a tomada de decisões institucionais que visem à efetividade das ações de segurança da informação e das comunicações;

III - orientar as áreas da Infraero para que assegurem a autenticidade, confidencialidade, disponibilidade e integridade das informações produzidas e armazenadas;

IV - garantir a transparência das informações de acesso irrestrito e a proteção adequada daquelas com restrição de acesso;

V - estabelecer competências e responsabilidades para garantir a efetiva proteção dos dados, informações e conhecimentos gerados; e

VI - reduzir os riscos de ocorrência de perdas, alterações e acessos indevidos aos ativos de informação.

CAPÍTULO V

DAS DISPOSIÇÕES GERAIS

Seção I

Da Gestão da Segurança da Informação e Comunicações

Art. 8º Os mecanismos de proteção utilizados em decorrência desta Política deverão ser mantidos com o objetivo de garantir a continuidade dos negócios da Infraero.

Art. 9º As informações criadas, adquiridas ou custodiadas pelos agentes mencionados no art. 2º, no exercício de suas atividades na Infraero, são consideradas como bem e propriedade da empresa, devendo ser protegidas segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

Art. 10. Os agentes mencionados no art. 2º desta Política são responsáveis pela segurança dos ativos de informação e comunicações, bem como pelas informações armazenadas, acessadas, produzidas e transmitidas pela Infraero, que estejam sob a sua responsabilidade.

Art. 11. É vedado o uso dos recursos de tecnologia da informação e comunicações para:

I - fins pessoais, próprios ou de terceiros;

II - entretenimento e veiculação de opiniões político-partidárias ou religiosas;

III - perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica; e

IV - praticar condutas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem da instituição, comprometendo a integridade, a confidencialidade, a confiabilidade, a autenticidade ou a disponibilidade das informações.

Art. 12. Os contratos, convênios e acordos de cooperação técnica celebrados pela Infraero que envolvam informação classificada em grau de sigilo deverão possuir cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, sendo exigida da entidade contratada a assinatura de termo de confidencialidade.

Seção II

Da Classificação e Tratamento da Informação

Art. 13. A classificação da informação terá por objetivo reduzir as ameaças, riscos e vulnerabilidades que poderão comprometer a confidencialidade, integridade e disponibilidade da informação, assegurando-se níveis adequados de proteção conforme seu valor, requisitos legais e criticidade.

Art. 14. As informações são passíveis de classificação quando são consideradas imprescindíveis à segurança da sociedade ou do Estado e se enquadrarem no rol de hipóteses de classificação previsto no art. 23 da Lei nº 12.527, de 2011.

Parágrafo único. Para a classificação da informação, deverá ser utilizado o critério menos restritivo possível.

Art. 15. É dever de todos os agentes mencionados no art. 2º desta Política assegurar a publicidade da informação ostensiva, bem como salvaguardar a informação sigilosa e a pessoal, utilizando-as exclusivamente para o exercício de suas atribuições, sob pena de responsabilização administrativa, civil e penal.

Parágrafo único. O tratamento das informações pessoais deverá ser feito de forma transparente e com respeito à intimidade, vida privada, honra, imagem das pessoas, liberdades e garantias individuais.

Art. 16. O acesso, a divulgação e o tratamento de informação classificada com algum grau de sigilo deverão ser restritos a pessoas com necessidade de conhecê-la e que sejam credenciadas, na forma estabelecida no Decreto nº 7.845, de 2012, e nas normas internas da Infraero, sem prejuízo das atribuições dos agentes públicos autorizados na legislação.

Art. 17. As informações institucionais deverão ser armazenadas nos servidores de arquivo e bases de dados sob gestão e administração da área de Tecnologia da Informação, se eletrônicas, e deverão ser mantidas em local que as salvaguardem adequadamente, se não eletrônicas.

Art. 18. As informações institucionais armazenadas em servidores de arquivo deverão ser salvaguardadas por meio de cópia de segurança sob administração da área de Tecnologia da Informação e mantidas em local que as proteja adequadamente e garanta sua recuperação em caso de perda da informação original.

Art. 19. As informações classificadas conforme a legislação vigente, produzida, armazenada e transportada em meios eletrônicos, quando necessário, deverão utilizar criptografia compatível com o grau de sigilo, em especial a autenticação dos usuários das aplicações.

Art. 20. No descarte de informações institucionais deverão ser observadas as políticas, as normas, os procedimentos internos, a classificação da informação e a temporalidade prevista na legislação.

Art. 21. Os empregados da Infraero deverão adotar a política de mesa limpa e tela protegida, ou práticas equivalentes, para diminuir a vulnerabilidade nos ambientes de trabalho.

Art. 22. Os critérios gerais aplicáveis à classificação e ao tratamento da informação deverão ser definidos por normativo elaborado pelo Comitê de Gestão de Segurança da Informação - CGSIC, com a participação de todas as áreas da Infraero que produzem, recepcionam ou custodiam informações essenciais às atividades da empresa.

Seção III

Dos Ativos de Informação

Art. 23. A gestão de ativos de informação da Infraero deverão observar normas internas e procedimentos específicos para garantir a sua operação segura e contínua.

Parágrafo único. Os ativos de informação da Infraero deverão ser periodicamente inventariados, subsidiando seu conhecimento, valoração, proteção, manutenção e identificação dos custodiantes, a fim de garantir a rastreabilidade do seu uso.

Art. 24. A aquisição, contratação de serviços de desenvolvimento, instalação e uso de sistemas e equipamentos deverão ser homologados e autorizados pela área de Tecnologia da Informação.

Art. 25. É vedada a utilização de equipamentos de terceiros na rede corporativa da Infraero, salvo exceção previamente justificada pelo gestor junto à área de Tecnologia da Informação.

Art. 26. É vedado adicionar, remover ou manipular os componentes físicos (hardware) de ativos de tecnologia da informação sem o consentimento da área de Tecnologia da Informação.

Art. 27. A movimentação dos ativos de tecnologia da informação deverá ser precedida de registro e autorização formal.

Parágrafo único. Na hipótese descrita no **caput**, bem como no caso de doação e descarte, deverão ser seguidos procedimentos adequados para que não haja risco de vazamento ou perda de informações.

Art. 28. Os recursos tecnológicos e as instalações de infraestrutura deverão ser protegidos contra indisponibilidade, acessos indevidos, falhas, perdas, danos, furtos, roubos e interrupções não programadas.

Parágrafo único. Ocorrências como extravio ou roubo deverão ser imediatamente comunicadas à área de Tecnologia da Informação, para que sejam registradas como incidente de segurança da informação, sem prejuízo das demais providências necessárias.

Art. 29. Os sistemas de informação e as aplicações da Infraero deverão ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Seção IV

Da Gestão de Incidentes de Segurança em Rede Computacional

Art. 30. A gestão de incidentes em segurança da informação e comunicações deverá assegurar que fragilidades e incidentes sejam identificados tempestivamente, para permitir a tomada de ação corretiva em tempo hábil.

Art. 31. A área de Tecnologia da Informação deverá manter Equipe de Tratamento e Resposta a Incidentes em Redes de Computadores - ETIR, instituída pelo Comitê de Gestão de Segurança da Informação e Comunicações - CGSIC, com a responsabilidade de receber, analisar, responder notificações e executar atividades relacionadas a incidentes de segurança em rede de computadores.

Art. 32. Os agentes mencionados no art. 2º desta Política são responsáveis por notificar imediatamente a ETIR sobre incidentes que afetem a segurança da informação ou o descumprimento da POSIC, para que as providências necessárias sejam adotadas a fim de sanar as causas.

Seção V

Da Gestão de Riscos

Art. 33. A gestão de riscos deverá ser realizada de forma sistemática e contínua e englobar todos os ativos de informação da Infraero, visando a tratar riscos relacionados a disponibilidade, integridade, confidencialidade, autenticidade, bem como a melhoria da segurança da informação e comunicações na empresa.

Art. 34. Os princípios e diretrizes de gestão de riscos aplicados à segurança da informação e comunicações deverão ser definidos por meio da Política de Gestão de Riscos da Infraero, com vistas a identificar ameaças e reduzir vulnerabilidades e impactos nos ativos de informação.

Seção VI

Da Gestão de Continuidade de Negócios

Art. 35. O Plano de Continuidade de Negócio - PCN da Infraero deverá alcançar os ativos de informação críticos e os serviços relativos à segurança da informação e comunicações, visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de Tecnologia da Informação e Comunicações que suportam as operações da empresa.

Art. 36. Todo sistema crítico da Infraero deverá estar suportado pelo PCN.

Seção VII

Do Monitoramento, Auditoria e Conformidade

Art. 37. Para a realização do monitoramento, da auditoria e da conformidade deverão ser observados os seguintes critérios:

I - o uso dos recursos de tecnologia da informação e comunicações disponibilizados pela Infraero é passível de monitoramento e auditoria, devendo ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade;

II - a entrada e a saída de ativos de informação da Infraero, inclusive publicação e disponibilização, devem ser registradas e autorizadas por autoridade competente mediante procedimento formal; e

III - as auditorias internas em segurança da informação devem ser reguladas por norma interna proposta pela área de Auditoria Interna da Infraero.

Art. 38. A Infraero deverá promover, periodicamente, avaliação de conformidade desta Política e suas normas e procedimentos complementares, bem como às regulamentações e legislações em vigor relativas à segurança da informação e comunicações, considerando os requisitos mínimos que assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Seção VIII

Do Controle de Acesso e Uso de Senhas

Art. 39. A autorização, o acesso e o uso das informações e dos recursos computacionais deverão ser controlados e limitados ao necessário, considerando as atribuições de cada usuário.

Art. 40. Os empregados da Infraero são responsáveis por todos os atos praticados com suas identificações, tais como, nome de usuário e senha, crachá, carimbo, correio eletrônico e certificado digital.

Parágrafo único. A identificação do empregado, qualquer que seja o meio e a forma, deverá ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Art. 41. A sistematização do controle de acesso a todos os sistemas institucionais, intranet, internet, informações, dados e instalações físicas da Infraero deverá ser definida e regulamentada por meio de norma interna, com o objetivo de garantir a segurança dos empregados e a proteção dos ativos da empresa.

Seção IX

Do Uso de E-mail e Acesso à Internet

Art. 42. O e-mail corporativo é uma ferramenta de trabalho da Infraero e deverá ser de uso restrito para as atividades vinculadas às atribuições e funções do cargo.

Art. 43. O e-mail corporativo é de uso exclusivo dos empregados, estagiários e prestadores de serviço da Infraero e terá como finalidade o envio e o recebimento eletrônico de mensagens e documentos institucionais.

Art. 44. As regras de acesso e utilização do e-mail corporativo deverão ser definidas por norma específica, em conformidade com esta Política e demais orientações governamentais e legislação em vigor.

Art. 45. O acesso à internet no ambiente de trabalho da Infraero estará condicionado às necessidades dos empregados no exercício de suas atribuições e funções.

Parágrafo único. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio.

Art. 46. O acesso à internet deverá ser regido por norma específica, em conformidade com esta Política e demais orientações governamentais e legislação em vigor.

Seção X

Do Uso de Computação em Nuvem

Art. 47. O uso de recursos de Computação em Nuvem, para atender demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deverá ser regido por normas específicas, atendendo a determinações desta Política e demais orientações governamentais e legislação em vigor.

Parágrafo único. A observância dos critérios descritos no **caput** visa garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas na nuvem, em especial aquelas sob custódia e gerenciamento de prestador de serviço.

Seção XI

Da Segurança em Recursos Humanos

Art. 48. Os procedimentos de segurança em recursos humanos deverão observar o seguinte:

I - o desligamento dos agentes mencionados no art. 2º desta Política extinguirá todos os direitos de acesso e de uso dos ativos a ele atribuídos; e

II - o afastamento, mudança de responsabilidade, lotação ou atribuições cominará na revisão imediata dos direitos de acesso e de uso dos ativos da Infraero.

Art. 49. A Infraero deverá promover continuamente ações de divulgação e conscientização de todos os agentes mencionados no art. 2º desta Política, por meio de programas de comunicação, sensibilização e capacitação em segurança da informação e comunicações, com o propósito de criar uma cultura de segurança na empresa.

CAPÍTULO VI

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 50. Compete à Diretoria Executiva da Infraero:

I - criar, manter e alterar as atribuições e a composição do Comitê de Gestão de Segurança da Informação e Comunicações - CGSIC;

II - envidar esforços para prover recursos, meios e condições favoráveis para aplicação e cumprimento desta Política; e

III - aprovar a Política de Segurança da Informação e Comunicações - POSIC.

Art. 51. Compete ao Comitê de Gestão de Segurança da Informação e Comunicações da Infraero - CGSIC:

I - assessorar na implementação das ações de segurança da informação e comunicações;

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

III - propor alterações nesta Política;

IV - propor normas relativas à segurança da informação e comunicações; e

V - desenvolver outras atividades inerentes à sua finalidade.

Art. 52. Compete à Presidência da Infraero nomear o Gestor de Segurança da Informação e Comunicações.

Art. 53. Compete ao Gestor de Segurança da Informação e Comunicações da Infraero:

I - promover a cultura de segurança da informação e comunicações;

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

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

IV - propor recursos necessários às ações de segurança da informação e comunicações;

V - propor normas relativas à segurança da informação e comunicações;

VI - coordenar o Comitê de Gestão de Segurança da Informação e Comunicações - CGSIC;

VII - realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações;

VIII - propor à Presidência da Empresa a nomeação de equipe técnica e especializada para atuar sob a coordenação do Gestor de Segurança da Informação e Comunicações no apoio à execução de suas atribuições e ao suporte ao CGSIC;

IX - propor, coordenar e supervisionar o orçamento destinado à implementação de ações que visem o aprimoramento da segurança da informação e comunicações;

XVIII - acompanhar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR; e

IX - manter contato direto com o Departamento de Segurança da Informação e Comunicações - DSIC, do Gabinete de Segurança Institucional - GSI da Presidência da República, para o trato de assuntos relativos à segurança da informação e comunicações.

Art. 54. Compete à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR:

I - suspender, a qualquer tempo, o acesso de usuário ou processo a informações ou recursos de tecnologia da informação, notificando, de imediato, o Gestor de Segurança da Informação e Comunicações da Infraero;

II - dar tratamento e encaminhamento aos incidentes de redes, tomando as medidas necessárias para conter as ameaças, minimizar os impactos e evitar futuras ocorrências, restabelecendo juntamente com o setor responsável a integridade, confidencialidade e disponibilidade dos ativos;

III - registrar, classificar e filtrar as notificações de incidentes de segurança;

IV - executar o Plano de Resposta a Incidentes;

V - recolher e preservar as evidências para subsidiar a forense computacional; e

VI - investigar as causas dos incidentes do ambiente computacional.

Art. 55. Compete a todos os gestores da Infraero contribuir, incentivar e fazer cumprir, no âmbito da sua dependência, as diretrizes estabelecidas nesta Política.

Art. 56. Compete aos empregados do quadro regular, comissionados, cedidos, requisitados e terceirizados, os estagiários, os colaboradores, os fornecedores e os prestadores de serviços que executem atividades nas instalações da Infraero:

I - conhecer e cumprir a presente Política, bem como os demais normativos relacionados à segurança da informação e comunicações;

II - observar as orientações estabelecidas pelo Gestor de Segurança da Informação e Comunicações da Infraero para atender aos preceitos desta Política;

III - contribuir, incentivar e fazer cumprir as diretrizes estabelecidas nesta Política; e

IV - comunicar ao Gestor de Segurança da Informação e Comunicações da Infraero eventuais ações que comprometam as diretrizes desta Política.

CAPÍTULO VII

DAS PENALIDADES

Art. 57. O descumprimento das disposições constantes nesta Política e em suas normas complementares e as ações que infrinjam os controles de segurança da informação e comunicações caracterizarão infração funcional e deverão ser devidamente apuradas em processo administrativo disciplinar, sem prejuízo das sanções civis e penais cabíveis.

Parágrafo único. A hipótese descrita no **caput** também resulta na suspensão temporária ou permanente de privilégios de acesso aos recursos de tecnologia da informação e comunicações.

Art. 58. O empregado deverá responder nas esferas disciplinar, civil ou penal, quando aplicáveis, cumulativamente ou não, pelo prejuízo que vier a ocasionar à Infraero, podendo culminar também no seu desligamento.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 59. Esta Política deverá ser revisada e atualizada no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

Art. 60. Os casos omissos e as dúvidas com relação a esta Política deverão ser submetidos ao Comitê de Gestão de Segurança da Informação e Comunicações - CGSIC.