‘

POLÍTICA DA INFRAERO

ASSUNTO

POLITÍCA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA INFRAERO

INTERESSADA

DIRETORIA FINANCEIRA E DE SERVIÇOS COMPARTILHADOS (DF)

SUPERINTENDÊNCIA DE GESTÃO DE RISCO E COMPLIANCE (DFRC)

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO (DGTI)

DATA DA APROVAÇÃO	DATA DA EFETIVAÇÃO
01/03/2016	23/03/2016

ATO DE INSTITUIÇÃO	APLICAÇÃO
VOTO N° 08/DF/DG/2016	GERAL

DIVULGAÇÃO

SUPERINTENDÊNCIA DE GESTÃO DE RISCO E COMPLIANCE (DFRC)

ASSINATURA DO SUPERINTENDENTE	ASSINATURA DO DIRETOR

I – DO ESCOPO

1 - Esta Política de Segurança da Informação e das Comunicações (Posic) tem por finalidade estabelecer as diretrizes para a segurança das informações e comunicações – incluindo seu manuseio, tratamento e controle –, e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio pelos sistemas de informação, a serem obrigatoriamente observadas na definição de regras operacionais e procedimentos no âmbito da Empresa Brasileira de Infraestrutura Aeroportuária – Infraero.

1.1 - O objetivo é estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações na Infraero.

1.2 - Esta Política aplica-se a todos os empregados do quadro regular, terceirizados e estagiários da Infraero que, oficialmente, executem atividade vinculada à atuação institucional da Empresa.

II – DOS CONCEITOS E DEFINIÇÕES

2 - Para os fins desta Política da Infraero, considera-se:

2.1 - Comitê Gestor de Segurança da Informação e Comunicações – CGSIC: grupo de empregados com a responsabilidade de assessorar a implementação das ações de segurança e comunicações no âmbito da Infraero;

2.2 - Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso de um usuário às redes de computadores, sistemas e estações de trabalho;

2.3 - Gestão de Continuidade de Negócios: um processo abrangente de gestão que identifica potenciais ameaças para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

2.4 - Gestão de Risco: Refere-se à arquitetura implantada internamente no âmbito da Infraero para gerenciar os riscos de maneira eficaz, contribuindo para reduzir a materialização de eventos que impactem negativamente seus objetivos estratégicos. A gestão de riscos, através de um enfoque estruturado e da melhor compreensão das inter-relações entre os diversos riscos, alinha estratégia, processos, pessoas e tecnologia, de modo que seja possível medir, agregar e estimar o relacionamento dessas informações em uma base corporativa;

2.5 - Gestão de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

2.6 - Gestor de Segurança da Informação e das Comunicações: é o empregado/grupo de empregados responsável pelas ações de segurança da informação e comunicações no âmbito da Infraero.

2.7 - Plano de Contingência: descreve as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais para fazer com que seus processos críticos voltem a funcionar plenamente ou em um estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;

2.8 - Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que a Infraero mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em casos de incidentes;

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

2.10 - Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive, a sigilosa;

2.11 - Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em 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 e também a identificação de tendências.

III – DAS REFERÊNCIAS

3 - Esta Política da Infraero está baseada nas seguintes legislações:

a) Lei 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação (LAI);

b) Decreto nº 7.724 de 16/05/2012, que regulamenta a Lei 12.527, de 18/11/2011 – Dispõe sobre o acesso a informações;

c) 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;

d) 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;

e) Instrução Normativa GSI Nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

f) Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

g) NBR/ISO/IEC 27002/2005, que institui o código de melhores práticas para gestão de segurança da informação;

h) NBR/ISO/IEC 27001/2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação; e

i) NBR/ISO 22301:2013, que estabelece os requisitos para sistemas de gestão de continuidade de negócios.

IV – DOS PRINCÍPIOS

4 - São princípios da Política de Segurança da Informação e das Comunicações da Infraero:

4.1 - A confidencialidade, disponibilidade e integridade dos dados, informações e conhecimentos produzidos na Infraero;

4.2 - Continuidades das atividades;

4.3 - Economicidade da proteção dos ativos de informação;

4.4 - Pessoalidade e utilidade de acesso aos ativos de informação.

V – DAS DIRETRIZES

5 - São diretrizes gerais da Política de Segurança da Informação e das Comunicações da Infraero os meios que garantam a preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação da Infraero;

5.1 - Para cada uma das diretrizes constantes das seções deste capítulo devem ser elaborados normas táticas específicas, manuais e procedimentos:

5.1.1 - Tratamento da Informação
5.1.2 - Tratamento de Incidentes de Rede
5.1.3 - Gestão de Riscos
5.1.4 - Gestão de Continuidade de Negócio
5.1.5 - Auditoria e Conformidade
5.1.6 - Controles de Acessos
5.1.7 - Uso de e-mail
5.1.8 - Acesso à *internet*

VI – DAS COMPETÊNCIAS E RESPONSABILIDADES

6 - Esta Política se aplica a todos os empregados do quadro regular, terceirizados e estagiários da Infraero que executem atividade vinculada à atuação institucional da Infraero.

6.1 - Compete a Diretoria Executiva da Infraero:

6.1.1 - Criar, manter e alterar as atribuições e/ou a composição do CGSIC.
6.1.2 - Prover recursos, meios e condições favoráveis para aplicação e cumprimento da Posic.
6.1.3 - Garantir a execução Posic e sua abrangência.

6.2 - Compete ao Comitê Gestor de Segurança da Informação e Comunicações da Infraero (CGSIC):

6.2.1 - Buscar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização.
6.2.2 - Empenhar os recursos necessários para a implementação e gestão da Posic da Infraero.
6.2.3 - Definir critérios para auditoria periódica destinada a aferir o cumprimento da Posic da Infraero.
6.2.4 - Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações.
6.2.5 - Propor alterações na Posic.
6.2.6 - Propor normas relativas à segurança da informação e comunicações.

6.3 - Compete ao Gestor de Segurança da Informação e Comunicações da Infraero:
6.3.1 - Assessorar na implementação das ações de segurança da informação e comunicações.
6.3.2 - Promover cultura de segurança da informação e comunicações.
6.1.3 - Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança.
6.3.4 - Propor recursos necessários às ações de segurança da informação e comunicações.
6.3.5 - Realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações.
6.3.6 - Editar Normas Complementares e Procedimentos de Segurança da Informação e das Comunicações, cabendo ao CGSIC a recomendação de alteração normativa.
6.3.7 - Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança.
6.3.8 - Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas.
6.3.9 - Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação.
6.3.10 - Manter a análise de risco atualizada, refletindo o estado corrente da organização.
6.3.11 - Identificar controles físicos, administrativos e tecnológicos para mitigação do risco.
6.3.12 - Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso.
6.3.13 - Planejar, coordenar, supervisionar e orientar a execução das atividades da Equipe de Tratamento de Incidentes de Rede.

VII – DAS PENALIDADES

7.1 - O não cumprimento das determinações da Posic sujeita o infrator às penalidades previstas na legislação vigente e nos regulamentos internos da Infraero.
7.2 - O descumprimento das disposições constantes nesta Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

7.3 - Os casos omissos e as dúvidas surgidas na aplicação dessa política serão submetidos ao CGSIC.

VIII – DAS ATUALIZAÇÕES

8 - Esta Posic deve ser revisada e atualizada periodicamente no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

IX – DA VIGÊNCIA

9 - Este documento entra em vigor na data de sua publicação.

X – DAS DISPOSIÇÕES FINAIS

10 - Os casos omissos e as dúvidas com relação a esta Posic serão dirimidos pelo Comitê de Gestão de Segurança da Informação e Comunicações - CGSIC.