POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC)

EM BRANCO

ATO NORMATIVO Nº SEDE-ANO-2024/00010

Rio de Janeiro, 03 de julho de 2024.

O Presidente da NAV Brasil Serviços de Navegação Aérea S.A., no uso de suas atribuições, com fundamento no art. 87, inciso I, do Estatuto Social, e considerando a deliberação do Conselho de Administração ocorrida durante a 37ª reunião ordinária, realizada em 25 de junho de 2024, conforme Ata n.º SEDE-ACO-2024/00011,

RESOLVE:

I. Instituir a Política de Segurança da Informação e Comunicações da NAV Brasil (POSIC);

II. Estabelecer que esta Política entra em vigor a partir da presente data; e

III. Determinar a sua imediata divulgação aos empregados da NAV Brasil.

JOSÉ POMPEU DOS MAGALHÃES BRASIL FILHO
PRESIDENTE
NAV BRASIL

SEDEANO202400010A

Classif. documental	010.010

NAV Brasil Serviços de Navegação Aérea - NAV Brasil
Endereço : Av. GENERAL JUSTO Nº 160 CENTRO
CEP:20021130 RIO DE JANEIRO-RJ-BRASIL

Sumário

CAPÍTULO I
DO ESCOPO E ABRANGÊNCIA

Art. 1º. A presente Política de Segurança da Informação e Comunicações - POSIC, elaborada nos termos da legislação em vigor, tem como finalidade estabelecer os objetivos, princípios e diretrizes relativos ao tema, no âmbito da empresa pública NAV Brasil Serviços de Navegação Aérea S.A.

Art. 2º. Esta Política aplica-se a todos os agentes públicos da NAV Brasil, assim como aos agentes externos, tais como prestadores de serviços, fornecedores, clientes ou qualquer outro que tenha acesso, de forma autorizada, aos dados computacionais ou às instalações da NAV Brasil.

CAPÍTULO II
DA FUNDAMENTAÇÃO LEGAL E NORMATIVA

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

I. Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso às 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, Lei Geral de Proteção de Dados Pessoais - LGPD;

III. Decreto nº 7.724, de 16 de maio de 2012, 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;

IV. Decreto nº 7.845, de 14 de novembro de 2012, 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;

V. Decreto nº 9.637, de 26 de dezembro de 2018, Política Nacional de Segurança da Informação (PNSI) 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. 75, caput, inciso VI, da Lei nº 14.133 de 01 de abril de 2021, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a Segurança Nacional;

VI. Decreto 10.748, de 19 de julho de 2021, institui a Rede Federal de Gestão de Incidentes Cibernéticos, com o fim de proporcionar prevenção contra ameaças cibernéticas e de elevar o nível de resiliência em segurança cibernética dos ativos de informação;

VII. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

VIII. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

IX. Portaria GSI/PR Nº 93, de 18 de outubro de 2021, Glossário de Segurança da Informação;

X. Instrução Normativa GSI/PR nº 6, de 27 de dezembro de 2021, que estabelece diretrizes de segurança da informação para uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal;

XI. Estatuto Social da NAV Brasil, aprovado pela Assembleia Geral Extraordinária em 12 de janeiro de 2024; e

XII. NN DOC Nº 16/2023, de 30 de agosto de 2023, dispõe sobre a Classificação e Tratamento da Informação.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

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

I. ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

II. Autenticação de Multifatores (MFA): utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);

III. 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 no âmbito da NAV Brasil;

IV. computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);

V. criptografia: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno);

VI. custodiante: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante, ou dos ativos de informação que compõem o sistema de informação, que não lhe pertence, mas que está sob sua custódia;

VII. gestor de segurança da informação e comunicações: responsável pelas ações de segurança da informação no âmbito da NAV Brasil;

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

IX. política de mesa limpa e tela protegida: são práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso; e

X. proprietário da informação: parte interessada do órgão ou entidade da administração pública federal, direta e indireta, ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação.

CAPÍTULO IV
DOS OBJETIVOS E PRINCÍPIOS

Seção I
Dos Objetivos

Art. 5º. Constituem objetivos da presente Política:

I. preservar os princípios de Segurança da Informação da NAV Brasil através da integração do Sistema de Gestão de Segurança da Informação (SGSI) com os processos da empresa e suas estruturas administrativas;

II. orientar o planejamento e a execução das ações relacionadas à Segurança da Informação no âmbito da NAV Brasil;

III. definir responsabilidades para o planejamento, execução, manutenção e controle das atividades relativas à Segurança da Informação;

IV. fomentar uma atitude favorável em relação à Segurança da Informação, bem como incrementar a conscientização a respeito da importância do assunto, no âmbito da empresa; e

V. implementar as orientações normativas advindas do Governo Federal, relacionadas à Gestão da Segurança da Informação.

Seção II
Dos Princípios

Art. 6º. Constituem princípios da presente Política:

I. Confidencialidade: garantir que as informações, fontes ou sistemas estejam acessíveis apenas a pessoas autorizadas.

II. Integridade: assegurar que a informação não seja alterada ou destruída de maneira não autorizada ou acidental;

III. Disponibilidade: assegurar um alto nível de disponibilidade das informações para as atividades críticas da NAV Brasil;

IV. Autenticidade: implementar mecanismos que permitam verificar a autoria da mensagem; e

V. Legalidade: assegurar que o tratamento das informações no âmbito da NAV Brasil esteja em conformidade com a legislação vigente.

CAPÍTULO V
DAS DIRETRIZES

Art. 7º. Constituem as diretrizes da presente Política:

I. Valorização e Proteção da Informação:

a) considerar a informação como um recurso vital e um valioso ativo de mercado, tratando-a como patrimônio a ser protegido e preservado;

b) classificar toda informação em termos do seu valor, requisitos legais, sensibilidade e criticidade para a NAV Brasil, de modo a protegê-la adequadamente quanto ao seu acesso e uso (obs.: Para aquelas com classificação sigilosa, adotar medidas especiais de tratamento); e

c) identificar e inventariar toda informação produzida e/ou manipulada no âmbito da NAV Brasil, submetendo-a aos procedimentos de segurança que minimizem o risco de violação ou perda.

II. Gestão e Normatização da Segurança da Informação:

a) garantir a gestão da segurança da informação por meio de um conjunto de objetivos, diretrizes, normas e procedimentos, visando assegurar a confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação;

b) estruturar a NAV Brasil para a gestão de toda documentação normativa relacionada à Segurança da Informação em consonância com esta Política e requisitos legais afetos ao tema;

c) prevenir o acesso físico não autorizado, interferências, danos, furto ou comprometimento de ativos e interrupção de atividades operacionais ou administrativas por meio de documentos normativos;

d) estabelecer normas para uso de serviços e tecnologias de rede, monitorando e registrando os eventos relativos ao funcionamento dos serviços;

e) considerar normas, requisitos operacionais e técnicos de segurança da informação no gerenciamento do ciclo de vida de sistemas, incorporando funcionalidades que usem certificados digitais ou autenticação de multifatores, garantindo integridade, autenticação, controle de acesso e confidencialidade nas transações eletrônicas; e

f) adotar medidas de segurança para garantir a continuidade das operações e proteger informações essenciais à operação dos serviços.

III. Identificação e Controle: preceder a adoção de qualquer solução ou serviço tecnológico com estudos sobre sua pertinência, abrangência, confiabilidade, permanência, manutenção, suporte e treinamento.

IV. Educação e Conscientização:

a) incentivar e divulgar continuamente o tema Segurança da Informação, desenvolvendo atitudes favoráveis à proteção das informações relevantes para a empresa;

b) promover campanhas periódicas de conscientização do público interno, baseadas nesta Política e em documentos normativos, reduzindo o risco de erro humano; e

c) assegurar aos mencionados no art. 2º desta Política, o entendimento de suas responsabilidades e atuações conforme seus papéis, desenvolvendo procedimentos de segurança da informação que reduzam riscos de roubo, fraude ou mau uso da informação.

V. Gerenciamento de Riscos e Incidentes:

a) estabelecer uma estrutura que promova o gerenciamento de incidentes de segurança da informação em todas as dependências da NAV Brasil; e

b) estruturar atividades de gestão de riscos, levantando impactos, probabilidades de ocorrência, ameaças, vulnerabilidades e selecionando os controles necessários para tratamento.

VI. Avaliação e Monitoramento:

a) manter serviços de Segurança da Informação, mecanismos de defesa, procedimentos de controle e avaliar periodicamente a efetividade das proteções adotadas; e

b) promover auditorias periódicas em todas as dependências, avaliando a utilização, armazenamento da informação, controle de serviços e ativos, e o alinhamento dos processos às normas e instruções voltadas para a Segurança da Informação.

CAPÍTULO VI
DAS DISPOSIÇÔES GERAIS

Seção I
Da Gestão da Segurança da Informação

Art. 8º. Informações criadas, adquiridas ou mantidas pelos mencionados no art. 2º desta Política, no exercício de suas funções na NAV Brasil, são consideradas como patrimônio da organização e devem ser protegidas segundo as diretrizes aqui descritas e demais regulamentações aplicáveis.

Art. 9º. Os mencionados no art. 2º devem, também, garantir a segurança dos ativos de informação e comunicações, bem como das informações sob sua responsabilidade, incluindo o acesso, a produção e a transmissão, relacionadas à NAV Brasil.

Art. 10. É vedado o uso dos recursos de tecnologia da informação e telecomunicações para:

I. uso pessoal, seja próprio ou em nome de terceiros;

II. entretenimento;

III. divulgação de opiniões de natureza político-partidária ou religiosa;

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

V. 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. 11. Contratos, convênios e acordos de cooperação técnica celebrados pela NAV Brasil que envolvam informações classificadas como sigilosas deverão conter uma cláusula específica que exija o cumprimento das diretrizes estabelecidas nesta Política.

Parágrafo único. As empresas contratadas também deverão assinar um Termo de Compromisso e Manutenção de Sigilo – TCMS.

Seção II

Da Classificação e Tratamento da Informação

Art. 12. Todas as informações consideradas imprescindíveis à segurança da sociedade ou do Estado e que se enquadrem nas situações definidas no art. 23 da Lei nº 12.527, de 2011, são passíveis de classificação.

Parágrafo único. As diretrizes para classificação da informação estão contidas em norma interna da NAV Brasil que aborda o assunto.

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

Art. 14. É dever de todos aqueles mencionados no art. 2º desta Política, assegurar a divulgação adequada das informações não sigilosas, bem como proteger aquelas que possuem restrição de acesso, utilizando-as exclusivamente para o exercício de suas atribuições, sob pena de responsabilização administrativa, civil e penal.

Art. 15. O tratamento das informações pessoais deverá ser feito com respeito à intimidade, vida privada, honra, imagem das pessoas, liberdades e garantias individuais.

Parágrafo único. As diretrizes para o tratamento das informações pessoais estão definidas em norma interna específica, em conformidade com a Lei nº 13.709, de 2018, que criou o arcabouço legal de proteção de dados pessoais, denominada Lei Geral de Proteção de Dados Pessoais - LGPD, com esta Política e demais diretrizes governamentais e legislação em vigor.

Art. 16. O acesso, divulgação e tratamento de informações classificadas com qualquer grau de sigilo deverão ser limitados a indivíduos que tenham uma necessidade legítima de conhecê-las e que estejam devidamente credenciados, na forma estabelecida no Decreto nº 7.845, de 2012, e nas normas internas da NAV Brasil, sem prejuízo das atribuições dos agentes públicos autorizados na legislação.

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

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 ou que possuam restrição de acesso conforme a legislação vigente, que sejam produzidas, armazenadas ou transportadas em meios eletrônicos deverão utilizar criptografia compatível com o grau de sigilo, com ênfase na autenticação dos usuários das aplicações.

Art. 20. A destinação das informações institucionais deverá se dar em conformidade com as políticas, normas e procedimentos internos estabelecidos, levando em consideração a classificação da informação e o período de guarda conforme previsto na legislação aplicável.

Art. 21. Devem ser adotadas políticas de “mesa limpa e tela protegida”, ou práticas equivalentes, visando reduzir as vulnerabilidades no controle das informações.

Art. 22. O Comitê de Gestão de Segurança da Informação e Comunicações - CGSIC, com a participação de todas as áreas da NAV Brasil que produzem, recebem ou mantém informações essenciais às atividades da empresa, deverá seguir os critérios abordados nesta seção, bem como aqueles tratados em norma interna.

Seção III
Da Gestão de Ativos de Informação

Art. 23. O processo de gestão de ativos de informação da NAV Brasil deverá observar normas internas e procedimentos específicos para garantir a sua operação segura e contínua.

Art. 24. Os ativos de informação da NAV Brasil deverão ser periodicamente inventariados, subsidiando seu conhecimento, valoração, proteção, manutenção e identificação dos custodiantes, a fim de garantir a rastreabilidade do seu uso.

Art. 25. Será garantida a proteção dos recursos tecnológicos, infraestrutura, sistemas de informação e aplicações contra eventos como indisponibilidade, acessos não autorizados, falhas, perdas, danos, furtos, roubos e interrupções não programadas.

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

Art. 26. Com o objetivo de proteger os ativos da NAV Brasil, as seguintes ações são vedadas:

I. utilizar equipamentos alheios à rede corporativa da NAV Brasil, salvo em situações previamente justificadas pelo gestor junto à área de Tecnologia da Informação;

II. realizar adições, remoções ou manipulações nos componentes físicos (hardware) dos ativos de tecnologia da informação sem a autorização da Gerência de Tecnologia da Informação e Comunicações; e

III. deslocar ativos de tecnologia da informação sem registro e autorização formal.

Art. 27. No caso de movimentação, doação e descarte de ativos, deverão ser seguidos procedimentos estabelecidos em normativos internos, para que não haja risco de vazamento ou perda de informações.

Art. 28. 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.

Seção IV
Da Gestão de Incidentes em Segurança da Informação

Art. 29. A gestão de incidentes será regida por diretrizes e procedimentos com o objetivo de prevenir, gerenciar e responder a eventos cibernéticos, visando aprimorar a resiliência da segurança cibernética dos ativos de informação da organização.

Art. 30. Em atendimento ao inciso IV, do art. 15, da IN GSI/PR nº 1, de maio de 2020, deverá ser implementada uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR.

Art. 31. A ETIR deverá ser composta, preferencialmente, por agentes públicos da NAV Brasil com capacitação técnica compatível com as atividades de competência desta equipe (§2º, Art. 22 - IN GSI/PR nº 1 de 27 de maio de 2020 e suas alterações dadas pela IN GSI/PR nº 2, de 24 de julho de 2020), conforme orientação do GSI-PR.

Art. 32. A ETIR da NAV Brasil deverá planejar e coordenar as atividades relacionadas ao tratamento e resposta a incidentes em redes de computadores.

Art. 33. Cabe à ETIR receber e notificar qualquer evento adverso, seja confirmado ou sob suspeita, que esteja relacionado à segurança dos sistemas de computação ou das redes de computadores, com o objetivo de assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações corporativas, bem como contribuir para a entrega adequada dos serviços da NAV Brasil.

Art. 34. Todos aqueles mencionados no art. 2º são obrigados a comunicar imediatamente à Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR qualquer incidente em

redes de computadores ou de violações desta Política que tiverem conhecimento, a fim de possibilitar a tomada das medidas necessárias.

Seção V
Da Gestão da Continuidade

Art. 35. O processo de gestão da continuidade de negócios em segurança da informação terá o objetivo de reduzir os efeitos advindos de falhas, desastres ou indisponibilidades significativas sobre as atividades da NAV Brasil, além de recuperar perdas de ativos de informação em nível aceitável, por meio do tratamento estabelecido em Planos de Continuidade de Negócios - PCN ou documentos equivalentes.

Art. 36. Os Planos de Continuidade de Negócios - PCN da NAV Brasil ou documentos equivalentes deverão abranger 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 NAV Brasil.

Art. 37. Todo sistema crítico da NAV Brasil deverá estar suportado por um PCN ou documento equivalente, de modo a assegurar a continuidade das operações da NAV Brasil.

Art. 38. Os princípios e diretrizes para esse processo são definidos em normas internas ou boas práticas de gestão de riscos e de continuidade de negócios.

Seção VI
Da Gestão de Riscos

Art. 39. O processo de gestão de riscos deverá visar à identificação, análise e avaliação das vulnerabilidades de forma sistemática e contínua para o tratamento dos riscos relacionados à disponibilidade, integridade, confidencialidade, autenticidade e legalidade, bem como os demais riscos identificados, com o intuito de mitigá-los para níveis aceitáveis.

Art. 40. Os princípios e diretrizes para a gestão de riscos aplicados à segurança da informação e comunicações, bem como aos seus ativos, são os mesmos definidos na Política de Conformidade, Gerenciamento de Riscos e Controles Internos da NAV Brasil, cujo objetivo é orientar e dispor sobre o gerenciamento dos possíveis eventos que possam impactar e comprometer os objetivos institucionais, sendo um deles a segurança da informação.

Seção VII
Da Gestão de Mudanças

Art. 41. A implementação do processo de gestão de mudanças deverá instruir e adaptar a NAV Brasil para as mudanças decorrentes da evolução de processos e de tecnologias da informação, com a finalidade de obter resultados eficazes e eficientes, e a mitigação de eventuais resistências.

Art. 42. O referido processo, além de promover o controle das mudanças planejadas, deverá considerar a análise crítica das consequências de mudanças não previstas, atuando em ações para amenizar os efeitos adversos.

Art. 43. A mudança poderá ser classificada como emergencial, rotineira ou proativa, e o processo de gestão de mudanças deverá ser baseado nas informações acerca dos riscos à segurança da informação mapeados.

Seção VIII
Da Avaliação de Conformidade e Auditoria

Art. 44. No que concerne à Segurança da Informação, a conformidade consiste em proporcionar adequado grau de confiança aos processos, por meio da verificação de atendimento aos requisitos estabelecidos nos normativos internos da NAV Brasil, bem como na legislação externa em vigor.

Art. 45. Nas avaliações, seja de auditoria ou conformidade, deverão ser observados os seguintes critérios:

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

II. a entrada e a saída de ativos de informação da NAV Brasil, inclusive publicação e disponibilização, devem ser registradas e autorizadas por autoridade competente, mediante procedimento formal.

Art. 46. A NAV Brasil deverá promover avaliações periódicas de conformidade desta Política, bem como das suas normas e procedimentos complementares, levando em consideração as regulamentações e leis relacionadas à segurança da informação e comunicações. Essas avaliações devem abranger os requisitos mínimos necessários para garantir a disponibilidade, integridade, confidencialidade, autenticidade e legalidade das informações.

Seção IX
Dos Controles de Acesso

Art. 47. As Políticas de controle de acesso deverão ser orientadas pelos princípios da necessidade de conhecer e da necessidade de uso. Portanto, para acessar informações ou recursos de processamento de informações (equipamentos de TI, aplicações, procedimentos, salas etc.), o usuário só deve ter acesso às informações necessárias para realizar suas tarefas ou funções específicas. Da mesma forma, a autorização, o acesso e a utilização das informações e recursos computacionais devem ser estritamente controlados e restritos ao que for necessário, levando em consideração as atribuições individuais de cada usuário.

Art. 48. Os mencionados no art. 2º desta Política são responsáveis por todos os atos praticados com suas identificações, tais como, nome de usuário e senha, crachá, carimbo, correio eletrônico, assinatura eletrônica e certificado digital.

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

Art. 49. A sistematização do controle de acesso a todos os sistemas institucionais, intranet, internet, informações, dados e instalações físicas da NAV Brasil deverá ser definida e regulamentada por meio de norma interna, com o objetivo de garantir a segurança dos mencionados no art. 2º desta Política e a proteção dos ativos da empresa.

Seção X
Da Segurança Física e do Ambiente

Art. 50. A implementação dos controles de segurança e proteção contra ameaças físicas e ambientais deverá ser regulamentada com o objetivo de garantir a segurança dos agentes públicos e a proteção dos seus ativos e informações.

§ 1º. Deverá ser instituído procedimento de credenciamento para permitir o acesso às instalações físicas da NAV Brasil.

§ 2º. O uso das credenciais de acesso é obrigatório nas instalações físicas da NAV Brasil, permitindo de maneira clara e inequívoca o reconhecimento dos agentes públicos da NAV Brasil, bem como os mencionados no art. 2º desta Política.

§ 3º. As credenciais de acesso são pessoais e intransferíveis.

Art. 51. As áreas de segurança deverão ser protegidas por perímetros de segurança definidos, com barreiras e controles apropriados.

Art. 52. O acesso físico às informações deverá ser permitido exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação.

Parágrafo único. O direito de acesso deverá ser garantido, levando em consideração a classificação da informação e as obrigações legais.

Seção XI
Do Uso de e-mail e Acesso à Internet

Art. 53. A Política de uso de recursos computacionais e de comunicação deve incorporar outras Políticas que contemplem a utilização de e-mail e correio eletrônico, e o acesso à internet.

Art. 54. O Correio eletrônico corporativo é uma ferramenta de trabalho da NAV Brasil e deverá ser de uso restrito para as atividades vinculadas às atribuições e funções do cargo e, terá como finalidade o envio e o recebimento eletrônico de mensagens de cunho corporativo e documentos institucionais.

Art. 55. As diretrizes de acesso e uso do e-mail corporativo devem ser estabelecidas por meio de uma norma específica, em conformidade com esta Política e demais orientações governamentais e legislação em vigor.

Art. 56. O acesso à internet no ambiente de trabalho da NAV Brasil estará condicionado às necessidades da empresa visando à realização das atividades pertinentes.

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

Art. 57. O acesso à internet deverá ser regido por norma específica, em conformidade com esta Política e demais orientações governamentais e legislação em vigor.

Seção XII
Do Uso Comum de Computação em Nuvem

Art. 58. A Política de uso de recursos computacionais e de comunicação deve incorporar outras Políticas que contemplem os recursos de Computação em Nuvem, a fim de atender demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação.

Art. 59. O uso de Computação em Nuvem deverá ser regulamentado por normas específicas, em conformidade com esta Política e outras diretrizes governamentais e legislação em vigor.

Seção XIII
Das Mídias Sociais

Art. 60. A Política de uso de recursos computacionais também deve abranger outras políticas relacionadas com a gestão do uso seguro das mídias sociais da NAV Brasil e regulamentada com o objetivo de definir diretrizes, critérios, restrições e responsabilidades.

Art. 61. O uso de mídias sociais deve estar alinhado com os propósitos institucionais da NAV Brasil.

Parágrafo único. É vedada a utilização de contas institucionais em mídias sociais para a postagem de conteúdo inapropriado, fazer recomendações profissionais ou que visem à promoção de produtos ou empresas não autorizados pela NAV Brasil.

Art. 62. A Assessoria de Comunicação Social é o setor responsável por todas as divulgações em mídias sociais em nome da NAV Brasil.

Art. 63. Informações classificadas em grau de sigilo ou de acesso restrito não poderão ser publicadas em mídias sociais.

Seção XIV
Da Segurança em Recursos Humanos

Art. 64. Em relação à segurança em Recursos Humanos, a POSIC deve observar os seguintes procedimentos:

I. o desligamento da Empresa dos mencionados no art. 2º desta Política resultará na revogação de todos os direitos de acesso e uso dos ativos a eles atribuídos; e

II. o afastamento, cessão, mudança de responsabilidade, lotação ou alteração nas atribuições implicará na revisão imediata dos direitos de acesso e de uso dos ativos da NAV Brasil.

Art. 65. A NAV Brasil deverá promover continuamente ações de divulgação e conscientização de todos os 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 VII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 66. Compete à Diretoria Executiva da NAV Brasil (DIREX):

I. prover recursos, meios e condições favoráveis para a aplicação e cumprimento, assim como a manutenção e o desenvolvimento desta Política;

II. assegurar a criação e a composição do Comitê de Gestão de Segurança da Informação e Comunicações (CGSIC); e

III. nomear o Gestor de Segurança da Informação e Comunicações, seu substituto, bem como outros comitês necessários para apoiar a Segurança da Informação.

Art. 67. Compete à Auditoria Interna (CAAI) realizar auditorias periódicas para avaliar os níveis de conformidade desta Política e dos Processos de Gestão da Segurança da Informação no âmbito da NAV Brasil.

Art. 68. Compete à Assessoria Jurídica (PRJU):

I. participar do processo de revisão desta Política quanto aos requisitos legais e regulatórios; e

II. assessorar a Presidência da NAV Brasil na definição de sanções legais, em caso de incidentes de segurança da informação.

Art. 69. Compete à Assessoria de Comunicação Social (PRCS), prover serviços de comunicação social, através de campanhas de conscientização sobre o tema e da divulgação das melhores práticas para o cumprimento desta Política.

Art. 70. Compete à Diretoria de Serviços (DS):

I. propor à Diretoria Executiva previsão de recursos no planejamento orçamentário a ser destinado à segurança da informação; e

II. normatizar e emitir diretrizes para os sistemas e para os seus respectivos suportes logísticos relacionados à segurança da informação.

Art. 71. Compete à Diretoria de Administração (DA):

I. garantir a ciência das responsabilidades inerentes a esta Política, mediante assinatura do Termo de Responsabilidade de Segurança da Informação por funcionários do quadro regular, comissionados, cedidos, requisitados, terceirizados e estagiários; e

II. informar, em tempo hábil, à DSTI, todos os desligamentos, afastamentos e mudanças de funções no âmbito da NAV Brasil.

Art. 72. Compete à Gerência de Tecnologia da Informação e Comunicações (DSTI):

I. supervisionar os requisitos de segurança da informação para os sistemas e para os seus respectivos suportes logísticos;

II. controlar e supervisionar todos os investimentos em infraestrutura de segurança da informação no âmbito da NAV Brasil;

III. revisar, coordenar a divulgação e facilitar o cumprimento desta Política;

IV. gerenciar e implementar atividades e projetos que promovam ações de interesse da empresa, programas educacionais e de conscientização;

V. estabelecer as normativas gerenciais, técnicas e outros documentos relativos à segurança da informação e mantê-los atualizados juntamente com as partes interessadas;

VI. auxiliar na aquisição de ferramentas que viabilizem a gestão da Segurança da Informação;

VII. supervisionar o processo de gestão de incidentes de segurança da informação no âmbito da NAV Brasil;

VIII. supervisionar o processo de gestão de riscos de segurança da informação no âmbito da NAV Brasil;

IX. supervisionar o processo de gestão da continuidade das operações afetas à segurança da informação no âmbito da NAV Brasil;

X. acompanhar projetos e estudos de implantação de novas tecnologias com o objetivo de identificar possíveis impactos para a segurança da informação;

XI. acompanhar as mudanças no ambiente organizacional da NAV Brasil, quanto a possíveis impactos para a segurança da informação;

XII. estabelecer diretrizes para os ambientes, equipamentos, processos de informação, pessoas, sistemas e redes de comunicação da NAV Brasil;

XIII. reportar às partes interessadas situações que comprometam a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações; e

XIV. normatizar a aplicação de processo disciplinar nos casos de incidentes de segurança da informação.

Art. 73. Compete à Gerência de Serviços de Navegação Aérea (DSNA), assegurar, com o apoio da DSTI, a integridade e a disponibilidade das informações necessárias às atividades operacionais da NAV Brasil, por meio da proteção adequada dos recursos tecnológicos e da implantação de Planos de Continuidade que visem à continuidade das operações.

Art. 74. Compete às Gerências das Dependências da NAV Brasil (DNBs):

I. garantir o cumprimento desta Política, bem como os procedimentos a ela relacionados, por parte dos usuários sob sua responsabilidade;

II. aplicar ações corretivas e disciplinares, nos casos de quebra da Segurança da Informação por usuários sob sua responsabilidade;

III. definir o responsável por informar as movimentações de usuários terceiros sob sua responsabilidade aos proprietários das informações;

IV. reportar aos proprietários de informações situações que comprometam a segurança da informação; e

V. definir os proprietários das informações sob sua responsabilidade.

Art. 75. Compete aos proprietários das informações:

I. identificar e classificar as informações sob sua responsabilidade;

II. definir os níveis de segurança para as informações sob sua responsabilidade, estabelecendo o controle de acesso e as condições de disponibilidade;

III. definir o custodiante das informações sob sua responsabilidade; e

IV. autorizar o custodiante a conceder as autorizações de acesso as informações sob sua responsabilidade, promovendo revisões periódicas das autorizações concedidas.

Art. 76. Compete aos custodiantes:

I. garantir a eficiência dos princípios da segurança da informação e dos recursos de informação sob sua custódia, conforme as condições estabelecidas pelo proprietário das informações;

II. comunicar aos proprietários de informações e usuários, restrições e recursos de controle da sua instalação, assim como quaisquer situações suspeitas que possam comprometer a segurança da informação sob sua custódia; e

III. prover salvaguardas físicas e procedimentos para recuperação de informações e recursos críticos sob sua responsabilidade.

Art. 77. As competências da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR estarão definidas em seu ato de instituição e em normativos internos da Empresa.

Art. 78. Compete a todos os gestores da NAV Brasil, contribuir, incentivar e fazer cumprir, no âmbito da sua área de atuação, as diretrizes estabelecidas nesta Política.

Art. 79. Compete aos mencionados no art. 2º desta Política:

I. conhecer e cumprir a presente Política, bem como, criar meios apropriados para desenvolver, implementar e mantê-la.

II. respeitar e seguir as diretrizes estabelecidas pelo Gestor de Segurança da Informação e Comunicações da NAV Brasil para atender ao previsto nesta Política;

III. contribuir, incentivar e se responsabilizar pelo cumprimento das diretrizes estabelecidas nesta Política; e

IV. informar imediatamente ao Gestor de Segurança da Informação e Comunicações da NAV Brasil eventuais ações que possam comprometer a conformidade com as diretrizes desta Política.

CAPÍTULO VIII
DAS PENALIDADES

Art. 80. A quebra de segurança ou o descumprimento das disposições constantes nesta Política e em normas complementares, assim como as ações que infrinjam os controles de segurança da informação e comunicações poderão categorizar infração funcional e deverão ser devidamente apuradas em processo administrativo disciplinar, sem prejuízo das sanções civis e penais cabíveis, podendo culminar no efetivo desligamento.

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.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 81. Esta Política deverá ser revisada e atualizada no máximo a cada 2 (dois) anos, ou em caso de fato relevante que exija uma revisão imediata.

Art. 82. 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 para submissão ao Conselho de Administração.