Ministério do Turismo

Secretaria Especial da Cultura

Fundação Biblioteca Nacional

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

(POSIN)

Rio de Janeiro, novembro de 2022

BIBLIOTECA NACIONAL

Presidente

Luiz Carlos Ramiro Junior

Comitê de Governança Digital

Diretor Executivo – João Carlos Nara Jr.

Coordenadora-geral de Coleções e Serviços aos Leitores – Maria José da Silva Fernandes

Coordenadora-geral de Processamento e Preservação – Suely Dias

Coordenador-geral de Pesquisa e Editoração – Elton Gomes dos Reis

Coordenador-geral de Cooperação e Difusão – João Alexandre Cupello Cabecinho

Coordenador de Tecnologia e Informação – Geraldo Gonçalves Chaves Junior

Ouvidora – Alessandra Guimarães Coutinho

Equipe Técnica de Elaboração

André Chang Kapp

Geraldo Gonçalves Chaves Junior

Hiram Gondim de Paula

Fundação Biblioteca Nacional | Comitê de Governança Digital
Avenida Rio Branco, 219 – Centro – CEP 20040-008, Rio de Janeiro/RJ

Sumário

1. Apresentação 5

2. Objetivo e Abrangência 5

3. Conceitos e Definições 6

4. Princípios da POSIN da FBN 8

5. Diretrizes Gerais 8

5.1. Do Tratamento das Informações 9

5.2. Da Segurança Física e do Ambiente 9

5.3. Da Gestão de Incidentes em Segurança da Informação 10

5.4. Da Gestão de Ativos da Informação 10

5.5. Da Gestão do Uso dos Recursos Operacionais e de Comunicações 11

5.6. Do Uso do Correio Eletrônico Institucional 11

5.7. Do Uso e Acesso à Internet 11

5.8. Do Uso Institucional das Redes Sociais 12

5.9. Do Uso de Dispositivos Móveis 12

5.10. Do Uso de Computação em Nuvem 12

5.11. Do Serviço de Backup e Restore 13

5.12. Do Data Center BN 13

5.13. Dos Controles de Acesso 14

5.14. Da Gestão de Riscos em Segurança da Informação 14

5.15. Da Gestão de Vulnerabilidades Técnicas 15

5.16. Da Gestão de Continuidade de Negócios em Segurança da Informação 15

5.17. Da Auditoria e Conformidade 15

6. Das Responsabilidades em Segurança da Informação 16

6.1. Da Estrutura para a Gestão da Segurança da Informação 16

6.2. Das competências do Gestor de Segurança da Informação 16

6.3. Das competências do Subcomitê de Segurança da Informação 17

6.4. Das competências da ETIR 17

6.5. Responsabilidades Gerais 18

6.6. Responsabilidade dos Usuários de Informação 18

6.7. Responsabilidade dos Gestores de Pessoas e Processos 18

6.8. Responsabilidade da Área de Tecnologia da Informação 19

7. Das infrações e penalidades aplicáveis 20

8. Estrutura Normativa de Gestão de Segurança da Informação 21

9. Referências Legais e Normativas 21

9.1. Segurança da Informação *21*
9.2. Proteção de Dados Pessoais *22*
9.3. Portarias da FBN *23*
10. Das Disposições Finais 23

1. Apresentação

A **Política de Segurança da Informação (POSIN)** é instituída a fim de assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações da Fundação Biblioteca Nacional.

Segurança da Informação é a disciplina dedicada à proteção das informações de forma a manter seus atributos e proteger contra danos que possam comprometer a organização ou gerar perdas. Nesse sentido, a **POSIN** é o documento formal que estabelece diretrizes corporativas e orientações para a proteção dos ativos de informação e para a gestão da segurança da informação.

No âmbito governamental, a **POSIN** deve seguir as recomendações e práticas propostas pelo Decreto nº 9.637, de 26 de dezembro de 2018, pela Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020**,** e pela norma internacional AFBNT ISO/IEC 27002:2005. Dessa forma, considerando o disposto no art. 4° do Decreto n° 9.637/2018, são objetivos genéricos da POSIN:

I – Contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais;

II – Fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação.

III – Aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação.

IV – Fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação.

V – Fortalecer a cultura da segurança da informação na sociedade.

VI – Orientar ações relacionadas a:

a) Segurança dos dados custodiados por entidades públicas.

b) Segurança da informação das infraestruturas críticas.

c) Proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica.

d) Tratamento das informações com restrição de acesso.

VII – Contribuir para a preservação da memória cultural brasileira.

2. Objetivo e Abrangência

Visando à orientação quanto ao uso adequado das informações e dos recursos de tecnologia da informação que as suportam, e evitando impactos prejudiciais às atividades da instituição, são objetivos da POSIN da FBN:

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

b) Apoiar a implantação das iniciativas relativas à Segurança da Informação.

c) Orientar o grupo responsável pela Segurança da Informação.

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

Esta POSIN e suas eventuais normas complementares aplicam-se em toda a FBN, incluindo nesta

política os servidores, prestadores de serviço, terceirizados, colaboradores, estagiários, consultores externos, e aplicam-se também aos ambientes, sistemas, processos e pessoas e a quem, de alguma forma, tenha acesso aos ativos de informação da FBN em qualquer meio ou suporte.

A POSIN trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito da FBN, em todo o seu ciclo de vida criação, manuseio, divulgação, armazenamento, transporte e descarte, visando a continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação.

Deve ser dado amplo conhecimento de seu teor a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos da FBN, por serem todos responsáveis por garantir a segurança das informações a que tenham acesso. Este documento, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do órgão poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

3. Conceitos e Definições

Os conceitos e as definições utilizados nesta Política de Segurança da Informação estão contidos no **Glossário de Segurança da Informação**, aprovado pelo Gabinete de Segurança Institucional da Presidência da República mediante a Portaria GSI/PF nº 93, de 18 de outubro de 2021, dentre eles:

Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação, ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da administração pública federal, direta e indireta.

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.

Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Backup: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.

Comitê de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados.

Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de Equipa de Tratamento de Incidentes de Rede.

Gestão de Continuidade de Negócios em Segurança da Informação: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse 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, a marca da organização e suas atividades de valor agregado.

Gestão de Riscos em Segurança da Informação: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Gestão de Segurança da Informação: processo que visa integrar 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 organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação.

Gestor de Segurança da Informação: responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores**.**

Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Plano de Continuidade de Negócios em Segurança da Informação: documentação dos procedimentos e das informações necessárias para que os órgãos ou entidades da administração pública federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente.

Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

POSIN: sigla de Política de Segurança da Informação.

Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Usuário de Informação: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade.

4. Princípios da POSIN da FBN

Além dos princípios elencados no artigo 37 da Constituição Federal, as ações de segurança da informação na FBN são norteadas pelos seguintes princípios:

a) **Alinhamento à missão institucional** e ao planejamento estratégico da FBN.

b) **Respeito à diversidade organizacional**, isto é, à natureza e à finalidade de cada órgão da FBN.

c) **Garantia da propriedade da informação:** todas as informações produzidas ou recebidas pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado do exercício de sua função ou atividade profissional contratada, pertencem à FBN, a não ser que a instituição atue como depositária de informação alheia; outras exceções devem ser formalizadas explicitamente entre as partes.

d) **Responsabilidade no uso dos ativos de informação** da FBN, inclusive os recursos comunicacionais e computacionais, os quais devem ser aplicados na consecução dos objetivos institucionais da instituição de forma consciente. Cada usuário de informação é individualmente responsável pela segurança das informações dentro da organização, principalmente daquelas que estejam sob sua guarda ou responsabilidade.

e) **Gerenciamento dos riscos associados aos ativos de informação** por meio da criação e manutenção de controles, registros de atividades e trilhas de auditoria para todos os processos ou sistemas que a FBN julgar necessário, de modo que todos os eventos significantes dos processos e sistemas sejam rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo acontecimento.

f) **Segurança da informação**, cujos requisitos deverão ser identificados prioritariamente na fase de levantamento do escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

g) **Segregação de função:** funções de planejamento, execução e controle devem ser segregadas, de forma a atender aos objetivos institucionais e reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos. Quando o objeto for pertinente, deverá constar em todos os contratos celebrados pelo órgão cláusula de confidencialidade e de obediência às normas internas de Segurança da Informação a ser observada pelas empresas fornecedoras e por todos os profissionais que vierem a desempenhar atividades profissionais no âmbito dos respectivos contratos, inclusive aqueles firmados junto a organismos internacionais.

5. Diretrizes Gerais

Para cada uma das diretrizes desta POSIN poderão ser elaboradas normas internas, metodologias ou procedimentos complementares de segurança da informação.

O uso e o compartilhamento de dados, informações e documentos no âmbito da FBN, em todo o seu ciclo de vida visam à continuidade de seus processos críticos em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação.

O ciclo de vida da informação refere-se às fases de criação, tratamento, uso, armazenamento, divulgação e descarte.

O sucesso das ações de segurança da informação está diretamente associado à capacitação científico-tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

Visando alcançar a abrangência definida nesta POSIN, toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela FBN é considerada ativo de informação e faz parte do seu patrimônio, observados os critérios de confidencialidade, autenticidade, disponibilidade e integridade, além do disposto na Lei nº 13.709, de 14 de agosto de 2018 – **Lei Geral de Proteção de Dados Pessoais (LGPD)**.

5.1. Do Tratamento das Informações

As diretrizes específicas e os procedimentos próprios de **tratamento da informação corporativa** serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

a) Documentos corporativos imprescindíveis às atividades dos usuários deverão ser salvos em dispositivos de rede. Os arquivos gravados localmente, nos computadores dos usuários, não serão cobertos pelo serviço de *backup* (cópias de segurança) estando sujeitos a perda e a não-recuperação.

b) Arquivos pessoais ou não pertinentes às atividades laborais do servidor (fotos, músicas, vídeos etc.) não deverão ser copiados ou movidos para os dispositivos de rede, pois podem sobrecarregar a capacidade de armazenamento e conter vulnerabilidades e riscos de segurança. Caso identificados, esses arquivos serão excluídos de forma imediata e definitiva sem necessidade de comunicação prévia ao usuário.

c) Normas de classificação de informações, acesso à informação, uso e descarte de ativos de informação, dentre outros temas afins, serão fixadas em estrita aderência às leis e normas atinentes à Administração Pública Federal – considerando as competências regimentais.

d) É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pela FBN.

e) As senhas utilizadas em sistemas da FBN deverão ser criptografadas para proteção contra acesso indevido ou vazamento.

5.2. Da Segurança Física e do Ambiente

A FBN deverá observar diretrizes específicas e **procedimentos próprios de segurança física e do ambiente** que deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

a) O acesso físico ao ambiente deverá ser monitorado e controlado para assegurar que somente pessoas autorizadas tenham acesso.

b) Agentes públicos e prestadores de serviços deverão ser identificados por meio do uso de crachá.

c) A área responsável pela segurança organizacional/corporativa da FBN deverá implementar perímetros de segurança a fim de garantir proteção e separação entre ambientes internos e externos.

d) Agentes públicos e prestadores de serviço desligados deverão ser excluídos da relação de pessoas autorizadas para acessar as dependências.

e) Os arquivos físicos, assim como os digitais, deverão ser protegidos e estabelecidos em locais de acesso restrito e devidamente trancados em sala ou armário específico com o controle de acesso sob responsabilidade do gestor responsável pelos ativos.

5.3. Da Gestão de Incidentes em Segurança da Informação

Nos termos da **Norma Complementar 05/IN01/DSIC/GSIPR**,

> *Tratamento de Incidentes de Segurança em Redes Computacionais é o 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.*

A **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)**, ficará responsável pela divulgação de práticas, recomendações e avaliações de segurança da informação considerando, no mínimo, as seguintes diretrizes:

a) Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas.

b) O tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

c) Durante o gerenciamento de incidentes de segurança em redes computacionais, havendo indícios de ilícitos criminais, a ETIR tem como dever, sem prejuízo de suas demais atribuições, acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços da FBN.

d) A ocorrência de incidentes de segurança em redes de computadores da FBN deverá ser comunicada pela ETIR ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) do Gabinete de Segurança Institucional da Presidência da República, conforme procedimentos definidos pelo próprio centro, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas.

e) A atuação da ETIR será orientada por normas, padrões e procedimentos técnicos exarados pelo **Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov)**, sem prejuízo das demais metodologias e padrões conhecidos ou que vierem aprovados pelo Comitê de Governança Digital.

5.4. Da Gestão de Ativos da Informação

a) Os ativos da informação, sistemas e banco de dados da FBN deverão ser protegidos contra indisponibilidade, acessos indevidos, alterações, falhas, perdas, danos, furtos, roubos e interrupções não programadas.

b) Os ativos de informação deverão ser inventariados e mapeados a fim de produzir subsídios para a Gestão de Segurança da Informação, Gestão de Riscos de Segurança da Informação, Gestão de Continuidade de Negócios, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas e de auditoria.

c) O processo de inventário e mapeamento de ativos de informação deve ser dinâmico, periódico e estruturado para manter a Base de Dados de Ativos de Informação atualizada para prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação no âmbito da FBN.

5.5. Da Gestão do Uso dos Recursos Operacionais e de Comunicações

Diretrizes específicas e procedimentos próprios da **gestão do uso dos recursos operacionais e de comunicações** serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

a) Os ativos de informação deverão ser disponibilizados pela área de tecnologia da informação da FBN somente para usuários de informação cadastrados, mediante a utilização de credenciais individuais e intransferíveis, concedidas conforme solicitação da chefia imediata.

b) Será autorizado o uso de equipamentos pessoais em atividades institucionais somente com a implementação de soluções de segurança da informação com padrões que atendam aos princípios definidos na POSIN, nesses equipamentos.

c) Os ativos de informação disponibilizados pela FBN deverão ser utilizados exclusivamente para a execução de atividades institucionais.

d) Toda a informação que trafega pelos ativos de informação poderá ser monitorada de acordo com as necessidades de segurança da informação estabelecidas em norma interna da FBN, conforme diretrizes desta POSIN e respeitada a legislação vigente.

e) Em caso de desligamento ou impedimento de um agente público que tenha executado atividades na FBN, sua chefia imediata poderá requisitar a recuperação de informações armazenadas em ativos de informação que estejam sob a guarda da instituição, com a finalidade de continuidade das atividades realizadas pelo agente público.

f) Serão estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os agentes públicos que executem atividades na FBN, de acordo com suas competências funcionais.

5.6. Do Uso do Correio Eletrônico Institucional

Diretrizes específicas e procedimentos próprios do **uso do serviço de correio eletrônico institucional (e-mail)** serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

a) O serviço de correio eletrônico institucional será oferecido como um recurso institucional para apoiar os seus usuários de informação no cumprimento das atividades institucionais.

b) O correio eletrônico institucional deverá ser utilizado somente para fins corporativos e relacionados às atividades do agente público, sendo vedado o uso para fins pessoais.

5.7. Do Uso e Acesso à Internet

Diretrizes específicas e procedimentos próprios de controles do **uso e acesso à internet** serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

a) A concessão de acesso à internet no âmbito da instituição será limitada às atividades de trabalho do usuário de informação, seguindo os procedimentos definidos em norma interna de segurança da informação, em conformidade com as diretrizes desta POSIN, orientações governamentais e legislações específicas em vigor.

b) As solicitações de exceção de acesso deverão ser justificadas pelo usuário de informação e consentidas pela autoridade hierarquicamente superior, cabendo à área de segurança da informação realizar a análise dos riscos da exceção e encaminhar à avaliação da aprovação final pelo Gestor de Segurança da Informação.

c) Os ativos de informação fornecidos pela FBN poderão ser analisados, a qualquer tempo, pela área de tecnologia da informação a fim de assegurar o cumprimento das disposições relacionadas as responsabilidades do usuário de informação, desta POSIN.

d) Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, a FBN, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à internet.

e) Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, caixa postal de correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação de trabalho ou em áreas privadas da rede, visando a assegurar o cumprimento de sua POSIN.

f) Publicações oficiais na internet deverão ser autorizadas pela área responsável pelo conteúdo.

5.8. Do Uso Institucional das Redes Sociais

Diretrizes específicas e procedimentos próprios do **uso institucional das redes sociais** serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

a) A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgar ou compartilhar informações da FCP será regida por normas internas específicas e deverá estar em consonância com esta POSIN e com os objetivos estratégicos da FCP.

b) Os perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo.

5.9. Do Uso de Dispositivos Móveis

Diretrizes específicas e procedimentos próprios do **uso de dispositivos móveis** serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

a) O uso de dispositivos móveis para acesso aos recursos computacionais da FBN deverá ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso.

b) Os procedimentos específicos para o uso de dispositivos móveis, pessoais e institucionais, que acessarem aos ativos de informação da FBN, serão definidos por norma interna de segurança, conforme diretrizes desta Política de Segurança da Informação.

5.10. Do Uso de Computação em Nuvem

Diretrizes específicas e procedimentos próprios para **a implementação ou contração de computação em nuvem** serão regulamentados em norma complementar considerando a **Instrução Normativa nº 5, de 30 de agosto de 2021** e as seguintes diretrizes gerais:

a) O uso de recursos de computação em nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação será regido por norma interna de segurança da informação que deverá ser instituída pela unidade responsável pelos ativos de tecnologia e atenderá às determinações desta POSIN.

b) Fica vedado o uso de recurso de computação em nuvem não disponibilizado pela FBN para o armazenamento de ativo de informação institucional.

5.11. Do Serviço de Backup e Restore

Os procedimentos próprios ao **serviço de *backup* (cópia de segurança) e *restore* (restauração de cópia de segurança)** serão regulamentados em norma complementar, considerando as seguintes diretrizes gerais:

a) O serviço de *backup* e *restore* deve ser automatizado por sistemas informacionais próprios considerando, inclusive, a execução agendada fora do horário de expediente normal da FBN, nas chamadas "janelas de *backup*" – períodos em que não há nenhum ou pouco acesso de usuários de informação ou processos automatizados aos sistemas de informática.

b) A solução de *backup* deverá ser mantida atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros).

c) A administração das mídias de *backup* deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter sua segurança e integridade.

d) É necessária previsão, em orçamento anual, da renovação das mídias de *backup* em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

e) As mídias de *backup*s deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas-cofre, objetivando manter a sua segurança e integridade.

f) Os *backups* críticos para o bom funcionamento dos serviços da FBN exigem uma regra de retenção especial, a ser prevista nos procedimentos específicos e de acordo com as normas de classificação da informação pública, seguindo ainda as determinações fiscais e legais existentes no país.

g) A execução de rotinas de *backup* e *restore* deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

5.12. Do Data Center BN

Os procedimentos para administração do **centro de processamento de dados (Data Center)** serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

a) A administração de dados e de serviços de Data Center é tarefa tecnicamente complexa cuja gestão é competência exclusiva da área de tecnologia da informação da FBN.

b) O acesso físico ao Data Center deverá ser feito por sistema de autenticação forte, mediante uso de solução de TIC adequada. O acesso físico por meio de chave apenas poderá ocorrer em emergências, quando a segurança física do Data Center estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

c) O acesso ao Data Center por visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor autorizado, que deverá preencher a solicitação de acesso prevista em norma complementar.

d) Deverá ser executada, em frequência predeterminada, auditoria dos acessos ao Data Center – por meio de relatório do sistema de registro próprio.

e) A lista de usuários com direito de acesso ao Data Center deverá ser constantemente atualizada. Ocorrendo o desligamento de usuários que possuam acesso ao Data Center, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de usuários autorizados.

f) A função de administrador do Data Center – incluindo seu sistema de autenticação forte – deverá ser atribuída exclusivamente a servidor público efetivo, preferencialmente vinculado à área de infraestrutura de TIC.

5.13. Dos Controles de Acesso

Diretrizes específicas e procedimentos próprios dos **controles de acesso físico e lógico** serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

a) Como condição imprescindível à concessão de acessos aos ativos de informação o usuário de informação deverá firmar termo de responsabilidade de ciência das normas gerais de segurança da informação contidas nesta política.

b) O controle de acesso deverá observar, na configuração das contas e concessão de credenciais de acesso o princípio do menor privilégio, que define que pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

c) A criação e administração de conta será realizada de acordo com procedimento específico para todo e qualquer usuário de informação. Para o usuário que não exerce funções de administração de rede será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

d) Os gestores, administradores e operadores dos recursos computacionais poderão, pela característica de suas credenciais (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários de informação – observadas as restrições quanto ao acesso às informações invioláveis e mediante estrita necessidade do serviço.

e) O acesso à rede corporativa deve ocorrer de forma a permitir a rastreabilidade e a identificação do usuário de informação, permitindo seu reconhecimento de maneira clara, inequívoca e irrefutável por período mínimo a ser definido em norma específica.

f) Sempre que ocorrer mudança nas atribuições de determinado usuário de informação, os seus privilégios de acesso aos ativos de informação deverão ser imediatamente readequados, devendo ser cancelados em caso de seu desligamento da FBN.

g) A FBN poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da POSIN ou das normas e procedimentos específicos dela decorrentes.

5.14. Da Gestão de Riscos em Segurança da Informação

Nos termos da **Instrução Normativa 03/GSI/PR,**

> *O processo de gestão de riscos de segurança da informação tem por objetivo direcionar e controlar o risco de segurança da informação, a fim de adequá-lo aos níveis aceitáveis para o órgão ou entidade.*

A Gestão de Riscos em Segurança da Informação será instituída por norma interna de segurança da informação da FBN com vistas a identificar os ativos de informação relevantes e determinar ações de gestão apropriadas, considerando as seguintes diretrizes:

a) O processo de levantamento de riscos deverá avaliar os riscos relativos à segurança dos ativos de informação e a conformidade com as exigências regulatórias ou legais.

b) A Gestão de Riscos em Segurança da Informação deverá estar alinhada às diretrizes desta POSIN e com a unidade administrativa responsável pela Gestão de Riscos da FBN, implementando, no que couber, suas diretrizes e procedimentos.

5.15. Da Gestão de Vulnerabilidades Técnicas

a) A Gestão de Vulnerabilidades Técnicas será implementada com vistas a prevenir a exploração de vulnerabilidades na rede corporativa da FBN por meio da aplicação sistemática de ações de identificação, classificação e tratamento de vulnerabilidades, sendo regulamentada por norma interna de segurança da informação da FBN.

b) O processo de Gestão de Vulnerabilidades deverá assegurar que sejam disponibilizadas à Alta Administração e ao Comitê de Governança Digital, sempre que solicitado, as informações sobre vulnerabilidades referentes aos ativos de rede e de sistemas informatizados geridos pela área de tecnologia da informação, de forma a permitir a eficaz detecção e remediação de vulnerabilidades no menor tempo possível.

c) O inventário completo e atualizado dos ativos de rede e sistemas informatizados será pré-requisito para o efetivo processo de gestão de vulnerabilidades e deverá identificar, no mínimo, os ativos de hardware, software, serviços em nuvem, o grau de criticidade e o respectivo responsável pela sua gestão.

5.16. Da Gestão de Continuidade de Negócios em Segurança da Informação

a) A FBN deverá manter processo de Gestão de Continuidade de Negócios em Segurança da Informação que forneça estrutura a fim de permitir a continuidade das atividades e, caso sejam interrompidas, assegurar a sua retomada em tempo hábil.

b) Os ativos de informação de propriedade ou custodiados pela FBN, quando armazenados em meio eletrônico, deverão ser providos de cópia de segurança atualizada e guardada em local seguro, de forma a garantir a continuidade das atividades do órgão.

c) Deverá ser elaborado um Plano de Continuidade de Negócios em Segurança da Informação que contenha os procedimentos e as informações necessárias para que a FBN mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente.

d) O Plano de Continuidade de Negócios em Segurança da Informação – PCN será elaborado pelo Subcomitê Gestor de Segurança da Informação (SGSI) e deverá ser testado e revisado periodicamente, de forma a se manter atualizado para responder às ameaças identificadas.

5.17. Da Auditoria e Conformidade

Para garantir a aplicação das diretrizes mencionadas nesta POSIN, além de fixar normas e procedimentos complementares sobre o tema, a FBN poderá:

a) Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

b) Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Governança Digital.

c) Realizar, a qualquer tempo e sem prévio aviso, inspeções físicas nos equipamentos e instalações de sua propriedade.

d) Instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança das informações e dos perímetros de acesso.

e) Desinstalar, a qualquer tempo e sem prévio aviso, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

6. Das Responsabilidades em Segurança da Informação

6.1. Da Estrutura para a Gestão da Segurança da Informação

De forma a estruturar a gestão da segurança da informação, a FBN designará:

a) **O Gestor de Segurança da Informação –** será designado dentre os servidores públicos ocupantes de cargo efetivo e militares de carreira, com formação ou capacitação técnica compatível com a legislação vigente;

b) **O Subcomitê Gestor de Segurança da Informação (SGSI) –** com atuação subordinada ao Comitê de Governança Digital; e

c) **A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) –** será estruturada em norma complementar.

6.2. Das competências do Gestor de Segurança da Informação

Ao **Gestor de Segurança da Informação** compete:

a. Coordenar o Subcomitê Gestor de Segurança da Informação (SGSI).

b. Planejar, coordenar, supervisionar, executar e controlar a execução das atividades de Tecnologia da Informação em conformidade com as diretrizes desta POSIN.

c. Assessorar a alta administração na implementação da Política de Segurança da Informação - POSIN e das normas complementares.

d. Definir estratégias para a implementação desta POSIN e suas normas internas de segurança da informação.

e. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas.

f. Encaminhar os fatos apurados, decorrentes de quebra de segurança, para a aplicação das penalidades previstas nesta POSIN.

g. Verificar se os procedimentos de Segurança da Informação estão sendo aplicados de forma a atender à conformidade com legislações vigentes a respeito do assunto e normativos internos específicos.

h. Promover, com apoio da alta administração, a ampla divulgação da Política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os usuários de informação e aos prestadores de serviço

i. Caberá ao gestor de segurança da informação propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos, avaliar os incidentes de segurança, propor ações corretivas e definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação - POSIN e/ou das normas de

segurança da informação complementares.

j. Acompanhar as atividades da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

k. Promover a melhoria contínua dos processos de gestão de segurança da informação e propor ajustes corretivos a serem incluídos nas revisões desta POSIN.

l. Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação

m. Propor conteúdo sobre segurança da informação, com vistas a facilitar a capacitação e a instrução dos servidores e colaboradores para a utilização de sistemas corporativos e acesso a informações nos níveis físico e lógico, em conformidade com as diretrizes desta POSIN.

6.3. Das competências do Subcomitê de Segurança da Informação

Compete ao **Subcomitê Gestor de Segurança da Informação da FBN (SGSI)**:

a) Subsidiar o Comitê de Governança Digital da FBN nas decisões relativas à Segurança da Informação.

b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação.

c) Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação.

d) Propor alterações e revisar periodicamente a POSIN e as normas internas de segurança da informação, em conformidade com a legislação existente sobre o tema.

e) Propor investimentos relacionados à segurança da informação.

f) Propor procedimentos administrativos e definir medidas corretivas e punitivas cabíveis nos casos de descumprimento da POSIN.

g) Coordenar a Equipe de Prevenção, Tratamento Resposta a Incidentes Cibernéticos (ETIR).

O Subcomitê Gestor de Segurança da Informação (SGSI) terá a seguinte composição:

a) O Gestor de Segurança da Informação, que o coordenará.

b) Um representante da Diretoria Executiva.

c) Um representante de cada Unidade Finalística.

d) O Encarregado pelo Tratamento de Dados Pessoais.

6.4. Das competências da ETIR

A **Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)** será composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacitação técnica compatível com as atividades dessa equipe. São competências da ETIR:

a) Subsidiar o Subcomitê de Gestão de Segurança da Informação nos assuntos relacionados à Segurança da Informação;

b) Gerenciar incidentes de segurança da informação;

c) Investigar e avaliar danos decorrentes de quebras de segurança;

d) Registrar todos os incidentes de segurança da informação, com a finalidade de assegurar registro histórico das atividades da ETIR;

e) Realizar tratamento da informação de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo (CTIR Gov), sem prejuízo das demais metodologias e padrões conhecidos.

6.5. Responsabilidades Gerais

São responsabilidades gerais e comuns a todos os usuários de informação e gestores de serviços de rede de dados, *internet*, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação da FBN:

a) Zelar pela segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso.

b) Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos corporativos de informação – utilizando-os sempre de forma ética, legal e consciente.

c) Manter-se atualizado em relação a esta POSIN e às suas normas complementares e procedimentos relacionados, buscando informação junto ao Gestor de Segurança da Informação sempre que não estiver absolutamente seguro quanto à obtenção, tratamento, uso ou descarte de informações.

6.6. Responsabilidade dos Usuários de Informação

O **Usuário de Informação** é a pessoa física, servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação da FBN.

Todo prejuízo ou dano decorrente da não obediência às diretrizes e normas referenciadas nesta POSIN e nas normas e procedimentos específicos delas decorrentes é de inteira responsabilidade do usuário de informação que o der causa.

Os usuários de informação devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos vigentes de segurança da informação.

A FBN poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários de informação em virtude do descumprimento desta POSIN ou das normas complementares e procedimentos específicos delas decorrentes.

O desconhecimento das regras contidas nesta POSIN é inescusável, ou seja, a alegação de seu desconhecimento não exime o usuário de suas responsabilidades por atos praticados em sua desconformidade.

6.7. Responsabilidade dos Gestores de Pessoas e Processos

Os gestores executivos da FBN devem manter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários de informação sob sua gestão.

Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de Segurança da Informação da FBN, tomando as ações necessárias para cumprir tal responsabilidade.

6.8. Responsabilidade da Área de Tecnologia da Informação

a) Zelar pela eficácia dos controles de segurança da informação utilizados e informar aos gestores e demais interessados os riscos residuais.

b) Negociar e acordar com os gestores níveis de serviço relacionados à segurança da informação, incluindo os procedimentos de resposta a incidentes.

c) Configurar os recursos informacionais e computacionais concedidos aos usuários de informação com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação.

d) Gerar e manter trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas ou mantidas em meio eletrônico, devem ser implantados controles de integridade, de modo a torná-las juridicamente válidas como evidências.

e) Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

f) Zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações.

g) Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para a FBN.

h) Implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

i) Informar previamente o Gestor de Segurança da Informação sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custo diante.

j) Nas movimentações internas dos ativos de TIC, assegurar-se de que as informações de determinado usuário de informação não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

k) Gerir a capacidade de armazenamento, processamento e transmissão de dados de forma a garantir os níveis de segurança requeridos.

l) Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta.

m) Proteger continuamente todos os ativos de informação contra ameaças de segurança, buscando assegurar que novos ativos apenas sejam integrados ao ambiente de produção após cumprirem os requisitos de segurança da informação definidos.

n) Zelar pela não introdução de vulnerabilidades ou fragilidades indesejadas nos ativos de informação ou nos ambientes informacionais da FBN durante sua operação ou durante eventos de mudança de ambiente (de desenvolvimento para teste, homologação ou produção, por exemplo).

o) Definir regras para instalação de softwares e hardwares no ambiente corporativo e demais ambientes vinculados, incluindo aqueles dedicados ao uso pelo público externo.

p) Definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos.

q) Responsabilizar-se pelo uso, manuseio, guarda de assinatura de certificados digitais corporativos.

r) Garantir, da forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários de informação por motivo de desligamento da FBN, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos do instituto.

s) Garantir que todos os servidores, estações de trabalho e demais dispositivos com acesso à rede operem com o relógio sincronizado com os servidores de tempo oficiais do Governo Brasileiro.

t) Monitorar o ambiente de TIC, gerando indicadores e históricos de uso da capacidade instalada da rede e dos equipamentos; tempo de resposta no acesso à internet e aos sistemas críticos; períodos de indisponibilidade no acesso à internet e aos sistemas críticos; incidentes de segurança; e atividade de todos os usuários durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos).

7. Das infrações e penalidades aplicáveis

A FBN, ao gerir e monitorar seus ativos de informação, pretende garantir a integridade destes. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, às quais a FBN responderá com a aplicação de todas as medidas administrativas, cíveis e judiciais cabíveis.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário de informação, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo superior hierárquico.

O uso de qualquer recurso em inobservância às normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes.

Os dispositivos de identificação e senhas protegem a identidade do usuário de informação, evitando e prevenindo que uma pessoa se faça passar por outra perante a FBN ou terceiros. Portanto, o usuário de informação vinculado a tais dispositivos identificadores será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal), sendo que o uso dos dispositivos ou senhas de identificação de outra pessoa viola as regras de segurança e poderá resultar na aplicação de medidas administrativas, cíveis e judiciais cabíveis.

O Código Penal Brasileiro (Decreto-Lei n° 2.848/1940, art. 154-A) tipifica como crime o ato de “invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita” (redação dada pela Lei nº 14.155/2021), assim como comete crime “quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento” (art. 154-B, incluído pela Lei nº 12.737/ 2012).

8. Estrutura Normativa de Gestão de Segurança da Informação

Os documentos que compõem a estrutura normativa serão divididos em três categorias:

a) **Política – nível estratégico:** constituída do presente documento, define as regras de alto nível que representam os princípios básicos que a FBN decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados.

b) **Normas complementares – nível tático:** especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nas diretrizes da política.

c) **Procedimentos – nível operacional:** instrumentalizam o disposto nas normas complementares e na política, permitindo sua aplicação direta nas atividades cotidianas da FBN.

9. Referências Legais e Normativas

9.1. Segurança da Informação

Decreto nº 10.748, de 16 de julho de 2021	Institui a Rede Federal de Gestão de Incidentes Cibernéticos.
Decreto nº 10.641, de 2 de março de 2021	Altera o 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 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.
Decreto nº 10.569, de 9 de dezembro de 2020	Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.
Decreto nº 10.222, de 5 de fevereiro de 2020	Aprova a Estratégia Nacional de Segurança Cibernética.
Decreto nº 9.832, de 12 de junho de 2019	Altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação.
Decreto nº 9.637, de 26 de dezembro de 2018	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. Alterado pelo Decreto nº 9.832, de 12 de junho de 2019. Alterado pelo Decreto nº 10.641, de 2 de março de 2021.
Decreto nº 9.573, de 22 de novembro de 2018	Aprova a Política Nacional de Segurança de Infraestruturas Críticas.
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.
Decreto nº 1.171, de 22 de junho de 1994	Dispõe sobre o Código de Ética do Servidor Público Civil do Poder Executivo Federal.
Instrução Normativa nº 5, de 30 de agosto de 2021	Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

Instrução Normativa GSI 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.
Instrução Normativa GSI nº 1, de 27 de maio de 2020	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
Portaria GSI nº 93, de 18 de outubro de 2021	Aprova o Glossário de Segurança da Informação.
Portaria GSI nº 40, de 8 de outubro de 2014	Homologa a Norma Complementar nº 21/IN01/DSIC/GSIPR - 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, direta e indireta.
Portaria GSI nº 57, de 23 de agosto de 2010	Homologa a Norma Complementar nº 08/IN01/DSIC/GSIPR - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais - Gestão de ETIR, nos órgãos e entidades da Administração Pública Federal.
Portaria GSI nº 38, de 14 de agosto de 2009	Homologa a Norma Complementar nº 05/IN01/DSIC/GSIPR - Disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.
Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.
NBR ISO/IEC 27001:2013	Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.
NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação.
NBR ISO/IEC 27003:2020	Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Orientações.
NBR ISO/IEC 27701:2019	Técnicas de segurança para gestão da privacidade da informação – Requisitos e diretrizes.
NBR ISO/IEC 27017:2016	Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação.

9.2. Proteção de Dados Pessoais

Lei nº 13.709, de 14 de agosto de 2018	Lei Geral de Proteção de Dados Pessoais.
Lei nº 12.965, de 23 de abril de 2014	Marco Civil da Internet - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Medida Provisória nº 1.124, de 13 de junho de 2022	Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão.
Decreto nº 8.771, de 11 de maio de 2016	Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

Instrução Normativa SGD nº 117, de 19 de novembro de 2020	Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

9.3. Portarias da FBN

Portaria nº 129, de 4 de setembro de 2013	Aprova o Plano Diretor de Tecnologia da Informação – PDTI 2013/2015 da FBN.
Portaria nº 36, de 11 de julho de 2022	Institui o Comitê de Governança Digital da FBN.

10. Das Disposições Finais

A atualização desta POSIN, bem como todos os instrumentos normativos gerados a partir dela, deverão ser revisados e atualizados sempre que se fizer necessário, não excedendo o **período máximo de 4 (quatro) anos**.

Esta POSIN e suas atualizações deverão ser divulgadas amplamente aos usuários de informações da FBN quando de sua admissão, e publicadas nos meios de comunicação corporativa, de maneira que seu conteúdo fique amplamente disponível e possa ser consultado por seus colaboradores a qualquer tempo.

Os casos omissos e as dúvidas na aplicação da POSIN e suas normas complementares serão encaminhadas ao Subcomitê de Gestão de Segurança da Informação (SGSI).