Boletim de Serviço Eletrônico em 30/06/2021

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
POLÍCIA RODOVIÁRIA FEDERAL
DIREÇÃO-GERAL

INSTRUÇÃO NORMATIVA PRF Nº 45, DE 22 DE JUNHO DE 2021

Institui a Política de Segurança da Informação da Polícia Rodoviária Federal.

O DIRETOR-GERAL DA POLÍCIA RODOVIÁRIA FEDERAL, no uso das atribuições que lhe foram conferidas no Decreto nº 9.662, de 1º de janeiro de 2019, observado o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, no Decreto nº 10.222, de 5 de fevereiro de 2020, na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, na Portaria MJ nº 3.530, de 3 de dezembro de 2013, no Decreto nº 10.139, de 28 de novembro de 2019, e tendo em vista o contido no Processo nº 08650.015719/2019-11, resolve:

Objeto e âmbito de aplicação

Art. 1º Instituir a Política de Segurança da Informação no âmbito da Polícia Rodoviária Federal (POSIN/PRF), a qual define competências e responsabilidades relativas ao manuseio de ativos de informação em conformidade com a legislação vigente, as especificidades da instituição, os valores éticos e com as melhores práticas de segurança da informação.

Parágrafo único. A POSIN/PRF aplica-se a todos os agentes públicos em atividade na PRF, devendo ser dado amplo conhecimento de seu teor a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos da PRF, com vistas a garantir a segurança das informações a que tenham acesso.

Art. 2º A POSIN/PRF alinha-se às diretrizes da Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018 e atualizada pelo Decreto nº 10.641, de 2 de março de 2021, às estratégias e POSIC do Ministério da Justiça e Segurança Pública (MJSP) e ao planejamento estratégico da PRF, cumprindo ao estabelecido no art. 9º e seguintes da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

CAPÍTULO I
DO ESCOPO

Objetivos

Art. 3º A POSIN/PRF tem por objetivo geral dotar as unidades da estrutura organizacional da PRF de princípios, diretrizes, critérios e instrumentos aptos a assegurar o

controle, disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, documentos, conhecimentos produzidos e/ou armazenados sob a guarda ou transmitidos por qualquer meio ou recurso da PRF, protegendo-os contra ameaças e vulnerabilidades.

Art. 4º São objetivos específicos da POSIN/PRF:

I - contribuir para a segurança da informação da instituição, do servidor e da sociedade 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 inovações relacionadas à segurança da informação e comunicação;

III - aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação e comunicação;

IV - fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação e comunicação; e

V - fortalecer a cultura e ações relacionadas com a segurança da informação especialmente as relacionadas a:

a) segurança das informações das ações de segurança pública;

b) segurança dos dados custodiados pela PRF;

c) segurança da informação das infraestruturas críticas;

d) proteção dos ativos de informação e de comunicação institucionais;

e) tratamento das informações que contenham dados pessoais; e

f) proteção dos materiais de acesso restrito.

Abrangência

Art. 5º A POSIN/PRF trata dos requisitos físicos, lógicos e humanos, bem como dos aspectos estratégicos, estruturais e organizacionais, abrangendo:

I - a segurança cibernética;

II - a segurança física dos ativos de informação e de comunicação;

III - a proteção dos dados organizacionais restritos ou classificados em grau de sigilo;

IV - a proteção dos conhecimentos institucionais;

V - a segurança dos planos operacionais;

VI - as ações destinadas a assegurar os princípios basilares da segurança da informação.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para efeitos da POSIN/PRF considera-se:

I - acessibilidade: qualidade do que é acessível;

II - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

III - agente público: toda pessoa física que presta serviços ao Estado, remuneradamente ou gratuitamente, permanentemente ou transitoriamente, politicamente ou administrativamente. Exemplo: servidor público, empregado público, agente terceirizado, estagiário, trabalhador que desempenha função temporária;

IV - algoritmo de Estado: função matemática utilizada na cifração e na decifração, desenvolvida pelo Estado, para uso exclusivo no interesse do serviço de órgãos ou entidades da Administração Pública Federal, direta e indireta, não comercializável;

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

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

VII - auditabilidade: atributo que garante a rastreabilidade dos diversos passos de um processo, identificando os participantes, ações e horários de cada etapa;

VIII - auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos;

IX - 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;

X - conformidade em segurança da informação: cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da instituição;

XI -confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados;

XII - conhecimento - corresponde aos conhecimentos que a instituição adquiriu e produziu ao longo do tempo e que torna possível que ela execute os processos inerentes as suas competências legais, assim, fornecendo serviços de segurança pública de excelência para sociedade;

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

XIV - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

XV - custodiante do ativo de informação: aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertença, mas que estejam sob sua guarda;

XVI - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou por determinado sistema, órgão ou entidade;

XVII - documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

XVIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e Autoridade Nacional de Proteção de Dados (ANPD);

XIX - Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRI): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores e de implementar a segurança da informação na PRF;

XX - ética: observância do Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto no 1.171, de 22 de junho de 1994, e demais regras de conduta normativamente delimitadas para os agentes públicos;

XXI - Gestão de Segurança da Informação (GSIN): ações e métodos que visam à integração das atividades de gestão de riscos, à continuidade de serviços, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional dos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto à tecnologia da informação e comunicações;

XXII - gestão de risco: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXIII - incidente de segurança: qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistema de computação ou de redes de computadores;

XXIV - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVI - interoperabilidade: habilidade de dois ou mais sistemas (computadores, meios de comunicação, redes, softwares e outros componentes de tecnologia da informação) de interagir e de intercambiar dados de acordo com um método definido, de forma a obter os resultados esperados;

XXVII - legalidade: observância dos parâmetros legais e regulamentares na implementação das ações de SIC;

XXVIII - manuseio: acesso, uso, compartilhamento, transmissão, arquivo, descarte e recuperação de ativos de informações;

XXIX - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XXX - política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta ou indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativos suficientes à implementação da segurança da informação e a comunicações;

XXXI - princípios: são ideias centrais que estabelecem diretrizes a uma instituição, delimitadas por instrumentos legais, diretrizes de governo, recomendações e determinações das instâncias de controle;

XXXII - privacidade: proteção do direito individual da pessoa contra a inviolabilidade de sua intimidade, de sua vida privada e do sigilo de suas comunicações, observado o disposto no art. 31 da Lei nº 12.527, de 18 de novembro de 2011, e nos arts. 55 a 62 do Decreto nº 7.724, de 16 de maio de 2012;

XXXIII - publicidade: divulgação da POSIN/PRF e de todas as normas complementares aos agentes públicos em exercício na PRF;

XXXIV - quebra de segurança: ação ou omissão, intencional ou acidental, que impacta negativamente na segurança da informação e das comunicações;

XXXV - rastreabilidade: é a capacidade de traçar o histórico, a aplicação ou a localização de um item por meio de informações previamente registradas;

XXXVI - segurança: proteção dos ativos de informação contra perda, corrupção, destruição, acesso, uso e alteração indevidos ou não autorizados;

XXXVII - Segurança da Informação (SI): ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXVIII - termo de responsabilidade para manuseio dos ativos de informação: documento assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XXXIX - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XL - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XLI - tratamento da informação: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XLII - usuário: qualquer pessoa que manuseie ativos de informação da PRF mediante autorização dos gestores de ativos; e

XLIII - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente de segurança, que pode ser evitado por uma ação de SI.

Referências legais e normativas

Art. 7º A POSIN/PRF observa a legislação e normas específicas, a seguir:

I - Lei nº 8.159, de 8 de janeiro de 1991: dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

II - Decreto nº 4.073, de 3 de janeiro de 2002: Regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

III - Lei nº 12.527, de 2011: dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

IV - Decreto nº 7.724, de 16 de maio de 2012: regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei nº 12.527, de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do **caput** do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

V - Decreto nº 7.845, de 14 de novembro de 2012: regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o núcleo de segurança e credenciamento;

VI - Portaria nº 3.530, de 3 de dezembro de 2013, do Ministério da Justiça: a Política de Segurança da Informação e Comunicações do Ministério da Justiça (POSIC/MJ), e dá outras providências;

VII - 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 e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria;

VIII - Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD): dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

IX - Decreto nº 9.637, de 26 de dezembro de 2018: institui a Política Nacional de Segurança da Informação (PNSI), dispõe sobre a governança da segurança da informação e demais providências e sua alteração disposta no Decreto nº 10.641, de 2 de março de 2021;

X - Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR): aprova o Glossário de Segurança da Informação;

XI - Decreto nº 10.222, de 5 de fevereiro de 2020: aprova a Estratégia Nacional de Segurança Cibernética;

XII - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020: disciplina a estrutura de gestão da segurança da informação nos órgãos e nas entidades da Administração Pública Federal;

XIII - Instrução Normativa GSI/PR nº 2, de 24 de julho de 2020: altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

XIV - Norma Complementar nº 5/IN nº1/DSIC/GSI/PR: disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal; e

XV - Norma Complementar nº 8/IN nº 1/DSIC/GSI/PR: estabelece as diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 8º A segurança da informação tem como princípios básicos a confidencialidade, a integridade, a disponibilidade e a autenticidade e buscam:

I - estabelecer medidas e procedimentos relativos ao manuseio dos ativos de informação, com o objetivo de viabilizar e assegurar os princípios básicos relacionados com a segurança da informação.

II - desenvolver, implementar e monitorar estratégias de segurança da informação que atendam aos objetivos estratégicos da PRF;

III - avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

IV - fornecer subsídios visando à verificação de conformidade em Segurança da Informação;

V - promover a melhoria contínua nos processos e controles de Gestão de Segurança da Informação; e

VI – promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação.

CAPÍTULO IV
DA ESTRUTURA E COMPETÊNCIAS DA POSIN/PRF

Gestão da Segurança da Informação

Art. 9º A Gestão da Segurança da Informação (GSIN) deve apoiar e orientar a tomada de decisões institucionais, estabelecer processos de controle e otimizar investimentos em segurança que visem à eficiência, à eficácia e à efetividade das atividades de segurança da informação.

Art. 10. A GSIN deve compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à segurança da informação, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiem, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais e especificidades da PRF.

Art. 11. A PRF contará com as seguintes estruturas de apoio à GSIN:

I - Gestor de Segurança da Informação e substituto, a serem designados pelo Diretor-Geral da PRF;

II - Comitê Gestor de Segurança da Informação (CGSI);

III - Gestores Regionais e substitutos de Segurança da Informação;

IV - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETRI);

V - Equipes de Tratamento e Resposta a Incidentes de Segurança da Informação Regionais - (ETRI-(UF));

VI - Comissão permanente de avaliação de documentos sigilosos para fins de assessoramento permanente ao comitê gestor de segurança da informação da polícia rodoviária federal, sem prejuízo das atribuições previstas no art. 34 do Decreto nº 7.724, de 16 de maio de 2012; e

VII - Comissões permanentes de avaliação de documentos sigilosos nas unidades desconcentradas.

Gestor de Segurança da Informação e Comunicações

Art. 12. O Gestor de Segurança da Informação deve ser servidor público efetivo, preferencialmente lotado na Diretoria de Inteligência – DINT ou sua congênere a depender da estrutura organizacional da PRF, cabendo-lhe:

I - promover a cultura de segurança da informação com apoio da alta administração, visando a ampla divulgação da política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os servidores, funcionários terceirizados, prestadores de serviços e estagiários;

II - promover o gerenciamento de riscos envolvendo ativos de informação;

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

IV - pesquisar e acompanhar estudos de novas tecnologias, ligados a segurança da informação;

V - propor normas internas e procedimentos relativos à segurança da informação no âmbito da PRF;

VI - examinar, formular, promover e coordenar as ações de segurança da informação, em articulação com o gestor de segurança da informação do Ministério da Justiça e Segurança Pública e com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

VII - propor às autoridades competentes os recursos necessários às ações de segurança da informação;

VIII - coordenar o comitê de segurança da informação e a equipe de tratamento e resposta a incidentes de segurança da informação; e

IX - resolver os casos omissos e as dúvidas surgidas na aplicação desta política.

Comitê Gestor de Segurança da Informação - CGSI

Art. 13. Fica instituído o Comitê Gestor de Segurança da Informação (CGSI), o qual será composto pelo Gestor de Segurança da Informação e um representante titular e um suplente indicados de cada unidade, ou sua congênere, a depender da estrutura organizacional da PRF, conforme abaixo:

I - Gabinete da Direção-Geral (GAB);

II - Diretoria-Executiva (DIREX);

III - Diretoria de Inteligência (DINT);

IV - Diretoria de Gestão de Pessoas (DGP);

V - Diretoria de Operações (DIOP);

VI - Diretoria de Administração e Logística (DIAD);

VII - Corregedoria-Geral (CG); e

VIII - Diretoria de Tecnologia da Informação e Comunicação (DTIC).

§ 1º Os representantes do comitê e seus suplentes serão designados mediante ato do Diretor-Geral.

§ 2º A participação no comitê será considerada serviço público relevante e não ensejará remuneração de qualquer espécie.

§ 3º O comitê poderá convidar outros técnicos para colaborarem nos trabalhos a serem desenvolvidos, sem direito a voto.

§ 4º As deliberações do comitê serão tomadas por maioria simples, presente a maioria absoluta de seus membros.

§ 5º O comitê se reunirá a cada três meses, podendo haver convocação extraordinária, a critério do gestor de segurança da informação.

Art. 14. Ao CGSI compete:

I - assessorar a Direção-Geral na implementação das ações e aperfeiçoamento da gestão da segurança da informação;

II - sugerir à Direção-Geral a constituição de grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - acompanhar averiguações e avaliações de danos decorrentes de quebras de segurança;

IV - propor alterações ou criação de normativos e procedimentos internos relativos à segurança da informação, em conformidade com as legislações existentes sobre o tema;

V - auxiliar na elaboração dos planos de gestão de riscos e de continuidade e na definição das diretrizes de auditoria e conformidade;

VI - revisar esta política a cada dois anos ou sempre que se fizer necessário;

VII - elaborar relatórios periódicos de suas atividades, encaminhando-os à Direção-Geral;

VIII - propor plano de investimentos em segurança da informação;

IX - promover, no âmbito da PRF, a cultura de segurança da informação, elaborando e implementando os programas destinados a conscientização e capacitação de servidores, funcionários terceirizados, prestadores de serviços e estagiários;

X - receber e analisar as comunicações de descumprimento das normas referentes à POSIN/PRF, apresentando parecer à autoridade competente; e

XI - auxiliar no gerenciamento de riscos organizacionais.

Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - ETRI

Art. 15. A ETRI será formada por integrantes da Diretoria de Tecnologia da Informação e Comunicação (DTIC) e da Diretoria de Inteligência (DINT), ou suas congêneres, sendo composta por dois representantes indicados de cada unidade a seguir:

I – Área de Contrainteligência;

II – Área de Infraestrutura e Aplicações; e

III - Área de Integração, Segurança e Ciência de Dados.

Parágrafo único. Os representantes da equipe e seus suplentes serão designados mediante ato conjunto do Diretor de Tecnologia da Informação e Comunicação e do Diretor de Inteligência, respectivamente.

Art. 16. Compete à ETRI:

I - receber, analisar e responder de forma tempestiva às notificações relacionadas a problemas e ou incidentes de segurança em redes computacionais da PRF;

II - comunicar sobre a ocorrência de todos os incidentes de segurança da informação;

III - gerar estatísticas sobre incidentes de segurança da informação;

IV - trabalhar em conjunto com outras equipes;

V - fazer gestão de riscos de segurança da informação;

VI - apoiar na definição de políticas e normas de segurança da informação no âmbito da PRF;

VII - realizar monitoramentos visando a prevenção de atividade maliciosa contra os ativos institucionais de informação;

VIII - desenvolver e melhorar soluções de segurança, com análise preventiva dos equipamentos e de sistemas de redes e internet;

IX - ajudar na disseminação da cultura de segurança da informação no âmbito da PRF;

X - investigar as causas dos incidentes no ambiente computacional; e

XI - elaborar e implementar o plano de resposta a incidentes de segurança da informação.

Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - ETRI-(UF)

Art. 17. A ETRI das unidades desconcentradas será formada por integrantes da área de Tecnologia da Informação e Comunicação e da área de Inteligência, sendo composta por um representante indicado de cada unidade e substitutos.

Parágrafo único. Os representantes da equipe e seus suplentes serão designados mediante ato do Superintendente Regional e terão as mesmas competências da ETRI nacional, porém relacionadas aos eventos locais.

Comissão Permanente de Avaliação de Documentos Sigilosos

Art. 18. Fica instituída a Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) no âmbito da Sede da PRF, nos termos do art. 34 do Decreto nº 7.724, de 16 de maio de 2012, e do art. 7º da Portaria MJ nº 631, de 26 de julho de 2017, a qual será composta por um representante indicado de cada unidade a seguir, ou sua congênere a depender da estrutura organizacional da PRF :

I - Gabinete da Direção-Geral (GAB);

II - Diretoria-Executiva (DIREX);

III - Diretoria de Inteligência (DINT);

IV - Diretoria de Gestão de Pessoas (DGP);

V - Diretoria de Operações (DIOP);

VI - Diretoria de Administração e Logística (DIAD);

VII - Corregedoria-Geral (CG); e

VIII - Diretoria de Tecnologia da Informação e Comunicação (DTIC).

Parágrafo único. Os representantes da Comissão e seus suplentes serão designados mediante ato do Diretor-Geral.

Art. 19. Compete à CPADS:

I - opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo;

II - assessorar a autoridade classificadora ou a autoridade hierarquicamente superior quanto à desclassificação, reclassificação ou reavaliação de informação classificada em qualquer grau de sigilo;

III - propor o destino final das informações desclassificadas, indicando os documentos para guarda permanente, observado o disposto na Lei nº 8.159, de 8 de janeiro de 1991; e

IV - subsidiar a elaboração do rol anual de informações desclassificadas e documentos classificados em cada grau de sigilo, a ser disponibilizado na internet.

Comissões Permanentes de Avaliação de Documentos Sigilosos nas Unidades Desconcentradas

Art. 20. Ficam instituídas as Comissões Regionais de Avaliação de Documentos Sigilosos (CRADS), no âmbito das Superintendências da PRF sendo composta por um representante de cada unidade a seguir indicados:

I - Gabinete do Superintendente;

II - Área de inteligência;

III - área de gestão de pessoas;

IV - Área de operações;

V - Área de administração;

VI - área de corregedoria; e

VII - área de tecnologia da informação e comunicação.

Parágrafo único. Os representantes da comissão e seus suplentes serão designados mediante ato do Superintendente.

Art. 21. Compete às CRADS:

I - opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em grau de sigilo;

II - assessorar a autoridade classificadora regional quanto à desclassificação, reclassificação ou reavaliação de informação classificada em qualquer grau de sigilo; e

III - propor o destino final das informações desclassificadas no âmbito regional, indicando os documentos para guarda permanente, observado o disposto na Lei nº 8.159, de 8 de janeiro de 1991.

Gestor Regional de Segurança da Informação

Art. 22. O gestor regional de segurança da informação deve ser servidor público efetivo designado pelo Superintendente, preferencialmente vinculado à Atividade de Inteligência, cabendo-lhe:

I - acompanhar a implementação desta política no âmbito da Superintendência em que atue;

II - acompanhar averiguações e avaliações de danos decorrentes de quebras de segurança no âmbito da regional;

III - fomentar o cumprimento das diretrizes desta política no âmbito da regional; e

IV - Presidir a ETRI regional.

CAPÍTULO V
DAS DIRETRIZES GERAIS E ATIVOS DA INSTITUIÇÃO

Diretrizes

Art. 23. São diretrizes gerais da POSIN/PRF, sempre relativas aos ativos da informação:

I - tratamento da informação;

II - gestão do conhecimento institucional produzido;

III - gestão das informações operacionais de segurança pública;

IV - tratamento dos dados pessoais;

V - segurança física e do ambiente;

VI - gestão de incidentes em segurança da informação;

VII - gestão de ativos;

VIII - gestão de uso dos recursos informacionais;

IX - gestão do uso dos meios de comunicações;

X - controle de acessos;

XI - gestão de riscos;

XII - gestão de continuidade; e

XIII - auditoria e conformidade.

Tratamento da Informação

Art. 24. As informações geradas, adquiridas ou custodiadas que estejam sob a responsabilidade da PRF são consideradas parte do seu patrimônio, não cabendo a seus criadores qualquer forma de direito autoral, salvo aqueles direitos garantidos no âmbito da Lei de Inovação e outros dispositivos legais, e devem ser protegidas segundo as diretrizes descritas nesta política, em seus documentos complementares e demais regulamentações em vigor.

Art. 25. É vedada a terceiros a utilização de informações produzidas para uso exclusivo da PRF, salvo se autorizada pela instituição, observada a legislação em vigor.

Art. 26. Informações tecnicamente processadas que compõem os conhecimentos institucionais são de acesso restrito, devendo sua difusão ser controlada, bem como não é permitida divulgação externa sem autorização do Gestor.

Parágrafo único. É vedado o uso dos conhecimentos institucionais para fins privados, ainda que por servidores envolvidos na produção desses ativos.

Art. 27. As informações da PRF contidas em planos: operacionais, de distribuição de materiais controlados, de emprego de efetivo, de instalações físicas e de capacitação são ativos institucionais restritos vinculados à finalidade da segurança pública, cujo acesso não autorizado implica risco ou dano aos interesses da sociedade e do Estado, devendo sua difusão ser controlada e mantida no ambiente institucional sob acesso restrito.

Tratamento dos Dados Pessoais

Art. 28. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e

II - seja indicado um controlador e operador para realizarem operações de tratamento de dados pessoais, nos termos previsto da Lei de Geral de Proteção de Dados Pessoais (LGPD).

Art. 29. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 30. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da Lei nº 13.709, de 14 de agosto de 2018.

Segurança Física e do Ambiente

Art. 31. Deverão ser estabelecidas regras de controle de acesso para garantir a segurança física e do ambiente onde sejam tratados, manuseados ou armazenados os ativos de informação da PRF, devendo ser observados minimamente os seguintes critérios:

I - necessidade e orientações de instalação de sistemas de detecção de intrusos nas áreas e instalações sob suas responsabilidades;

II - classificação das áreas e instalações como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando aquelas áreas e instalações consideradas críticas;

III - orientação quanto ao uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída;

IV - estabelecimento de rotinas ou ações de prevenção contra ações de vandalismo, sabotagem, ataques, dentre outros, especialmente em relação àqueles considerados críticos;

V - levantamento da necessidade de implementação de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais;

VI - definição de pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado;

VII - a guarda segura dos materiais combustíveis ou perigosos, a uma distância apropriada das áreas de trabalho e áreas de segurança; e

VIII - intensificação de controles para as áreas e instalações consideradas críticas ou sensíveis em conformidade com a legislação vigente, deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física.

Parágrafo único. O controle de acesso, por meio de sistema biométrico, deve ser utilizado em conjunto com outro sistema de identificação (cartão, crachá, senha, chave, entre outros), a fim de atender os conceitos da autenticação de multifatores.

Art. 32. Todas as instalações de processamento de dados, transmissão ou armazenamento de informações sensíveis, devem ser mantidas em áreas de segurança com a utilização de barreiras de segurança e mecanismos de controle de acesso, de forma a prevenir acessos não autorizados ou contaminação ambiental, como as causadas por fogo ou inundação.

§1º Deve ser evitada a utilização de informações visuais que identifiquem essas salas de processamento.

§2º É proibido o manuseio de alimentos e bebidas, bem como o consumo nessas salas.

§3º Os cabeamentos, bem como as instalações elétricas dessas salas devem ser verificadas pelo pessoal de TIC com frequência;

§4º A rede elétrica deve ser estabilizada e equipada com dispositivos de proteção ativa e de autonomia de segurança.

Art. 33. Devem-se adotar mecanismos seguros para o descarte de mídias (incineração, trituração, etc.) a fim de garantir que informações armazenadas e sem uso sejam irrecuperáveis, observando as legislações pertinentes.

Art. 34. Devem ser considerados os requisitos de segurança em todas as fases de criação:

I - definição;

II - projeto;

III - desenvolvimento;

IV - implantação; e

V - manutenção.

Gestão de Ativos

Art. 35. Os ativos de informação, tangíveis e intangíveis, devem ser protegidos, de acordo com o seu valor, sua sensibilidade e sua criticidade de forma assegurar a sua disponibilidade, confidencialidade, integridade e autenticidade.

Art. 36. Os eventos que impactam na segurança da informação dos ativos de informação devem ser registrados, criando-se mecanismos para garantir a sua auditabilidade.

Art. 37. Os ativos de informação devem:

I - ser inventariados, preservados e protegidos;

II - ter identificados, formalmente, o gestor e o custodiante do ativo de informação;

III - ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - ser passíveis de monitoramento e ter seu uso rastreado quando houver indícios de quebra de segurança;

V - ser utilizados para o propósito único da consecução dos interesses institucionais;

VI - ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas;

VII - ser dotados de recursos criptográficos para trânsito de informações classificadas em seu grau de sigilo;

VIII - passar por processos de controle de segurança quando do encaminhamento para manutenção; e

IX - ser descartados observando procedimentos definidos na legislação em vigor.

Art. 38. Os materiais que, por sua utilização ou finalidade, demandarem proteção, terão acesso restrito às pessoas autorizadas pela PRF.

Parágrafo único. Será criado por normativo específico, em ato do Diretor Geral, os sistemas informacionais que conterão a especificação dos ativos que serão classificados como de Acesso Restrito.

Gestão de Uso dos Recursos Informacionais Orçamentários

Art. 39. Os investimentos em segurança da informação serão realizados de forma planejada, devendo estar previstos na Lei Orçamentária Anual (LOA).

Art. 40. O plano de investimentos será elaborado com base na priorização das análises de riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 41. O plano de investimentos e a correspondente proposta orçamentária devem ser propostos no âmbito do Comitê Gestor de Segurança da Informação (CGSI).

Art. 42. Nos editais de licitação, nos contratos, nos convênios, nos acordos e nos instrumentos congêneres deverá constar cláusula específica sobre a obrigatoriedade de ciência e observância da POSIN/PRF a todas as partes, incluindo seus empregados e prepostos envolvidos em atividades na PRF.

Gestão do Uso dos Meios de Comunicação

Uso do e-mail funcional

Art. 43. As regras de acesso e utilização de e-mail institucional devem atender a todas as orientações desta POSIN/PRF e normativos internos específicos, além das demais diretrizes do Governo.

Art. 44. O correio eletrônico é um recurso de comunicação corporativa da PRF , assim, de forma a preservar o funcionamento do serviço de correio eletrônico institucional, o usuário da desse recurso deve:

I - acessá-lo com frequência;

II - evitar o uso de serviços de e-mail privados para atividades institucionais;

III - utilizá-lo apenas para fins institucionais e de forma a não cometer qualquer ato que possa prejudicar o trabalho, a imagem de terceiros ou do próprio Estado, em consonância com as determinações legais;

IV - eliminar, periodicamente, as mensagens desnecessárias de sua caixa postal, inclusive as existentes nas pastas personalizadas, na lixeira, rascunho e enviados, de forma a não exceder o limite de tamanho da caixa postal;

V - evitar clicar em links de acesso a páginas de internet existentes em mensagens de correio eletrônico recebidas de origem desconhecida, com vistas a evitar a instalação de softwares maliciosos ou direcionar o usuário da rede de dados para um sítio falso, possibilitando a captura de informações;

VI - evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico, sem antes verificá-los quanto à sua procedência, e em caso de suspeita de irregularidade na mensagem, deve solicitar ajuda à área de TI correlata; e

VII - deixar de informar o e-mail funcional em cadastros nas transações particulares, evitando a vinculação da instituição à vida privada.

Art. 45. O e-mail particular não deve ser utilizado para o envio ou recebimento de informações da PRF, salvo em situações que não tenha como acessar o e-mail institucional.

Acesso à Internet

Art. 46. O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deve ser regido por normativos internos específicos, atendendo às determinações desta POSIN/PRF, e demais orientações governamentais e legislação em vigor.

Art. 47. O acesso à internet concedido ao usuário de rede da PRF é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos causados à Instituição por meio de seu uso.

Art. 48. A PRF permite o uso parcimonioso da internet para interesses particulares dos usuários da rede, apenas para navegação em sítios cujo conteúdo seja adequado, e que não exceda os limites da ética, bom senso e razoabilidade;

§1º É vedada a utilização da internet para:

I - acessar sítios com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;

II - acessar sítios ou arquivos que contenham conteúdo criminoso ou ilegal, ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares;

III - acessar sítios ou arquivos com conteúdo de incitação à violência, que não respeitem os direitos autorais ou com objetivos comerciais particulares; e

IV - realizar atividades relacionadas a jogos eletrônicos pela internet.

§2º O usuário deve sempre se certificar da procedência do sítio verificando, quando cabível, do certificado digital do mesmo, principalmente para realizar transações eletrônicas via internet, digitando o endereço do sitio diretamente no navegador.

§3º É vedado aos usuários disponibilizar informações de propriedade da PRF em sítios da internet ou redes sociais privadas, salvo aqueles que já constam nos sítios da comunicação institucional da PRF.

Uso de Redes Sociais

Art. 49. O uso das redes sociais disponíveis na rede mundial de computadores (internet), com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações da PRF, deve ser regido por normativos internos específicos, atendendo às determinações desta POSIN/PRF, e demais orientações governamentais e legislação em vigor, sendo vedadas iniciativas individuais sem autorização do Gestor.

Parágrafo único. Enquanto o normativo de que trata o **caput** não for editado, deverão ser observadas as orientações expedidas pelas áreas de Comunicação Institucional, da Corregedoria-Geral (CG) e da Contrainteligência sobre o uso de mídias sociais vinculadas à PRF, nos casos em que houver autorização.

Uso de Dispositivos Móveis

Art. 50. As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail da PRF devem considerar, prioritariamente, os requisitos legais e a estrutura da instituição, atendendo a esta POSIN/PRF e regidas por normativos internos específicos, a qual contemplará recomendações sobre o uso desses dispositivos.

Art. 51. O uso de dispositivos móveis na PRF deve ser pautado na necessidade e interesse da instituição e devem ser utilizados somente pelos usuários, após serem orientados e assumiram a responsabilidade pelo seu uso, devendo minimamente:

I - ser orientado a respeito dos procedimentos de segurança e da responsabilidade que o mesmo passa a assumir acerca do uso dos dispositivos móveis, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido;

II - bloquear seu dispositivo móvel ao se afastar do mesmo, evitando que outras pessoas tenham acesso às informações armazenadas; e

III - proteger o equipamento portátil de TI e os dados nele contidos contra situações de risco, adotando medidas contra a perda, extravio ou furtos.

O uso dos Aplicativos de Mensagens Eletrônicas

Art. 52. A utilização dos aplicativos de mensagens comerciais para difusão de informações, nos dispositivos móveis de uso funcional disponibilizados pela instituição, deve atender aos seguintes requisitos:

I - disponibilidade;

II - interesse público;

III - destinação aos assuntos institucionais;

IV - compartimentação;

V - não transmissão de informações restritas ou classificadas; e

VI - criptografia de ponta a ponta assegurada privacidade e segurança on-line.

Parágrafo único. Norma específica para utilização de aplicativos de mensagens eletrônicas pela PRF deverá ser elaborada.

Uso de Computação em Nuvem

Art. 53. 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, deve ser regido por normativos internos específicos, atendendo à determinações desta POSIN/PRF e demais orientações governamentais e legislação em vigor, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento de um prestador de serviço, com a garantia de que os servidores de arquivos estejam em solo brasileiro.

Art. 54. Os mecanismos de proteção estabelecidos devem estar alinhados aos riscos identificados.

Controle de Acessos aos Ativos de Informação

Art. 55. A permissão de acesso às redes da PRF dependerá do processo de credenciamento do usuário junto à área de gestão de pessoas da unidade, e da situação correcional do usuário, estabelecida pela área competente.

Art. 56. O manuseio dos ativos de informação deve ser controlado e limitado ao que for necessário para o cumprimento das atividades de cada usuário.

Parágrafo único. O acesso e manuseio dos ativos de informação, quando autorizado, deve ser condicionado à assinatura do Termo de Responsabilidade para Manuseio dos Ativos de Informação, na forma do Anexo desta Instrução Normativa (IN), observando a legislação em vigor.

Art. 57. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso aos ativos de informação devem ser reavaliados, devendo ser readequados imediatamente, conforme a nova avaliação.

Parágrafo único. Em caso de desligamento do usuário, os acessos aos sistemas devem ser cancelados imediatamente pelos gestores, bem como devem ser devolvidos, pelo ex-usuário, os ativos tangíveis de que tinha posse.

Art. 58. Os dispositivos de identificação são únicos e intransferíveis, não podendo ser compartilhados ou divulgados para terceiros.

Art. 59. Os acessos às redes sem fio - WIFI devem ser controlados com a identificação dos usuários que as utilizam, possibilitando auditorias.

Art. 60. Todos os dispositivos de armazenamento de dados de uso institucional, tais como: notebook, celulares, pendrives, cartões de memória, entre outros, deverão ser preparados para dar segurança aos dados neles contidos, por meio de sistemas de criptografia e de permissão de acesso adequados à sensibilidade das informações armazenadas.

Art. 61. O acesso aos equipamentos ou softwares que venham a ser empregados para navegação e marcação de posicionamento geográfico dos ativos institucionais da PRF é restrito aos servidores com credencial de acesso compatível.

Gestão de Riscos

Art. 62. A Gestão de Riscos dos ativos de informação deve:

I - avaliar os riscos relativos à segurança de informação, além da conformidade com as exigências regulatórias e legais; e

II - priorizar a segurança e a imagem institucionais da PRF e do Estado.

Art. 63. As áreas responsáveis por ativos de informação devem implantar o gerenciamento contínuo de riscos visando à proteção dos serviços da PRF, por meio da eliminação, redução ou transferência desses riscos, conforme seja mais viável estratégica e economicamente.

Gestão de Continuidade

Art. 64. Os procedimentos que garantam a continuidade de serviço e a recuperação do fluxo de informações e comunicações devem ser mantidos de forma a não permitir a interrupção das atividades de negócios e proteger os processos críticos contra falhas e danos, atendendo aos seguintes objetivos:

I - proteção dos dados armazenados, com replicações em servidores geograficamente distantes;;

II - contingência e recuperação do funcionamento normal dos sistemas dentro de períodos de tempos determinados;

III - avaliação em regime emergencial das consequências de desastres, falhas de segurança e perda de serviços;

IV - restabelecimento tempestivo das operações consideradas essenciais; e

V - comunicação oportuna aos usuários sobre a situação anormal e oferecendo previsão de restabelecimento à normalidade.

Auditoria e Conformidade

Art. 65. Devem ser realizadas auditorias periódicas, inopinadas ou sob demanda visando certificar o cumprimento dos requisitos de segurança da informação.

Parágrafo único. A verificação de conformidade das práticas de segurança da informação da PRF deve ser realizada com periodicidade máxima de dois anos.

Art. 66. A verificação de conformidade deve abranger todas as unidades da PRF, além dos contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados com a PRF.

Art. 67. Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação, o qual será encaminhado pelo gestor de segurança da informação ao gestor do ativo de informação da unidade verificada, para ciência e tomada das ações cabíveis.

Parágrafo único. Demandas originadas pela Atividade de Inteligência deverão ter prioridade sobre as outras, devendo receber pronta resposta de modo a assessorar os gestores na tomada de decisão.

CAPÍTULO VI
COMPETÊNCIAS RESIDUAIS E PENALIDADES

Usuários

Art. 68. Todos são responsáveis e devem estar comprometidos com a segurança da informação com a finalidade de reduzir os riscos de: erro humano, furto, roubo, apropriação indébita, fraude, sabotagem e uso indevido dos ativos de informação da PRF.

Art. 69. Os usuários devem ter ciência de suas responsabilidades e obrigações no âmbito desta política, e são responsáveis pelos ativos de informação aos quais têm acesso, pelos processos que estejam envolvidos e por todos atos executados com sua identificação.

Art. 70. Todos os usuários devem difundir o cumprimento desta política, de seus documentos complementares, das normas de segurança e da legislação vigente acerca do tema.

§1º Os gestores das unidades administrativas da PRF são responsáveis pelo nível de acesso e/ou pelas credenciais de cada usuário sob sua responsabilidade, especialmente dos colaboradores.

§ 2º A utilização do Sistema Eletrônico de Informações - SEI pelos colaboradores deve receber atenção especial quando da concessão das credenciais de acesso, devendo ser avaliada a pertinência do acesso aos dados contidos em cada processo antes da tramitação entre unidades.

Art. 71. Compete aos usuários da PRF:

I - aceitar formalmente o termo de responsabilidade para manuseio dos ativos de informação, declarando ciência e conhecimento da política de segurança da informação da PRF, assumindo responsabilidade por seu cumprimento;

II - cumprir esta política, as normas, os procedimentos e as orientações de segurança da informação da PRF;

III - buscar orientação institucional em caso de dúvidas relacionadas à segurança da informação;

IV - proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela PRF;

V - assegurar que os ativos de informação à sua disposição sejam utilizados apenas para as finalidades aprovadas pela PRF; e

VI - comunicar imediatamente a sua chefia imediata qualquer descumprimento ou violação desta política e/ou de seus documentos complementares.

Art. 72. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários, de acordo com suas competências funcionais.

Controlador e Operador

Art. 73. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 74. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 75. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

III - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Penalidades

Art. 76. O descumprimento ou violação, pelo agente público, das regras previstas na POSIN/PRF e/ou de seus documentos complementares poderão ser apuradas mediante procedimento administrativo correcional.

Parágrafo único. Os responsáveis por prejuízos ou irregularidades mencionadas no **caput** poderão também responder na esfera civil e/ou penal pelos seus atos.

CAPÍTULO VII
DAS CONSIDERAÇÕES FINAIS

Art. 77. A POSIN/PRF norteará a elaboração de outros documentos relacionados à segurança da informação, como normas, orientações e/ou manuais que disciplinam e/ou facilitem a implementação desta POSIN/PRF, os quais deverão observar as diretrizes e terminologias apresentadas neste documento, com o intuito de assegurar um padrão documental.

Art. 78. As diretrizes e regras previstas na POSIN/PRF apresentam as principais atividades a serem desenvolvidas e a sua priorização será definida pelos gestores e comitês de segurança da informação da PRF.

Art. 79. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao serviço de segurança da informação.

§1º Em casos de quebra de segurança da informação por meio de recursos de TIC, o serviço de segurança da informação da área de Tecnologia da Informação e Comunicação deve ser imediatamente notificado a fim de adotar as providências necessárias.

§2º Nos casos em que a violação da segurança não estiver diretamente relacionada aos recursos de TIC, especialmente quanto aos ativos intangíveis de informação, a área responsável pela atividade de inteligência deve ser imediatamente notificada.

Art. 80. Nos casos de suspeita de infração à POSIN/PRF, a área de TIC e de Contrainteligência poderão ser demandadas para análise preliminar, mediante autorização formal do dirigente máximo do órgão, ou da unidade desconcentrada, sem prejuízo dos procedimentos previstos no art. 76.

Art. 81. Todo trabalho realizado por terceiros que envolva questões de segurança da informação deve ser registrado em processo próprio no Sistema Eletrônico de Informações - SEI e supervisionado pelo chefe do setor ou por alguém por ele designado.

Art. 82. Os casos omissos nesta IN serão decididos pelo gestor de segurança da informação, ouvidos, quando for o caso, os membros do referido comitê.

Art. 83. Esta política, bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma crítica e periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

Art. 84. Ficam revogadas:

I - a Instrução Normativa nº 7, de 28 de maio de 2004, da Direção-Geral da Polícia Rodoviária Federal;

II - a Instrução Normativa nº 3, de 27 de junho de 2011, da Direção-Geral da Polícia Rodoviária Federal;

III - a Portaria Normativa nº 118, de 31 de agosto de 2012, da Direção-Geral da Polícia Rodoviária Federal; e

IV - a Instrução Normativa nº 54, de 16 de abril de 2015, da Direção-Geral da Polícia Rodoviária Federal;

Art. 85. Tornar sem efeito o arquivo SEI Nº 33444976.

Art. 86. Esta Instrução Normativa entra em vigor em 1º de julho de 2021.

SILVINEI VASQUES

PRF

Documento assinado eletronicamente por **SILVINEI VASQUES**, **Diretor-Geral**, em 30/06/2021, às 17:29, horário oficial de Brasília, com fundamento no art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020, e no art. 42 da Instrução Normativa nº 116/DG/PRF, de 16 de fevereiro de 2018.

A autenticidade deste documento pode ser conferida no site https://sei.prf.gov.br/verificar, informando o código verificador **33581950** e o código CRC **81D04C12**.

ANEXO DA INSTRUÇÃO NORMATIVA PRF Nº 45, DE 22 DE JUNHO DE 2021

TERMO DE RESPONSABILIDADE PARA O MANUSEIO DOS ATIVOS DE INFORMAÇÃO

Eu,_____, CPF: _____._____._____-____, declaro, nesta data, estar de acordo com as diretrizes previstas na Política de Segurança da Informação

e Comunicações da Polícia Rodoviária Federal, comprometendo-me a cumpri-las integralmente e ciente que é minha responsabilidade:

a. Cuidar da integridade, confidencialidade, disponibilidade e autenticidade dos ativos de informação da Polícia Rodoviária Federal;

b. Cumprir as normas, os procedimentos e as orientações de segurança da informação e comunicações da PRF;

c. Buscar orientação institucional em caso de dúvidas relacionadas à segurança da informação e comunicações;

d. Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela PRF;

e. Assegurar que os ativos de informações à minha disposição sejam utilizados apenas para as finalidades aprovadas pela PRF; e

f. Comunicar imediatamente ao meu superior hierárquico qualquer descumprimento ou violação dos procedimentos de segurança da informação e comunicações.

Para efeitos da segurança da informação e comunicações da Polícia Rodoviária Federal, ativos de informação são pessoas, documentos, materiais, equipamentos, meios de armazenamento, transmissão e processamento, ferramentas, sistemas de informação e tudo que manuseie a informação, inclusive ela própria, bem como os locais onde se encontram esses meios.

A não observância desta Política e/ou de seus documentos complementares pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais.

Brasília/DF, _____ de _____ de 20__.

Nome do Usuário
Matrícula ou CPF

De acordo,

Nome do Responsável pela Autorização
Matrícula ou CPF