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

INSTRUÇÃO NORMATIVA PRF Nº 164, DE 24 DE MARÇO DE 2026

Institui a Política de Segurança da Informação no âmbito da Polícia Rodoviária Federal.

O DIRETOR-GERAL DA POLÍCIA RODOVIÁRIA FEDERAL, no uso das atribuições que lhe foram conferidas no art. 58 do Decreto nº 11.348, de 1º de janeiro de 2023, tendo em vista o disposto no Decreto nº 12.572, de 4 de agosto de 2025, no Decreto nº 12.573, de 4 de agosto de 2025, na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e na Portaria MJSP nº 2, de 28 de janeiro de 2022, e observado o contido no processo nº 08650.022562/2022-85, resolve:

CAPÍTULO I
DISPOSIÇÕES GERAIS
Seção I
Objeto e âmbito de aplicação

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito da Polícia Rodoviária Federal, com o objetivo de estabelecer diretrizes, competências e responsabilidades relativas ao tratamento dos ativos de informação, em conformidade com a legislação vigente, com valores institucionais e éticos e com as melhores práticas reconhecidas em segurança da informação.

Parágrafo único. A Política de Segurança da Informação de que trata o *caput* aplica-se a todos os agentes públicos em exercício na Polícia Rodoviária Federal e deverá ser amplamente divulgada às pessoas físicas ou jurídicas que utilizem os meios físicos ou lógicos da Instituição, com vistas a assegurar a proteção das informações.

Seção II
Objetivos e abrangência

Art. 2º A Política de Segurança da Informação tem por objetivo geral garantir a segurança da informação no âmbito da Polícia Rodoviária Federal, especialmente quanto ao controle, à disponibilidade, à integridade, à confidencialidade e à autenticidade dos dados, informações, documentos e conhecimentos produzidos, armazenados sob sua guarda ou por ela transmitidos, de modo a protegê-los contra ameaças e vulnerabilidades.

Art. 3º São objetivos específicos da Política de Segurança da Informação da Polícia Rodoviária Federal:

I - contribuir para a proteção das informações sob guarda da instituição, orientando as ações de segurança da informação, com observância dos direitos e das garantias fundamentais;

II - fomentar as atividades de pesquisa científica, desenvolvimento tecnológico e inovação

relacionadas à segurança da informação e da comunicação;

III - promover o aprimoramento contínuo do arcabouço normativo de segurança da informação e da comunicação;

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

V - fortalecer a cultura institucional e promover ações voltadas à segurança da informação, com ênfase em:

a) proteção das informações relacionadas às ações de segurança pública;

b) guarda e segurança dos dados custodiados pela Polícia Rodoviária Federal;

c) defesa das infraestruturas críticas de informação;

d) preservação dos ativos institucionais de informação e comunicação;

e) tratamento adequado das informações que contenham dados pessoais; e

f) proteção de materiais classificados como de acesso restrito;

VI - estabelecer medidas e procedimentos para o tratamento dos ativos de informação;

VII - desenvolver, implementar e monitorar estratégias de segurança da informação alinhadas aos objetivos estratégicos da Polícia Rodoviária Federal;

VIII - avaliar, selecionar, implantar e monitorar controles adequados para a proteção dos ativos de informação; e

IX - promover a melhoria contínua dos processos e dos controles de gestão da segurança da informação.

Art. 4º A Política de Segurança da Informação da Polícia Rodoviária Federal abrange os aspectos físicos, lógicos, humanos, organizacionais, estratégicos e estruturais necessários à proteção dos ativos de informação da Instituição, compreendendo, entre outros, os seguintes aspectos:

I - segurança cibernética;

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

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

IV - proteção dos conhecimentos institucionais;

V - segurança dos planos operacionais; e

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

Seção III
Princípios

Art. 5º A segurança da informação, no âmbito da Polícia Rodoviária Federal, fundamenta-se nos seguintes princípios:

I - confidencialidade;

II - integridade;

III - disponibilidade;

IV - autenticidade;

V - respeito e 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;

VI - visão abrangente e sistêmica da segurança da informação;

VII - promoção do intercâmbio científico e tecnológico relacionado à segurança da

informação entre os órgãos e as entidades da administração pública federal;

VIII - educação como elemento estruturante para o fortalecimento da cultura de segurança da informação;

IX - orientação à gestão de riscos e à gestão da segurança da informação; e

X - prevenção, detecção e tratamento de incidentes de segurança da informação.

CAPÍTULO II
ESTRUTURAS E COMPETÊNCIAS
Seção I
Da gestão da segurança da informação

Art. 6º A Gestão da Segurança da Informação, no âmbito da Polícia Rodoviária Federal, tem por finalidade apoiar e orientar a tomada de decisões institucionais, estabelecer processos de controle e otimizar investimentos em segurança da informação, visando à eficiência, à eficácia e à efetividade das ações correlatas.

Art. 7º A Gestão da Segurança da Informação compreende ações e métodos destinados ao estabelecimento de parâmetros adequados de segurança da informação na disponibilização de serviços, sistemas e infraestruturas, de modo a atender aos requisitos mínimos de qualidade e às necessidades operacionais e institucionais da Polícia Rodoviária Federal.

Art. 8º Constituem estruturas de apoio à Gestão da Segurança da Informação:

I - Comitê Gestor de Segurança da Informação;

II - Equipe Nacional de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos no âmbito da Polícia Rodoviária Federal;

III - Equipes Regionais de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos no âmbito da Polícia Rodoviária Federal;

IV - Comissão Nacional Permanente de Avaliação de Documentos Sigilosos, para assessoramento do Comitê Gestor de Segurança da Informação; e

V - Comissões Regionais Permanentes de Avaliação de Documentos Sigilosos.

§ 1º Compete ao Diretor-Geral designar:

I - os membros do Comitê Gestor de Segurança da Informação; e

II - os membros da Comissão Nacional Permanente de Avaliação de Documentos Sigilosos.

§ 2º Compete ao Diretor de Tecnologia da Informação e Comunicação e ao Diretor de Inteligência, em ato conjunto, designar os membros da Equipe Nacional de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

§ 3º Compete aos gestores máximos das Unidades Desconcentradas da Polícia Rodoviária Federal designar:

I - os membros das Equipes Regionais de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, no âmbito das unidades descentralizadas; e

II - os membros das Comissões Regionais Permanentes de Avaliação de Documentos Sigilosos.

Seção II
Do gestor nacional de segurança da informação

Art. 9º O Diretor-Geral designará servidor público efetivo, preferencialmente lotado na Diretoria de Inteligência, para exercer o encargo de Gestor Nacional de Segurança da Informação,

competindo-lhe:

I - promover a cultura de segurança da informação, no âmbito da Polícia Rodoviária Federal, assegurando ampla divulgação da Política de Segurança da Informação e demais normas afetas ao tema, aos públicos interno e externo;

II - gerenciar os riscos relacionados aos ativos de informação;

III - acompanhar investigações e avaliações de danos decorrentes de incidentes de segurança;

IV - pesquisar e acompanhar o desenvolvimento de novas tecnologias relacionadas à segurança da informação;

V - propor edição ou revisão de normas internas e procedimentos de segurança da informação no âmbito da Polícia Rodoviária Federal;

VI - formular, promover e coordenar ações de segurança da informação, observadas a Legislação e demais normas afetas à temática, no âmbito da Polícia Rodoviária Federal;

VII - propor a alocação de recursos orçamentários e logísticos necessários às ações de segurança da informação; e

VIII - coordenar o Comitê Gestor de Segurança da Informação e a Equipe Nacional de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

Seção III
Do comitê gestor de segurança da informação

Art. 10. O Comitê Gestor de Segurança da Informação será composto pelo Gestor Nacional de Segurança da Informação, que o presidirá, e por representantes, titular e suplente, das seguintes áreas:

I - Gabinete da Direção-Geral;

II - Diretoria-Executiva;

III - Diretoria de Inteligência;

IV - Diretoria de Gestão de Pessoas;

V - Diretoria de Operações;

VI - Diretoria de Administração e Logística;

VII - Corregedoria-Geral; e

VIII - Diretoria de Tecnologia da Informação e Comunicação.

§ 1º A participação no Comitê será considerada prestação de serviço público relevante, não remunerada.

§ 2º O presidente do Comitê poderá convidar técnicos e especialistas para colaborar nos trabalhos, sem direito a voto.

§ 3º As deliberações do comitê serão tomadas por maioria simples, desde que com a presença da maioria absoluta de seus membros, cabendo ao Gestor Nacional de Segurança da Informação o voto de desempate.

§ 4º O comitê reunir-se-á, de forma presencial ou remota, ordinariamente a cada três meses, ou, extraordinariamente, por convocação do Gestor Nacional de Segurança da Informação.

§ 5º O Gabinete da Direção-Geral exercerá a função de Secretaria-Executiva do Comitê.

Art. 11. Compete ao Comitê Gestor de Segurança da Informação:

I - assessorar a Direção-Geral na implementação e no aprimoramento da gestão da segurança da informação;

II - sugerir a constituição de grupos de trabalho para tratar de temas específicos, bem como

propor soluções;

III - acompanhar investigações e avaliações de danos decorrentes de incidentes ou quebras de segurança da informação;

IV - propor a revisão ou a edição de normativos internos afetos à segurança da informação, em consonância com a legislação vigente;

V - colaborar na elaboração dos planos de gestão de riscos e de continuidade, bem como na definição de diretrizes de auditoria e de conformidade;

VI - elaborar relatórios periódicos de suas atividades e encaminhá-los à Direção-Geral;

VII - propor planos de investimento em segurança da informação;

VIII - promover a cultura organizacional de segurança da informação, por meio de programas de capacitação e de conscientização;

IX - receber e analisar comunicações de descumprimento da Política de Segurança da Informação, emitindo parecer à autoridade competente; e

X - apoiar o gerenciamento de riscos institucionais relacionados à segurança da informação.

Seção IV
Do gestor regional de segurança da informação

Art. 12. O gestor máximo das Unidades Desconcentradas da Polícia Rodoviária Federal designará servidor público efetivo, preferencialmente lotado na área de Inteligência, para exercer o encargo de Gestor Regional de Segurança da Informação, ao qual compete, no respectivo âmbito de atuação:

I - acompanhar a implementação da Política de Segurança da Informação;

II - acompanhar investigações e avaliações de danos decorrentes de incidentes ou quebras de segurança;

III - promover e fomentar o cumprimento das diretrizes da Política de Segurança da Informação; e

IV - coordenar a Equipe Regional de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

Seção V
Das equipes de prevenção, tratamento e resposta a incidentes cibernéticos

Art. 13. As Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos constituem grupos de agentes públicos responsáveis por prestar serviços relacionados à segurança cibernética no âmbito da Polícia Rodoviária Federal, em observância a esta Política de Segurança da Informação e aos processos de gestão de riscos institucionais.

Art. 14. A Equipe Nacional de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos será composta, no mínimo, por dois representantes, titular e suplente, das seguintes áreas:

I - Inteligência Cibernética;

II - Contrainteligência;

III - Infraestrutura e Serviços de Tecnologia da Informação e Comunicação;

IV - Aplicações;

V - Integração e Ciência de Dados;

VI - Segurança da Informação; e

VII - Governança de Tecnologia da Informação e Comunicação.

Art. 15. As Equipes Regionais de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos serão compostas, no mínimo, por um representante, titular e suplente, da respectiva unidade desconcentrada, das áreas de:

I - Tecnologia da Informação e Comunicação; e

II - Inteligência.

Parágrafo único. As Equipes Regionais exercerão as mesmas competências atribuídas à Equipe Nacional, no âmbito de suas respectivas unidades desconcentradas.

Seção VI
Da comissão nacional permanente de avaliação de documentos sigilosos

Art. 16. A Comissão Nacional Permanente de Avaliação de Documentos Sigilosos será composta por dois representantes, titular e suplente, das seguintes áreas:

I - Gabinete da Direção-Geral;

II - Diretoria-Executiva;

III - Diretoria de Inteligência;

IV - Diretoria de Gestão de Pessoas;

V - Diretoria de Operações;

VI - Diretoria de Administração e Logística;

VII - Corregedoria-Geral; e

VIII - Diretoria de Tecnologia da Informação e Comunicação.

Art. 17. Compete à Comissão Nacional Permanente de Avaliação de Documentos Classificados:

I - opinar sobre as informações produzidas 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, à reclassificação ou à reavaliação de informações classificadas;

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 de documentos classificados em cada grau de sigilo, a ser disponibilizado na internet.

Parágrafo único. A Diretoria de Inteligência publicará portarias com o detalhamento da atuação das Comissões Permanentes de Avaliação de Documentos Sigilosos, competindo-lhe, especialmente:

I - designar papéis e responsabilidades dos integrantes das Comissões;

II - definir os procedimentos administrativos e técnicos aplicáveis à atuação das Comissões; e

III - instituir manuais técnicos destinados a orientar e balizar a atuação dos diversos atores envolvidos na consecução dos objetivos da Comissão.

Seção VII
Comissões regionais de avaliação de documentos sigilosos

Art. 18. As Comissões Regionais de Avaliação de Documentos Sigilosos serão compostas por dois representantes, titular e suplente, das seguintes áreas, no âmbito de suas respectivas unidades desconcentradas:

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.

Art. 19. As Comissões Regionais de Avaliação de Documentos Sigilosos exercerão as mesmas competências atribuídas à Comissão Nacional, no âmbito de suas respectivas unidades desconcentradas.

CAPÍTULO III
DIRETRIZES E ATIVOS DA INSTITUIÇÃO
Seção I
Das diretrizes

Art. 20. São diretrizes da Política de Segurança da Informação, relativas aos ativos de informação:

I - tratamento da informação;

II - gestão do conhecimento institucional produzido;

III - gestão das informações operacionais de segurança pública;

IV - tratamento de dados pessoais;

V - segurança física e do ambiente;

VI - gestão de incidentes em segurança da informação;

VII - gestão de ativos;

VIII - gestão do uso dos recursos informacionais;

IX - gestão do uso dos meios de comunicação;

X - controle de acessos;

XI - gestão de riscos;

XII - gestão de continuidade; e

XIII - auditoria e conformidade.

Seção II
Do tratamento da informação

Art. 21. As informações geradas ou produzidas, sob a responsabilidade da Polícia Rodoviária Federal, integram o seu patrimônio institucional, não cabendo a seus criadores qualquer forma de direito autoral, ressalvados os direitos assegurados em legislação específica, devendo ser protegidas de acordo com as diretrizes estabelecidas nesta norma.

Art. 22. É vedada a utilização de informações produzidas para uso exclusivo da Polícia Rodoviária Federal, salvo mediante autorização expressa do Diretor-Geral ou, por delegação, aos Diretores Setoriais ou ao Gestor Nacional de Segurança da Informação (GNSI), observada a criticidade da informação.

Art. 23. Informações tecnicamente processadas que integram os conhecimentos institucionais são consideradas de acesso restrito, devendo sua difusão ser controlada e sua divulgação

externa condicionada à autorização do gestor responsável.

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

Art. 24. As informações da Polícia Rodoviária Federal constantes em planos operacionais, de distribuição de materiais controlados, de emprego de efetivo, de instalações físicas e de capacitação são consideradas ativos institucionais de acesso restrito, vinculados à finalidade da segurança pública, cujo acesso não autorizado possa implicar risco ou dano aos interesses da sociedade e do Estado, devendo sua difusão ser controlada e mantida no ambiente institucional com acesso restrito.

Seção III
Do tratamento de dados pessoais

Art. 25. O tratamento de dados pessoais pela Polícia Rodoviária Federal deverá ser realizado para o atendimento de sua finalidade pública e para a execução de suas competências legais, sendo necessário que:

I - sejam explicitadas as hipóteses em que, no exercício de suas competências, a Polícia Rodoviária Federal realiza o tratamento de dados pessoais, com o fornecimento de informações claras, precisas e atualizadas sobre a base legal, a finalidade, os procedimentos e as práticas adotadas, em canais de fácil acesso ao público, preferencialmente em seus sítios eletrônicos; e

II - sejam indicados o encarregado pelo tratamento de dados pessoais, o controlador e o operador, para a realização das operações de tratamento de dados pessoais, nos termos do previsto na Lei nº 13.709, de 14 de agosto de 2018.

Art. 26. Os dados pessoais deverão ser armazenados em formato interoperável e estruturado, apto ao uso compartilhado entre órgãos e entidades da administração pública, com vistas à implementação de políticas públicas, à melhoria da prestação de serviços públicos, à descentralização de atividades e à ampliação do acesso público à informação, observadas as restrições legais aplicáveis.

Art. 27. O uso compartilhado de dados pessoais pelo Poder Público deverá atender a finalidades específicas de execução de políticas públicas e de atribuição legal dos órgãos e das entidades públicas, respeitados os princípios e as garantias de proteção de dados pessoais previstos na Lei nº 13.709, de 14 de agosto de 2018.

Seção IV
Da Gestão de Ativos

Art. 28. Os ativos de informação, tangíveis e intangíveis, devem ser protegidos de acordo com o seu valor, sensibilidade e criticidade, de modo a assegurar a sua disponibilidade, confidencialidade, integridade e autenticidade.

Art. 29. Os eventos que impactam a segurança dos ativos de informação deverão ser registrados, com a instituição de mecanismos que garantam a sua auditabilidade.

Art. 30. Os ativos de informação deverão:

I - ser inventariados, preservados e protegidos;

II - ter formalmente identificados o gestor e o custodiante;

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

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

V - ser utilizados exclusivamente para a consecução dos interesses institucionais;

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

VII - ser dotados de recursos criptográficos adequados para o trânsito de informações classificadas, observado o respectivo grau de sigilo;

VIII - submeter-se a processos de controle de segurança quando do encaminhamento para manutenção; e

IX - ser descartados em observância aos procedimentos previstos na legislação vigente.

Art. 31. Os materiais que, em razão de sua utilização ou finalidade, demandem proteção terão seu acesso restrito às pessoas previamente autorizadas.

Art. 32. A Diretoria de Tecnologia da Informação e Comunicação, mediante ato ordinatório específico, deverá estabelecer processo de gestão dos ativos de Tecnologia da Informação e Comunicação com foco em segurança da informação, que contemple, no mínimo, as etapas de planejamento da necessidade, especificação técnica, uso e manutenção dos ativos de TIC, em conformidade com as diretrizes institucionais.

Art. 33. Os profissionais envolvidos no processo de gestão de ativos de Tecnologia da Informação e Comunicação deverão:

I - zelar pelo cumprimento das regras estabelecidas pela Polícia Rodoviária Federal sobre o tema;

II - prestar esclarecimentos, sempre que demandados, no âmbito de suas atribuições;

III - assegurar a exatidão das informações repassadas; e

IV - identificar e reportar à Diretoria de Tecnologia da Informação e Comunicação necessidades de aprimoramento no processo de gestão dos ativos de TIC.

Seção V
Da Gestão do Uso dos Meios de Comunicação

Art. 34. Sem prejuízo da aplicação desta norma, ato específico disporá sobre:

I - as regras de acesso e de utilização de *e-mail* institucional;

II - o acesso à rede mundial de computadores no ambiente de trabalho;

III - o uso de redes sociais na *internet* para a prestação de serviços públicos;

IV - as diretrizes para uso de dispositivos móveis no acesso às informações, aos sistemas, às aplicações e ao *e-mail* da Polícia Rodoviária Federal;

V - as regras de utilização de aplicativos de mensagens comerciais nos dispositivos móveis de uso funcional disponibilizados pela Polícia Rodoviária Federal; e

VI - as diretrizes para o uso de recursos de computação em nuvem, destinados a suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação.

§ 1º Nas hipóteses dos incisos III e VI, é vedada a utilização sem autorização prévia do Gestor Nacional de Segurança da Informação.

§ 2º A utilização de aplicativos de mensagens a que se refere o inciso V deverá observar os seguintes requisitos:

I - disponibilidade adequada dos recursos de comunicação;

II - atendimento ao interesse público;

III - destinação exclusiva a assuntos institucionais;

IV - compartimentação das informações;

V - vedação à transmissão de informações de acesso restrito ou classificadas; e

VI - utilização de plataformas que adotem criptografia de ponta a ponta, capazes de assegurar a privacidade e a segurança das comunicações eletrônicas, desde que devidamente autorizadas.

§ 3º Todos os dados e comunicações transitados ou armazenados nos ativos e nos meios da Polícia Rodoviária Federal são de sua propriedade e estão sujeitos a monitoramento e a auditoria, nos termos da legislação vigente.

Seção VI
Da Gestão de Riscos

Art. 35. A gestão de riscos dos ativos de informação deverá:

I - avaliar os riscos relacionados à segurança da informação, considerando, adicionalmente, a conformidade com as exigências legais e regulatórias; e

II - priorizar a preservação da segurança institucional e da imagem da Polícia Rodoviária Federal.

Art. 36. As áreas responsáveis pelos ativos de informação deverão implantar o gerenciamento contínuo de riscos, com o objetivo de proteger os serviços da Polícia Rodoviária Federal, por meio da eliminação, mitigação ou transferência dos riscos, conforme a alternativa mais adequada do ponto de vista estratégico e econômico.

Seção VII
Gestão de Continuidade

Art. 37. Os procedimentos destinados a garantir a continuidade dos serviços e a recuperação do fluxo de informações e comunicações deverão ser mantidos de forma a evitar a interrupção das atividades institucionais e a proteger os processos críticos contra falhas e danos, atendendo, no mínimo, aos seguintes objetivos:

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

II - elaboração, implementação e execução de planos de backup, com a realização de testes periódicos;

III - adoção de medidas de contingência e de recuperação do funcionamento normal dos sistemas, dentro de prazos previamente estabelecidos;

IV - avaliação, em regime emergencial, das consequências de desastres, falhas de segurança e indisponibilidade de serviços;

V - restabelecimento tempestivo das operações consideradas essenciais; e

VI - comunicação oportuna aos usuários acerca de situações anormais, com a indicação de previsão de restabelecimento da normalidade.

Art. 38. As diretrizes relacionadas à continuidade dos serviços e à recuperação do fluxo de informações e comunicações deverão atender às orientações da Política de Segurança da Informação e de norma interna específica, sendo vedada a adoção de diretrizes ou ações diversas sem prévia autorização do Gestor Nacional de Segurança da Informação.

Seção VIII
Auditoria e verificação de conformidade

Art. 39. Deverão ser realizadas auditorias periódicas, inopinadas ou sob demanda, com a finalidade de verificar o cumprimento dos requisitos de segurança da informação.

Parágrafo único. A verificação de conformidade das práticas de segurança da informação da Polícia Rodoviária Federal deverá ocorrer com periodicidade máxima de dois anos.

Art. 40. A verificação de conformidade deverá abranger todas as unidades da Polícia

Rodoviária Federal.

Art. 41. Os resultados de cada verificação de conformidade deverão ser formalizados em relatório de avaliação, a ser encaminhado pelo Gestor Nacional de Segurança da Informação ao gestor do ativo de informação da unidade verificada, para ciência e adoção das providências cabíveis.

Parágrafo único. As Demandas oriundas das atividades de inteligência ou de assuntos internos terão prioridade sobre as demais, devendo receber resposta célere, com vistas a subsidiar a tomada de decisão pelos gestores competentes.

Art. 42. As soluções de Tecnologia da Informação e Comunicação da Polícia Rodoviária Federal deverão ser auditáveis e manter registros históricos (*logs*) das ações realizadas por seus usuários.

§ 1º O acesso aos logs somente será permitido nas seguintes hipóteses:

I - sustentação de sistemas;

II - tratamento de incidentes de segurança da informação;

III - atendimento a demandas oriundas da Corregedoria-Geral; e

IV - cumprimento de determinações judiciais.

§ 2º Toda solicitação e todo acesso aos *logs* deverá ser registrado em processo sigiloso ou, alternativamente, por meio de *logs* adicionais ou da Central Nacional de Serviços de Tecnologia da Informação e Comunicação.

§ 3º A comunicação de qualquer incidente, suspeita ou violação, a que se refere o inciso II do § 1º, deverá ocorrer no menor prazo possível, sendo a Central Nacional de Serviços de Tecnologia da Informação e Comunicação o canal oficial para essa comunicação.

CAPÍTULO IV
COMPETÊNCIAS RESIDUAIS E PENALIDADES
Seção I
Dos Usuários

Art. 43. Todos os usuários são responsáveis e devem estar comprometidos com a segurança da informação, com vistas a reduzir os riscos de erro humano, furto, roubo, apropriação indébita, fraude, sabotagem e uso indevido dos ativos de informação da Polícia Rodoviária Federal.

Art. 44. Os usuários devem ter ciência de suas responsabilidades e obrigações no âmbito da Política de Segurança da Informação, respondendo:

I - pelos ativos de informação aos quais tenham acesso;

II - pelos processos nos quais estejam envolvidos; e

III - pelos atos praticados mediante sua identificação de acesso.

Art. 45. Todos os usuários deverão promover o cumprimento da Política de Segurança da Informação, de seus documentos complementares, das normas internas e da legislação vigente sobre segurança da informação.

§ 1º Os gestores das unidades administrativas da Polícia Rodoviária Federal são responsáveis pela definição, concessão e supervisão dos níveis de acesso e das credenciais de seus subordinados, incluindo colaboradores terceirizados.

§ 2º A utilização do Sistema Eletrônico de Informações – SEI por colaboradores deverá ser criteriosamente avaliada quanto à pertinência do acesso, especialmente antes da tramitação de processos entre unidades.

§ 3º Em caso de desligamento de colaborador, a unidade à qual estiver vinculado deverá abrir chamado imediatamente junto à Central Nacional de Serviços de Tecnologia da informação e Comunicação imediatamente, para que a área técnica responsável proceda ao cancelamento dos acessos.

Art. 46. Compete aos usuários de informação da Polícia Rodoviária Federal:

I - aceitar formalmente o termo de responsabilidade para uso dos ativos de informação, conforme modelo publicado pela Diretoria de Tecnologia da Informação e Comunicação, declarando ciência da Política de Segurança da Informação e assumindo o compromisso com seu cumprimento;

II - cumprir esta Política de Segurança da Informação, bem como as normas, procedimentos e as orientações de segurança da informação da Polícia Rodoviária Federal;

III - buscar orientação institucional sempre que houver dúvida quanto à aplicação das normas de segurança da informação;

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

V - utilizar os ativos de informação exclusivamente para os fins autorizados pela Polícia Rodoviária Federal; e

VI - comunicar imediatamente à chefia imediata ou à Central Nacional de Serviços de Tecnologia da Informação e Comunicação qualquer descumprimento da Política de Segurança da Informação, de seus documentos complementares ou de quaisquer outras normas, bem como incidentes de segurança da informação.

Art. 47. A Polícia Rodoviária Federal deverá manter processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, voltados a todos os usuários, observadas as respectivas competências funcionais.

Seção II
Do controlador, operador e encarregado pelo tratamento de dados pessoais

Art. 48. O controlador e o operador deverão manter registros das operações de tratamento de dados pessoais que realizarem, nos termos da legislação vigente.

Art. 49. O operador deverá realizar o tratamento de dados pessoais exclusivamente conforme as instruções fornecidas pelo controlador, cabendo a este verificar o cumprimento dessas instruções e da legislação aplicável à matéria.

Art. 50. Compete ao controlador designar o encarregado setorial pelo tratamento de dados pessoais, nos termos da legislação vigente e da Portaria MJSP nº 561, de 31 de dezembro de 2021.

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

§ 2º Compete ao encarregado setorial:

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

II - orientar os servidores, colaboradores e contratados da Polícia Rodoviária Federal quanto às práticas relativas à proteção de dados pessoais; e

III - exercer as demais atribuições definidas pelo controlador ou previstas em normas complementares.

CAPÍTULO V
CONSIDERAÇÕES FINAIS

Art. 51. A priorização das ações decorrentes da Política de Segurança da Informação da Polícia Rodoviária Federal será definida pelo Comitê Gestor de Segurança da Informação.

Art. 52. Nos casos de quebra de segurança envolvendo recursos de Tecnologia da

Informação e Comunicação, a área técnica responsável deverá ser imediatamente notificada, para a adoção das medidas cabíveis.

Parágrafo único. Quando a violação não estiver diretamente relacionada aos recursos de Tecnologia da Informação e Comunicação, especialmente quanto a ativos intangíveis de informação, a notificação deverá ser direcionada à área de inteligência institucional.

Art. 53. Os acessos a todos os sistemas da Polícia Rodoviária Federal deverão ser precedidos da utilização de autenticação de múltiplos fatores.

Parágrafo único. Excepcionalmente, na hipótese de inviabilidade técnica, devidamente justificada pela Diretoria de Tecnologia da Informação e Comunicação, será admitido o uso de outro mecanismo de segurança equivalente, desde que assegure a autenticidade do usuário e o reforço da proteção no acesso.

Art. 54. Em casos de suspeita de infração à Política de Segurança da Informação, as áreas de Tecnologia da Informação e Comunicação, Contrainteligência e Assuntos Internos poderão ser demandadas para análise preliminar, mediante autorização formal do Diretor-Geral ou do Superintendente competente.

Art. 55. Todo trabalho realizado por terceiros que envolva aspectos relacionados à segurança da informação deverá ser registrado em processo próprio no Sistema Eletrônico de Informações – SEI, sob supervisão do chefe do setor responsável ou de servidor por ele designado.

Art. 56. A Política de Segurança da Informação da Polícia Rodoviária Federal será revisada de forma crítica e periódica, sempre que necessário.

Art. 57. Os editais de licitação, contratos, convênios, acordos e demais instrumentos congêneres deverão conter cláusula específica quanto a obrigatoriedade de ciência e de observância da Política de Segurança da Informação da Polícia Rodoviária Federal por todas as partes envolvidas.

Art. 58. Fica revogada a Instrução Normativa PRF nº 45, de 22 de junho de 2021.

Art. 59. Esta Instrução Normativa entra em vigor na data de sua publicação.

ANTONIO FERNANDO SOUZA OLIVEIRA

PRF

Documento assinado eletronicamente por **ANTONIO FERNANDO SOUZA OLIVEIRA**, **Diretor-Geral**, em 26/03/2026, às 22:40, 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 **72328115** e o código CRC **3563FFAF**.