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

INSTRUÇÃO NORMATIVA PRF Nº 156, DE 05 DE MAIO DE 2025

Dispõe sobre a estratégia de uso de *software* e de serviços de computação em nuvem no âmbito da Polícia Rodoviária Federal - PRF.

O DIRETOR-GERAL DA POLÍCIA RODOVIÁRIA FEDERAL, no uso das atribuições que lhe foram conferidas no Decreto nº 11.348, de 1º de janeiro de 2023, observados os termos da Portaria MJSP nº 665, de 24 de junho de 2024, e considerando o disposto nos processos nº 08650.188414/2024-94 e nº 08650.016812/2022-48, resolve:

Objeto e âmbito de aplicação

Art. 1º Esta Instrução Normativa disciplina a estratégia de uso de *software* e de serviços de computação em nuvem no âmbito da Polícia Rodoviária Federal - PRF.

§ 1º Para fins desta Instrução Normativa, serão considerados os conceitos constantes do Glossário de Segurança da Informação, aprovado e atualizado pelo Gabinete de Segurança Institucional da Presidência da República, nos termos da Portaria GSI/PR nº 93, de 18 de outubro de 2021, ou outra norma que venha a substituí-la.

§ 2º Fica estabelecido na PRF o modelo híbrido para a computação em nuvem (nuvem híbrida), consubstanciado pelo uso de infraestrutura composta de dois ou mais provedores distintos (nuvem privada, comunitárias ou públicas), as quais permanecem com suas próprias características, agrupadas por padronização de tecnologia, permitindo interoperabilidade e portabilidade de dados, serviços e aplicações.

§ 3º São objetivos do processo de estratégia de soluções de computação em nuvem no âmbito da PRF:

I - otimização do controle e gestão dos custos relacionados ao armazenamento e processamento de dados e soluções tecnológicas, garantindo maior eficiência na alocação de recursos;

II - agilidade e escalabilidade para o armazenamento e processamento de grandes volumes de dados, especialmente em operações críticas de segurança e fiscalização;

III - aprimoramento da performance e disponibilidade das plataformas analíticas da PRF, facilitando o acesso a dados relevantes para a tomada de decisões estratégicas e operacionais;

IV - redução do tempo de adaptação às inovações tecnológicas, especialmente nas áreas de inteligência artificial e outras tecnologias emergentes, para garantir que a PRF se mantenha atualizada com as tendências do setor de segurança pública;

V - desenvolvimento e suporte de soluções tecnológicas que acompanhem e promovam a evolução dos processos internos da PRF, em linha com eventuais mudanças legislativas ou operacionais que impactem suas atividades; e

VI - promoção de soluções inovadoras e disruptivas que aumentem a produtividade interna da PRF, seja em processos administrativos ou operacionais, ou ainda no aprimoramento dos serviços

prestados ao cidadão, com foco na melhoria contínua da segurança e eficiência nas rodovias federais.

§ 4º Ficam estabelecidas as seguintes metas para o serviço de computação em nuvem da PRF:

I - garantir que os serviços em nuvem atendam às normas de segurança e proteção de dados aplicáveis;

II - implementar mecanismos de proteção e criptografia para os dados armazenados e transmitidos na nuvem;

III - automatizar processos de gestão e operação na nuvem para aumentar a eficiência e reduzir custos;

IV - estabelecer procedimentos para garantir a recuperação rápida dos serviços em caso de falha; e

V - adotar soluções tecnológicas para otimizar o uso da infraestrutura em nuvem e aprimorar a operação dos serviços digitais.

§ 5º A estratégia tratada no *caput* deve ser aplicada para novas contratações de *software* e de serviços de computação em nuvem no âmbito da PRF, tais como:

I - *software* sob o modelo de licenciamento permanente de direitos de uso;

II - *software* sob o modelo de cessão temporária de direitos de uso;

III - *software* sob o modelo de Subscrição ou como Serviço - SaaS;

IV - Infraestrutura como Serviço - IaaS;

V - Plataforma como Serviço - PaaS;

VI - suporte técnico para software e serviços de computação em nuvem;

VII - serviço de operação e gerenciamento de recursos em nuvem;

VIII - serviço de migração de recursos para ambiente de nuvem;

IX - integração de serviços de computação em nuvem; e

X - consultoria especializada em software e/ou serviços de computação em nuvem.

§ 6º O Diretor de Tecnologia da Informação e Comunicação ou Superintendente responsável pela demanda deverá identificar e avaliar as necessidades de negócio antes da contratação de *software* e de serviços de computação em nuvem, determinando quais sistemas, aplicações, dados e serviços precisam ser movidos para a nuvem, como eles serão acessados e quais recursos computacionais e de armazenamento serão necessários.

Requisitos para estratégia de uso de Software e de Serviços de Computação em Nuvem

Art. 2º Ao adotar *softwares*, serviços ou informações em infraestrutura de nuvem, a PRF deverá:

I - garantir aderência à legislação brasileira, em especial no que se refere à privacidade, proteção de dados pessoais e sigilo das comunicações privadas, devendo haver registros das seguintes operações:

a) coleta, armazenamento, guarda e tratamento de registros de dados pessoais; e

b) comunicações realizadas por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional.

II - realizar o gerenciamento de riscos, precedido de análise e relatório de impacto de dados pessoais, em conformidade com a legislação, dos seguintes itens:

a) o tipo de informação a ser migrada;

b) o fluxo de tratamento dos dados que podem ser afetados com a adoção da solução;

c) o valor dos ativos envolvidos; e

d) os benefícios da adoção de uma solução de computação em nuvem, em relação aos riscos de segurança e privacidade referentes à disponibilização de informações e serviços a um terceiro;

III - definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

IV - utilizar, para os sistemas estruturantes, somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas de órgãos ou de entidades;

V - avaliar quais informações serão hospedadas na nuvem, considerando:

a) o processo de classificação da informação de acordo com a legislação;

b) o valor do ativo de informação; e

c) os controles de acessos físico e lógico relativos à segurança da informação;

VI - definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução;

VII - planejar os custos de migração das informações e dos serviços, nos casos de ingresso e saída do serviço de computação em nuvem.

VIII - garantir que seja efetuado por parte do demandante, em se tratando de novo projeto, levantamento de custos entre os diversos provedores, nos termos do contrato de nuvem vigente, para fins de verificação do melhor custo-benefício (preço + técnica);

IX - aplicar o procedimento do inciso anterior para verificação da viabilidade de absorção e aderência, no caso de absorção de projeto desenvolvido em fornecedor de nuvem contemplado dentro do contrato vigente, porém fora do âmbito do mesmo contrato;

X - garantir que a contratação esteja aderente ao Manual de Serviços Regionais Essenciais de TIC - M-107, o qual dispõe sobre os requisitos mínimos para contratação de serviços de TIC; e

XI - garantir que a contratação, adoção e utilização dos recursos estejam alinhadas às diretrizes, aos objetivos estratégicos e às ações previstas no Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC vigente.

§ 1º A migração tratada no inciso VII do *caput* deverá ser devidamente justificada pelo demandante ou gestor negocial, que também será responsável pelo levantamento dos custos operacionais envolvidos na migração do sistema ou serviço para a nuvem.

§ 2º Os custos tratados no inciso VIII do *caput,* valores referenciais dos serviços dos fornecedores de nuvem, a serem considerados para fins comparativos, deverão ser aqueles pactuados no contrato vigente.

§ 3º Não sendo constatada a viabilidade econômica de absorção e aderência tratada no inciso IX do *caput,* dentro do contrato, no mesmo provedor de nuvem onde o projeto tenha sido desenvolvido, o demandante deverá providenciar o plano de migração para o fornecedor com melhor custo benefício verificado, sob pena de não absorção dentro do contrato.

Art. 3º Em função da capacidade de o provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a PRF deverá, no mínimo:

I - definir os critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem; e

II - revisar e atualizar periodicamente seus processos internos de gestão de riscos de segurança da informação.

Gerenciamento de Identidades e Registros

Art. 4º Em relação ao gerenciamento de identidades e de registros, a PRF deverá, no mínimo:

I - adotar um padrão de identidade federada para permitir o uso de tecnologia *single sign-on*, sempre que possível, no processo de autenticação de seus usuários no provedor de serviço de nuvem;

II - negar ao provedor de serviço de nuvem permissão de uso e acesso direto ao ambiente de autenticação da PRF;

III - adotar, de acordo com o nível de criticidade da informação, o uso da tecnologia *single sign-on*, o qual deve ser acompanhado:

a) de autenticação multi-fator; ou

b) de outra alternativa que aumente o grau de segurança no processo de autenticação de seus usuários no provedor de serviço de nuvem.

IV – garantir, por meio de checagem regulares, que o provedor de serviço de nuvem:

a) registre todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações; e

b) armazene, pelo período de 01 (um) ano, todos os registros de que trata a alínea anterior.

V - armazenar os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, por 05 (cinco) anos, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, a critério da PRF;

VI - manter em ambiente próprio controlado, pelo período de 05 (cinco) anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem;

VII - capacitar a equipe de segurança para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem;

VIII - possuir procedimentos de controle de acesso que abordem a transição entre as funções, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;

IX - configurar mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;

X - permitir à PRF gerenciar suas próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem; e

XI - atender aos requisitos legais e a outros critérios exigidos pela PRF em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso).

Recursos Criptográficos

Art. 5º Em relação à necessidade do uso de recursos criptográficos, a PRF deverá, no mínimo:

I - verificar se os dados da organização estão sendo tratados e armazenados de acordo com a legislação;

II - analisar a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios;

III - utilizar, sempre que possível, chaves de encriptação baseadas em *hardware*; e

IV – exigir ao provedor de nuvem que forneça as informações sobre as criptografias utilizadas, bem como checar sua utilização nos seguintes casos:

a) dados em trânsito: no mínimo VPN *site to site* com protocolo IPSEC;

b) dados em repouso: a utilização do protocolo *Advanced Encripted Standard* 256 bits AES-256 e apresentação de sua adoção;

c) política de controle de acesso às chaves criptográficas com adoção do mínimo privilégio; e

d) comprovação de controle de acesso aos serviços de nuvem com *Multiple Factor Autentication* - MFA.

Segregação de Dados

Art. 6º Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, a PRF, em conjunto com o provedor de serviço de nuvem, deverá estabelecer, no mínimo, as seguintes ações:

I - garantir que o ambiente contratado seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas;

II - implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelos diferentes órgãos ou entidades da administração pública federal e por outros usuários do serviço em nuvem;

III - garantir que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados;

IV - garantir a separação de todos os recursos utilizados pelo Provedor de Serviço de Nuvem daqueles recursos utilizados pela administração interna da PRF; e

V - avaliar os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem.

Gerenciamento dos Ambientes

Art. 7º O gerenciamento de nuvem será realizado pela unidade de infraestrutura de Tecnologia da Informação e Comunicação pertencente à Diretoria de Tecnologia da Informação e Comunicação - DTIC, ou área que venha a substituí-la.

§ 1º As áreas interessadas no uso de recursos em nuvem deverão acionar a respectiva unidade de infraestrutura de TIC, através de chamados técnicos a serem registrados na ferramenta de ITSM adotada pelo órgão.

§ 2º A unidade de infraestrutura de Tecnologia da Informação e Comunicação poderá, a qualquer tempo, conceder, limitar e/ou cortar acessos nas consoles dos provedores de nuvem, em razão da conveniência do serviço, visando estabelecer governança em nuvem.

Art. 8º A utilização de recursos de computação em nuvem no âmbito da Diretoria de Inteligência - DINT será detalhada em portaria específica da Diretoria de Tecnologia da Informação e Comunicação - DTIC, que estabelecerá as diretrizes e procedimentos para a gestão, monitoramento e controle desses recursos.

Tratamento de Dados e Informações

Art. 9º No que se refere ao tratamento de dados e informações em ambiente de computação em nuvem, deverão ser observadas as disposições da legislação vigente sobre proteção de dados, bem como as seguintes diretrizes:

I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;

II - informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada, não poderá ser tratada em ambiente de computação em nuvem pública; e

III - poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:

a) o material de acesso restrito regulado pela própria instituição;

b) a informação pessoal relativa à intimidade, vida privada, honra e imagem; e

c) o documento preparatório não previsto no inciso II do *caput*.

Art. 10. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela PRF, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:

I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança

fora do território brasileiro, conforme legislação aplicável;

III - a informação com restrição de acesso prevista na legislação e o documento preparatório não previsto no inciso II do art. 9º desta Instrução Normativa, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável; e

IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e demais legislações sobre o assunto.

Cláusulas Contratuais Obrigatórias

Art. 11. A PRF deve garantir que os instrumentos contratuais objetivando contratação de serviços de computação em nuvem devem ser adequados ao previsto nesta Instrução Normativa, devendo conter, no mínimo, os seguintes procedimentos de segurança:

I - termo de confidencialidade que impeça o provedor de serviço de usar, transferir e/ou liberar dados, sistemas, processos e informações da PRF para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II - garantia da exclusividade de direitos, por parte da PRF, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como *backups* de segurança;

III - proibição do uso de informações da PRF pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário, não autorizado;

IV - conformidade com a política de segurança da informação da PRF e com a legislação brasileira;

V - devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem à PRF ao término do contrato;

VI - eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema da PRF sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados; e

VII - garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018.

Requisitos para Provedores

Art. 12. A PRF deverá exigir que os prestadores de serviço, para a habilitação, cumpram no mínimo, os seguintes requisitos:

I - possuir metodologia de gestão de riscos, elaborada em conformidade com a legislação, bem como realizar o gerenciamento de riscos descrito nesta Instrução Normativa;

II - implementar práticas de fortalecimento dos mecanismos de virtualização, que devem incluir, no mínimo, os seguintes procedimentos:

a) desabilitar ou remover todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional;

b) configurar com segurança todas as interfaces de rede e áreas de armazenamento virtuais;

c) estabelecer limites para a utilização dos recursos de máquina virtual (*Virtual Machine*);

d) manter todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais;

e) validar a integridade das operações de gerenciamento de chaves criptográficas;

f) possuir controles que permitam aos usuários autorizados do órgão ou da entidade acessarem os registros de acesso administrativo do monitor de máquina virtual (*Hypervisor*);

g) habilitar o registro completo do *Hypervisor*; e

h) suportar o uso de máquinas virtuais confiáveis (*Trusted VM*) fornecidas pela PRF, que estejam em conformidade com as políticas e práticas de fortalecimento de redes exigidas ao provedor de serviço de nuvem.

III - em relação à segurança de aplicações *web* disponibilizadas no ambiente de nuvem:

a) utilizar *firewalls* especializados na proteção de sistemas e aplicações;

b) desenvolver código *web* em conformidade com os normativos existentes;

c) aplicar regras e práticas de segurança de sistemas operacionais e de aplicações definidas pela PRF;

d) realizar periodicamente testes de penetração de redes e de aplicações; e

e) possuir um programa de correção de vulnerabilidades;

IV - possuir processos de gestão de continuidade de negócios e de gestão de mudanças, em conformidade com os normativos existentes nessas áreas;

V - possuir um plano de recuperação de desastres que estabeleça procedimentos de recuperação e de restauração de plataforma, infraestrutura, aplicações e dados após incidentes de perda de dados;

VI - estabelecer um canal de comunicação seguro utilizando, no mínimo, *Secure Sockets Layer/Transport Layer Security* - SSL/TLS;

VII - utilizar padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pelo órgão;

VIII - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do órgão em relação à segregação de dados:

a) isolar, utilizando separação lógica, todos os dados e serviços do órgão de outros clientes de serviço em nuvem;

b) segregar o tráfego de gerenciamento do tráfego de dados da PRF; e

c) implementar dispositivos de segurança entre zonas;

IX - possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:

a) sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta;

b) destruir, de modo seguro, ativo de informação no fim do ciclo de vida ou considerado inservível, com o fornecimento de um Certificado de Destruição de Equipamento Eletrônico (*Certificate of Electronic Equipment Destruction* - CEED) e discriminar os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição; e

c) armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e de saída de dispositivos;

X - notificar, imediatamente, à PRF incidente cibernético contra os serviços ou dados sob sua custódia;

XI - possuir procedimentos necessários para preservação de evidências, conforme legislação; e

XII - demonstrar estar em conformidade com os padrões de segurança de nuvem, por meio de auditoria anual *Service and Organization Controls 2* - SOC 2, conduzida por um auditor independente, com a apresentação dos relatórios de tipo I e tipo II.

Utilização de *Cloud Brokers*

Art. 13. A PRF deverá, em seu processo de contratação, garantir a utilização de *cloud*

broker como integrador dos serviços de computação em nuvem com 02 (dois) ou mais provedores de serviço de nuvem.

Art. 14. O *cloud broker* é o responsável por garantir que os provedores de serviço de nuvem que ele representa cumpram todos os requisitos previstos nesta IN e na legislação brasileira e operem de acordo com as políticas de segurança da PRF.

Parágrafo único. A PRF deverá prever no instrumento contratual que o *cloud broker* poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

Das competências, atribuições e responsabilidades

Art. 15. Compete ao Comitê de Segurança da Informação:

I - aprovar as minutas de elaboração e de revisões do ato normativo sobre estratégia e o uso seguro de computação em nuvem e divulgá-las às partes interessadas;

II - estabelecer os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados em soluções de computação em nuvem;

III - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem; e

IV - analisar, em caráter conclusivo, as minutas de elaboração e de revisões do ato normativo sobre estratégia e o uso seguro de computação em nuvem.

Art. 16. Compete ao Gestor de Segurança da Informação:

I - instituir e coordenar a equipe para elaboração e revisões do ato normativo sobre estratégia e o uso seguro de computação em nuvem;

II - supervisionar a aplicação do ato normativo sobre estratégia e o uso seguro de computação em nuvem;

III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, de forma a assegurar que os controles e os níveis de serviço relacionados à segurança da informação acordados sejam cumpridos;

IV - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios relacionados à segurança da informação;

V - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida;

VI - encaminhar para aprovação da alta administração as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem; e

VII - propor ações de segurança da informação para a implementação ou a contratação, de tecnologias de computação em nuvem em conformidade com as orientações contidas neste documento.

Art. 17. Compete à Diretoria de Tecnologia da Informação e Comunicação - DTIC e demais setores de Tecnologia da Informação e Comunicação das Unidades Desconcentradas da PRF, implementar os procedimentos relativos ao uso de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta Instrução Normativa e legislação pertinente.

Art. 18. Compete à Diretoria de Tecnologia da Informação e Comunicação - DTIC, com relação ao gerenciamento de nuvem, no mínimo:

I - promover a capacitação da equipe responsável pelo gerenciamento, nas tecnologias utilizadas pelo provedor de serviço de nuvem;

II - exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem;

III - elaborar uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias com, no mínimo, os papéis e funções constantes no Anexo desta Instrução Normativa; e

IV - elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem e comunicá-lo à equipe responsável pelo gerenciamento da nuvem.

Disposições Finais

Art. 19. A revisão desta Instrução Normativa deverá ocorrer no máximo de 02 (dois) em 02 (dois) anos ou sempre que houver fatos supervenientes que ensejem a mudança.

Art. 20. Fica revogada a Instrução Normativa PRF nº 98, de 19 de dezembro de 2022 (SEI Nº 45602845).

Art. 21. Esta Instrução Normativa entra em vigor na data de publicação.

ANTONIO FERNANDO SOUZA OLIVEIRA

PRF

Documento assinado eletronicamente por **ANTONIO FERNANDO SOUZA OLIVEIRA**, **Diretor-Geral**, em 05/05/2025, às 23:07, 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 **65201832** e o código CRC **E6E24074**.

ANEXO DA INSTRUÇÃO NORMATIVA PRF Nº 156, DE 05 DE MAIO DE 2025 (SEI Nº 65201832)

MATRIZ DE RESPONSABILIDADES

Atividade/Função	PRF	Fornecedor	Área Responsável
Gerenciamento de Contrato			
Revisão de contrato	R	A	Gerente de Projetos ou função similar
Renegociação de termos	R	A	Gerente de Projetos ou função similar
Segurança			
Avaliação de Riscos	R	A	Especialista em Segurança
Implementação de políticas de segurança	R	A	Especialista em Segurança
Monitoramento de compliance	R	A	Auditor de Segurança
Gerenciamento de Recursos			
Provisionamento de recursos	R	A	Administrador de Sistemas
Monitoramento de uso de recursos	R	A	Analista de Recursos
Otimização de custos	R	A	
Interface de Comunicação			
Reuniões de status	R	A	Gerente de Projetos ou função similar
Relatórios de desempenho	R	A	Analista de Serviços
Gestão de incidentes	R	A	Analista de Suporte
Atividades Operacionais Técnicas			
Implementação de soluções técnicas	R	A	Analista especializado em Nuvem
Gestão de backups	R	A	Administrador de Sistemas
Atualizações e manutenção	R	A	Analista especializado em Nuvem
Resolução de problemas	R	A	Analista de Suporte

Legenda: R - Responsável pela execução da atividade. / A - Apoio ou fornecimento da atividade.