Processo nº 08650.016812/2022-48 SEI nº 45602845

Boletim de Serviço Eletrônico em 19/12/2022

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

INSTRUÇÃO NORMATIVA PRF Nº 98, DE 19 DE DEZEMBRO DE 2022

Dispõe sobre a utilização de soluções 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 pelo Decreto nº 11.103, de 24 de junho de 2022, tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, na Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, na Instrução Normativa GSI/PR nº 05, de 30 de agosto 2021, e na Instrução Normativa PRF nº 45, de 22 de junho de 2021, bem como o contido nos autos do processo SEI nº 08650.016812/2022-48, resolve:

Objeto e âmbito de aplicação

Art. 1º Dispor sobre a utilização de soluções 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.

Requisitos para Adoção de Computação em Nuvem

Art. 2º Ao alocar 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; e

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

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 - exigir do provedor de serviço de nuvem que:

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

b) armazene, pelo período de 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 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 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; e

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

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; e

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

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 Em relação ao gerenciamento de nuvem, a PRF deverá, no mínimo:

I - capacitar a equipe responsável por esse 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; 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.

Tratamento de Dados e Informações

Art. 8º Em relação ao tratamento de dados e informações em ambiente de computação em nuvem, a PRF, além de cumprir as orientações contidas na legislação sobre proteção de dados, deverá observar 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 poderão ser tratados 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. 9º 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 **caput** art. 8º, 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. 10. Os instrumentos contratuais objetivando contratação de serviços de computação em nuvem devem ser adequados ao previsto nesta IN, 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 da política de segurança da informação do provedor de serviço de nuvem 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 PPRF 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. 11. Para que esteja habilitado a prestar serviços de computação em nuvem para a PRF, o provedor de serviço de nuvem deverá cumprir, 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 IN;

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 ao gerenciamento de identidades e registros:

a) 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;

b) impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;

c) suportar tecnologia **single sign-on** para autenticação;

d) suportar mecanismos de autenticação multi-fator ou uma alternativa que aumente o grau de segurança no processo de autenticação de usuários do órgão ou da entidade no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;

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

f) 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);

IV - 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;

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

VI - 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;

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

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

IX - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do órgão;

X - 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;

XI - 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;

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

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

XIV - 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. 12. O **cloud broker** deverá atuar como integrador dos serviços de computação em nuvem entre a PRF e dois ou mais provedores de serviço de nuvem.

Art. 13. Caso a PRF contrate, por meio do **cloud broker,** plataforma de gestão multinuvem para realizar procedimentos de provisionamento e orquestração do ambiente, é necessário que a ferramenta possua, no mínimo:

I - em relação às funcionalidades de provisionamento e orquestração de multinuvem:

a) um único portal integrado de provisionamentos para o usuário final;

b) utilização de modelos de provisionamento;

c) automação segura de provisionamento simultâneo e utilização, no que couber, ferramentas de código aberto e interoperáveis;

d) fluxos de trabalho de orquestração baseada em eventos; e

e) soluções seguras integradas de criação de infraestrutura por código (IaaC);

II - em relação às funcionalidades de monitoramento e análise em multinuvem:

a) relatórios de monitoramento de desempenho de recursos na nuvem;

b) coleta e monitoramento de registros; e

c) procedimentos de monitoramento de alertas;

III - em relação às funcionalidades de inventário e classificação em multinuvem:

a) inventário de recursos na nuvem;

b) procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem; e

c) detecção de recursos sem etiqueta; e

IV - em relação às funcionalidades de gerenciamento de segurança, conformidade e identidade:

a) mecanismos de **single sign-on** e de autenticação multifator das plataformas em nuvem;

b) gerenciamento seguro de usuários e de grupos de usuários;

c) gerenciamento de segurança dos recursos;

d) notificações de eventos de alerta multicanal;

e) gerenciamento de identidade e acesso (IAM); e

f) registros de atividade da plataforma em nuvem.

Parágrafo único. O **cloud broker** poderá utilizar ferramenta de **Software as a Service (SaaS)** comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar essa plataforma.

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.

Disposições Finais

Art. 15. Para garantir a segurança de que trata esta IN, a PRF poderá adotar outras diretrizes complementares, desde que não confrontem as previsões da legislação.

Art. 16. A apresentação dos relatórios de tipo I e tipo II da auditoria **SOC 2**, comprovada a conformidade com os padrões de segurança em nuvem, é condição essencial, tanto para habilitar a participação em processo licitatório, como para renovar o contrato de prestação de serviço em nuvem.

Parágrafo único. Na hipótese de utilização de **cloud broker**, esse será o responsável por apresentar os relatórios de tipo I e tipo II da auditoria SOC 2 de todos os provedores de serviço de nuvem que ele representa.

Art. 17. Os contratos de serviços de provedor de serviço de nuvem já contratados pela PRF, terão um prazo de doze meses, após a entrada em vigor desta IN, para sua adequação.

Art. 18. Nos termos do inciso V do Art. 5º da Instrução Normativa GSI/PR nº 5, de 2021, esta IN deverá ser revisada no mínimo a cada dois anos, conforme proposta a ser apresentada e aprovada pelo Comitê Gestor de Segurança da Informação (CGSI).

§1º A revisão da IN poderá ocorrer a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem o uso seguro de computação em nuvem, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

§2º Não identificada a necessidade de revisão da IN após o transcurso do biênio previsto no **caput,** o CGSI deverá documentar em ata tal deliberação.

Art. 19. Esta Instrução Normativa entra em vigor em 2 de janeiro de 2023.

SILVINEI VASQUES

Documento assinado eletronicamente por **SILVINEI VASQUES**, **Diretor-Geral**, em 19/12/2022, às 21:01, 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 **45602845** e o código CRC **A5FE0246**.

Processo nº 08650.016812/2022-48 SEI nº 45602845