MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS

PORTARIA Nº 195 DG, DE 04 DE JULHO DE 2025

Ministério da Integração e do Desenvolvimento Regional - MDR
Departamento Nacional de Obras Contra as Secas – DNOCS
Comitê de Governança Digital - CGD

Institui a Política de **Gestão de Provedor de Serviços** do Departamento Nacional de Obras Contra as Secas – DNOCS.

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS – DNOCS, no uso das atribuições legais que lhe confere o disposto no Art. 68 e respectivo inciso XII da Portaria DNOCS/DG/GAB nº 43, de 31 de janeiro de 2017, em atendimento à Estratégia Federal de Governo Digital e à Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

R E S O L V E:

Art. 1º Aprovar a **Política de Gestão de Provedor de Serviços** do Departamento Nacional de Obras Contra as Secas – DNOCS, na forma do Anexo I desta Portaria, de observância obrigatória no âmbito dessa Autarquia Federal.

Art. 2º Esta Portaria entra em vigor em 29 de Agosto de 2025.

Fernando Marcondes de Araújo Leão
Diretor-Geral do DNOCS

Documento assinado eletronicamente por **Fernando Marcondes de Araújo Leão**, **Diretor Geral**, em 04/07/2025, às 14:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

ANEXO I

POLÍTICA DE GESTÃO DE PROVEDOR DE SERVIÇOS

Das Diretrizes Gerais

Art. 1º. O DNOCS estabelecerá a PGPS, que deve estar de acordo com as diretrizes estipuladas na Política de Segurança da Informação e na Política de Proteção de Dados Pessoais do órgão.

Art. 2º. A PGPS demonstrará aspectos micros e macros de privacidade, proteção de dados e segurança da informação na relação do DNOCS com seus provedores de serviços de tecnologia da informação. Os relacionamentos com provedores de serviços e produtos também devem seguir as diretrizes da PGPS.

Art. 3º. O Comitê de Governança Digital deverá estipular os prazos que os departamentos e provedores de serviço se adequem as diretrizes da PGPS.

Art. 4º. A PGPS e suas atualizações deverão ser aprovadas pelo Comitê de Governança Digital do órgão.

Art. 5º. A PGPS deve ser devidamente divulgada e estará disponível para todos os colaboradores do DNOCS.

Art. 6º. Os compromissos de melhoria contínua dos provedores de serviço devem estar expostos na PGPS.

Art. 7º. A PGPS deverá ser revisada e atualizada de forma periódica, ou quando houver necessidade por motivos que o DNOCS julgar relevantes (como por exemplo, adequação a novas leis, boas práticas, incidentes de segurança).

Art. 8º. O DNOCS deverá seguir as orientações da Instrução Normativa SGD/ME nº 94/22 para a gestão e governança de contratos de prestação de serviços.

Art. 9º. A avalição de provedores de serviço deverá ser realizada levando em consideração, mas não se limitando, as diretrizes da Instrução Normativa SGD/ME nº 94/22.

Art. 10. O DNOCS deverá estabelecer nos requisitos de contratação de provedores de serviços os aspectos mínimos e relevantes de proteção de dados e segurança da informação.

Art. 11. Os acordos e contratos entre o DNOCS e os provedores devem ser estabelecidos e documentados para que haja um entendimento claro entre as partes sobre as obrigações de cumprimento os requisitos mínimos e relevantes de proteção de dados e segurança da informação.

Art. 12. Os acordos e contratos podem conter os seguintes termos de segurança da informação e proteção de dados:

I. Descrição das informações a serem fornecidas ou acessadas e os métodos e meios de fornecimento ou acesso as estas informações aos provedores;

II. Classificação das informações de acordo com o esquema de classificação das informações do DNOCS;

III. Mapeamento e análise de convergência entre o método de classificação de

informações do DNOCS e do provedor de serviços;

IV. Requisitos mínimos de segurança da informação em relação a infraestrutura de TI do provedor;

V. Requisitos e procedimentos para a gestão de incidentes de segurança da informação e violação de proteção de dados e privacidade;

VI. Contatos relevantes de ambas as partes, para possível tratamento de incidentes.

Art. 13. O DNOCS deve definir um plano de ação para mitigar não conformidades de um provedor quando forem identificadas por meio de monitoramento.

Art. 14. O DNOCS deve definir em seus contratos com provedores de serviços as obrigações de cada parte contratual de implementar um conjunto de controles acordados, incluindo controle de acesso, análise crítica de desempenho, monitoramento, relatos e auditorias, e as obrigações do provedor de serviços de estar em conformidade com os requisitos de proteção de dados e segurança da informação do DNOCS.

Art. 15. O DNOCS deverá implementar um processo de monitoramento com métodos estabelecidos para a validação de serviços e produtos em conformidade com os requisitos de proteção de dados e segurança da informação pré-estabelecidos.

Da Avaliação de Riscos

Art. 16. A avaliação de riscos poderá ocorrer antes e durante o contrato com um provedor de serviços.

Art. 17. O DNOCS deve conduzir uma avaliação detalhada dos riscos associados à terceirização de serviços. Isso inclui, mas não se limita, a uma análise de vulnerabilidades potenciais, conformidade regulatória e impacto nas operações do DNOCS.

Art. 18. Estabelecer processos e procedimentos para gerenciar a proteção de dados e a segurança da informação e os riscos que podem ser associados com o uso de serviços e produtos de provedores.

Art. 19. O DNOCS deve estipular os responsáveis pela avaliação.

Art. 20. O DNOCS deve definir quando os resultados da avaliação serão analisados e por quem.

Art. 21. Analisar os relatórios elaborados após as avaliações e auditorias de seus provedores de serviço.

Art. 22. Avaliar e gerenciar riscos à proteção de dados e à segurança da informação associados a:

I. Uso das informações internas por provedores e seus associados.

II. Vulnerabilidades e mal funcionamento de produtos ou serviços operados e criados pelos provedores e seus associados. (por exemplo, software, API, componentes de hardware e utilizados para a manutenção ativa dos produtos e serviços).

Art. 23. Implementar ferramentas de análise de risco contínuo para identificar e mitigar proativamente novas ameaças à segurança de dados apresentadas pelos provedores de serviços.

Art. 24. O DNOCS deverá realizar a gestão de risco adequada em cada fornecedor e seus respectivos serviços.

Art. 25. A avaliação pode ser realizada após a ocorrência de um incidente de segurança.

Dos Contratos e Acordos

Art. 26. Todos os contratos com provedores de serviços devem incluir cláusulas específicas relacionadas à privacidade, proteção de dados, segurança da informação, responsabilidades, conformidade regulatória e requisitos de relatórios.

Art. 27. Quando necessário, o DNOCS deverá estabelecer procedimentos para a continuação da prestação de serviço em caso alteração do provedor, seja por conclusão do contrato ou por incapacidade do provedor original.

Art. 28. O DNOCS deve solicitar a assinatura de termos de confidencialidade por parte dos funcionários e colaboradores dos provedores de serviço, sendo esta, uma condição a ser cumprida antes dos associados do provedor de serviço iniciarem a operação de serviços e produtos.

Art. 29. Os contratos devem ser revisados por profissionais jurídicos e de segurança cibernética para garantir que as obrigações sejam claramente definidas e aplicáveis.

Art. 30. Incluir cláusulas contratuais que estabeleçam o direito do DNOCS de auditar as práticas de proteção de dados e segurança da informação do provedor de serviços.

Art. 31. Estabelecer um mecanismo para revisar e atualizar periodicamente os requisitos de privacidade, proteção de dados e segurança da informação do contrato à medida que novas ameaças e regulamentações surjam.

Art. 32. Definir os recursos de TI e informações que os provedores de serviços podem acessar, usar, monitorar ou controlar.

Art. 33. Definir e fazer cumprir os prazos de confidencialidade das informações, produtos e serviços do DNOCS.

Art. 34. Definir o nível de segurança física e lógica esperado dos provedores e associados e suas instalações.

Art. 35. Definir os requisitos de segurança da informação que irá utilizar para adquirir produtos ou serviços de TI.

Art. 36. Exigir que seus provedores propaguem e façam cumprir os requisitos de proteção de dados e segurança da informação do DNOCS em toda a cadeia de fornecimento;

Art. 37. Solicitar que os provedores de produtos e serviços de TI forneçam informações descrevendo os controles de proteção de dados e segurança da informação implementados em seus produtos e serviços e as configurações necessárias para a sua operação segura;

Art. 38. Obter garantia de que os produtos e serviços de TI entregues estejam funcionando como o esperado;

Art. 39. Especificar as responsabilidades do provedor de serviços em relação à exclusão segura de dados ao final do contrato ou quando não forem mais necessários.

Art. 40. Incluir disposições contratuais que garantam a conformidade do provedor de serviços com as diretrizes de segurança de dados disposto na Seção II (Da responsabilidade) da Lei Geral de Proteção de Dados - LGPD.

Art. 41. Estabelecer protocolos para revisão e aprovação de quaisquer subcontratados ou provedores de serviços adicionais que o provedor de serviços possa envolver.

Art. 42. Definir procedimentos para resolver divergências relacionadas à proteção de dados e à segurança da informação entre o DNOCS e o provedor de serviços.

Dos Provedores de Serviço

Art. 43. O DNOCS deve criar e manter um inventário de provedores de serviço e seus ativos associados, incluindo o número do contrato, tipo de serviço contratado, quantidade de operadores, e habilidades dos operadores.

Art. 44. O DNOCS deverá realizar a atualização do inventário quando ocorrerem novas

contratações, alterações e encerramento de contratos.

Art. 45. O inventário é um ativo de informação como um catálogo de serviços, e devem ser aplicados controles de privacidade, proteção de dados e segurança da informação para evitar acessos indevidos, adulterações e conteúdo e vazamento de informações.

Art. 46. O inventário deve conter informações sobre os ativos de informação necessários a serem utilizados pelos provedores para a entrega e operação de serviços.

Classificação

Art. 47. A classificação dos provedores de serviço deve ser realizada a cada 3(três) anos.

Art. 48. Estabelecer como classificar os provedores de serviço de acordo com a sensibilidade das informações, produtos e serviços utilizados pelos provedores.

Art. 49. Definir os tipos de componentes de serviços de infraestrutura de TI e nuvem fornecidos pelos fornecedores que podem degradar a proteção de dados e segurança da informação.

Art. 50. Os provedores de serviço devem ser classificados de acordo com a criticidade do serviço prestado para o DNOCS. Os responsáveis pela gestão do contrato devem auxiliar o processo de classificação dos provedores de serviço.

Art. 51. Incluir uma ou mais características, como sensibilidade dos dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis, risco inerente e risco mitigado.

Art. 52. A classificação deverá ser atualizada a cada [período] ou quando ocorrerem mudanças significativas nas execuções dos contratos que possam impactar esta salvaguarda.

Art. 53. O DNOCS deverá avaliar se é interessante criar grupos de provedores de acordo com suas classificações, para que assim, sejam aplicadas medidas de privacidade, proteção de dados e segurança da informação específicas para cada grupo.

Da Avaliação e do Monitoramento Contínuo

Art. 54. Os provedores de serviços devem ser reavaliados de forma contínua.

Art. 55. Avaliar se os requisitos de proteção de dados e segurança da informação estão sendo cumpridos com cada provedor e contrato de forma individual.

Art. 56. Avaliar a qualidade e eficiência dos provedores de serviço de acordo com produtos e serviços entregues e em execução.

Art. 57. Realizar avaliações, utilizando-se ou não de terceiros independentes, para verificar a conformidade do provedor de serviços com as normas de proteção de dados e segurança da informação.

Art. 58. O DNOCS deve implementar processos de monitoramento contínuo para avaliar o desempenho do provedor de serviços em relação aos padrões acordados de privacidade, proteção de dados, segurança da informação e conformidade regulatória.

Art. 59. O monitoramento pode envolver auditorias regulares, revisões de relatórios de segurança e testes de penetração.

Art. 60. O DNOCS deve determinar o que deve ser monitorado e medido, incluindo processos, controles e requisitos de proteção de dados e segurança da informação.

Art. 61. Métodos para o monitoramento que consigam gerar resultados válidos e comparáveis devem ser definidos pelo DNOCS.

Art. 62. O DNOCS deve definir o período para a realizar o monitoramento do provedor de serviços e suas soluções de TI.

Art. 63. Definir quando os resultados do monitoramento e de medições devem ser analisados.

Art. 64. Definir quem deve analisar e avaliar o resultado do monitoramento e da medição.

Art. 65. Definir quem é o responsável pelo monitoramento do provedor de serviços.

Art. 66. Toda a documentação do monitoramento deve ser retida como evidência dos resultados.

Art. 67. O monitoramento de conformidade do provedor de serviços pode ser implementado de maneira automatizada por meio de soluções de gerenciamento de riscos e conformidade.

Art. 68. Os registros detalhados de todas as interações com o provedor de serviços, incluindo comunicações, incidentes de segurança e auditorias deve ser mantido por no mínimo 5(cinco) anos.

Art. 69. Implementar um sistema de alerta precoce para notificar o DNOCS sobre quaisquer anomalias ou comportamentos suspeitos por parte do provedor de serviços.

Art. 70. Um inventário organizado dos provedores de serviços deve ser mantido atualizado de forma a permitir identificar um ponto de contato com cada prestador de serviços.

Art. 71. Os provedores de serviços devem ser listados, classificados e designados em contato formal para cada provedor de serviços.

Art. 72. A revisão e atualização do inventário de provedores de serviços deve ser feita quando ocorrerem mudanças significativas que possam impactar esta salvaguarda.

Art. 73. Desenvolver painéis de controle personalizados para visualizar métricas de privacidade, proteção de dados e segurança da informação em tempo real relacionadas aos provedores de serviços.

Art.74. Realizar processo abrangente de diligência (due diligence) para avaliar a credibilidade, reputação e práticas de segurança cibernética do provedor de serviços. Isso envolve revisar suas políticas de segurança, histórico de incidentes de segurança e certificações relevantes.

Art. 75. O DNOCS poderá utilizar a avaliação dos serviços e produtos prestados pelos provedores de serviço para verificar se estes atingiram os níveis de proteção de dados e segurança da informação necessários.

Da Gestão de Incidentes

Art. 76. Definir os requisitos mínimos de notificação de incidentes de segurança de dados pelo provedor de serviços, incluindo prazos e formato da comunicação.

Art. 77. Procedimentos claros e responsabilidades devem ser estabelecidos para lidar com incidentes de segurança cibernética relacionados aos serviços fornecidos pelo provedor.

Art. 78. Dentre os procedimentos pode-se incluir a comunicação eficaz, investigação de incidentes e ações corretivas para mitigar danos e evitar recorrências.

Art. 79. Tratar incidentes de segurança da informação e violações a proteção de dados e privacidade que por algum motivo estejam correlacionados a algum provedor de serviços.

Art. 80. Fazer uso de medidas de recuperação, contingência e resiliência cibernética para garantir a disponibilidade do tratamento de dados e informações dos provedores e do DNOCS.

Art. 81. Mitigar qualquer ação do provedor de serviços que venha causar dano o DNOCS, independente da maneira que o DNOCS tomou conhecimento da ação.

Art. 82. Integrar planos de resposta a incidentes comuns com o provedor de serviços para facilitar a coordenação e colaboração durante incidentes de segurança de dados.

Art. 83. Designar pontos de contato dedicados entre o DNOCS e o provedor de serviços para facilitar a comunicação e a troca de informações durante incidentes de segurança.

Art. 84. Implementar simulações regulares de incidentes de segurança com o provedor de serviços para garantir uma resposta coordenada e eficaz.

Art. 85. Documentar todas as interações e atividades relacionadas à resposta a incidentes com o provedor de serviços para fins de revisão e análise pós-incidente.

Art. 86. Estabelecer um protocolo claro para a condução de investigações conjuntas com o provedor de serviços para identificar a causa raiz de incidentes de segurança.

Art. 87. Realizar revisões pós-incidente em colaboração com o provedor de serviços para identificar áreas de melhoria nos processos de resposta a incidentes.

Art. 88. Fornecer treinamento regular aos colaboradores sobre os procedimentos de notificação de incidentes e como interagir com o provedor de serviços durante um incidente de segurança.

Da Revisão e Melhoria Contínua

Art. 89. A PGPS dever ser revisada a cada [período] para garantir sua eficácia contínua e alinhamento com as melhores práticas de privacidade, proteção de dados e segurança da informação.

Art. 90. Manter-se atualizado sobre a legislação e melhores práticas de mercado em relação a gestão de provedores de serviço e adaptar as políticas conforme necessário para manter a relevância e eficácia.

Art. 91. Estabeleça canais de comunicação para receber feedback contínuo dos usuários internos e externos sobre a qualidade dos serviços dos provedores, utilizando essas informações para ajudar a melhorar a PGPS.

Art. 92. Lições aprendidas com incidentes passados e mudanças no ambiente operacional devem ser incorporadas para aprimorar os processos e controles.

Art. 93. Estabelecer um processo formal para revisão e validação dos relatórios de conformidade fornecidos pelo provedor de serviços.

Treinamento e Conscientização

Art. 94. Desenvolver materiais de treinamento personalizados para colaboradores de diferentes níveis e funções no DNOCS sobre a gestão de provedores de serviços.

Art. 95. Realizar sessões de treinamento interativo e workshops para simular cenários práticos envolvendo provedores de serviços e práticas recomendadas de segurança.

Art. 96. Estabelecer um programa de recompensas e reconhecimento para funcionários que demonstrarem um bom entendimento e adesão às políticas de gestão de provedores de serviços.

Art. 97. Fornecer recursos online acessíveis, como vídeos, guias e FAQs, para facilitar o aprendizado contínuo sobre segurança de dados e gestão de provedores de serviços.

Art. 98. Incorporar o treinamento sobre gestão de provedores de serviços e segurança de dados em programas de integração de novos funcionários e treinamentos regulares de reciclagem.

Art. 99. Realizar avaliações periódicas de conhecimento e conscientização entre os funcionários para medir a eficácia do treinamento sobre gestão de provedores de serviços.

Art. 100. Incentivar a participação em eventos e conferências do setor relacionados a proteção de dados e segurança da informação para promover a educação contínua e a conscientização.

Encerramento de Contrato

Art. 101. O provedor de serviço deverá realizar atividades para o descarte seguro de dados e informações nos ativos de informação que estão sob sua responsabilidade ou foram utilizados para a prestação de serviço.

Art. 102. Contratos que utilizem a locação de ativos computacionais devem estabelecer o estado de preservação quando o ativo for devolvido.

Art. 103. Definir requisitos para garantir o término seguro de relacionamentos com os provedores e associados, incluindo, mas não se limitando a:

I. Tratamento de informações;

II. Desprovisionamento de direitos de acessos;

III. Determinação da propriedade intelectual dos artefatos desenvolvidos durante o contrato;

IV. Possível portabilidade e repasse de informações em caso de alteração de provedor ou internalização de serviços;

V. Atualização do inventário de provedores;

VI. Gerenciamento de registros;

VII. Devolução de ativos de informação;

VIII. Descarte e eliminação segura de informações e ativos de informação utilizados pelos provedores e seus associados.

104. O prestador de serviço deverá realizar a limpeza segura dos ativos de informação utilizados no contrato.

Anexo II

Não conformidade

As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

1. Processo Administrativo disciplinar de acordo com a legislação aplicável

2. Exoneração.

3. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.

4.Rescisão contratual ao bem do serviço público.

ANEXO III

Concordância

Li e entendi a Política de Gestão de Provedor de Serviços do DNOCS . Entendo que caso venha a violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais ou disciplinares de acordo com as leis aplicáveis ou normas internas do DNOCS .

_____

Nome do Servidor/Empregado

_____

Assinatura do Servidor/Data