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

PORTARIA Nº 140 DG, DE 22 DE MARÇO DE 2024

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

Institui a Política Gerenciamento de Vulnerabilidades 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 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 Gerenciamento de Vulnerabilidades 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 1º de Abril de 2024.

Fernando Marcondes de Araújo Leão
Diretor-Geral do DNOCS

Documento assinado eletronicamente por **Fernando Marcondes de Araújo Leão**, **Diretor Geral**, em 22/03/2024, às 13:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.dnocs.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1598984** e o código CRC **5247CE41**.

ANEXO I
POLÍTICA GERENCIAMENTO DE VULNERABILIDADES

CAPÍTULO I
PROPÓSITO

Art. 1º O objetivo da Política de Gerenciamento de Vulnerabilidades é estabelecer as regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades.

Art. 2º Contempla, também, ações e boas práticas que devem ser observadas para se evitar que vulnerabilidades estejam presentes nos ativos da organização.

Parágrafo Único: A revisão, a avaliação, a aplicação e a verificação das atualizações de ativos de informação auxiliam a mitigar as vulnerabilidades no ambiente de Tecnologia da Informação e Telecomunicações, bem como os riscos associados a tais vulnerabilidades.

CAPÍTULO II
ESCOPO

Art. 3º Esta política de gerenciamento de vulnerabilidades se aplica aos sistemas e ativos informacionais *do DNOCS* , incluindo servidores, gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem ativos informacionais.

Art. 4º Os serviços de TI críticos do DNOCS devem ser formalmente elencados pelo Comitê de Governança Digital.

Art. 5º Já ficam previamente estabelecidos os processos de Monitoramento e Segurança de Barragens, Estudos e Implantação de Infraestruturas Hídricas e Execução de Projetos e Planos de Irrigação como processos críticos do DNOCS.

Art. 6º A unidade de TIC é responsável por elaborar, manter e fazer cumprir a Política de Gerenciamento de Vulnerabilidades do DNOCS.

CAPÍTULO III
EXCEÇÕES

Art. 7º Pode ocorrer que alguns ativos de informação do DNOCS não serem contemplados por possíveis dificuldades técnicas ou obrigações contratuais e normativas. Quaisquer exceções a esta política deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções do DNOCS

CAPÍTULO IV
PÚBLICO

Art. 8º Esta Política de Gerenciamento de Vulnerabilidades (PGV) do DNOCS se aplica a indivíduos responsáveis pela gestão e a indivíduos que utilizam qualquer Ativo de Informação da Rede Computadores em nome do DNOCS. Além disso, a presente política se aplica a quaisquer provedores e entidades terceirizadas com acesso a informações, redes e aplicativos do DNOCS.

CAPÍTULO V
TERMOS E DEFINIÇÕES

Art. 9º São termos chave, siglas e conceitos que serão utilizados na política(conforme Portaria GSI/PR Nº 93, de 18 de outubro 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República):

I. AMEAÇA – Conjunto de fatores externos com o potencial de causarem dano para um sistema ou organização.

II. ANÁLISE DE VULNERABILIDADES – Verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas.

III. ATIVOS DE INFORMAÇÃO – Meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

IV. BANCO DE DADOS – Coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.

V. CTIR GOV – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

VI. CVE (*Common Vulnerabilities and Exposures*) – Vulnerabilidades e Exposições Comuns.

VII. CVSS (*Common Vulnerability Scoring System*) – Sistema comum de pontuação de vulnerabilidade.

VIII. HOST – Um computador ou dispositivo de TI (por exemplo, roteador, switch, gateway, firewall).

IX. ID CVE – Identificação para um CVE específico.

X. GERENCIAMENTO DE VULNERABILIDADE – Processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades.

XI. GESTÃO DE MUDANÇAS NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO – Processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

XII. GESTOR DE SEGURANÇA DA INFORMAÇÃO – Responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

XIII. LOG (REGISTRO DE AUDITORIA) – Registro de eventos relevantes em um dispositivo ou sistema computacional.

XIV. NTP (*Network Time Protocol*) – Protocolo de Tempo para Redes.

XV. PATCH – Uma parte de código adicional desenvolvido para resolver um problema ou falha em um software existente.

XVI. PENTEST – Acrônimo de teste de penetração (*penetration test*).

XVII. REMEDIAÇÃO – O ato de corrigir uma vulnerabilidade ou eliminar uma ameaça.

XVIII. RISCO – No sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade.

XIX. RISCO DE SEGURANÇA DA INFORMAÇÃO – Risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

XX. TESTE DE INVASÃO – Metodologia para testar a eficácia e a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante.

XXI. TESTE DE PENETRAÇÃO (PENTEST) – Também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos softwares que estão sendo utilizados pelo órgão ou entidade.

XXII. VULNERABILIDADE – Condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

CAPÍTULO VI
REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Art. 10 São leis, regulamentos ou guias de boas práticas que regem a presente política ou com as quais deve estar em conformidade ou em cumprimento:

Orientação	**Seção**
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2023	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2º, inciso XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art. 3º, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art. 2º, Incisos III e IV CAPÍTULO II - Art. 3º, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art. 15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Framework de segurança cibernética do CIS 8	Salvaguardas do controle 7 (*Continuous Vulnerability Management*), controle 11 (*Data Recovery Capabilities*), e controle 18 (*Penetration Testing*)
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI	Gestão da Segurança da Informação
Guia de Framework de Privacidade e Segurança da Informação (PPSI)	Controle 7 em sua íntegra
Instrução Normativa 01/GSI/PR	Art. 12, Inciso IV, alíneas g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – art. 46, Seção II - art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos	A.12.3 Cópias de segurança

Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação	12.3 Cópias de segurança 18 Conformidade
National Institute of Standards and Technology (NIST)	CSF: SP 800-40 Rev.2, *Creating a Patch and Vulnerability Management Program* CSF: SP 800-40 Rev 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Guia de Gerenciamento de Vulnerabilidades SGD	Em sua íntegra
NGINX.org	Correções de bugs
Office of the Chief Technology Officer – OCTO	Política de gerenciamento de vulnerabilidades
Vulnerability Management Policy Template for CIS Control 7	Em sua íntegra

CAPÍTULO VII
DECLARAÇÕES DA POLÍTICA

Art. 11 Os sistemas e os dispositivos conectados à rede do DNOCS, sejam eles próprios ou aqueles em processo de desenvolvimento e suporte por terceiros, devem passar periodicamente por varreduras em busca de vulnerabilidades que possam representar um risco para a infraestrutura e os dados sensíveis do DNOCS

Art. 12. Novos aplicativos/sistemas construídos pela equipe de desenvolvimento do DNOCS ou de terceiros devem ser verificados no que concerne a vulnerabilidades antes de serem implantados no ambiente de produção.

CAPÍTULO VIII
PROCESSO DE GERENCIAMENTO DE VULNERABILIDADES

Art. 13. Um processo de Gerenciamento de Vulnerabilidades (PGV) deve ser criado, implementado, mantido e aplicado no DNOCS.

Art. 14. O processo deve conter a implementação de mecanismos para obter informações oportunas sobre vulnerabilidades técnicas dos sistemas e ativos de informação, a avaliação da exposição da organização a tais vulnerabilidades e a implementação de salvaguardas apropriadas para lidar com o risco associado.

Art. 15. O processo deve contemplar o gerenciamento de vulnerabilidades dos diversos ativos que sustentam os serviços da organização, como a ativos que compõe a rede da organização, aplicações web, aplicativos móveis, sistemas operacionais, dentre outros.

Art. 16. O processo deve incluir atividades de suporte, incluindo, mas não se limitando a métricas de relatório e treinamento para implementação eficaz do PGV.

Art. 17. O processo deve incluir funções e responsabilidades das equipes/funções para realizar todas as atividades de maneira oportuna e eficaz para o DNOCS.

Art. 18. O processo deve estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

Art. 19 A consistência e a eficácia do processo devem ser medidas por meio de métricas de gerenciamento de vulnerabilidades.

Art. 20.As métricas de gerenciamento de vulnerabilidades devem ser definidas pelo Comitê de Governança Digital e suas medições devem ser apresentadas a cada 1(um) ano.

CAPÍTULO IX
MAPEAMENTO DE ATIVOS DA INFORMAÇÃO

Art. 21.Um mapeamento de ativos de informação deve constar no escopo do processo de gerenciamento de vulnerabilidades e patches para determinar qual marca, modelo e versão de equipamento de hardware, sistemas operacionais, banco de dados, sistema, servidor web e aplicativos de software são usados no DNOCS .

Art. 22. O mapeamento de ativos de informação deve ser atualizado a cada 6(seis) meses ou sempre que ocorrerem alterações significativas para garantir que os recursos informacionais estejam cobertos pelo processo de gerenciamento de vulnerabilidades do DNOCS.

CAPÍTULO X
DETECÇÃO DE VULNERABIILIDADES

Art. 23.As principais ações relacionadas à detecção de vulnerabilidades têm como enfoque definir e refinar o escopo que será avaliado; preparar as ferramentas necessárias e verificar sua integridade; e realizar testes e verificar resultados:

I. As funções e as responsabilidades das equipes/funções para realizar atividades de detecção de vulnerabilidades devem ser estabelecidas.

II. As ferramentas devem ser configuradas e ajustadas adequadamente de acordo com o escopo avaliado.

III. Os tipos de varreduras e os tipos de teste devem ser avaliados e ajustados para que sejam congruentes com o escopo avaliado.

IV. A frequência de testes de segurança deve levar em consideração os requisitos legais, regulamentares e contratuais que o DNOCS deve cumprir e os riscos associados aos ativos avaliados.

V. As varreduras de vulnerabilidades na rede corporativa devem ser realizadas por períodos determinados ou após alteração significativa na rede, por equipe interna ou por terceiro ou uma combinação de ambos.

VI. Os testes de segurança devem utilizar o feed de vulnerabilidade mais recente, de forma a evitar que determinadas vulnerabilidades não sejam detectadas.

VII. Para cada teste, é necessário verificar a integridade da ferramenta utilizada e se ela varreu corretamente os ativos analisados e se existem exceções de vulnerabilidades.

VIII. As ferramentas utilizadas devem ser ajustadas continuamente, de forma a evitar que varreduras feitas por ferramentas distintas gerarem resultados distintos.

IX. O teste de invasão ou o teste de penetração (Pentest) deve ser realizado conforme critério de necessidade *do DNOCS* ou pelo menos *a cada 6(seis) meses*, utilizando especialistas qualificados externos como parte de um exercício planejado, que inclui o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar o funcionamento normal do DNOCS

X. A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.

XI. A detecção manual de vulnerabilidades deve ser considerada como complemento à detecção automática de vulnerabilidades.

CAPÍTULO XI
BANCO DE DADOS DE VULNERABILIDADES

Art. 24. Deve ser mantido um banco de dados de vulnerabilidades coletadas de várias fontes, como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de software, que precisam ser aplicadas aos sistemas e ativos informacionais do DNOCS.

Art. 25. O banco de dados poderá incluir informações de vulnerabilidade, análise de vulnerabilidade para priorização e plano de correção de vulnerabilidade

Art. 26. É recomendável que o banco de dados de vulnerabilidades seja integrado com outras ferramentas de segurança, como scanners de vulnerabilidades e sistemas de gerenciamento de patches. Isso ajuda a identificar e corrigir vulnerabilidades de forma mais rápida e eficiente.

Art. 27. As informações coletadas no banco de dados de vulnerabilidades devem ser analisadas regularmente para identificar tendências e padrões visando a tomada de medidas proativas para evitar futuras vulnerabilidades.

CAPÍTULO XII
PRIORIZAÇÃO E CORREÇÃO DE VULNERABILIDADES

Art. 28. O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou host impactado tem para o negócio do DNOCS.

Art. 29. As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados abaixo.

Nível de severidade	**Prazo de correção**	**Descrição do risco**
Muito Crítico (6)	*Até 2 dias*	*Condição totalmente inaceitável quando medidas imediatas devem ser tomadas para eliminar a materialização do risco e mitigar perigos e impactos.*
Crítico (5)	*Até 30 dias*	*Pessoas mal-intencionadas podem facilmente obter o controle do host, o que pode comprometer toda a sua rede. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e backdoors.*
Alto (4)	*Até 45 dias*	*Pessoas mal-intencionadas podem obter o controle do host ou coletar informações altamente confidenciais, incluindo acesso de "leitura" ao arquivo, backdoors em potencial ou uma lista de todas as contas de usuário no host.*
Médio (3)	*Até 90 dias*	*Pessoas mal-intencionadas podem obter acesso às configurações de segurança no host, o que pode levar ao acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços.*
Baixo (2)	*Até 120 dias*	*Pessoas mal-intencionadas podem coletar informações confidenciais do host, como versões de software instaladas, que podem revelar vulnerabilidades conhecidas.*
Muito baixo (1)	*Até 180 dias*	*Pessoas mal-intencionadas podem coletar informações sobre o host por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades.*

Art. 30 Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída na lista de exceções por pessoal autorizado, com base no processo de aceitação de risco.

Art. 31. Devem-se estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente, utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

Art. 32. Quando as vulnerabilidades não puderem ser corrigidas dentro do prazo estabelecido no art. 29, *unidade de TIC* deve enviar uma "solicitação de renúncia" ao Comitê de Governança Digital. A solicitação deve conter as seguintes informações:

I. Detalhes do sistema ou ativo.
II. Descrição detalhada da vulnerabilidade
III. Avaliação de risco que justifique a não correção imediata
IV. A justificativa clara pela qual a correção não pode ser realizada no prazo estabelecido.
V. Detalhes dos controles existentes (se houver).
VI. Novo prazo de correção.
VII. Plano de ação da remediação (obedecendo o novo prazo de correção).

Parágrafo único: A decisão de aceitar ou rejeitar a solicitação de renúncia deve ser tomada pelo Comitê de Governança Digital, com base na avaliação de risco apresentada. Se a solicitação de renúncia for aceita, a vulnerabilidade deve ser monitorada continuamente, pautado pelo plano de ação apresentado devendo ser corrigida assim que possível.

Art. 33. Os alertas de vulnerabilidades, as correções de patches e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de informação devem ser monitorados.

CAPÍTULO XIII
GERENCIAMENTO DE EXCEÇÕES

Art. 34. Para os ativos de informação do DNOCS não contemplados por esta política em função de dificuldades técnicas ou obrigações contratuais e normativas ou outras razões legítimas, as exceções deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções do DNOCS

Art. 35. A lista de exceções de ativos de informação deve ter validade de 1(um) ano, devendo ser revisada após esse período.

CAPÍTULO XIV
DOS REGISTROS DE LOGS

Art. 36. Identificar quais eventos dos ativos de informação devem ser registrados, com base nos requisitos regulatórios, nas melhores práticas e nos objetivos do DNOCS..

Art. 37. Ativos, físicos ou virtuais, como servidores e recursos de rede, devem recuperar informações baseadas em tempo de uma única fonte de tempo de referência (servidor NTP) regularmente para que os relógios de registro sejam consistentes.

Art. 38. As configurações referentes a ativos de informação devem incluir configurações de log para registrar ações que possam afetar ou que sejam relevantes para a segurança da informação.

Art. 39. Definir procedimento para análise de logs, como ferramentas de análise e correlação, para identificar possíveis ameaças e vulnerabilidades.

Art. 40. Uma revisão dos arquivos de registro (logs) deve ser conduzida pelo menos *1(um) ano.*

Art. 41. Os arquivos de registro (logs) devem ser protegidos contra adulteração e acesso não autorizado ou exfiltração.

Art. 42. Registros de logs dos sistemas e ativos informacionais classificados como críticos devem ser mantidos por pelo menos5(cinco) anos tempo suficiente para cumprir os requisitos regulatórios e permitir a detecção de ameaças passadas.

Art. 43. Monitorar regularmente os registros de logs para identificar quaisquer tentativas de exploração de vulnerabilidades.

Art. 44. Registros de log devem ser excluídos de forma segura, garantindo que os registros sejam completamente apagados sem deixar vestígios ou dados remanescentes.

CAPÍTULO XV
COMUNICAÇÃO DA OCORRÊNCIA DE VULNERABILIDADES E CORREÇÕES

Art. 45. As vulnerabilidades e respectivas informações de correção devem ser informadas aos usuários afetados, incluindo, mas não se limitando a: administradores de sistema, proprietários de sistema e usuários finais.

Art. 46. As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de verificação de vulnerabilidades de rede e host, verificação de logs de patches, testes de invasão/penetração (Pentest) e verificação das definições de configuração.

CAPÍTULO XVI
IMPLEMENTAÇÃO E VERIFICAÇÃO DAS CORREÇÕES DE VULNERABILIDADES

Art. 47. As correções de vulnerabilidades devem ser verificadas a saber se não há novas vulnerabilidades introduzidas. Isso pode ser feito por meio de testes de penetração, testes de vulnerabilidade e análise de logs.

Art. 48. Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas devem ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, bem como a ajustes de configuração e/ou remoção de software.

Art. 49. Quando instalações de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser enviadas por meio do *processo de gestão de mudanças* para que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

CAPÍTULO XVII
IMPLEMENTAÇÃO E VERIFICAÇÃO DAS CORREÇÕES DE VULNERABILIDADES

Art. 50 Para serviços em nuvem, as responsabilidades do provedor de serviços em nuvem pública com o cliente do serviço em nuvem devem ser definidas e acordadas

Art. 51 Terceiros devem cumprir os requisitos desta Política de Gerenciamento de Vulnerabilidades (PGV). Sempre que possível, essa obrigação e outras responsabilidades que envolvam o gerenciamento de vulnerabilidades devem ser incluídas em contratos com terceiros.

CAPÍTULO XVII
DISPOSIÇÕES FINAIS

Art. 52 Os casos omissos serão resolvidos pelo Comitê de Governança Digital(CGD).

Anexo II

Termo de Concordância

Eu li e entendi a Política Gerenciamento de Vulnerabilidades do DNOCS. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas do DNOCS.

_____

Nome do Servidor/Empregado

Assinatura do Colaborador/Data