MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS
PORTARIA Nº 136 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 de Gestão de Ativos 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 de Gestão de Ativos 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 14:53, 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 **1598948** e o código CRC **C79DFF83**.

ANEXO I

POLÍTICA DE GESTÃO DE ATIVOS

CAPÍTULO I
PROPÓSITO

Art. 1º O objetivo desta política é garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Art. 2º Para manter a segurança e continuidade do negócio do DNOCS, em sua missão é fundamental mapear e monitorar os ativos tecnológicos, para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de risco da organização. Auxiliando também na recuperação de incidentes.

Art. 3º Os ativos de informação do DNOCS devem ser classificados a fim de permitir a definição de níveis de segurança para eles. Cada ativo de informação deverá ter um "dono", no qual realizará a classificação do ativo de informação e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

CAPÍTULO II
ESCOPO

Art. 4º Esta política se aplica a todos os ativos de informação no DNOCS, incluindo ativos fora do DNOCS armazenados em um serviço de nuvem. Ativos de informação neste contexto, incluem: Documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistemas, planos, guias, programas de computador, servidores, computadores, e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo da web específicos.

Art. 5º A classificação dos ativos de informação e o escopo desta política serão revisados anualmente.

CAPÍTULO III
TERMOS E DEFINIÇÕES

Art. 6º 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. 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;

II. INCIDENTE - interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

CAPÍTULO IV
REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Art. 7º 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	Secção
Decreto Nº 10.332/2020 - Estratégia de Governo Digital 2020-2023	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, 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.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Guia do Framework de Privacidade e Segurança da Informação	Controles 1 e 2
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
Guias Operacionais SGD	Todos
Instrução Normativa Nº 01/GSI/PR, de 27 de maio de 2020	Art.12, Inciso IV, alínea d
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo II
Instrução Normativa Nº 05/GSI/PR, de 30 de agosto de 2021	Anexo
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
NIST SP 800-53 v4	AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-2, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos;	A.8 (A.8.1., A.8.2., A.8.3.)
Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) - Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Enterprise Asset Management Policy Template CIS v8	Em sua íntegra
Software Asset Management Policy Template CIS v8 - November 2022	Em sua íntegra

CAPÍTULO V
DECLARAÇÕES DA POLÍTICA

Art. 8º São regras que compõem a política:

Dos princípios gerais:

I. A Política de Gestão de Ativos de informação deve estar alinhada com à Política de Segurança da Informação do DNOCS.

II. A Política de Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

III. O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

IV. As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.

V. O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.

VI. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

Os seguintes ativos de informação devem ser considerados no processo no mapeamento de ativos de informação

I. Ativos Físicos.

II. Bancos de dados;

III. Dispositivos móveis;

IV. Hardwares;

V. Mídias removíveis;

VI. Níveis de permissões;

VII. Serviços;

VIII. Softwares.

Art. 9º São Diretrizes da Política de Gestão de Ativos:

I. Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.

II. A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização

III. A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software.

IV. A organização deve assegurar que os ativos de informação inventariados possuam contrato de suporte em vigor.

V. A organização empregará o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.

VI. A organização utilizará ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado.

VII. A organização assegurará que exista um processo semanal para lidar com ativos não autorizados.

VIII. A organização utilizará controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado, sendo estes reavaliados semestralmente ou com mais frequência.

IX. A organização utilizará controles técnicos para garantir que apenas bibliotecas e scripts autorizados, e assinados digitalmente tenham permissão para serem executados.

X. A organização utilizará ferramenta de gerenciamento de endereços IP - ex.: Dynamic Host Configuration Protocol (DHCP) - para atualizar o inventário de ativos da instituição.

XI. O inventário também deverá incluir atualizações ou remoções dos softwares, bem como dos sistemas de informação.

XII. As atualizações e novas versões de softwares devem ser avaliadas e aprovadas antes da instalação.

XIII. Cada ativo de informação (por exemplo, desktops, laptops, servidores, tablets), quando aplicável, deve ter uma etiqueta afixada ao dispositivo com esse identificador.

XIV. Registre o identificador de ativos da informação juntamente com outras informações relevantes no inventário de TI. Isso inclui:

i. Identificador de ativos

ii. Data da compra

iii. Preço de compra

iv. Descrição do item

v. Fabricante

vi. Número do modelo

vii. Número de série

viii. Nome do proprietário do ativo corporativo (por exemplo, administrador, usuário), função ou unidade de negócios, quando aplicável.

ix. Localização física do ativo da empresa, quando aplicável

x. Endereço físico (controle de acesso à mídia (MAC))

xi. Endereço de Protocolo de Internet (IP)

xii. Data de validade da garantia/vida útil

xiii. Qualquer informação de licenciamento relevante

xiv. No caso de softwares instalados na organização deve ser registrado no inventário informações como:

1. Título do software;
2. Desenvolvedor ou editor de software;
3. Data de aquisição;
4. Data de instalação;
5. Duração do uso;
6. Finalidade comercial;

7. Lojas de aplicativos;
8. Versões;
9. Mecanismo de implantação;
10. Data de fim do suporte, se conhecida;
11. Qualquer informação de licenciamento relevante;
12. Data de descomissionamento.

Art. 10 Das responsabilidades do proprietário do processo (Art. 9º da IN GSI/PR nº 3/2021)

I. Identificar potenciais ameaças aos ativos de informação;
II. Identificar vulnerabilidades dos ativos de informação;
III. Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;
IV. Avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.
V. Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na política de controle de acesso e catalogadas no sistema de gestão de ativos.
VI. Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.
VII. Todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

Art. 11 Criticidade do ativo de informação:

I. A criticidade dos ativos de informação críticos da organização é determinada pelo:
    i. Requisitos legais;
    ii. Pelo valor financeiro;
    iii. Pelo seu potencial de agregar valor ao negócio;
    iv. Por sua vida útil.

Art. 12 Classificação de Nível de Acesso das Informações:

I. Todos os ativos de informação devem ser classificados de acordo com seu nível de acesso, a fim de assegurar o direito fundamental de acesso à informação, bem como dispor sobre a devida restrição de acesso sobre informações sigilosas, conforme previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e demais normas aplicáveis.
II. As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação do DNOCS, independentemente de seu formato e suporte, devem ser classificadas segundo seu nível de acesso, de acordo com a legislação pertinente, sobretudo com as disposições da LAI, do Decreto nº 7.724, de 16 de maio de 2012, e orientações ou normas complementares editadas por órgãos competentes.
III. A classificação de nível de acesso das informações deve observar às diretrizes constantes na LAI, Decreto nº 7.724, de 16 de maio de 2012 e outros normativos complementares que abordam o assunto.
IV. As informações devem ser classificadas conforme os seguintes níveis de acesso:
    i. **Pública**, com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;

ii. **Restrita**, quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso; e

iii. **Sigilosa classificada em grau de sigilo**, nos termos do art. 23 da Lei nº 12.527/2011, subdividida nos graus ultrassecreto, secreto ou reservado.

V. Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de nível de acesso de informações usados pela organização.

Art. 13 Manipulação de mídia:

I. A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.

II. A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados.

III. A mídia contendo informações confidenciais e internas do DNOCS devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

Art. 14 Uso aceitável:

I. Padrões ou diretrizes para o uso aceitável de ativos devem ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.

II. Os seguintes itens devem ser cobertos nas diretrizes de uso aceitáveis:
   i. Uso do computador e dos sistemas de informação;
   ii. Uso de softwares e dados;
   iii. Uso da Internet e e-mail;
   iv. Uso do telefone;
   v. Uso de equipamentos e materiais de escritório.

III. Como requisito de acesso ao ativo de informação e como componente do treinamento de conscientização de segurança, todos os usuários dos ativos de informação, sejam funcionários ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis

CAPÍTULO VI
PROCEDIMENTOS RELEVANTES

Art. 15 Podem ser criados documentos de procedimentos formais que reforcem e apoiem as determinações, a critério do Comitê de Governança Digital e da Alta Administração do DNOCS.

CAPÍTULO VII
NÃO CONFORMIDADE

Art. 16 As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

I. Processo Administrativo disciplinar de acordo com a legislação aplicável

II. Exoneração.

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

CAPÍTULO VIII
CONCORDÂNCIA

Art. 17 O termo de concordância em anexo firma o entendimento e o acordo para cumprir a política pelos colaboradores do DNOCS.

CAPÍTULO XVII
DISPOSIÇÕES FINAIS

Art. 18 Os casos omissos serão resolvidos pelo Comitê de Governança Digital(CGD)

ANEXO II

TERMO DE CONCORDÂNCIA

Eu li e entendi a Política de Gestão de Ativos 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