MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS
PORTARIA Nº 138 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 Registros (Logs) de Auditoria(PGRA) – DNOCS.

O DIRETOR-GERAL O 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 Registros (Logs) de Auditoria (PGRA) 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 14:17, 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 **1598966** e o código CRC **117EF4B8**.

ANEXO I

POLÍTICA DE GESTÃO DE REGISTROS (LOGS) DE AUDITORIA (PGRA)

CAPÍTULO I
PROPÓSITO

Art. 1º O objetivo desta política é estabelecer e manter um processo de gestão de log de auditoria que defina os requisitos de log do órgão ou entidade.

Art. 2º O referido processo deve tratar da coleta, armazenamento, uso e exclusão de logs de auditoria e sistemas para os ativos de informação do DNOCS.

Art. 3º Definir os princípios de atuação da auditoria interna nos processos de TI [do órgão ou entidade] e as diretrizes para a administração e gerenciamento de registros de logs gerados pelos ativos de informação.

CAPÍTULO II
ESCOPO

Art. 4º Esta **Política de Gestão de Registros (Logs) de Auditoria – PGRA** se aplica aos ativos informacionais do DNOCS, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e ou os utilize.;

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

Art. 6º A unidade de TIC é responsável por elaborar, manter e fazer cumprir a Política de Gestão de Registros (Logs) de Auditoria – PGRA do DNOCS*.*

CAPÍTULO III
EXCEÇÕES

Art. 7º Podem ocorrer de 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.*

Art. 8º É importante salientar que tais exceções precisam ser tratadas no mapeamento de riscos de segurança da informação que o órgão ou a entidade deve efetuar em cumprimento ao Capítulo III da Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021.

CAPÍTULO IV
PÚBLICO

Art. 9º Esta Política de Gestão de Registros (Logs) de Auditoria – PGRA se aplica aos ativos informacionais do DNOCS, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e ou os utilize, com responsabilidades específicas a indivíduos atuantes na gestão, processo e desenvolvimento em nome do DNOCS Além disso, essa política se aplica, nos limites estabelecidos contratualmente, a quaisquer provedores e entidades terceirizadas com acesso aos ativos de informação do DNOCS.

CAPÍTULO V
TERMOS E DEFINIÇÕES

Art. 10 Abaixo definições de termos chaves, siglas ou conceitos que serão utilizados na política

I. ATIVO **-** Qualquer coisa que tenha valor para a organização.

II. ATIVO DE REDE - Equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores.

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. DESCARTE - eliminação correta de informações, documentos, mídias e acervos digitais.

V. ETIR - Sigla de Equipe de Prevenção, Tratamento, e Resposta a Incidentes Cibernéticos.

VI. EVENTO - Qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Ou seja, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao usuário.

VII. EVENTO DE SEGURANÇA - Qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança.

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

IX. 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.

X. INCIDENTE CIBERNÉTICO – Ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não autorizadas de firmware, hardware ou software em um ambiente computacional; d) ataques de negação de serviço (DoS); e demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada.

XI. INCIDENTE DE SEGURANÇA – Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

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

XIII. LOG DE AUDITORIA – Fornecem eventos no nível do sistema que mostram vários horários de início/término de processo do sistema, travamentos etc. São nativos dos sistemas e exigem menos configurações para ativarem.

XIV. LOG DE SISTEMA – Incluem eventos no nível do usuário - quando um usuário faz login, acessa um arquivo etc.

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

XVI. 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.

XVII. SANITIZAÇÃO DE DADOS - Eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados.

XVIII. TRILHA DE AUDITORIA - registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.

CAPÍTULO VI
REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Art. 11 Abaixo lista de leis, regulamentos e guias de boas práticas que regem a política em sua conformidade e cumprimento.

Orientação	Seção
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	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
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
Guia do Framework de Privacidade e Segurança da Informação	Controles 3 e 8
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 01/GSI/PR	Art.12, Inciso IV, alínea 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
Norma Complementar nº 21/IN01/DSIC/GSIPR	Em sua íntegra
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Publicação do TCU sobre descarte de mídias, disponível em: link	Em sua íntegra
Audit Log Management Policy Template for CIS Control 8	Em sua íntegra

CAPÍTULO VII
GESTÃO DE REGISTRO DE AUDITORIA

Art. 12 A PGRA é organizada em quatro fases: Coleta, Armazenamento, Uso e Exclusão. Dentro dessas fases foram inseridas medidas de segurança, todas oriundas do *Center for Internet Security* CIS, framework *Critical Security Control v8.0 Assessment Tool* - contidas no Controle 8 (*Audit Log Management*).

Art. 13 Cada fase compreende uma etapa do ciclo de vida de um log, seja esse log de auditoria ou um log de sistema. Importante ressaltar que se deve fazer cumprir a ordem das fases, pois se trata de uma ordem lógica, o mesmo não equivale para ordem das medidas encontradas no framework.

Art. 14 Todas as 12 medidas, encontradas no controle 8 do CIS foram divididas de acordo com as quatro fases (coleta, armazenamento, uso e exclusão). A inserção das medidas nas fases se deu conforme a orientação descrita pelo framework, ou seja, as medidas foram classificadas de acordo com a fase do ciclo de vida de um log.

CAPÍTULO VIII
DECLARAÇÕES DA POLÍTICA

Art. 15 As premissas e responsabilidades da PGRA são:

I. A atividade de auditoria é de competência da unidade de TIC do DNOCS

II. A equipe responsável pela auditoria interna deve se reportar ao Comitê de Governança Digital do DNOCS .

III. A unidade de TIC deve possuir capacidade técnica e experiência nas áreas de gerenciamento de logs, dispor de competências técnico-administrativas necessárias ao bom desempenho de suas funções, quais sejam: independência, autonomia, imparcialidade, zelo, integridade e ética profissional, além de autoridade para avaliar as funções próprias e as funções terceirizadas do DNOCS.

IV. A unidade de TIC pode obter assessoria de especialistas/consultores externos ou mesmo equipe terceirizada para subsidiar a área quando essa não for suficientemente proficiente.

V. A unidade de TIC, quando executa a atividade de auditoria, deve possuir acesso irrestrito às informações necessárias ao bom desempenho de suas funções, quais sejam: acesso irrestrito a quaisquer informações, ambientes e ativos de informação.

VI. É dever dos responsáveis pelas unidades de negócio do DNOCS cooperar com a unidade de TIC quanto ao acesso a ativos de informação, instalações e trânsito de dados.

VII. Os membros da unidade de TICdevem ter canal de comunicação permanente com osresponsáveis pelas unidades de negócio do DNOCS para apoiar na atuação corretiva, de forma apropriada e tempestiva, em resposta às recomendações decorrentes dos trabalhos de auditoria.

VIII. Os eventos de log devem ser gerados, selecionados e armazenados para todos os ativos.

IX. A unidade de TIC deve selecionar os eventos e os respectivos tempos de guarda, bem como as demais características de uso dos eventos.

X. As exceções deverão ser documentadas.

Art. 16 São requisitos do plano de registros de auditoria:

I. Ativos de informação devem estar com as informações de data e hora sincronizadas. Pelo menos duas fontes de tempo devem ser configuradas para sincronizar o tempo dos ativos de informação, onde houver suporte.

II. Ativos de informação do DNOCS devem ser configurados de forma a sincronizar data e hora via protocolo NTP (Network Time Protocol), onde houver suporte.

III. Deve ser Utilizado o horário de Greenwich em sistemas hospedados em provedores de nuvem onde o fuso local pode ser diferente do fuso do provedor.

IV. Processos, procedimentos e medidas técnicas devem ser definidos e implementados visando a proteção dos dados sensíveis ao longo de seu ciclo de vida.

V. Devem ser mapeados os ativos de informação que podem ter suas configurações de log mais detalhadas com informações como: *ID de usuário de acesso, IP do host, data, hora e fuso horário, acessos de usuários privilegiados*.

VI. Devem ser mapeados os ativos de informação, que por qualquer motivo, não possa apresentar dados detalhados conforme item art. 16, inciso V.

VII. Além de eventos em ativos de informação, o DNOCS pode registrar eventos de segurança da informação como os a seguir: Utilização de usuários, perfis e grupos privilegiados; Acoplamento e desacoplamento de dispositivos de hardware, principalmente mídias removíveis; Inicialização, suspensão e reinicialização de serviços; Criação, modificação e exclusão de grupos ou listas de grupos com acessos privilegiados; Atualização das regras da política de senhas de usuários; Criação, acesso e modificação de arquivos de sistemas considerados críticos; Qualquer evento realizado nos ativos de informação de segurança existentes.

VIII. Em caso de incidentes de segurança da informação, ou quaisquer outros eventos de segurança, a unidade de TIC deve coletar e preservar todos os registros de eventos citados no item e as mídias de armazenamento dos ativos de informação afetados pelo evento.

IX. Caso não seja possível cumprir com as diretrizes apontadas no item art. 16, inciso V. , em razão do reestabelecimento dos sistemas e serviços afetadas de forma rápida, a unidade de TIC deve coletar e armazenar cópias dos registros e arquivos afetados pelo incidente de segurança como: Logs; Arquivos de sistema operacional; Configurações do sistema operacional; e Demais arquivos e logs que foram necessários para reestabelecimento do serviço ou sistema.

X. O *DNOCS* deve manter a estrutura original de diretórios além dos “metadados” destes arquivos tais como: *data, hora de criação e atualização e permissões*.

XI. Em caso de impossibilidade de preservar as evidências do evento de segurança, o CGD deve justificar em relatório, a falta destas evidências.

XII. As ações para o reestabelecimento do serviço e sistema afetados pelo evento de segurança não devem impossibilitar a coleta, a preservação e disponibilidade das evidências de forma integra.

XIII. Devem ser promovidas ações para a preservação dos arquivos coletados.

Art. 17 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. 18 Criticidade do ativo de informação:

I. A criticidade dos ativos de informação críticos da organização é determinada pelo:
   a. Requisitos legais;
   b. Pelo valor financeiro;
   c. Pelo seu potencial de agregar valor ao negócio;
   d. Por sua vida útil.

Art. 19 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:
   a. **Pública**, com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;
   b. **Restrita**, quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso; e
   c. **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. 20 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. 21 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:

1. Uso do computador e dos sistemas de informação;
2. Uso de softwares e dados;
3. Uso da Internet e e-mail;
4. Uso do telefone;
5. 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. 22 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. 23 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. 24 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. 25 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 Registros (Logs) de Auditoria(PGRA) 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