CONTROLADORIA-GERAL DA UNIÃO

PORTARIA NORMATIVA SE/CGU N° 187, DE 03 DE DEZEMBRO DE 2024

Institui a Política de Gestão de *Logs* de Segurança no ambiente de computação da Controladoria-Geral da União.

A SECRETÁRIA-EXECUTIVA DA CONTROLADORIA-GERAL DA UNIÃO , no exercício das atribuições previstas no art. 35 do Anexo I ao Decreto nº 11.330, de 1º de janeiro de 2023, e no art. 5º, *caput*, inciso II, da Portaria Normativa CGU nº 164, de 30 de agosto de 2024, e considerando o disposto no Decreto nº 12.069, de 21 de junho de 2024, na Portaria SE/CGU nº 587, de 10 de março de 2021, e na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e conforme com o que consta no Processo Administrativo nº 00190.107015/2024-93,

R E S O L V E:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria Normativa institui a Política de Gestão de *Logs* de Segurança e estabelece princípios, diretrizes e responsabilidades relacionadas à gestão e auditoria de *logs* de segurança no ambiente de computação da Controladoria-Geral da União.

Art. 2º Para os efeitos desta Portaria Normativa, considera-se:

I - ativos de informação - meios de armazenamento, transmissão e processamento de informação, equipamentos necessários, sistemas utilizados, locais onde se encontram, recursos humanos que a eles têm acesso e conhecimento, ou, ainda, dado que tem valor para um indivíduo ou uma organização;

II - ativos de informação críticos - ativos de informação que compõem os sistemas críticos definidos na Instrução Normativa CGU nº 31, de janeiro de 2024, e demais ativos considerados críticos pela Diretoria de Tecnologia da Informação da Secretaria-Executiva da Controladoria-Geral da União;

III - auditoria - processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;

IV - auditoria de *logs* - auditoria realizada por meio de análises em registros gerados pelos ativos de informação da Controladoria-Geral da União;

V - custodiante da informação - indivíduo responsável pela unidade gestora que tenha responsabilidade formal sobre as informações;

VI - gestão de *logs* - conjunto de ações que sistematizam o planejamento, a coleta, a análise e a revisão dos *logs* gerados pelos ativos de informação da Controladoria-Geral da União;

VII - *logs* - registros detalhados de eventos em ativos de informação como autenticações, acessos a dados, alterações em configurações de serviços, erros, com as respectivas datas e horários;

VIII - *logs* de segurança - tipo específico de *log* que registra eventos relacionados à segurança, sendo usados para detectar atividades maliciosas, investigar incidentes de segurança e atender a requisitos de conformidade;

IX - *network time protocol* – NTP - protocolo de tempo para redes; e

X - *security information and event management* – SIEM - solução de gerenciamento de eventos e informações de segurança com o objetivo de detectar anomalias de comportamento por meio de correlação automatizada de eventos.

Parágrafo único. Na aplicação desta Portaria Normativa, deverão ser observados, no que couber, os conceitos constantes do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

Objetivos

Art. 3º São objetivos da Política de Gestão de *Logs* de Segurança:

I - instituir princípios e responsabilidades da gestão de registros de *logs* de segurança gerados pelos ativos de informação; e

II - estabelecer e manter um processo de gestão de *logs* que defina os requisitos de registros de segurança do órgão, tratando do planejamento, da coleta, da análise e da revisão dos *logs* gerados pelos ativos de informação da Controladoria-Geral da União.

Abrangência

Art. 4º As disposições desta Portaria Normativa e da regulamentação correlata aplicam-se:

I - aos ativos informacionais da Controladoria-Geral da União; e

II - aos responsáveis pela gestão das soluções de tecnologia da informação e comunicação – TIC, membros da área de tecnologia e usuários, bem como provedores e entidades terceirizadas que tenham acesso a esses ativos.

Regime de excepcionalidades

Art. 5º Os ativos de informação críticos da Controladoria-Geral da União que, por possíveis dificuldades técnicas ou obrigações contratuais e normativas, não estejam contemplados em algum requisito desta política serão tratados de forma excepcional.

Parágrafo único. As excepcionalidades a esta política deverão ser aprovadas e registradas pela área de segurança cibernética da Diretoria de Tecnologia da Informação.

CAPÍTULO II

DAS RESPONSABILIDADES

Art. 6º A Diretoria de Tecnologia da Informação é responsável por elaborar, manter e fazer cumprir a política e o processo de gestão de *logs* de segurança da Controladoria-Geral da União.

Art. 7º A gestão de *logs* de segurança é de responsabilidade conjunta da Diretoria de Tecnologia da Informação da Secretaria-Executiva da Controladoria-Geral da União e dos responsáveis pela gestão das soluções de TIC da Controladoria-Geral da União.

§ 1º A Diretoria de Tecnologia da Informação é responsável por implementar a geração de *logs* de segurança nos ativos de informação.

§ 2º Os responsáveis pela gestão das soluções de TIC são responsáveis por:

I - definir prazo de retenção adicional ao mínimo descrito no art. 11 de acordo com a criticidade e a

relevância da informação; e

II - definir as informações que deverão ser registradas nos *logs* de segurança de acordo com requisitos administrativos, legais ou de auditoria.

§ 3º A área de segurança cibernética da Diretoria de Tecnologia da Informação é responsável pelas soluções de gerenciamento e validação das configurações de *logs* de segurança nos ativos de informação.

CAPÍTULO III

DOS PRINCÍPIOS GERAIS

Art. 8º Os ativos físicos ou virtuais, como servidores e recursos de rede, devem ser configurados de forma sincronizada com base em uma fonte única de tempo de referência, servidor NTP, para que os relógios de registro sejam consistentes.

Art. 9º Os processos, procedimentos e medidas técnicas devem ser definidos e implementados visando à proteção de *logs* de segurança sensíveis ao longo de seu ciclo de vida.

Art. 10. Os *logs* de segurança dos ativos informacionais que tratam de dados pessoais devem observar as orientações contidas na Lei nº 13.709, de 14 de agosto de 2018, e em demais regulamentações de proteção de dados e privacidade.

Art. 11. Os *logs* de segurança em ativos de informação devem observar o prazo de retenção mínimo de noventa dias.

§ 1º Os registros de acesso de aplicações da Controladoria-Geral da União disponíveis na *internet* deverão ser mantidos pelo prazo de seis meses.

§ 2º Em casos de indisponibilidade orçamentária ou de recursos, físicos e lógicos, de infraestrutura, o prazo de retenção mínimo será atendido, prioritariamente, para sistemas críticos.

Art. 12. O *backup* dos *logs* de segurança deverá estar incluído nos *backups* dos respectivos ativos de informação.

Art. 13. A Diretoria de Tecnologia da Informação deverá prover soluções de gestão de *logs* de segurança para seus ativos de informação críticos com o objetivo de aperfeiçoar o gerenciamento destes *logs*.

Parágrafo único. A área de segurança cibernética da Diretoria de Tecnologia da Informação deve garantir a disponibilidade dos *logs* de segurança de ativos institucionais críticos e deve manter o controle de acesso lógico às soluções de gestão de *logs* de segurança.

CAPÍTULO IV

DAS FASES DO PROCESSO DE GESTÃO DE *LOGS* DE SEGURANÇA

Do planejamento

Art. 14. Os *logs* de segurança devem registrar, quando aplicável, os seguintes eventos de segurança:

I - criação, modificação e exclusão de usuários;

II - *logon/logoff* do usuário;

III - concessão ou revogação de privilégios de usuários;

IV - modificação de perfis de acesso de usuários;

V - alteração de senhas de usuário;

VI - ativação ou desativação de funcionalidades;

VII - acesso, inclusão, modificação, exclusão, impressão e *download* de informações;

VIII - inicialização, suspensão e reinicialização de serviços; e

IX - acoplamento e desacoplamento de dispositivos de *hardware*, principalmente mídias removíveis.

§ 1º É recomendado que os *logs* de segurança registrem informações, dentre as quais:

I - identificação do ativo de informação;

II - identificação da origem do evento;

III - identificação única do usuário;

IV - data e hora do evento;

V - endereço de IP de origem do cliente, para tráfego de entrada;

VI - endereço de IP de destino, para tráfego de saída;

VII - ação de tratamento do dado, como consulta, inclusão, modificação ou exclusão; e

VIII - *status* do resultado.

§ 2º Devem ser avaliados outros elementos úteis que podem ajudar em uma investigação forense, a depender da sensibilidade da informação.

Art. 15. Para sistemas e serviços que tratam dados pessoais, deve-se registrar apenas as informações estritamente necessárias, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), garantindo a proteção e a privacidade dos titulares dos dados.

Art. 16. O prazo de retenção adicional ao mínimo descrito no art. 11 deve ser formalizado por meio de Acordo de Nível de Serviço pelos responsáveis pela gestão das soluções de TIC.

Da coleta

Art. 17. A retenção dos *logs* de segurança deve ser configurada de acordo com os padrões mínimos definidos nesta política ou conforme definido no Acordo de Nível de Serviço.

Art. 18. A geração de *logs* de segurança deve ser implementada para todos os ativos de informação, priorizando aqueles classificados como críticos.

Art. 19. Os administradores dos sistemas ou serviços devem configurar os ativos de informação para gerar e armazenar localmente os *logs* de segurança.

Art. 20. A área de segurança cibernética da Diretoria de Tecnologia da Informação deve implementar a coleta centralizada de *logs* de segurança de ativos de informação críticos.

Da análise

Art. 21. Os *logs* de segurança dos ativos de informação devem ser monitorados continuamente em busca de comportamento anômalo ou suspeito, preferencialmente utilizando solução de SIEM.

Art. 22. Em caso de incidentes de segurança da informação, ou quaisquer outros eventos de segurança, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Controladoria-Geral da União – ETIR/CGU deve preservar as evidências dos incidentes detectados.

Parágrafo único. Na impossibilidade de preservar as evidências originais, como em situações de necessidade do reestabelecimento, de forma rápida, dos sistemas e serviços afetados, a ETIR/CGU deve coletar e armazenar cópias dos registros e arquivos afetados pelo incidente de segurança.

Art. 23. Os *logs* de segurança para processos de auditoria serão disponibilizados pela Diretoria de Tecnologia da Informação, respeitando a privacidade e o sigilo das informações, nos seguintes casos:

I - instrução de procedimentos e processos administrativos investigativos e acusatórios conduzidos pela Corregedoria-Geral da União ou pela Secretaria de Integridade Privada da Controladoria-Geral da União;

II - cumprimento de determinação judicial; e

III - compartilhamento de informações solicitadas por órgãos de persecução criminal, civil ou administrativa, para instrução de processos instaurados no órgão ou entidade solicitante.

Parágrafo único. Os *logs* de segurança de que trata o *caput* devem ser disponibilizados apenas ao solicitante.

Da revisão

Art. 24. Os *logs* de segurança devem ser revisados periodicamente pela área de segurança cibernética da Diretoria de Tecnologia da Informação, com prioridade para os ativos de informação críticos.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 25. Os casos omissos serão resolvidos pela Diretoria de Tecnologia da Informação.

Art. 26. A revisão desta Portaria Normativa deve ser realizada a cada dois anos ou sempre que se fizer necessário.

Art. 27. Esta Portaria Normativa entra em vigor na data de sua publicação.

EVELINE MARTINS BRITO

Secretária-Executiva da Controladoria-Geral da União

Documento assinado eletronicamente por **EVELINE MARTINS BRITO**, **Secretária-Executiva**, em 03/12/2024, às 18:30, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://super.cgu.gov.br/conferir informando o código verificador 3445803 e o código CRC 335BA17A

Referência: Processo nº 00190.107015/2024-93 SEI nº 3445803