Ministério da Educação
Universidade Federal de Alfenas
Rua Gabriel Monteiro da Silva, 700 - Bairro centro, Alfenas/MG - CEP 37130-001
Telefone: (35) 3701-9000 - http://www.unifal-mg.edu.br

Resolução Nº 04/2024, DE 05 DE novembro DE 2024

Aprova a norma que estabelece a Política de Gestão de Registros (LOGS) de Auditoria no âmbito da UNIFAL-MG.

O Comitê de Governança Digital (CGD) da Universidade Federal de Alfenas – UNIFAL-MG, no uso de suas atribuições regimentais,

CONSIDERANDO o constante dos autos do processo nº 23087.017974/2024-09,

R E S O L V E :

Art. 1º Aprovar, na forma do anexo SEI Nº 1386366, a norma que estabelece a Política de Gestão de Registros (LOGS) de Auditoria no âmbito da UNIFAL-MG;

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

Assinado Eletronicamente

SANDRO AMADEU CERVEIRA

Presidente do Comitê de Governança Digital

Documento assinado eletronicamente por **Sandro Amadeu Cerveira**, **Reitor**, em 11/12/2024, às 14:43, 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.unifal-mg.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1386359** e o código CRC **8E040E05**.

Referência: Processo nº 23087.017974/2024-09 SEI nº 1386359

POLÍTICA DE GESTÃO DE REGISTROS (LOGS) DE AUDITORIA

CAPÍTULO I
DO ESCOPO

Art. 1° A Política de Gestão de Registros (logs) de Auditoria tem o objetivo de estabelecer diretrizes, competências e responsabilidades para governar o ciclo de vida da gestão dos registros (logs) de auditoria no âmbito da UNIFAL-MG, garantindo assim que os logs sejam criados e analisados adequadamente.

Art. 2° Esta política se aplica aos ativos de Tecnologia da Informação e Comunicação (TIC) da UNIFAL-MG, incluindo servidores, estações de trabalho, switches, roteadores, access points, sistemas operacionais, banco de dados, servidores de arquivos, sistemas de informação e demais recursos e serviços de TIC.
Parágrafo Único. Alguns ativos de TIC podem eventualmente não ser contemplados devido a dificuldades técnicas ou a obrigações contratuais e normativas. Qualquer exceção a esta política deverá ser devidamente documentada.

Art. 3° Este documento passa a compor a Política de Segurança da Informação e Comunicação - PSIC da UNIFAL-MG.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 4° Para fins de compreensão dos termos utilizados neste documento serão utilizadas as terminologias conforme o Glossário de Segurança da Informação publicado pela Portaria do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) Nº 93, de 18 de outubro de 2021.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 5° Esta política considera os seguintes princípios:

I. respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;
II. garantia de integridade, autenticidade e disponibilidade da informação sob a custódia da UNIFAL-MG, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;
III. alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;
IV. responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e
V. conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 6° As diretrizes gerais constituem os pilares da gestão de registro de *logs* de auditoria na UNIFAL-MG, norteando a elaboração de normas, planos, procedimentos, metodologias, ações e controles que garantem que os princípios de segurança da informação definidos na política de segurança da informação sejam atingidos.

§ 1º Registros (logs) de auditoria de eventos contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos de acordo com o arcabouço legal aplicável, sendo que as exceções deverão ser devidamente registradas.

§ 2º A atividade de auditoria de recursos, sistemas de informação e serviços de TIC é de competência da Gerência de Segurança da Informação (GSI), vinculada ao Núcleo de Tecnologia de Informação (NTI) da UNIFAL-MG. Nos casos referentes à Incidentes de Segurança de TIC, a atividade de auditoria também será de competência da ETIR/UNIFAL-MG, que poderá solicitar cópia total ou parcial dos registros, passando a ser responsável pela guarda da cópia até o término da auditoria.

§ 3º Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de segurança da informação, tais como: autenticação, tanto as bem sucedidas quanto as mal sucedidas, acesso a recursos e dados privilegiados, acesso a dados pessoais e acesso e alteração nos registros de auditoria.

§ 4º Deve-se implementar medidas de salvaguarda para os logs, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao serviço de gerenciamento de logs, de forma que esses não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades.

§ 5º Os serviços críticos contemplados nesta política devem ser formalmente elencados pela ETIR/UNIFAL-MG.

§ 6º Procedimentos para o monitoramento do uso dos recursos de processamento da informação devem ser estabelecidos e os resultados das atividades de monitoramento devem ser analisados criticamente de forma regular.

§ 7º A ETIR/UNIFAL-MG, responsável pela auditoria interna de recursos, sistemas e serviços, deve se reportar, quando necessário, ao Comitê de Governança Digital (CGD).

§ 8º A equipe responsável pelo serviço de gerenciamento de logs 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.

§ 9º É dever dos responsáveis cooperarem com a ETIR/UNIFAL-MG quanto ao acesso a ativos de informação, instalações e trânsito de dados.

CAPÍTULO V
GESTÃO DE REGISTRO DE (LOGS) DE AUDITORIA

Art. 7° O processo de gestão de registro de *logs* de auditoria deve gerenciar o ciclo de vida dos eventos realizados em recursos, sistemas, *softwares*, aplicativos, banco de dados, sistemas de informação e serviços de TI conforme determina a legislação

pertinente.
Parágrafo Único. Este processo é composto por um conjunto de fases e atividades responsáveis pela coleta, armazenamento, uso e eliminação de eventos de segurança da informação que podem ajudar a detectar, compreender e recuperar-se de um ataque cibernético.

Seção I
Da coleta

Art. 8° A coleta de *logs* de auditoria registra os eventos de acesso à rede e atividades realizadas pelos usuários nos ativos de TI. Os logs são gerados por diversas fontes, incluindo software de segurança, antivírus, firewalls e sistemas de prevenção e detecção de intrusão, sistemas operacionais em servidores, estações de trabalho e equipamentos de rede e aplicações.
§ 1º A geração de *logs* de auditoria de eventos realizados pelos usuários deve estar habilitada nos ativos de informação, seguindo as diretrizes do processo de gestão de registros de *logs* de auditoria.
§ 2º *Logs* de auditoria de ativos de informação devem ser coletados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.
§ 3º Sempre que possível *logs* devem ser coletados em um ou mais repositórios centrais, devendo ser registrado oficialmente a justificativa quando houver a impossibilidade.
§ 4º Ativos de informação classificados como críticos devem ter *logs* de auditoria registrados conforme legislação pertinente.
§ 5º Sempre que possível os ativos de informação da UNIFAL-MG devem gerar registros de *logs* auditoria para eventos definidos. Esses eventos definidos incluem a identificação de eventos significativos relevantes para a segurança da informação que precisam ser auditados.
§ 6º Devem ser registrados os eventos de: tentativas de logon, gerenciamento de contas de usuários, acesso ao serviço de diretório, uso privilegiado, acompanhamento de processos, acessos, inclusões, exclusões e alterações de dados em sistemas e destruição de arquivos de *logs* de auditoria.
§ 7º Ativos de informação que contêm dados sensíveis devem possuir os *logs* de auditoria que contenham registros de eventos que ajudem em uma eventual investigação forense, como por exemplo: identificação inequívoca do usuário que acessou o recurso; natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc; data e hora do evento; e endereço IP, identificador do ativo de informação e outras informações que possam identificar a possível origem do evento.
§ 8º Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (Logs) em formato que permita a completa identificação dos fluxos de dados.
§ 9º Ativos de informação que tratem dados pessoais devem possuir registro de auditoria de inclusão, alteração, exclusão e consulta desses dados nos termos da Lei Geral de Proteção de Dados (LGPD).

Seção II
Do armazenamento

Art. 9º O armazenamento e retenção de logs de auditoria deve ser centralizado, com período de retenção definido com base no arcabouço legal aplicável.

Art. 10º No caso de os logs armazenados contiverem dados pessoais, deve-se observar o previsto pela LGPD a fim de avaliar se os logs devem ser eliminados ou conservados após o término do tratamento dos dados pessoais.
§ 1º Os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável, sempre que possível.
§ 2º Quando houver necessidade de transferência de *logs* para armazenamento alternativo deve-se proteger a confidencialidade e integridade dos registros de auditoria.
§ 3º Os registros de *logs* de auditoria e outros *logs* de eventos de segurança da informação e comunicação devem ser revisados e retidos de maneira segura.
§ 4º A capacidade de armazenamento dos *logs* deve ser constantemente verificada e readequada conforme a necessidade da UNIFAL-MG.
§ 5º Registros de auditoria devem ser correlacionados quando houver mais de um repositório de *logs* ou coletados de várias fontes de *logs.*
§ 6º Cópias de segurança (backups) de arquivos de trilhas de auditoria de *logs* devem ser armazenados de forma segura, conforme legislação pertinente.

Seção III
Do uso

Art. 11° A UNIFAL-MG deve garantir que os *logs* de auditoria estejam disponíveis para o acesso quando for necessário, e manter o controle de acesso lógico aos diretórios onde os logs estão armazenados.
§ 1º Análises de *logs* de auditoria de eventos devem ser realizadas de maneira sistematizada para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.
§ 2º Em casos de resposta a incidentes cibernéticos, a coleta de dados forenses deve ser utilizada nos sistemas afetados, garantindo a proteção de tais dados.
§ 3º Quando suportado, *logs* de provedores de serviços devem ser coletados.
§ 4º Processos de revisão, análise e relatórios de registros de auditoria devem ser correlacionados, para investigação e resposta a indicações de atividades ilegais, não autorizadas, suspeitas ou incomuns.

Seção IV
Da exclusão

Art. 12° Os eventos de auditoria em ativos de TI considerados críticos devem ser armazenados por um período pré-estabelecido e quando este prazo vencer, a UNIFAL-MG deve ser capaz de realizar a eliminação de *logs* de forma eficiente, com base nas melhores práticas de segurança da informação e normativos como LGPD e LAI (Lei

de Acesso à Informação).
§ 1º A exclusão regular de logs de auditoria de eventos considerados desnecessários deve reduzir a quantidade de dados que precisam ser filtrados para atender às requisições de resgate de informações além de reduzir os custos de armazenamento e gerenciamento de dados.
§ 2º Quando não forem mais necessários para requisitos legais, regulatórios (incluindo federais, estaduais e municipais) ou de negócios *da UNIFAL-MG*, os dados de *logs* devem ser eliminados dos registros usando-se um método seguro aprovado.
§ 3º Quando possível deve-se implementar medidas de salvaguarda para os *logs*, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto, de forma que esses não tenham permissão de exclusão ou desativação dos registros (*logs*) de suas próprias atividades.
§ 4º A exclusão de logs de auditoria de eventos deve ser feita de modo a assegurar a irrecuperabilidade, destruindo inclusive as cópias, mídias digitais, impressos e discos rígidos.

CAPÍTULO VI
DO PLANO DE REGISTROS DE AUDITORIA

Art. 13° O plano de registros de logs de auditoria de eventos deve minimamente observar as seguintes diretrizes:

I. Os ativos de TI da UNIFAL-MG devem ser configurados de forma a sincronizar data e hora via protocolo NTP (*Network Time Protocol*) seguindo o Horário Padrão de Brasília - GMT-3. Pelo menos dois servidores NTP devem ser configurados para sincronizar o tempo dos ativos de informação, quando houver suporte;
II. Em caso de incidentes de segurança da informação, ou quaisquer outros eventos de segurança, a ETIR deve coletar e preservar todos os registros de eventos do sistema operacional, serviço de TIC, sistema de informação ou ativo de informação;
III. A estrutura original de diretórios, incluindo todos os metadados associados, como data, hora de criação e atualização, e permissões dos arquivos deve ser mantida, para garantir a integridade das evidências;
IV. No caso de impossibilidade de preservar as evidências do evento de segurança, o responsável pela área de TIC deve justificar em relatório, a falta destas evidências.

CAPÍTULO VII
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Art. 14° Compete à alta administração:

I. prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos, planos institucionais, estrutura organizacional e com as leis e regulamentos pertinentes; e
II. garantir recursos (humanos, tecnológicos e financeiros) para a execução de ações relacionadas ao registro de logs de auditoria no âmbito da UNIFAL-MG.

Art. 15° Compete ao Comitê de Governança Digital:

I. deliberar sobre política e norma interna complementar de registro de *logs* de auditoria;
II. assessorar a implementação das ações para o registro de *logs* de auditoria; e
III. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre registro de *logs* de auditoria.

Art. 16° Compete ao Diretor do Núcleo de Tecnologia Gestor de Tecnologia da Informação:

I. coordenar o planejamento, implementação e melhoria contínua dos controles de registro de *logs* de auditoria em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na Administração Pública Federal; e
II. propor diretrizes e responsabilidades para o registro de *logs* de auditoria.

Art. 17° Compete ao Gestor de Segurança da Informação:

I. propor diretrizes e responsabilidades para a gestão de registro de *logs* de auditoria.
II. coordenar a elaboração da política e norma interna complementar sobre registro de logs de auditoria, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;
III. assessorar a alta administração na implantação da Política de Gestão de Registros (*logs*) de Auditoria e das normas internas de segurança da informação da UNIFAL-MG;
IV. incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à registros de *logs* de auditoria;
V. propor recursos necessários às ações de registros de *logs* de auditoria;
VI. verificar os resultados dos trabalhos de auditoria sobre a gestão de registros de *logs* de auditoria; e
VII. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos relacionados à gestão de registros de *logs* de auditoria.

Art. 18° Compete à Gerência de Segurança da Informação do NTI da UNIFAL-MG:

I. acompanhar o processo de gestão de registro de *logs* de auditoria;
II. deliberar sobre procedimentos internos para registro de *logs* de auditoria; e
III. deliberar sobre os ativos de TI que terão *logs* de auditoria gerenciados de acordo com a sua criticidade;
IV. pesquisar, implantar e manter soluções para gestão de registro de *logs* de auditoria no âmbito da UNIFAL-MG;
V. propor e gerenciar procedimentos de gestão de registro de *logs* de auditoria para a rede de comunicação de dados da UNIFAL-MG;
VI. implantar, configurar, gerenciar e monitorar a estrutura de registro de *logs* de auditoria;
VII. implementar rotinas para gestão de *logs* de auditoria; e
VIII. definir o fluxo do processo de gestão de *logs* de registro de auditoria.

Art. 19° Compete aos usuários:

I. atender aos princípios e diretrizes contidos nesta política, incluindo normas e procedimentos complementares destinados à segurança da informação e comunicação; e
II. guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades.

CAPÍTULO VIII
DAS PENALIDADES

Art. 20° Ações que violem esta política, norma interna complementar, procedimentos, ou que quebrem os controles de segurança da informação serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

CAPÍTULO IX
DA REVISÃO E ATUALIZAÇÃO

Art. 21° Esta política bem como a norma interna complementar gerada a partir dela deverão ser revisadas, aprovadas e atualizadas em função de alterações nas normativas da UNIFAL-MG, legislação pertinente, diretrizes e políticas do governo federal ou quando considerada necessária pelo Comitê de Governança Digital.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 22° Esta política e suas atualizações, bem como norma interna complementar, deverão ser divulgadas amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 23° Os casos omissos serão avaliados pelo Comitê de Governança Digital.

Art. 24° Esta política entra em vigor a partir da data de sua publicação.