Processo nº 08650.049824/2024-11 SEI nº 56855643

Boletim de Serviço Eletrônico em 03/06/2024

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
POLÍCIA RODOVIÁRIA FEDERAL
DIREÇÃO-GERAL

INSTRUÇÃO NORMATIVA PRF Nº 130, DE 29 DE MAIO DE 2024

Institui a Política de Gestão de Registros (**logs**) de Auditoria no âmbito da Polícia Rodoviária Federal (PRF).

O DIRETOR-GERAL DA POLÍCIA RODOVIÁRIA FEDERAL, no uso das atribuições que lhe foram conferidas pelo Decreto nº 11.348, de 1º de janeiro de 2023, bem como o contido nos autos dos processos SEI nº 08650.049824/2024-11, resolve:

Objeto e âmbito de aplicação

Art. 1º Instituir a Política de Gestão de Registros (**logs**) de Auditoria no âmbito da Polícia Rodoviária Federal (PGRA/PRF).

Parágrafo único. A PGRA/PRF tem por objetivo normatizar e manter o processo de armazenamento de **logs** de ativos de TI com a finalidade de auditoria na PRF, definindo o escopo e as atividades necessárias para coletar, analisar, reter, bem como possibilitar detecção, compreensão ou recuperação de um ataque cibernético, visando garantir segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação da PRF (POSIN/PRF).

Termos e Definições

Art. 2º Para fins desta Instrução Normativa (IN), considera-se:

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 - evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação.

VI - 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;

VII - **host:** computador ou dispositivo de TI (por exemplo, roteador, **switch**, **gateway**, **firewall**);

VIII - 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;

IX - 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, podendo também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação da política de segurança, do procedimento de segurança ou da política de uso.

X - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XI - **log** (registro de auditoria): registro de eventos relevantes em um dispositivo ou sistema computacional;

XII - **log** de auditoria: registros nativos dos sistemas que exigem menos configurações para ativação e que fornecem eventos no nível do sistema que mostram vários horários de início/término de processo do sistema, travamentos etc.

XIII - **log** de sistema: incluem eventos no nível do usuário como quando um usuário faz **login**, acessa um arquivo etc;

XIV - NTP (**Network Time Protocol**): Protocolo de Tempo para Redes;

XV - risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos, podendo ser mensurado em termos de impacto e de probabilidade;

XVI - sanitização de dados: eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados; e

XVII - 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.

Definição de Escopo de Ativos

Art. 3º A PGRA/PRF tem como objetivo o estabelecimento de diretrizes, competências e responsabilidades para governar o ciclo de vida da gestão dos registros (**logs**) de auditoria, garantindo que os **logs** sejam criados e analisados adequadamente.

Art. 4º A PGRA/PRF aplica-se aos ativos informacionais da PRF, incluindo:

I - servidores;

II - gestores;

III - prestadores de serviços; e

IV - contratados que tenham acesso e/ou utilizem ativos informacionais.

Art. 5º Ficam previamente estabelecidos como serviços e sistemas essenciais àqueles

constantes no endereço eletrônico "sistemas.prf.gov.br."

Art. 6º Compete à Diretoria de Tecnologia e Comunicação (DTIC) a elaboração, manutenção e a garantia do cumprimento da PGRA/PRF.

Premissas e Responsabilidades

Art. 7º A atividade de auditoria nos ativos de TI é de competência da Coordenação de Integração, Segurança e Ciência de Dados (CISC), que se reportará ao Diretor de Tecnologia da Informação e Comunicação da PRF.

Art. 8º Somente poderão ser realizadas auditorias externas à DTIC mediante solicitação formal da Corregedoria-Geral ou através de Pedido de Informação formalizado pela Diretoria de Inteligência.

Art. 9º É dever dos responsáveis pelos áreas envolvidas na auditoria cooperarem com a CISC quanto ao acesso a ativos de informação, instalações e trânsito de dados.

Requisitos Mínimos de Registro de Eventos (Logs)

Art. 10. Os registros de eventos devem conter informações mínimas e relevantes, especialmente:

I - identificação inequívoca do usuário que acessou o recurso;

II - identificação dos usuários de origem e destino do evento, quando for o caso;

III - natureza do evento, como sucesso ou falha de autenticação, tentativa de troca de senha, entre outros;

IV - **timestamp**, formado por data, hora e fuso horário;

V - endereço de **Internet Protocol** (IP), identificador do ativo de processamento, coordenadas geográficas, se disponíveis, e outras informações que permitam identificar a possível origem e destino do evento;

VI - endereços, serviços e protocolos de rede utilizados;

VII - arquivos acessados e tipo de acesso; e

VIII - alarmes provocados pelo sistema de controle de acesso.

Art. 11. Os ativos de informação deverão estar com as informações de data e hora sincronizadas.

§ 1º Pelo menos duas fontes de tempo devem ser configuradas para sincronizar o tempo dos ativos de informação, onde houver suporte.

§ 2º Os ativos serão configurados de forma a sincronizar data e hora via protocolo NTP, onde houver suporte.

Art. 12. Os ativos de processamento que não permitam os registros de eventos conforme indicado devem ser mapeados e documentados quanto ao tipo e ao formato de registro de eventos que o sistema permite armazenar.

Da Coleta dos Logs

Art. 13. A geração de **log** de auditoria deverá estar habilitada nos ativos de informação, incluindo **softwares** 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.

Parágrafo único. A Coordenação de Infraestrutura e Aplicações (CIA) assegurará que os

ativos de informação registrem **logs** de auditoria.

Art. 14. **Logs** e registros de auditoria de ativos de informação devem ser criados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

Art. 15. A DTIC promoverá o monitoramento dos ativos de informação em busca de comportamentos anômalos ou suspeitos.

Art. 16. Quando apropriado, **logs** de auditoria de consultas DNS e URL em ativos de informação devem ser coletados, bem como **logs** do provedor de serviços.

Art. 17. Os ativos de rede e ativos de informação devem registrar os seguintes eventos:

I - tentativas de **logon** (do sistema ou domínio) bem-sucedidas e malsucedidas;

II - gerenciamento de contas de usuários, tais como troca de senhas, criação, alteração e remoção de usuários, perfis e grupos privilegiados;

III - modificação de política de senhas, como tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, entre outras;

IV - acesso aos serviços de armazenamento na nuvem;

V - acesso ou modificação de arquivos, serviços e sistemas de informação;

VI - alteração na configuração de sistemas operacionais, serviços e sistemas de informação;

VII - inicialização, suspensão e reinicialização de serviços;

VIII - uso de aplicativos e utilitários do sistema operacional;

IX - ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção e prevenção de intrusos;

X - acesso físico por senha, cartão magnético ou biometria em área de segurança com ativos de processamento críticos como **data center**, sala de roteadores, entre outros;

XI - acoplamento e desacoplamento de dispositivos de **hardware**, com especial atenção para mídias removíveis; e

XII - acesso e alteração nos **logs**.

Art. 18. Os registros de eventos de administradores e operadores com privilégios para ações e comandos especiais na rede corporativa, como super usuários, administradores de rede, entre outros, devem ter mecanismos adicionais de gerenciamento e monitoramento, considerando, no mínimo, os seguintes aspectos:

I - os registros de eventos dos administradores e operadores da rede corporativa devem ser protegidos e analisados criticamente, a intervalos regulares;

II - os administradores e operadores da rede corporativa não devem fazer parte da equipe de monitoramento e análise crítica de suas próprias atividades; e

III - os administradores e operadores da rede corporativa não devem ter permissão para apagar, alterar ou desativar os registros de eventos de suas próprias atividades.

Do Armazenamento dos Logs

Art. 19. Os registros de eventos devem ser armazenados por um período mínimo de 2 (dois) anos, sem prejuízo de outros prazos previstos em referências legais e normativas específicas.

Parágrafo único. Os registros de eventos decorrentes de aplicações da PRF não serão

excluídos pelo mero decurso de prazo.

Art. 20. Os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria, local e remotamente, por meio do uso de tecnologia aplicável, quando possível.

Art. 21. No caso de os **logs** armazenados contiverem dados pessoais, deve-se observar o previsto pelo art. 16 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) a fim de avaliar se os **logs** devem ser eliminados ou conservados após o término do tratamento dos dados pessoais.

Art. 22. Os registros de **log** de auditoria e outros **logs** de eventos de segurança devem ser revisados e retidos de maneira segura.

Art. 23. A capacidade de armazenamento dos **logs** deve ser constantemente verificada e readequada conforme a necessidade da PRF.

Art. 24. Registros de auditoria devem ser correlacionados quando houver mais de um repositório de **logs** ou coletados de várias fontes de **logs**.

Art. 25. Cópias de segurança (**backups**) de arquivos de trilhas de auditoria de **log** devem ser armazenados de forma segura, em mídia de difícil alteração.

Do Uso dos Logs

Art. 26. A frequência, escopo e/ou profundidade da revisão, análise e relatório dos registros de auditoria devem ser ajustados para atender às necessidades da PRF com base nas informações recebidas.

Art. 27. Análises de **logs** de auditoria devem ser realizadas pelo menos 2 (duas) vezes ao ano para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.

Art. 28. Processos, procedimentos e medidas técnicas devem ser definidas, implementadas e avaliadas para reporte de anomalias e falhas do sistema de monitoramento e notificação imediata ao responsável, caso confirmado.

Art. 29. Eventos relacionados à segurança nos aplicativos e na infraestrutura subjacente serão identificados e monitorados pela DTIC.

Art. 30. **Logs** e registros de auditoria de sistemas devem ser configurados e armazenados na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

Art. 31. Em casos de resposta a incidentes cibernéticos, a coleta de dados forenses deve ser utilizada nos sistemas afetados, garantindo a transferência e a proteção de tais dados.

Art. 32. Componentes do sistema e a operação desses componentes devem ser monitorados em busca de anomalias que sejam indicativas de atos maliciosos, desastres naturais e erros que afetem a capacidade da PRF de atingir seus objetivos.

Parágrafo único. As anomalias mencionadas no **caput** devem ser analisadas para determinar se representam eventos ou incidentes de segurança.

Art. 33. As implementações de coleta de **logs** podem incluir a coleta de **logs** de auditoria de linhas de comando (CLI) tais como **PowerShell,** BASH e terminais administrativos remotos.

Art. 34. O comportamento dos ativos de informação deve ser analisado para detectar e mitigar a execução de comandos e **scripts** que possam indicar ações maliciosas.

Art. 35. 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.

Da Exclusão dos Logs

Art. 36. Os dados de **logs** devem ser removidos dos registros usando um método seguro aprovado quando não forem mais necessários para requisitos legais, regulatórios (incluindo federais, estaduais e municipais) ou de negócios no âmbito da PRF.

Art. 37. 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 (**log**) de suas próprias atividades.

Art. 38. A exclusão deve ser feita de modo a assegurar a irrecuperabilidade, destruindo inclusive as cópias, mídias digitais, impressos e discos rígidos.

Art. 39. No caso em que o descarte/exclusão for realizado por meio de terceiro, deve-se incluir registro/rastreamento quando enviado por correio seguro ou outro método de entrega.

Art. 40. Mídias digitais de armazenamento ou discos rígidos podem ser reutilizados, desde que seja realizada a sobrescrição de dados na mídia a ser reutilizada.

Disposições Finais

Art. 41. Quando possível, as ferramentas ou soluções terão habilitadas suas funcionalidades que proíbam a alteração e deleção dos **logs** registrados.

Art. 42. Os casos omissos serão resolvidos pelo Comitê de Governança Digital (CGD).

Art. 43. Eventual exceção a esta Política deverá ser aprovada pelo CGD, ou pela estrutura que venha a substituí-lo, assegurando a avaliação das alternativas disponíveis e a adequação dos controles compensatórios para atenuação dos riscos.

Art. 44. Fica estabelecido o prazo de 120 (cento e vinte dias), a contar da data de vigência desta IN, para adequação pela áreas responsáveis pela coleta e armazenamento do logs.

Art. 45. Esta Instrução Normativa entra em vigor em 3 de junho de 2024.

ANTONIO FERNANDO SOUZA OLIVEIRA

PRF

Documento assinado eletronicamente por **ANTONIO FERNANDO SOUZA OLIVEIRA**, **Diretor-Geral**, em 30/05/2024, às 16:12, horário oficial de Brasília, com fundamento no art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020, e no art. 42 da Instrução Normativa nº 116/DG/PRF, de 16 de fevereiro de 2018.

A autenticidade deste documento pode ser conferida no site https://sei.prf.gov.br/verificar, informando o código verificador **56855643** e o código CRC **FBAC34F6**.