SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

RESOLUÇÃO SUSEP Nº 95, DE 11 DE SETEMBRO DE 2026

Institui a Política de Gestão de Registros de Auditoria em Ambientes Computacionais no âmbito da Superintendência de Seguros Privados - Susep

O SUPERINTENDENTE DA SUPERINTENDÊNCIA DE SEGUROS PRIVADOS - Susep, torna público que o Conselho Diretor desta Autarquia, em reunião ordinária realizada em 9 de setembro de 2026, no uso das atribuições que lhe confere o inciso VI do art. 8º do Regimento Interno, aprovado pela Resolução CNSP nº 490, de 12 de março de 2026, tendo em vista o disposto na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, na Resolução Susep nº 45, de 17 de outubro de 2024, e na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, bem como o que consta do Processo Susep nº 15414.666235/2025-31,

RESOLVE:

Art. 1º Fica instituída a Política de Gestão de Registros de Auditoria em Ambientes Computacionais - PGRAC no âmbito da Susep.

CAPÍTULO I

DOS OBJETIVOS

Art. 2º A PGRAC estabelece diretrizes estratégicas, competências e responsabilidades voltadas à rastreabilidade e à identificação de eventos ocorridos no ambiente computacional da Susep.

Art. 3º A PGRAC disciplina os procedimentos de coleta, armazenamento e manutenção de registros de eventos e trilhas de auditoria.

Art. 4º A implementação da PGRAC assegurará o rastreamento, o acompanhamento, o controle e a verificação de acessos aos ativos computacionais.

Art. 5º Os processos decorrentes da PGRAC têm por objetivo:

I - identificar detalhadamente as causas de eventos ocorridos em recursos computacionais;

II - obter dados para a investigação de incidentes de segurança da informação;

III - reduzir o tempo de resposta a incidentes; e

IV - ampliar a capacidade de identificação precisa da autoria e da origem dos eventos ocorridos no ambiente computacional da Susep.

CAPÍTULO II

DO ESCOPO

Art. 6º A PGRAC se aplica a todos os recursos de tecnologia da informação da Susep, exceto os que:

I - não disponham de capacidade técnica para registro de logs;

II - estejam protegidos por cláusulas contratuais ou disposições normativas que restrinjam a geração ou o acesso a registros;

III - sejam considerados tecnicamente inviáveis para fins de gestão de logs e trilhas de auditoria; ou

IV - pertençam a terceiros, hipótese em que a PGRAC não se aplica aos registros de eventos gerados por sistemas operacionais ou aplicações sob sua responsabilidade.

Parágrafo único. As unidades responsáveis por recursos de tecnologia da informação considerados isentos da aplicação da PGRAC deverão formalizar, junto à área operacional de segurança da informação, a devida justificativa da isenção.

Art. 7º Esta Resolução e eventuais normas complementares deverão ser observadas por servidores e prestadores de serviço que possuam privilégios administrativos sobre recursos do ambiente computacional da Susep aptos a gerar registros de eventos ou trilhas de auditoria.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 8º Para fins desta Resolução, além dos termos constantes do glossário de segurança da informação instituído pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, e na Política de Segurança da Informação da Susep - POSIN, aplicam-se também as seguintes definições:

I - ambiente computacional: conjunto de recursos de tecnologia da informação, incluindo hardware, software e infraestrutura, utilizados no âmbito da Susep;

II - área gerencial de segurança da informação: unidade organizacional responsável pela gestão de segurança da informação nos ativos e serviços de TI, pela definição de diretrizes, normas e padrões relacionados ao tema, bem como pela coordenação das atividades a ele associadas;

III - área operacional de segurança da informação: unidade organizacional responsável pela execução das atividades de segurança da informação, incluindo a implementação de controles, o tratamento de incidentes e solicitações de TI, a disseminação da cultura de segurança da informação e demais atividades operacionais relacionadas ao tema, em conformidade com as diretrizes estabelecidas pela área gerencial;

IV - áreas operacionais de tecnologia da informação: unidades organizacionais responsáveis pela infraestrutura de TI e pelo desenvolvimento e manutenção de sistemas informatizados;

V - gestor de segurança da informação: autoridade formalmente designada, titular ou setorial, conforme designação vigente, responsável pela supervisão e aprovação das diretrizes de segurança da informação no âmbito institucional;

VI - descarte: retirada definitiva de uso de mídia ou de outro meio de suporte à informação, com sua correspondente destinação final, observados os requisitos de segurança aplicáveis;

VII - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR: equipe responsável pelo planejamento e pela execução das atividades de tratamento e resposta a incidentes que possam comprometer a segurança dos dados, sistemas e redes de computadores no âmbito da Susep;

VIII - incidente de segurança: qualquer evento adverso, confirmado ou suspeito, relacionado à segurança dos ambientes computacionais, das informações neles contidas ou das redes de computadores;

IX - retenção: tempo de armazenamento de determinada informação ou registro, definido conforme o risco e criticidade do recurso computacional e determinações legais ou infralegais;

X - registro de eventos: registros de ações realizadas em um dispositivo computacional, sistema ou ativo de informação;

XI - sanitização de dados: eliminação efetiva de informação armazenada em meio eletrônico, de forma a impedir sua reconstrução ou recuperação; e

XII - trilha de auditoria: registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia que possibilitam indicar, de forma cronológica e inequívoca o autor e a respectiva ação realizada em determinada operação, procedimento ou evento.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 9º A PGRAC tem por princípio a proteção dos seguintes atributos da informação sob custódia da

Susep:

I - a confidencialidade;

II - a integridade;

III - a autenticidade;

IV - a disponibilidade; e

V - a irretratabilidade.

CAPÍTULO V

DAS INSTÂNCIAS, COMPETÊNCIAS E RESPONSABILIDADES

Art. 10. As instâncias de supervisão, controle e normatização correspondem ao nível estratégico e central da gestão de registros de auditoria em ambientes computacionais e são responsáveis por:

I - definir a estratégia de implementação da PGRAC;

II - coordenar e estruturar a gestão dos registros de auditoria;

III - autorizar o acesso a registros e trilhas de auditoria em ambientes computacionais; e

IV - instruir e revisar normas complementares a esta Política, com vistas à sua atualização e aderência às alterações do ambiente de tecnologia da informação da SUSEP.

Parágrafo único. As instâncias de que trata o *caput* são compostas pelo Comitê de Segurança da Informação (CSI), pelo Gestor de Segurança da Informação, titular ou setorial, conforme designação vigente, e pela área gerencial de segurança da informação.

Art. 11. As instâncias táticas e operacionais são responsáveis por:

I - habilitar a geração de registros de eventos e trilhas de auditoria nos recursos computacionais da SUSEP;

II - habilitar o trânsito de dados e proporcionar acesso físico e lógico necessários ao cumprimento desta PGRAC;

III - garantir a conformidade dos recursos computacionais da SUSEP com esta Política; e

IV - assegurar a conformidade dos recursos computacionais de terceiros utilizados para o tráfego ou armazenamento de dados da Susep.

Parágrafo único. As instâncias de que trata o *caput* compreendem a área operacional de segurança da informação e as áreas operacionais de tecnologia da informação da SUSEP.

Art. 12. Compete ao Gestor de Segurança da Informação, titular ou setorial, conforme designação vigente:

I - aprovar formalmente as requisições de acesso a registros de eventos e trilhas de auditoria;

II - publicar normas complementares a esta Política; e

III - tratar situações relacionadas aos registros de eventos e trilhas de auditoria não previstas nesta Política.

Art. 13. Compete à área operacional de segurança da informação:

I - monitorar eventos de acesso e uso de recursos computacionais;

II - instruir, manter e operar rotinas periódicas de revisão dos registros para identificação de eventos anômalos; e

III - correlacionar e interpretar registros de eventos e trilhas de auditoria.

Art. 14. Compete à ETIR tratar os incidentes identificados por meio da análise de registros de auditoria em recursos computacionais.

CAPÍTULO VI

DA GESTÃO DE REGISTROS DE AUDITORIA EM AMBIENTES COMPUTACIONAIS

Art. 15. Todos os recursos computacionais conectados à infraestrutura da Susep, sejam próprios ou de terceiros, devem gerar registros de eventos e trilhas de auditoria nos termos do art. 3º desta Política, observadas as exceções previstas no art. 6º.

Parágrafo único. Os registros de auditoria de que trata o *caput* devem ser continuamente coletados, transmitidos e armazenados em ambiente centralizado, redundante e protegido por controles de acesso físico e lógico, conforme requisitos definidos em norma complementar.

Art. 16. A área gerencial de segurança da informação estabelecerá normas complementares com o detalhamento dos registros, os formatos de gravação, os requisitos técnicos mínimos e a lista mínima de eventos auditáveis, incluindo as características e os dados a serem registrados.

Art. 17. O Termo de Responsabilidade de Acesso a Recursos Computacionais deverá conter cláusula de ciência quanto ao monitoramento, registro, análise e auditoria das ações realizadas por meio dos referidos recursos.

Art. 18. Os registros de eventos e trilhas de auditoria são considerados informações sensíveis, devendo seu acesso ser restrito ao pessoal responsável pela implementação desta Política.

Art. 19. A retenção dos registros de eventos e trilhas de auditoria observará o disposto na legislação e nos instrumentos infralegais vigentes.

Parágrafo único. Na ausência de determinação específica, o período mínimo de armazenamento será de noventa dias.

Art. 20. Todos os registros de eventos e trilhas de auditoria devem ser objeto de cópias de segurança (*backups*), armazenadas em local geograficamente distinto daquele onde se efetua seu armazenamento principal e em conformidade com a Política de Backup e Restauração de Dados Digitais da Superintendência de Seguros Privados.

Art. 21. Fica vedada a exclusão precoce ou alteração de registros de eventos ou trilhas de auditoria.

Parágrafo único. As exclusões de cópias de segurança deverão observar procedimentos de descarte seguro e sanitização, em conformidade com a legislação, os instrumentos infralegais e as normas internas aplicáveis.

Art. 22. Os registros de eventos devem conter horário em padrão Tempo Universal Coordenado - UTC, sem conversão para fuso horário local.

Art. 23. Os recursos computacionais deverão manter sincronismo de seus relógios por meio da utilização de protocolo padrão, atendendo aos requisitos mínimos a serem definidos em norma complementar.

Art. 24. Todos os incidentes de segurança identificados por meio da análise de registros de eventos e trilhas de auditoria deverão ser comunicados imediatamente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Susep (ETIR).

Art. 25. Quando houver a participação de entes externos para subsidiar as atividades relacionadas ao tema desta Política, os acessos deverão ser concedidos de forma pontual, pelo tempo estritamente necessário e com o escopo mínimo indispensável ao desempenho das atividades.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 26. As disposições estabelecidas nesta Política deverão ser implementadas no prazo de até vinte e quatro meses, contado da data de sua publicação.

Art. 27. A PGRAC deverá ser revista na superveniência de alterações normativas ou de mudanças no ambiente de tecnologia da informação da Susep que demandem sua atualização.

Art. 28. As exceções a que se refere o art. 6º poderão ser revistas pelas áreas operacional e gerencial de segurança da informação.

Art. 29. Os casos omissos em relação ao disposto na presente Política deverão ser submetidos ao Gestor de Segurança da Informação, titular ou setorial, conforme designação vigente.

Art. 30. Esta Resolução entra em vigor na data de sua publicação.

ALESSANDRO SERAFIN OCTAVIANI LUIS

Superintendente

Documento assinado eletronicamente por **ALESSANDRO SERAFIN OCTAVIANI LUIS (MATRÍCULA 1860655)**, **Superintendente da Susep**, em 15/09/2026, às 08:57, conforme horário oficial de Brasília, de acordo com o art. 6º do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site https://sei.susep.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2901742** e o código CRC **5E1C1499**.

Referência: Processo nº 15414.662325/2025-52 SEI nº 2901742