Portaria Nº 168/2026/IPAM-DRFP

Porto Velho, 18 de março de 2026.

Aprova o manual que sobre a auditoria e o monitoramento da segurança da informação no Instituto de Previdência e Assistência dos Servidores do Município de Porto Velho – IPAM e dá outras providências.

A DIRETORA PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA E ASSISTÊNCIA DOS SERVIDORES DO MUNICÍPIO DE PORTO VELHO – IPAM, no uso de suas atribuições legais, e considerando o disposto na Política de Segurança da Informação do IPAM e a necessidade de garantir a conformidade e a eficácia dos controles de segurança da informação,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria regulamenta a realização de auditorias internas e externas, bem como o monitoramento contínuo de logs e eventos de segurança, para verificar a conformidade e a eficácia dos controles de segurança do IPAM.

Art. 2º As disposições desta Portaria aplicam-se a todos os sistemas, redes, dados e processos que envolvem a segurança da informação no IPAM.

CAPÍTULO II

DA REALIZAÇÃO DE AUDITORIAS

Art. 3º O IPAM compromete-se a realizar auditorias regulares para avaliar a eficácia de seus controles de segurança da informação e a conformidade com as políticas internas, regulamentos externos e melhores práticas.

Art. 4º As auditorias internas serão conduzidas periodicamente pela Controladoria Geral, em coordenação com a Área de Tecnologia da Informação (CPD) e o Comitê de Segurança da Informação (CSI), se houver.

§ 1º O objetivo é revisar os processos, sistemas e a aplicação das políticas de segurança, identificando pontos de melhoria e garantindo que as diretrizes sejam seguidas por todas as áreas.

§ 2º Os resultados das auditorias internas serão reportados à Diretoria de Presidência e ao Comitê de Segurança da Informação (CSI), se houver, para a implementação de ações corretivas.

Art. 5º O IPAM poderá ser submetido a auditorias externas por órgãos reguladores, parceiros ou certificadoras, conforme a necessidade e os requisitos legais ou contratuais.

§ 1º A instituição cooperará plenamente com essas auditorias, fornecendo as informações e acessos necessários, visando demonstrar a aderência às normas e padrões de segurança da informação.

CAPÍTULO III

DO MONITORAMENTO DE LOGS E EVENTOS DE SEGURANÇA

Art. 6º O IPAM implementará sistemas para coletar e armazenar logs de eventos de segurança de todos os sistemas críticos, computadores, servidores, dispositivos de rede e aplicações.

§ 1º Estes logs incluirão registros de acesso, tentativas de login (bem-sucedidas e falhas), alterações de configuração, atividades de usuários privilegiados e alertas de segurança.

Art. 7º Os logs serão monitorados de forma contínua pela Área de Tecnologia da Informação (CPD), utilizando ferramentas de Gerenciamento de Informações e Eventos de Segurança (SIEM - Security Information and Event Management) **prioritariamente por meio de soluções automatizadas de correlação e geração de alertas, admitindo-se procedimentos manuais apenas de forma complementar e excepcional**, para identificar padrões incomuns, atividades não autorizadas ou potenciais violações de segurança.

Art. 8º Alertas gerados pelo monitoramento de logs e eventos serão investigados prontamente pela Área de Tecnologia da Informação (CPD) ou pela equipe de resposta a incidentes, seguindo os procedimentos estabelecidos na Portaria sobre Gestão de Incidentes de Segurança da Informação.

Art. 9º Os logs de segurança serão retidos por um período definido pela Área de Tecnologia da Informação (CPD), em conformidade com os requisitos legais e regulatórios, para fins de auditoria, investigação de incidentes e análise forense, **observado o prazo mínimo de 06 (seis) meses para guarda de registros de acesso a aplicações de internet, nos termos da Lei nº 12.965/2014 (Marco Civil da Internet), sem prejuízo de prazos superiores previstos em legislação específica ou necessidade administrativa devidamente justificada.**

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 10. A Controladoria Geral é a principal responsável por:

I – Planejar e executar as auditorias internas de segurança da informação;

II – Acompanhar as auditorias externas;

III – Monitorar a implementação das ações corretivas resultantes das auditorias.

Art. 11. A Área de Tecnologia da Informação (CPD) é responsável por:

I – Implementar e manter os sistemas de coleta e armazenamento de logs;

II – Realizar o monitoramento contínuo de logs e eventos de segurança;

III – Responder prontamente aos alertas de segurança.

Art. 12. O Comitê de Segurança da Informação (CSI), se instituído, é responsável por:

I – Aprovar o plano anual de auditorias de segurança da informação;

II – Avaliar os relatórios de auditoria e monitoramento.

CAPÍTULO V

DAS SANÇÕES

Art. 13. O descumprimento das diretrizes estabelecidas nesta Portaria, intencional ou por negligência, poderá acarretar sanções disciplinares, administrativas e/ou legais, conforme previsto no item 7.1.2 da Política de Segurança da Informação do IPAM e na **Lei Complementar nº 385/2010 (Estatuto dos Servidores Públicos do Município de Porto Velho)**.

§ 1º As sanções serão aplicadas de acordo com a gravidade da infração, o impacto gerado, a reincidência e as normas internas do IPAM.

§ 2º O descumprimento das diretrizes pode expor o IPAM e o indivíduo responsável a responsabilidades civis e criminais, especialmente em casos de vazamento de dados pessoais, conforme previsto na Lei nº 13.709/2018 (LGPD) e demais legislações pertinentes.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 14. Esta Portaria será revisada e atualizada anualmente, ou sempre que houver mudanças significativas na legislação, na infraestrutura tecnológica do IPAM, nos processos de negócio ou na identificação de novos riscos relevantes.

Art. 15. Os casos omissos serão resolvidos pela Diretoria de Presidência, mediante consulta à Área de Tecnologia da Informação (CPD), à Procuradoria Geral e à Controladoria Geral.

Art. 16. Todos os servidores, empregados públicos, estagiários, terceirizados e demais usuários que possuam acesso a sistemas, redes ou dados institucionais do IPAM deverão assinar Termo de Ciência e Responsabilidade, declarando conhecimento integral das disposições desta Portaria e da Política de Segurança da Informação vigente.

§ 1º A assinatura do Termo de Ciência e Responsabilidade constitui condição obrigatória para concessão e manutenção de acesso aos sistemas institucionais.

§ 2º A Área de Tecnologia da Informação (CPD) manterá registro atualizado dos termos assinados, em meio físico ou eletrônico, para fins de controle e responsabilização administrativa.

§ 3º A recusa injustificada na assinatura do termo implicará na suspensão ou não concessão de acesso aos sistemas institucionais, sem prejuízo de outras medidas administrativas cabíveis.

§ 4º A obrigatoriedade aplica-se tanto aos usuários atualmente ativos quanto àqueles que vierem a ingressar no IPAM após a publicação desta Portaria.

Art. 17. Nenhuma medida que implique cessação, suspensão, bloqueio ou redução de proventos, benefícios ou vantagens será adotada sem a prévia instauração de procedimento administrativo, assegurados o contraditório e a ampla defesa.

§ 1º O interessado será formalmente notificado para apresentar defesa no prazo mínimo de 10 (dez) dias úteis, podendo juntar documentos e requerer diligências.

§ 2º A decisão administrativa deverá ser motivada, com análise expressa dos argumentos apresentados.

§ 3º Da decisão caberá recurso, no prazo de 10 (dez) dias úteis quando se tratar de medida que implique cessação de pagamento.

§ 4º Em situações de indício de fraude ou irregularidade grave que exijam medida cautelar imediata, poderá ser adotada suspensão provisória devidamente fundamentada, devendo o interessado ser notificado para manifestação no prazo máximo de 5 (cinco) dias úteis, sob pena de nulidade da medida.

Art. 18. Esta Portaria entra em vigor na data de sua publicação.

CLAUDINEIA ARAÚJO DE OLIVEIRA BORTOLETE
Diretora-Presidente

011.000253/2026-00	0673891v7

Documento assinado eletronicamente por **Claudineia Araújo de Oliveira Bortolete**, **Presidente**, em 18/03/2026, às 12:23, conforme art. 17, § 1º, do Decreto nº 21.393, de 07 de outubro de 2025.

A autenticidade do documento pode ser conferida no site https://www.portovelho.ro.gov.br/sei informando o código verificador **0674560** e o código CRC **0FB843F6**.

011.000253/2026-00	0674560v4