Portaria Nº 167/2026/IPAM-DRFP

Porto Velho, 18 de março de 2026.

Aprova o manual que dispõe sobre as diretrizes da Superintendência Municipal de Tecnologia da Informação e Pesquisa (SMTI) e o uso do acesso remoto externo à rede de dados da SMTI pelo 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 regulamentar o acesso remoto externo à rede de dados da SMTI,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria estabelece o processo formal para detecção, notificação, resposta, comunicação e análise pós-incidente de segurança da informação, visando minimizar danos e fortalecer a postura de segurança do IPAM.

Art. 2º As disposições desta Portaria aplicam-se a todos os servidores, colaboradores, estagiários e terceirizados do IPAM, bem como a todos os ativos de informação da instituição.

CAPÍTULO II

DO PROCESSO DE DETECÇÃO, NOTIFICAÇÃO E RESPOSTA A INCIDENTES

Art. 3º O IPAM manterá um processo formal e documentado para a gestão de incidentes de segurança, que incluirá as seguintes etapas:

I – Detecção: Monitoramento contínuo de sistemas, redes e logs para identificar atividades anômalas ou indicadores de comprometimento, utilizando ferramentas de segurança (antivírus, firewall, sistemas de detecção de intrusão) e a vigilância dos usuários;

II – Notificação: Qualquer servidor ou colaborador que identificar ou suspeitar de um incidente de segurança deve notificá-lo imediatamente à Área de Tecnologia da Informação (CPD) **e ao Encarregado de Dados (DPO)**, fornecendo o máximo de detalhes possível sobre o ocorrido;

III – Análise e Classificação: A equipe da Área de Tecnologia da Informação (CPD) ou o time de resposta a incidentes avaliará a notificação para determinar a natureza, a extensão e a gravidade do incidente, classificando-o de acordo com seu potencial impacto;

IV – Contenção: Serão aplicadas medidas imediatas para conter o incidente e evitar sua propagação, minimizando os danos, o que pode incluir o isolamento de sistemas, o bloqueio de acessos ou a desativação de contas comprometidas;

V – Erradicação: Após a contenção, o incidente será erradicado, removendo a causa raiz do problema (ex: remoção de malware, correção de vulnerabilidades, restauração de sistemas limpos);

VI – Recuperação: Os sistemas e dados afetados serão restaurados a um estado operacional seguro, utilizando as cópias de segurança e os procedimentos de recuperação estabelecidos, garantindo a integridade e a disponibilidade dos serviços.

CAPÍTULO III

DA COMUNICAÇÃO DE VIOLAÇÕES DE DADOS

Art. 4º Em caso de violação de dados pessoais que possa acarretar risco ou dano relevante aos titulares, o IPAM seguirá rigorosamente as determinações da Lei nº 13.709/2018 (LGPD).

§ 1º A Autoridade Nacional de Proteção de Dados (ANPD) será notificada sobre a violação **no prazo de até 3 (três) dias úteis, contados do conhecimento do incidente**, conforme estabelecido na regulamentação vigente da ANPD, contendo as informações necessárias sobre o incidente.

§ 2º Os titulares dos dados afetados serão comunicados sobre a violação, de forma clara e acessível, descrevendo a natureza dos dados envolvidos, as medidas técnicas e de segurança utilizadas, os riscos envolvidos e as providências que o IPAM adotou ou pretende adotar para mitigar os impactos.

CAPÍTULO IV

DA ANÁLISE PÓS-INCIDENTE E LIÇÕES APRENDIDAS

Art. 5º Após a resolução de um incidente de segurança, uma análise detalhada será conduzida para extrair lições valiosas e fortalecer a postura de segurança do IPAM.

§ 1º Será realizada uma revisão completa do incidente, desde a detecção até a recuperação, para identificar o que funcionou bem e o que pode ser melhorado nos processos, tecnologias e na resposta da equipe.

§ 2º O objetivo é identificar as causas raiz do incidente, sejam elas falhas de processo, vulnerabilidades técnicas, erro humano ou outros fatores.

§ 3º Com base nas lições aprendidas, será elaborado um plano de ação com medidas corretivas e preventivas para evitar a recorrência de incidentes semelhantes e para aprimorar continuamente as defesas de segurança da informação do IPAM.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 6º A Área de Tecnologia da Informação (CPD) é a principal responsável por:

I – Monitorar continuamente os sistemas e redes para detecção de incidentes;

II – Liderar o processo de resposta, contenção, erradicação e recuperação de incidentes;

III – Manter a documentação do processo de gestão de incidentes atualizada.

Art. 7º O Encarregado de Dados (DPO) é responsável por:

I – Orientar sobre as obrigações da LGPD em relação a incidentes de dados pessoais;

II – Coordenar a comunicação de violações de dados à ANPD e aos titulares, quando aplicável;

III – Colaborar na análise pós-incidente, especialmente em relação aos aspectos de proteção de dados.

Art. 8º O Comitê de Segurança da Informação (CSI), se instituído, é responsável por:

I – Aprovar o plano de gestão de incidentes;

II – Avaliar os relatórios de incidentes e os planos de ação pós-incidente.

Art. 9º Todos os servidores e colaboradores do IPAM têm o dever de:

I – Estar vigilantes e reportar imediatamente quaisquer incidentes ou suspeitas de segurança;

II – Colaborar com a equipe de resposta a incidentes, fornecendo as informações necessárias.

CAPÍTULO VI

DAS SANÇÕES

Art. 10. 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 VII

DAS DISPOSIÇÕES FINAIS

Art. 11. 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. 12. 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. 13. 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. 14. 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. 15. Esta Portaria entra em vigor na data de sua publicação.

CLAUDINEIA ARAÚJO DE OLIVEIRA BORTOLETE
Diretora-Presidente

011.000253/2026-00	0673880v7

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 **0674541** e o código CRC **A2BE5DBF**.

011.000253/2026-00	0674541v4