Portaria Nº 166/2026/IPAM-DRFP

Porto Velho, 18 de março de 2026.

Aprova o manual que dispõe sobre a gestão de cópias de segurança (backups), continuidade de negócios e recuperação de desastres 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 disponibilidade e integridade dos dados e sistemas críticos da instituição,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria define os procedimentos para a realização de cópias de segurança (backups), testes de restauração e a elaboração e manutenção dos Planos de Continuidade de Negócios (PCN) e Recuperação de Desastres (PRD).

Art. 2º As disposições desta Portaria aplicam-se a todos os dados e sistemas considerados críticos para as operações do IPAM, abrangendo, mas não se limitando a sistemas informatizados essenciais, bancos de dados de segurados e beneficiários, documentos digitais de gestão, arquivos de configuração de rede e sistemas operacionais.

CAPÍTULO II

DAS CÓPIAS DE SEGURANÇA (BACKUP)

Art. 3º Todas as informações consideradas críticas para as operações do IPAM devem ser incluídas no escopo das cópias de segurança.

§ 1º A identificação e classificação desses ativos são realizadas em conjunto pela Área de Tecnologia da Informação (CPD) e pelos gestores das áreas de negócio.

Art. 4º O IPAM implementará um cronograma de cópias de segurança que contemple diferentes frequências e tipos, de acordo com a criticidade e o volume de alteração dos dados, podendo incluir:

I – Backup Diário;
II – Backup Semanal;
III – Backup Mensal.

§ 1º Serão utilizados backups completos, diferenciais e incrementais, otimizando o tempo de execução e o espaço de armazenamento.

Art. 5º As cópias de segurança serão armazenadas em múltiplos locais para garantir a proteção contra desastres localizados:

I – Cópias On-site;
II – Cópias Off-site.

§ 1º O transporte e o armazenamento off-site devem seguir rigorosos protocolos de segurança e criptografia.

§ 2º A implementação do armazenamento off-site dependerá de prévia disponibilidade orçamentária e formalização contratual adequada, precedida de estudo técnico preliminar elaborado pela Área de Tecnologia da Informação (CPD), contendo estimativa de custos, análise de riscos e definição da solução tecnológica a ser adotada.

§ 3º Até a efetiva implementação do armazenamento off-site, a Área de Tecnologia da Informação deverá adotar medidas compensatórias de mitigação de risco, devidamente justificadas e formalizadas em relatório técnico submetido à Diretoria Executiva.

Art. 6º Será definida uma política de retenção de cópias de segurança, especificando o período mínimo pelo qual cada tipo de backup deve ser guardado.

§ 1º Cópias de longo prazo serão mantidas para fins de auditoria e conformidade.

CAPÍTULO III

DA RECUPERAÇÃO DE DADOS E SISTEMAS (RESTORE)

Art. 7º Serão desenvolvidos e documentados procedimentos detalhados para a restauração de dados e sistemas.

§ 1º Estes processos incluirão a ordem de recuperação dos sistemas, a configuração de ambientes alternativos e a verificação da integridade dos dados restaurados.

Art. 8º A eficácia dos backups e dos procedimentos de restauração será validada por meio de testes periódicos.

§ 1º Os testes deverão ser realizados, no mínimo, semestralmente, ou sempre que houver alteração significativa na infraestrutura tecnológica.

§ 2º Esses testes simularão cenários de falha e desastre, garantindo recuperação dentro dos tempos de recuperação esperados (RTO) e com a perda máxima de dados aceitável (RPO).

§ 3º Os parâmetros de RTO e RPO deverão ser formalmente definidos pela Área de Tecnologia da Informação (CPD) e aprovados pela Diretoria Executiva.

§ 4º Os resultados dos testes serão documentados e as melhorias necessárias implementadas pela Área de Tecnologia da Informação (CPD) e pelo Comitê de Segurança da Informação (CSI), quando instituído.

CAPÍTULO IV

DOS PLANOS DE CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES (PCN/PRD)

Art. 9º O IPAM manterá um Plano de Continuidade de Negócios (PCN) e um Plano de Recuperação de Desastres (PRD) devidamente documentados, aprovados e comunicados.

§ 1º O PCN visa assegurar a continuidade das funções essenciais.

§ 2º O PRD foca na recuperação da infraestrutura de TI.

§ 3º Ambos os planos serão revisados e testados regularmente pela Área de Tecnologia da Informação (CPD) e pelo Comitê de Segurança da Informação (CSI), quando instituído.

§ 4º Enquanto não instituído formalmente o Comitê de Segurança da Informação (CSI), as atribuições estratégicas de aprovação, supervisão e monitoramento previstas nesta Portaria serão exercidas pela Diretoria Executiva, com apoio técnico da Área de Tecnologia da Informação (CPD).

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 10. Compete à Área de Tecnologia da Informação (CPD):

I – Implementar e manter os processos de cópias de segurança e recuperação de dados;
II – Desenvolver, documentar, testar e manter atualizados o PCN e o PRD;
III – Fornecer suporte técnico para execução dos planos.

Art. 11. O Comitê de Segurança da Informação (CSI), quando formalmente instituído, é responsável por:

I – Aprovar diretrizes estratégicas;
II – Monitorar a eficácia dos planos.

Parágrafo único. Enquanto não instituído o CSI, as competências previstas neste artigo serão exercidas pela Diretoria Executiva, mediante parecer técnico da Área de Tecnologia da Informação (CPD).

Art. 12. Compete aos Gestores das áreas de negócio:

I – Identificar e classificar dados e sistemas críticos;
II – Participar da elaboração e revisão do PCN e PRD.

CAPÍTULO VI

DAS SANÇÕES

Art. 13. O descumprimento das diretrizes poderá acarretar sanções disciplinares, administrativas e legais, conforme a Política de Segurança da Informação do IPAM e a Lei Complementar nº 886/2022.

§ 1º As sanções observarão a gravidade, impacto e reincidência.

§ 2º O descumprimento pode expor o IPAM e o responsável a responsabilidades civis e criminais, especialmente nos termos da Lei nº 13.709/2018 (LGPD).

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 14. Esta Portaria será revisada anualmente.

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	0673866v7

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 **0674521** e o código CRC **7E8C2C76**.

011.000253/2026-00	0674521v4