Portaria Nº 169/2026/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 detalha as regras para a utilização do serviço de acesso remoto externo à rede de dados da Superintendência Municipal de Tecnologia da Informação e Pesquisa (SMTI) pelo IPAM, garantindo a segurança das informações previdenciárias e a conformidade com as diretrizes da SMTI.

Art. 2º As diretrizes estabelecidas pela SMTI são obrigatoriamente aplicáveis ao IPAM, em consonância com o Capítulo VIII, Seção III da Lei Complementar nº 385/2010, especialmente os dispositivos sobre controle de acesso (Art. 8.3.1), monitoramento e registro (Art. 8.3.2) e continuidade dos serviços (Art. 8.3.3).

CAPÍTULO II

DAS REGRAS PARA UTILIZAÇÃO DO SERVIÇO DE ACESSO REMOTO EXTERNO

Art. 3º O acesso remoto externo à rede de dados da SMTI pelos servidores do IPAM somente será disponibilizado àqueles que:

I – Executem serviços corporativos vinculados às atividades previdenciárias e de assistência à saúde no âmbito do IPAM;

II – Necessitem daquele acesso para execução de atividades externas relacionadas à gestão previdenciária e de assistência à saúde no âmbito do IPAM;

III – Sejam devidamente autorizados pelo Diretor Presidente ou Controlador Geral do IPAM;

IV – Sejam certificados pela SMTI quanto aos aspectos técnicos de segurança.

Art. 4º É expressamente vedada a utilização do acesso remoto para fins não relacionados às atividades previdenciárias e de assistência à saúde no âmbito do IPAM do IPAM.

Art. 5º A SMTI, em coordenação com a Controladoria Geral do IPAM, monitorará e registrará toda conexão remota e acesso à rede de dados, com logs específicos para auditoria previdenciária.

Art. 6º Os administradores de sistemas previdenciários do IPAM poderão ter permissão de acesso remoto aos recursos de TIC, exclusivamente quando necessário para manutenção de sistemas críticos (SISAM, SIGAP, sistemas de folha de pagamento).

Art. 7º A solicitação de acesso remoto pelos servidores do IPAM ocorrerá por meio de chamado registrado no sistema GLPI, contendo:

I – Nome completo e CPF do servidor;

II – Cargo e lotação no IPAM;

III – E-mail institucional (@ipam.ro.gov.br) e telefone corporativo;

IV – Sistema previdenciário específico a ser acessado (SISAM, SIGAP, etc.);

V – Justificativa detalhada da necessidade previdenciária e de assistência à saúde no âmbito do IPAM;

VI – Período de validade (máximo 30 dias, renovável);

VII – Aprovação expressa da chefia imediata e Controladoria Geral.

Art. 8º O serviço de acesso remoto será automaticamente cancelado nas seguintes condições:

I – Finalização do período especificado na solicitação;

II – Perda da necessidade de utilização para atividades previdenciárias e de assistência à saúde no âmbito do IPAM;

III – Transferência, exoneração ou aposentadoria do servidor;

IV – Identificação de acesso irregular a dados previdenciários sensíveis;

V – Violação às normas da Lei nº 13.709/2018 (LGPD) ou sigilo previdenciário.

Art. 9º As conexões remotas à rede de dados da SMTI pelos servidores do IPAM cumprirão requisitos técnicos específicos:

I – **Utilização obrigatória de mecanismo de autenticação com Múltiplo Fator de Autenticação (MFA), admitindo-se, quando tecnicamente viável e houver disponibilidade orçamentária específica, o uso de certificado digital padrão ICP-Brasil;**

II – Criptografia avançada das senhas e informações previdenciárias;

III – Dupla autenticação para sistemas críticos;

IV – Monitoramento em tempo real pela Área de Tecnologia da Informação (CPD) do IPAM.

CAPÍTULO III

DA GESTÃO DE PESSOAS E CONTROLE DE ACESSO

Art. 10. Os procedimentos de segurança da informação previdenciária serão rigorosamente documentados e implementados, garantindo que todos os servidores, estagiários, terceirizados ou prestadores de serviços do IPAM que sejam transferidos, remanejados, promovidos ou desligados tenham todos os privilégios de acesso aos sistemas previdenciários devidamente revistos, modificados ou revogados.

Art. 11. No afastamento, mudança de atribuições ou transferência de servidores, será responsabilidade solidária do:

I – Chefe imediato: Comunicação imediata à Área de Tecnologia da Informação (CPD);

II – Setor de Gestão de Pessoas (GEAD): Formalização da alteração;

III – Controladoria Geral: Verificação da efetivação das restrições de acesso.

Art. 12. No desligamento definitivo de qualquer usuário, serão imediatamente suspensos todos os direitos de acesso, sendo que:

I – Dados previdenciários produzidos serão mantidos sob custódia da Controladoria Geral;

II – Senhas serão imediatamente alteradas em todos os sistemas;

III – Equipamentos serão periciados antes da devolução.

Art. 13. A instalação de softwares não autorizados nos equipamentos do IPAM sujeitará o usuário:

I – À responsabilização civil por danos aos sistemas previdenciários;

II – Às penalidades disciplinares previstas na **Lei Complementar nº 385/2010 (Estatuto dos Servidores Públicos do Município de Porto Velho)**;

III – Ao ressarcimento de eventuais multas e licenças irregulares.

Art. 14. Somente serão instalados no IPAM softwares licenciados e previamente aprovados pela SMTI e Controladoria Geral, com registro atualizado junto ao fabricante.

CAPÍTULO IV

DO CONTROLE INTERNO E AUDITORIA

Art. 15. A Controladoria Geral do IPAM, em conformidade com o Art. 8.3.1 e 8.3.2 da Lei Complementar nº 385/2010, monitorará a conformidade destas diretrizes, podendo:

I – Auditar acessos remotos a qualquer tempo;

II – Verificar logs de atividades em sistemas previdenciários;

III – Aplicar medidas corretivas imediatas;

IV – Propor melhorias nos controles de segurança.

Art. 16. Os relatórios de auditoria de acesso remoto serão trimestrais e encaminhados à Diretoria de Presidência.

Art. 17. Violações às diretrizes serão comunicadas imediatamente ao Ministério Público e órgãos de controle externo, quando envolverem dados previdenciários sensíveis.

CAPÍTULO V

DA CONFORMIDADE COM LGPD E SIGILO PREVIDENCIÁRIO

Art. 18. Todos os acessos remotos aos sistemas do IPAM devem observar rigorosamente:

I – A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais);

II – O sigilo previdenciário previsto na legislação;

III – As normas específicas do Conselho Nacional de Previdência Social;

IV – As diretrizes da Autoridade Nacional de Proteção de Dados (ANPD).

Art. 19. Qualquer vazamento de dados previdenciários via acesso remoto sujeitará o responsável às sanções administrativas, civis e criminais cabíveis.

Art. 20. A SMTI e o IPAM implementarão medidas técnicas adicionais sempre que identificados riscos à proteção de dados dos segurados.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 21. 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. 22. 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. 23. 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. 24. 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. 25. Esta Portaria entra em vigor na data de sua publicação.

CLAUDINEIA ARAÚJO DE OLIVEIRA BORTOLETE
Diretora-Presidente

011.000253/2026-00	0673907v7

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 **0674575** e o código CRC **8B028F2C**.

011.000253/2026-00	0674575v4