CIDADE DE PORTO VELHO

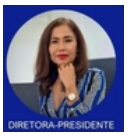
PREVIDÊNCIA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

www.ipam.ro.gov.br

2025, Instituto de Previdência e Assistência dos Servidores do Município de Porto Velho

Diretora Presidente
Claudinéia Araújo de Oliveira Bortolete



Coordenador Administrativo e Financeiro
Júlio Cesar de Souza Ferreira

Coordenador de Previdência
Orisvaldo Bezerra de Sales

Coordenadora de Assistência Médica
Priscilla Bezerra Giroto Farias Lima

Coordenadora Técnica
Odalice Pereira da Silveira Tinoco

Grupo de Trabalho Responsável pela Implementação e Acompanhamento do Programa de Certificação Institucional e Modernização da Gestão de Regimes Próprios de Previdência Social - de Trabalho Pro-Gestão-IPAM

Marcelo Augusto Mendes Barbosa - Presidente
Maria Irisney Barbosa de Souza - Membra
Marivaldo Rosa da Silva - Membro
Ruanne Emely Borges Celestino - Membra
Diego Ferrucio Marqueti - membro
Odilon José de Santana Júnior

Portaria 110/2026 IPAM-DRFP
https://transparencia-ipam.portovelho.ro.gov.br/storage/portarias/portarias-2026/fevereiro/portaria-n-110-de-24-de-fevereiro-de-2026-aprova-e-institui-manuais-politicas-e-instrumentos-normativos-institucionais-do-ipam.pdf

Mensagem da Presidente

Prezados Servidores, Segurados e Beneficiários,
A segurança da informação no Instituto de Previdência e Assistência dos Servidores do Município de Porto Velho (IPAM) não é apenas uma exigência legal, mas um compromisso ético com todos que confiam em nossa instituição a proteção de seus dados pessoais e a gestão de seus direitos previdenciários.

Como gestora do regime próprio de previdência municipal, assumo o compromisso de implementar uma Política de Segurança da Informação rigorosa e eficaz, alinhada à Lei Geral de Proteção de Dados (LGPD) e aos critérios do Programa Pro-Gestão Nível II. Esta política protege informações sensíveis de mais de 15 mil segurados ativos, inativos e dependentes, garantindo confidencialidade, integridade e disponibilidade dos dados que processamos diariamente.

Nossa estratégia de segurança fundamenta-se em três pilares essenciais: prevenção contra ameaças cibernéticas e acessos não autorizados; conformidade integral com a legislação vigente, especialmente LGPD e normas previdenciárias; e cultura organizacional que valoriza a proteção da informação como responsabilidade de todos.

Implementamos controles rígidos de acesso, monitoramento contínuo dos sistemas, backups seguros e protocolos de resposta a incidentes. Nossos servidores recebem capacitação regular sobre práticas seguras, e mantemos interface permanente com órgãos reguladores e de controle.

A efetividade desta política depende do engajamento de todos. Cada servidor, terceirizado ou colaborador é responsável por aplicar as diretrizes estabelecidas, reportar irregularidades e manter-se atualizado sobre as melhores práticas de segurança.

Reafirmo nosso compromisso com a transparência através de relatórios periódicos de conformidade e canais diretos de comunicação. A Controladoria Geral e a Ouvidoria estão à disposição para esclarecer dúvidas e receber sugestões sobre nossa política de segurança.

A segurança da informação é fundamental para a sustentabilidade do IPAM. Proteger dados significa proteger direitos, assegurar benefícios e manter a confiança pública na gestão previdenciária. É nossa obrigação legal, ética e institucional.

Convido todos a serem protagonistas desta cultura de segurança. Juntos, fortalecemos o IPAM como uma instituição moderna, confiável e alinhada às melhores práticas nacionais de gestão previdenciária.

Claudinéia Araújo de Oliveira Bortolete
Diretora Presidente Instituto de Previdência e Assistência dos Servidores do Município de Porto Velho

1. IDENTIFICAÇÃO INSTITUCIONAL

Sobre o IPAM

Denominação: Instituto de Previdência e Assistência dos Servidores do Município de Porto Velho – IPAM
CNPJ: 34.481.804/0001-71

Endereço: Av. Carlos Gomes, nº 1645, Bairro São Cristóvão, CEP: 76.804.086, Porto Velho - RO

Contatos:

- E-mail Institucional: ipam@ipam.ro.gov.br
- Página eletrônica: https://ipam.portovelho.ro.gov.br/
- Portal da Transparência: https://transparencia-ipam.portovelho.ro.gov.br/
- Telefone: (69) 2181-1342

Natureza Jurídica: Autarquia dotada de personalidade jurídica de direito público, com autonomia administrativa, financeira e patrimonial.

2. CONTEXTO HISTÓRICO E LEGAL

O Instituto de Previdência e Assistência dos Servidores do Município de Porto Velho – IPAM foi criado pela Lei Complementar nº 001, de 23 de julho de 1990, sendo instituído como órgão gestor único do Regime Próprio de Previdência Social de Porto Velho.
Base Legal Consolidada:
Decreto nº 4.123 de 18 de Outubro de 1990
Lei Complementar nº 271 de 22 de dezembro de 2006
Lei Complementar nº 146 de 21 de agosto de 2002
Lei Complementar nº 147 de 21 de agosto de 2002
Lei Complementar nº 706 de 28 de dezembro de 2017
Lei Complementar nº 886 de 11 de março de 2022
Lei Complementar nº 898 de 28 de abril de 2022
Lei Complementar nº 943 de 12 de julho de 2023
Lei Complementar nº 940 de 14 junho de 2023
Lei Complementar nº 952 de 12 de setembro de 2023

2. DIRETRIZES ORGANIZACIONAIS

2.1 MISSÃO ORGANIZACIONAL

Conceder e gerir com qualidade e responsabilidade aos segurados e seus dependentes, Benefícios Previdenciários e Serviços de Assistência à Saúde, fornecendo informações e soluções adequadas trabalhando com transparência, zelando pelo princípio da administração pública no que diz respeito à legalidade, impessoalidade, moralidade, publicidade e eficiência no Regime Próprio de Previdência Social do Município de Porto Velho.

2.2 VISÃO ORGANIZACIONAL

Ser um Instituto modelo na gestão de Regimes Próprios de Previdência Social no Estado de Rondônia. Nossa meta é ser um referencial no equilíbrio financeiro e atuarial previdenciário, ser um marco em gestão transparente, humana e participativa, com tecnologia atualizada para dar melhores condições e informações aos nossos segurados, dependentes e servidores do IPAM. Além de oferecer condições que proporcionem a valorização dos mesmos e seus beneficiários.

3.3 VALORES INSTITUCIONAIS

- **Respeito ao cidadão e compromisso com os segurados e seus dependentes**
- **Elevado sentido ético de serviço público**
- **Honestidade, integridade e justiça**
- **Desempenhar as atividades orientadas pelos resultados**
- **Manter espírito de colaboração mútua em equipe**
- **Transparência e eficiência nos atos administrativos**
- **Capacidade institucional de gestão e inovação**
- **Qualidade, excelência, competência e ética profissional**

3.INTRODUÇÃO

3.1 APRESENTAÇÃO E OBJETIVOS DO GUIA

A segurança da informação representa um pilar fundamental para a sustentabilidade e a confiabilidade das operações do Instituto de Previdência e Assistência do Município de Porto Velho (IPAM). Em um cenário onde a informação é um ativo estratégico e os riscos cibernéticos são crescentes, proteger os dados e os sistemas é essencial para garantir a continuidade dos serviços, preservar a imagem da instituição e, acima de tudo, salvaguardar os interesses dos segurados e beneficiários. Este guia estabelece as diretrizes e os procedimentos necessários para fortalecer a postura de segurança da informação no IPAM, promovendo um ambiente digital mais seguro e resiliente.

Este documento está alinhado com os requisitos do Programa Pró-Gestão, especificamente na Dimensão de Controle Interno, buscando atender ao Nível II, que exige a indicação de regras normativas para o uso de recursos tecnológicos e a definição de procedimentos de contingência, incluindo cópias de segurança e controle de acesso. A implementação dessas diretrizes visa não apenas a conformidade regulatória, mas também a adoção das melhores práticas de governança e gestão de riscos.

A base legal e normativa para este guia inclui a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), que rege o tratamento de dados pessoais, as Instruções Normativas do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que fornecem diretrizes para a segurança da informação na administração pública federal, e a legislação municipal aplicável. Essas referências garantem que as ações e políticas de segurança da informação do IPAM estejam em conformidade com o arcabouço legal vigente, protegendo os direitos dos titulares de dados e a integridade dos sistemas governamentais.

Este Guia de Segurança da Informação do IPAM tem como objetivos principais:

- Definir Regras Claras de Uso: Estabelecer diretrizes explícitas para o uso adequado da internet, correio eletrônico, computadores e demais recursos tecnológicos do IPAM por todos os servidores, colaboradores e terceirizados.

- Garantir a Continuidade Operacional: Instituir procedimentos robustos de contingência, incluindo a existência e a gestão de cópias de segurança (backups) dos sistemas informatizados e bancos de dados, bem como a definição de planos de recuperação.

- Assegurar o Controle de Acesso: Implementar e manter controles de acesso físico e lógico eficazes, garantindo que apenas pessoas autorizadas tenham acesso às instalações, sistemas e informações sensíveis do IPAM;

- Proteger a Confidencialidade, Integridade e Disponibilidade: Salvaguardar as informações do IPAM contra acessos não autorizados, modificações indevidas ou perdas, assegurando que estejam disponíveis quando necessário;

- Promover a Conscientização: Fomentar uma cultura de segurança da informação entre todos os membros do IPAM, por meio de orientações e treinamentos contínuos;

- Mitigar Riscos: Identificar, avaliar e tratar os riscos de segurança da informação, minimizando a probabilidade e o impacto de incidentes;

- Atender à Conformidade Regulatória: Assegurar a aderência às leis e regulamentos pertinentes, como a Lei Geral de Proteção de Dados Pessoais (LGPD) e as normas de segurança da informação aplicáveis à administração pública;

- Cumprir os Requisitos do Pró-Gestão: Atender integralmente aos requisitos do Nível II da Dimensão de Controle Interno do Programa Pró-Gestão, fortalecendo a governança e a gestão institucional;

Este Guia de Segurança da Informação do IPAM estabelece as diretrizes e responsabilidades aplicáveis a todos os indivíduos que interagem com os ativos de informação da instituição, bem como aos próprios ativos. Seu escopo abrange de forma abrangente:

- Pessoas: Todos os servidores efetivos, comissionados, colaboradores, estagiários, prestadores de serviços terceirizados, consultores e qualquer outra pessoa, física ou jurídica, que tenha acesso ou utilize os recursos de informação do IPAM, independentemente do vínculo empregatício ou contratual;

- Ativos de Informação: Inclui todos os dados (em formato físico ou digital), sistemas informatizados, aplicativos, bancos de dados, redes de comunicação (internas e externas), equipamentos de hardware (computadores, notebooks, servidores, dispositivos móveis, impressoras, etc.), softwares, serviços de tecnologia da informação e infraestrutura tecnológica do IPAM;

Ambientes Físicos: As instalações físicas do IPAM, incluindo escritórios, salas de servidores, arquivos e quaisquer outras áreas onde informações ou ativos tecnológicos da instituição sejam armazenados, processados ou acessados.

Exclusões ou Exceções:

Não há exclusões gerais ao escopo deste guia. Qualquer exceção específica às diretrizes aqui estabelecidas deverá ser formalmente solicitada, justificada e aprovada pela área de Tecnologia da Informação e/ou pelo Comitê de Segurança da Informação do IPAM, sendo devidamente documentada e revisada periodicamente. O não cumprimento desta política, mesmo em casos de exceção não autorizada, estará sujeito às sanções cabíveis.

4. GLOSSÁRIO TÉCNICO

Para assegurar uma compreensão uniforme e evitar ambiguidades ao longo deste Guia de Segurança da Informação, esta seção apresenta um glossário de termos-chave, siglas e conceitos relevantes. O objetivo é padronizar a linguagem utilizada, facilitando a interpretação e a aplicação das diretrizes por todos os envolvidos.

Entre os termos que serão detalhados neste glossário, incluem-se conceitos fundamentais como Confidencialidade, Integridade e Disponibilidade, que são os pilares da segurança da informação. Também serão abordadas definições específicas relacionadas à proteção de dados pessoais, como Dado Pessoal, Titular do Dado e Tratamento, em conformidade com a legislação vigente. Outros termos técnicos e operacionais importantes, como Acesso Físico, Acesso Lógico, Contingência, Malware, Phishing, entre outros, também serão explicados para garantir clareza nas políticas e procedimentos.

Para a elaboração destas definições, recomenda-se fortemente a consulta e o uso das terminologias estabelecidas pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e pelo Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). A adoção dessas fontes oficiais garante a consistência e a validade das definições, alinhando o IPAM às melhores práticas e exigências regulatórias nacionais.

Para facilitar a compreensão e a aplicação das diretrizes contidas neste Guia de Segurança da Informação, são apresentados a seguir os termos e conceitos mais relevantes. As definições buscam alinhar-se com a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

- **Acesso Físico:** Refere-se à capacidade de entrar em instalações, salas ou áreas restritas onde ativos de informação (como computaores, servidores, equipamentos de rede ou documentos físicos) estão localizados. O controle de acesso físico visa impedir a entrada de pessoas não autorizadas;

- **Acesso Lógico:** Refere-se à capacidade de interagir com sistemas, redes, aplicativos e dados por meio de credenciais digitais (usuário e senha, certificados, biometria). O controle de acesso lógico visa garantir que apenas usuários autorizados e com os privilégios corretos possam acessar recursos digitais;

- **Confidencialidade:** Propriedade que garante que a informação não esteja disponível ou não seja divulgada a indivíduos, entidades ou processos não autorizados. É um dos pilares da segurança da informação;

- **Contingência:** Conjunto de medidas e planos desenvolvidos para permitir que uma organização continue suas operações críticas ou as restabeleça rapidamente após a ocorrência de um incidente, falha ou desastre. Determinando a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados, o controle de acesso (físico e lógico) e a área responsável por elas, estando esses procedimentos mapeados e manualizados. Deverá contar com servidor ou área de Gestão da Segurança da Informação, no âmbito do ente federativo ou do RPPS, com a responsabilidade de: Prover todas as informações de Gestão de Segurança da Informação da unidade gestora do RPPS; prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os servidores e prestadores de serviços; propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação; elaborar e manter política de classificação da informação, com temporalidade para guarda;

- **Dado Pessoal**: Informação relacionada a pessoa natural identificada ou identificável. (Conforme LGPD, Art. 5º, I);

- **Disponibilidade:** Propriedade que garante que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. É um dos pilares da segurança da informação;

- **Integridade:** Propriedade que garante que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, e que está completa e precisa. É um dos pilares da segurança da informação;

- **Malware (Software Malicioso):** Termo genérico para qualquer software projetado para se infiltrar, danificar ou desabilitar sistemas de está completa e precisa. É um dos pilares da segurança da informação.

- **Phishing:** Tipo de ataque de engenharia social que tenta enganar os usuários para que revelem informações confidenciais (como senhas ou dados bancários) ou instalem malware, geralmente por meio de e-mails, mensagens ou sites falsos que se passam por entidades legítimas;

- **Spam:** Mensagens eletrônicas não solicitadas, geralmente enviadas em massa, com fins comerciais, fraudulentos ou maliciosos.

- **Titular do Dado:** Conforme a LGPD, é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- **Tratamento:** Conforme a LGPD, é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

5. PRINCÍPIOS E DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação no IPAM é guiada por um conjunto de princípios e diretrizes que norteiam todas as ações e decisões relacionadas à proteção dos ativos de informação. Estes fundamentos são essenciais para estabelecer uma cultura de segurança robusta e garantir que os objetivos institucionais sejam alcançados de forma segura.

5.1 PRINCÍPIOS FUNDAMENTAIS DA SEGURANÇA DA INFORMAÇÃO (CID)

(C)Confidencialidade: Assegurar que a informação seja acessível somente por pessoas autorizadas. Isso implica proteger dados sensíveis contra divulgação não autorizada, seja por acesso físico, lógico ou por meio de engenharia social.

(I) Integridade: Garantir que a informação seja precisa, completa e não tenha sido alterada de forma não autorizada. A integridade assegura que os dados permaneçam fidedignos e confiáveis ao longo de todo o seu ciclo de vida.

(D) Disponibilidade: Assegurar que os usuários autorizados tenham acesso à informação e aos ativos relacionados quando necessário. A disponibilidade é crucial para a continuidade dos serviços e operações do IPAM, prevenindo interrupções por falhas técnicas ou ataques.

5.2 CONFORMIDADE LEGAL E REGULATÓRIA:

O IPAM compromete-se a operar em estrita conformidade com todas as leis, regulamentos e normas aplicáveis à segurança da informação e proteção de dados. Isso inclui, mas não se limita à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), às Instruções Normativas do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e a outras legislações setoriais ou municipais pertinentes. A conformidade é monitorada e revisada periodicamente para garantir a adequação contínua.

5.3 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO:

A segurança da informação no IPAM é abordada de forma proativa, por meio de um processo contínuo de gestão de riscos. Este processo envolve a identificação, análise, avaliação e tratamento dos riscos que podem comprometer a confidencialidade, integridade e disponibilidade dos ativos de informação. As ações de tratamento visam mitigar, transferir, aceitar ou evitar os riscos a níveis aceitáveis, priorizando a proteção dos ativos mais críticos.

5.4 CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO:

Reconhecendo que o fator humano é um elo crucial na cadeia de segurança, o IPAM investe em programas contínuos de conscientização e treinamento. O objetivo é educar todos os servidores, colaboradores e terceirizados sobre as políticas de segurança, as ameaças existentes e as melhores práticas para proteger as informações. A participação ativa e responsável de cada indivíduo é fundamental para o sucesso da estratégia de segurança da instituição.

6. DECLARAÇÃO DA POLÍTICA E REQUISITOS ESPECÍFICOS

Esta seção detalha as políticas e os requisitos específicos que o IPAM adota para garantir a segurança da informação, em alinhamento com as melhores práticas. As declarações aqui apresentadas servem como normas mandatórias para todos os que interagem com os ativos de informação da instituição.

6.1. REGRAS NORMATIVAS PARA O USO DE RECURSOS TECNOLÓGICOS

O uso dos recursos tecnológicos do IPAM deve ser pautado pela responsabilidade, ética e em conformidade com as diretrizes de segurança da informação estabelecidas. Estas regras visam proteger a infraestrutura, os dados e a reputação da instituição, garantindo que os recursos sejam utilizados para fins institucionais e de forma segura.

6.1.1. Uso da Internet:

A navegação na internet utilizando a infraestrutura do IPAM deve ser realizada de forma consciente e profissional.

- **Diretrizes para Navegação e Downloads**: É permitido o acesso a sites e serviços que sejam relevantes para o desempenho das atividades laborais. O acesso a conteúdos que possam comprometer a segurança da rede (como sites maliciosos, de conteúdo adulto, jogos online ou de pirataria) é estritamente proibido. Downloads de arquivos e softwares devem ser restritos a fontes confiáveis e autorizadas, preferencialmente por meio dos sistemas e repositórios oficiais do IPAM, para evitar a introdução de malware e outras ameaças;

- **Uso de Redes Sociais e Serviços de Streaming:** O uso de redes sociais e serviços de streaming (áudio e vídeo) para fins pessoais durante o horário de trabalho é desencorajado, devendo ser minimizado e não interferir nas atividades profissionais, nem comprometer a largura de banda da rede ou a segurança. Conteúdos que possam denegrir a imagem do IPAM ou de seus colaboradores são proibidos;

- **Monitoramento do Uso da Internet:** O IPAM reserva-se o direito de monitorar o tráfego de internet, os sites acessados e os downloads realizados em sua rede, com o objetivo de garantir a segurança, o cumprimento das políticas e a otimização dos recursos. Este monitoramento será realizado em conformidade com a legislação vigente e com a política de privacidade da instituição.

6.1.2. Uso do Correio Eletrônico:

O correio eletrônico institucional é uma ferramenta de trabalho e seu uso deve refletir o profissionalismo e a segurança.

- **Padrões de Uso para E-mails Institucionais:** Os e-mails institucionais devem ser utilizados exclusivamente para comunicação relacionada às atividades do IPAM. É vedado o envio de correntes, mensagens de cunho pessoal excessivo, material publicitário não autorizado ou qualquer conteúdo que não esteja alinhado aos objetivos da instituição;

- **Proibição de Envio de Informações Confidenciais sem Criptografia:** Informações classificadas como confidenciais ou sensíveis não devem ser enviadas por e-mail sem a devida proteção, como criptografia ou uso de canais seguros. A responsabilidade pela proteção da informação é do remetente;

- **Uso de E-mails Pessoais em Equipamentos Institucionais:** O acesso a contas de e-mail pessoais em equipamentos do IPAM é desencorajado, e, quando permitido, deve ser feito com cautela e sem comprometer a segurança da rede ou dos dados institucionais. O IPAM não se responsabiliza pela segurança de dados pessoais em contas de e-mail não institucionais;

- **Conscientização sobre Phishing e Spam:** Todos os usuários devem estar vigilantes quanto a e-mails suspeitos (phishing) e mensagens não solicitadas (spam). É proibido clicar em links ou abrir anexos de e-mails de remetentes desconhecidos ou com conteúdo duvidoso. Qualquer suspeita deve ser reportada imediatamente à área de TI.

6.1.3. Uso de Computadores e Dispositivos (Notebooks, Smartphones, Tablets):

Os equipamentos fornecidos pelo IPAM são ferramentas de trabalho e devem ser utilizados com responsabilidade e cuidado:

- **Responsabilidades sobre Equipamentos Institucionais:** Cada usuário é responsável pela guarda, integridade e segurança física e lógica dos equipamentos institucionais sob sua custódia. Danos, perdas ou furtos devem ser comunicados imediatamente à área de TI e à gestão;

- **Instalação de Softwares (Permitidos/Proibidos):** A instalação de softwares em equipamentos do IPAM é restrita à área de TI. É proibida a instalação de programas não autorizados, shareware, freeware ou qualquer software que não possua licença válida ou que não seja essencial para as atividades laborais;

- **Uso de Dispositivos Pessoais em Ambiente de Trabalho (BYOD - Bring Your Own Device, se aplicável):** Caso o IPAM adote uma política de BYOD, diretrizes específicas serão estabelecidas para o uso de dispositivos pessoais na rede e para o acesso a dados institucionais, garantindo a segurança da informação. Nesses casos, o usuário concorda com a aplicação de controles de segurança e monitoramento;

- **Proteção Física dos Dispositivos:** Os dispositivos devem ser protegidos contra acesso não autorizado, roubo e danos físicos. Isso inclui o uso de senhas de bloqueio de tela, não deixar equipamentos desacompanhados em locais públicos e garantir o armazenamento seguro após o expediente.

6.1.4. Uso de Outros Recursos Tecnológicos:

Outros recursos tecnológicos também estão sujeitos a diretrizes de segurança.

- **Impressoras, Scanners, Softwares Específicos:** O uso de impressoras, scanners e softwares específicos deve seguir as orientações da área de TI e as políticas de uso consciente, evitando o desperdício e a exposição indevida de informações. Documentos confidenciais não devem ser deixados em impressoras ou scanners;

- **Armazenamento em Nuvem (Públicas/Privadas):** O armazenamento de dados institucionais em serviços de nuvem deve ser feito exclusivamente em plataformas autorizadas pelo IPAM. É proibido o uso de serviços de nuvem pessoais (públicas) para armazenar, compartilhar ou processar informações confidenciais ou sensíveis da instituição.

6.1.5. Proibições e Restrições:

Certos comportamentos e ações são estritamente proibidos para manter a segurança e a integridade do ambiente do IPAM:

- **Atividades Ilegais ou Antiéticas:** É proibida a utilização dos recursos tecnológicos do IPAM para qualquer atividade ilegal, antiética, discriminatória, ofensiva ou que viole direitos autorais e de propriedade intelectual;

- **Instalação de Softwares Não Autorizados:** Conforme mencionado, é expressamente proibida a instalação de qualquer software em equipamentos do IPAM sem a prévia autorização e instalação pela área de TI;

- **Compartilhamento de Senhas:** O compartilhamento de senhas de acesso a sistemas, redes ou equipamentos é terminantemente proibido. Cada senha é pessoal e intransferível, e o usuário é o único responsável pelas ações realizadas com suas credenciais.

6.2 CONTROLE DE ACESSO (FÍSICO LÓGICO)

O controle de acesso é fundamental para garantir que apenas indivíduos autorizados tenham permissão para acessar os ativos de informação do IPAM, sejam eles físicos ou digitais. Esta política estabelece as diretrizes para gerenciar e monitorar o acesso, protegendo a confidencialidade, integridade e disponibilidade dos dados e sistemas da instituição.

6.2.1. Controle de Acesso Físico:

O controle de acesso físico visa proteger as instalações e os equipamentos do IPAM contra acessos não autorizados, danos, roubos ou uso indevido.

- **Acesso às Instalações do IPAM:** O acesso às dependências do IPAM é restrito a servidores, colaboradores, estagiários e visitantes devidamente identificados e autorizados. Todos os indivíduos devem portar sua identificação funcional ou de visitante em local visível durante sua permanência nas instalações;

- **Acesso a Áreas Restritas:** Áreas que contêm ativos de informação críticos, como salas de computadores e servidores, arquivos físicos com documentos sensíveis e salas de controle, possuem controles de acesso físico mais rigorosos. O acesso a essas áreas é limitado a pessoal autorizado e essencial para a operação, com registro de entrada e saída;

- **Uso de Crachás, Biometria e Chaves:** O controle de acesso físico pode ser implementado através de diversos mecanismos, incluindo o uso obrigatório de crachás de identificação, sistemas de controle de acesso biométrico (digitais, faciais, etc.) para áreas de alta segurança e o gerenciamento rigoroso de chaves para portas e armários que contenham informações confidenciais. A perda ou extravio de qualquer um desses meios de acesso deve ser comunicada imediatamente.

6.2.2. Controle de Acesso Lógico:

O controle de acesso lógico regula quem pode acessar sistemas, redes, bancos de dados e informações digitais, e o que podem fazer com esses recursos.

- **Acesso a Sistemas, Redes, Bancos de Dados e Informações:** O acesso aos recursos digitais do IPAM é concedido com base na necessidade de trabalho e na função de cada usuário. Todos os acessos são individualizados e rastreáveis, exigindo autenticação para garantir a identidade do usuário;

Princípio do Menor Privilégio: A concessão de acesso lógico deve seguir o princípio do menor privilégio, ou seja, cada usuário deve ter apenas o nível de acesso mínimo necessário para desempenhar suas funções. Privilégios adicionais são concedidos apenas mediante solicitação formal e aprovação, e são revisados periodicamente.

Gestão de Senhas e Autenticação:

- **Complexidade:** As senhas devem atender a requisitos mínimos de complexidade, incluindo comprimento mínimo, uso de caracteres maiúsculos, minúsculos, números e símbolos;

- **Troca Periódica:** Os usuários são obrigados a trocar suas senhas periodicamente, conforme política de segurança estabelecida, para reduzir o risco de comprometimento;

- **Autenticação Multifator (MFA):** Para sistemas e informações consideradas de alto risco, a autenticação multifator (MFA) pode ser exigida, adicionando uma camada extra de segurança além da senha;

- **Segregação de Funções:** A segregação de funções é implementada para evitar que uma única pessoa tenha controle sobre todas as etapas de um processo crítico, o que poderia levar a fraudes ou erros. As responsabilidades e privilégios de acesso são distribuídos entre diferentes indivíduos para garantir a verificação e o controle mútuo.

6.2.3. Gestão de Identidades e Credenciais:

A gestão eficaz de identidades e credenciais é crucial para manter o controle sobre quem tem acesso aos recursos do IPAM.

- **Criação, Modificação e Exclusão de Contas de Usuário:** O processo de criação de novas contas de usuário é formalizado, exigindo aprovação e baseando-se na necessidade de acesso. Modificações em perfis de acesso são realizadas apenas mediante solicitação justificada. A exclusão ou desativação de contas é imediata em casos de desligamento do colaborador ou mudança de função que elimine a necessidade de acesso;

- **Revisão Periódica de Acessos:** Auditorias e revisões periódicas dos privilégios de acesso são realizadas para verificar se os direitos concedidos ainda são apropriados e necessários para as funções atuais dos usuários. Acessos indevidos ou desnecessários são prontamente removidos.

6.2.4 Controles Específicos de Comunicação e Acesso Externo

- **Canal Corporativo via WhatsApp - Proibições**
  - É vedado o uso de WhatsApp pessoal para comunicações oficiais do IPAM, incluindo grupos informais entre servidores para tratar de assuntos institucionais;
  - Qualquer canal via WhatsApp deve ser previamente aprovado pela Diretoria e gerenciado exclusivamente pela área de Tecnologia da Informação.
- **Diretrizes para o Canal Ofícial**
  - Caso seja instituído canal corporativo via WhatsApp, deve utilizar WhatsApp Business com número institucional;
  - Implementação de criptografia ponta a ponta e backup seguro das conversas;
  - Monitoramento periódico do conteúdo para garantir conformidade com LGPD;
  - Treinamento obrigatório dos usuários sobre uso adequado da ferramenta.
- **E-mails Setoriais Não Institucionais - proibição absoluta**
  - É expressamente proibido o uso de e-mails pessoais ou não institucionais (ex.: gefin@gmail.com, coordenacao@hotmail.com) para comunicações oficiais do IPAM;
  - Toda comunicação oficial deve utilizar exclusivamente endereços corporativos (@ipam.ro.gov.br).
- **Sanções**
  - O descumprimento sujeitará o servidor às penalidades previstas no art. 6.4.3 da Lei Complementar nº 886/2022;
  - Responsabilização por eventual vazamento de dados previdenciários sensíveis.
- **Acessos a Instituições Bancárias - Controles Obrigatórios**
  - Acesso ao Auto Atendimento de instituições bancárias (ex.: Banco do Brasil) restrito a Gerentes e Chefes previamente autorizados;
  - Dupla autenticação obrigatória para todos os acessos bancários;
  - Log detalhado de todas as operações realizadas, com revisão mensal pela Controladoria.

- **Vedações**
  - Proibido compartilhamento de credenciais bancárias entre servidores;
  - Vedado uso de dispositivos pessoais para acesso a sistemas bancários institucionais;
  - Não permitido acesso remoto a sistemas bancários fora das dependências do IPAM, salvo emergência prévia autorizada.
- **Procedimentos**
  - Credenciais bancárias devem ser renovadas trimestralmente;
  - Supervisão da área de TI e Controle Interno em todos os acessos;
  - Notificação imediata de qualquer irregularidade detectada.
- **Criação de Usuários para Sistemas da Prefeitura - Competência Excusiva**
  - A criação de usuários e senhas para sistemas municipais (GPI tributário, Orçamentário, Financeiro) é competência exclusiva da área de TI do IPAM;
  - Vedada a criação direta por chefias ou estagiários.
- **Procedimentos para Estagiários**
  - Solicitação formal da chefia imediata com justificativa detalhada;
  - Aprovação prévia do Controlador Geral;
  - Acessos temporários com prazo máximo equivalente ao período do estágio;
  - Princípio do menor privilégio: acesso apenas aos módulos estritamente necessários.
- **Requisitos de Segurança**
  - Senhas complexas: mínimo 12 caracteres, incluindo maiúsculas, minúsculas, números e símbolos especiais;
  - Expiração automática a cada 60 dias;
  - Bloqueio após 3 tentativas incorretas de login;
  - Auditoria mensal de todos os acessos concedidos.
- **Responsabilização**
  - Chefes responsáveis pelos acessos concedidos a seus estagiários;
  - Monitoramento contínuo das atividades realizadas;
  - Revogação imediata em caso de término do estágio ou irregularidade.

Violações:

- Criação não autorizada de usuários sujeitará o responsável a processo administrativo disciplinar;
- Responsabilização civil e criminal por eventual prejuízo ao erário ou vazamento de dados.

6.3. PROCEDIMENTOS DE CONTINGÊNCIA E RECUPERAÇÃO DE DESASTRES

A capacidade de o IPAM manter suas operações e recuperar-se de incidentes, falhas ou desastres é um pilar essencial da segurança da informação e da continuidade dos serviços. Esta política estabelece as diretrizes para a criação e manutenção de cópias de segurança e para a execução de planos de recuperação, garantindo a disponibilidade dos sistemas e dados críticos.

6.3.1. Cópias de Segurança (Backup):

As cópias de segurança são a primeira linha de defesa contra a perda de dados e a interrupção de serviços. Sua gestão deve ser rigorosa e sistemática.

- **Definição de Dados e Sistemas a Serem Copiados:** Todas as informações consideradas críticas para as operações do IPAM devem ser incluídas no escopo das cópias de segurança. Isso abrange, mas não se limita a, sistemas informatizados essenciais, bancos de dados de segurados e beneficiários, documentos digitais de gestão, arquivos de configuração de rede e sistemas operacionais. A identificação e classificação desses ativos são realizadas em conjunto pela área de TI e pelos gestores das áreas de negócio;

- **Frequência e Tipos de Backup:** 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. Isso pode incluir:

    - *Backup Diário:*Para dados e sistemas com alta taxa de alteração e criticidade;

    - *Backup Semanal:*Para sistemas e dados que necessitam de um ponto de recuperação semanal;

    - *Backup Mensal:* Para cópias de segurança de longo prazo ou de sistemas mais estáveis;

- *Tipos de Backup:* Serão utilizados backups completos, diferenciais (copiam dados alterados desde o último backup completo) e incrementais (copiam dados alterados desde o último backup, seja ele completo ou incremental), otimizando o tempo de execução e o espaço de armazenamento.

- **Local de Armazenamento:** Para garantir a proteção contra desastres localizados, as cópias de segurança serão armazenadas em múltiplos locais:

  - *Cópias On-site:* Armazenadas dentro das instalações do IPAM, mas em local fisicamente separado dos sistemas de produção, para recuperação rápida em caso de falhas menores;

  - *Cópias Off-site:* Armazenadas em um local externo, seguro e fisicamente distante das instalações principais do IPAM, para proteção contra desastres maiores (incêndios, inundações, etc.). O transporte e o armazenamento off-site devem seguir rigorosos protocolos de segurança e criptografia;

  - *Retenção de Cópias:* Será definida uma política de retenção de cópias de segurança, especificando o período mínimo pelo qual cada tipo de backup deve ser guardado, em conformidade com requisitos legais, regulatórios e necessidades de negócio do IPAM. Cópias de longo prazo serão mantidas para fins de auditoria e conformidade.

6.3.2. Recuperação de Dados e Sistemas (Restore):

A existência de backups é ineficaz sem a capacidade de restaurá-los com sucesso.

- **Processos de Restauração:** Serão desenvolvidos e documentados procedimentos detalhados para a restauração de dados e sistemas a partir das cópias de segurança. Estes processos incluirão a ordem de recuperação dos sistemas, a configuração de ambientes alternativos e a verificação da integridade dos dados restaurados;

- **Testes Periódicos de Recuperação:** A eficácia dos backups e dos procedimentos de restauração será validada por meio de testes periódicos. Esses testes simularão cenários de falha e desastre, garantindo que os dados possam ser recuperados e os sistemas restabelecidos dentro dos tempos de recuperação esperados (RTO - Recovery Time Objective) e com a perda máxima de dados aceitável (RPO - Recovery Point Objective). Os resultados dos testes serão documentados e as melhorias necessárias implementadas.

6.3.3. Planos de Continuidade de Negócios e Recuperação de Desastres (PCN/PRD):

O IPAM reconhece a importância estratégica de possuir planos formais para garantir a continuidade de suas operações e a recuperação de sua infraestrutura tecnológica em situações de crise.

- **Visão Geral da Existência e Importância desses Planos para o IPAM:** O IPAM manterá um Plano de Continuidade de Negócios (PCN) e um Plano de Recuperação de Desastres (PRD) devidamente documentados, aprovados e comunicados. O PCN visa assegurar que as funções essenciais do IPAM possam continuar a ser executadas durante e após um incidente disruptivo, enquanto o PRD foca na recuperação da infraestrutura de TI. A existência desses planos demonstra o compromisso do IPAM com a resiliência operacional, a proteção dos dados dos segurados e a manutenção da prestação de serviços mesmo diante de adversidades. Ambos os planos serão revisados e testados regularmente.

6.4. RESPONSABILIDADES

A segurança da informação no IPAM é uma responsabilidade compartilhada por todos os indivíduos que interagem com os ativos da instituição. Contudo, para garantir a efetividade das políticas e procedimentos, é essencial que as atribuições específicas de cada nível hierárquico e função sejam claramente definidas. Esta seção detalha as responsabilidades de cada parte envolvida na manutenção de um ambiente seguro.

6.4.1. Comitê de Segurança da Informação (CSI):

O Comitê de Segurança da Informação (CSI), se instituído no IPAM, atua como o órgão consultivo e deliberativo de alto nível para todas as questões relacionadas à segurança da informação.

- **Atribuições:**
    - Definir e aprovar as diretrizes estratégicas e as políticas de segurança da informação do IPAM;
    - Monitorar e avaliar o nível de risco de segurança da informação da instituição;

- Aprovar planos de ação para tratamento de riscos e incidentes de segurança;
- Promover a cultura de segurança da informação em todos os níveis do IPAM;
- Revisar e aprovar as políticas de conformidade legal e regulatória, incluindo a LGPD;
- Tomar decisões estratégicas relativas a investimentos em tecnologia e processos de segurança.

6.4.2. Área de Tecnologia da Informação (TI):

A Área de Tecnologia da Informação (TI) é a principal responsável pela implementação, manutenção e operação dos controles técnicos de segurança.

- **Responsabilidades:**
  - Implementar e manter os controles técnicos de segurança da informação, incluindo firewalls, sistemas de detecção de intrusão, antivírus e outras ferramentas de proteção;
  - Gerenciar a infraestrutura de rede e sistemas, garantindo sua segurança e disponibilidade;
  - Administrar e monitorar os processos de cópias de segurança (backup) e recuperação de dados;
  - Executar o controle de acesso lógico aos sistemas, redes e bancos de dados, conforme as políticas estabelecidas;
  - Responder a incidentes de segurança da informação, investigando, contendo e recuperando-se de ataques ou falhas;
  - Fornecer suporte técnico e orientação sobre segurança da informação aos usuários;
  - Manter a documentação técnica dos sistemas e procedimentos de segurança atualizada.

6.4.3. Encarregado de Dados (DPO):

O Encarregado de Dados (Data Protection Officer - DPO) é o profissional responsável por atuar como canal de comunicação entre o IPAM, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), com foco na Lei Geral de Proteitação de Dados Pessoais (LGPD).

- **Funções:**
    - Orientar e aconselhar o IPAM e seus colaboradores sobre as obrigações da LGPD e outras regulamentações de proteção de dados;
    - Atuar como ponto de contato para os titulares dos dados, recebendo e processando suas solicitações e reclamações;
    - Receber comunicações da ANPD e adotar as providências necessárias;
    - Realizar o monitoramento da conformidade do IPAM com a LGPD e outras normas de proteção de dados;
    - Colaborar na avaliação de riscos relacionados à proteção de dados pessoais e na implementação de medidas de segurança;
    - Gerenciar incidentes de segurança que envolvam dados pessoais, reportando-os conforme exigido pela LGPD.

6.4.4. Gestores:

Os gestores de cada área do IPAM têm um papel crucial na aplicação e disseminação das políticas de segurança da informação em seus respectivos departamentos.

- **Responsabilidade:**
    - Assegurar que suas equipes compreendam e cumpram integralmente as políticas e procedimentos de segurança da informação do IPAM;
    - Promover a conscientização sobre a importância da segurança da informação entre os membros de suas equipes;

- Identificar e reportar à área de TI quaisquer riscos ou vulnerabilidades de segurança observados em suas operações;
- Aprovar as solicitações de acesso a sistemas e informações para seus colaboradores, garantindo o princípio do menor privilégio;
- Garantir a proteção das informações e ativos sob sua responsabilidade, tanto em formato físico quanto digital.

6.4.5. Servidores e Colaboradores:

Todos os servidores, colaboradores, estagiários e terceirizados do IPAM são responsáveis pela segurança da informação em suas atividades diárias.

- **Deveres Individuais:**
  - Cumprir todas as políticas, normas e procedimentos de segurança da informação estabelecidos pelo IPAM;
  - Proteger suas credenciais de acesso (senhas, crachás) e não as compartilhar com terceiros;
  - Reportar imediatamente à área de TI quaisquer incidentes de segurança, suspeitas de violação ou vulnerabilidades;
  - Utilizar os recursos tecnológicos do IPAM de forma responsável, ética e exclusivamente para fins institucionais;
  - Participar ativamente dos programas de conscientização e treinamento em segurança da informação;
  - Proteger as informações confidenciais e sensíveis da instituição contra acesso, alteração ou divulgação não autorizada.

6.5 GESTÃO DE INCIDENTES DE SEGURANÇA

Mesmo com as melhores práticas de segurança implementadas, incidentes podem ocorrer. A capacidade de detectar, responder e se recuperar de forma eficaz é vital para minimizar danos, restaurar as operações e manter a confiança. Esta política estabelece o framework para a gestão de incidentes de segurança da informação no IPAM.

6.5.1 Processo de Detecção, Notificação e Resposta a Incidentes de Segurança:

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

    - **Detecção:** Monitoramento contínuo de sistemas, redes e logs para identificar atividades anômalas ou indicadores de comprometimento. Ferramentas de segurança (antivírus, firewall, sistemas de detecção de intrusão) e a vigilância dos usuários são essenciais para a detecção precoce;

    - **Notificação:** Qualquer servidor ou colaborador que identificar ou suspeitar de um incidente de segurança deve notificá-lo imediatamente à Área de Tecnologia da Informação (TI) ou ao Encarregado de Dados (DPO), conforme o tipo de incidente. A notificação deve incluir o máximo de detalhes possível sobre o ocorrido;

    - **Análise e Classificação:** A equipe de TI 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;

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

    - **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);

    - **Recuperação:** Os sistemas e dados afetados serão restaurados a um estado operacional seguro, utilizando as cópias de segurança e os procedimentos de recuperação estabelecidos. A recuperação deve garantir a integridade e a disponibilidade dos serviços.

6.5.2 Comunicação de Violações de Dados (ANPD, Titulares):

Em caso de violação de dados pessoais que possa acarretar risco ou dano relevante aos titulares, o IPAM seguirá rigorosamente as determinações da Lei Geral de Proteção de Dados Pessoais (LGPD).

- **Notificação à ANPD:** A Autoridade Nacional de Proteção de Dados (ANPD) será notificada sobre a violação em prazo razoável, conforme exigido pela legislação, contendo as informações necessárias sobre o incidente;

- **Comunicação aos Titulares:** 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;

6.5.3 Análise Pós-Incidente e Lições Aprendidas:

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:

- **Revisão do Incidente:** 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;

- **Identificação de Causas Raiz:** O objetivo é identificar as causas raiz do incidente, sejam elas falhas de processo, vulnerabilidades técnicas, erro humano ou outros fatores;

- **Plano de Ação:**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.

6.6. AUDITORIA E MONITORAMENTO

A auditoria e o monitoramento são atividades contínuas e fundamentais para garantir que as políticas e os controles de segurança da informação do IPAM estejam funcionando conforme o esperado, identificando não conformidades, vulnerabilidades e potenciais ameaças. Essas práticas contribuem para a melhoria contínua da postura de segurança da instituição.

6.6.1 Realização de Auditorias Internas e Externas:

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

- **Auditorias Internas:** Serão conduzidas periodicamente por equipes internas designadas ou por consultores independentes contratados. 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. Os resultados das auditorias internas serão reportados à alta direção e ao Comitê de Segurança da Informação (se houver) para a implementação de ações corretivas;

- **Auditorias Externas:** O IPAM poderá ser submetido a auditorias externas por órgãos reguladores, parceiros ou certificadoras, conforme a necessidade e os requisitos legais ou contratuais. 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.

6.6.2 Monitoramento de Logs e Eventos de Segurança:

O monitoramento proativo de logs e eventos é uma ferramenta crucial para a detecção precoce de atividades suspeitas e incidentes de segurança.

- **Coleta e Análise de Logs:** 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. Estes logs incluirão registros de acesso, tentativas de login (bem-sucedidas e falhas), alterações de configuração, atividades de usuários privilegiados e alertas de segurança;

- **Monitoramento Contínuo:** Os logs serão monitorados de forma contínua, utilizando ferramentas de Gerenciamento de Informações e Eventos de Segurança (SIEM - Security Information and Event Management) ou processos manuais, para identificar padrões incomuns, atividades não autorizadas ou potenciais violações de segurança;

- **Resposta a Alertas:** Alertas gerados pelo monitoramento de logs e eventos serão investigados prontamente pela Área de Tecnologia da Informação ou pela equipe de resposta a incidentes, seguindo os procedimentos estabelecidos na política de Gestão de Incidentes de Segurança;

- **Retenção de Logs:**Os logs de segurança serão retidos por um período definido, em conformidade com os requisitos legais e regulatórios, para fins de auditoria, investigação de incidentes e análise forense.

6.7. DIRETRIZES DO SMTI E ACESSO REMOTO

6.7.1 Fundamentação e Alinhamento Institucional

As diretrizes estabelecidas pela Superintendência Municipal de Tecnologia da Informação e Pesquisa (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).

6.7.2 Regras para Utilização do Serviço de Acesso Remoto Externo

As regras para utilização do serviço de acesso remoto externo à rede de dados da SMTI pelo IPAM visam à prevenção do acesso não autorizado às informações previdenciárias, evitando ameaças à integridade e sigilo das informações sensíveis dos segurados e beneficiários.

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

- Executem serviços corporativos vinculados às atividades previdenciárias do IPAM;
- Necessitem daquele acesso para execução de atividades externas relacionadas à gestão previdenciária;
- Sejam devidamente autorizados pelo Diretor Presidente ou Controlador Geral do IPAM;
- Sejam certificados pela SMTI quanto aos aspectos técnicos de segurança.

É expressamente vedada a utilização do acesso remoto para fins não relacionados às atividades previdenciárias do IPAM.

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

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).

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

- Nome completo e CPF do servidor;
- Cargo e lotação no IPAM;
- E-mail institucional (@ipam.ro.gov.br) e telefone corporativo;
- Sistema previdenciário específico a ser acessado (SISAM, SIGAP, etc.);
- Justificativa detalhada da necessidade previdenciária;
- Período de validade (máximo 30 dias, renovável);
- Aprovação expressa da chefia imediata e Controladoria.

O serviço de acesso remoto será automaticamente cancelado nas seguintes condições:

- Finalização do período especificado na solicitação;
- Perda da necessidade de utilização para atividades previdenciárias;
- Transferência, exoneração ou aposentadoria do servidor;
- Identificação de acesso irregular a dados previdenciários sensíveis;
- Violação às normas da LGPD ou sigilo previdenciário.

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

- Utilização obrigatória de certificado digital ICP-Brasil;
- Criptografia avançada das senhas e informações previdenciárias;
- Dupla autenticação para sistemas críticos;
- Monitoramento em tempo real pela área de TI do IPAM.

6.7.3 Gestão de Pessoas e Controle de Acesso

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.

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

- Chefe imediato: Comunicação imediata à área de TI;
- Setor de Gestão de Pessoas: Formalização da alteração;
- Controladoria: Verificação da efetivação das restrições de acesso.

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

- Dados previdenciários produzidos serão mantidos sob custódia da Controladoria;
- Senhas serão imediatamente alteradas em todos os sistemas;
- Equipamentos serão periciados antes da devolução.

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

- À responsabilização civil por danos aos sistemas previdenciários;
- Às penalidades disciplinares previstas na LC 886/2022;
- Ao ressarcimento de eventuais multas e licenças irregulares.

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

6.7.4 Controle Interno e Auditoria

A Controladoria do IPAM, em conformidade com o Art. 8.3.1 e 8.3.2 da LC 385/2010, monitorará a conformidade destas diretrizes, podendo:

- Auditar acessos remotos a qualquer tempo;
- Verificar logs de atividades em sistemas previdenciários;
- Aplicar medidas corretivas imediatas;
- Propor melhorias nos controles de segurança.

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

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

6.7.5 Conformidade com LGPD e Sigilo Previdenciário

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

- Lei Geral de Proteção de Dados (Lei 13.709/2018);
- Sigilo previdenciário previsto na legislação;
- Normas específicas do Conselho Nacional de Previdência Social;
- Diretrizes da Autoridade Nacional de Proteção de Dados.

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

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

7. DISPOSIÇÕES FINAIS

Esta seção conclui as Declarações da Política e Requisitos Específicos, estabelecendo a importância da sua manutenção contínua e as consequências do seu descumprimento. Ela reforça o compromisso do IPAM com a segurança da informação e a responsabilidade de todos os envolvidos.

7.1.1 Revisão e Atualização do Guia:

O Guia de Segurança da Informação e Proteção de Dados do IPAM é um documento vivo e dinâmico, que deve se adaptar às constantes mudanças tecnológicas, aos riscos emergentes e às evoluções regulatórias.

- **Periodicidade:** Este guia será revisado e atualizado anualmente, ou sempre que houver mudanças significativas na legislação (como a LGPD), na infraestrutura tecnológica do IPAM, nos processos de negócio ou na identificação de novos riscos relevantes;

- **Responsabilidade:** A responsabilidade pela coordenação da revisão e atualização do guia recai sobre a Área de Tecnologia da Informação (TI), com a colaboração do Encarregado de Dados (DPO) e a aprovação do Comitê de Segurança da Informação (CSI), se houver, ou da alta direção do IPAM;

- **Comunicação:** Todas as atualizações e revisões do guia serão devidamente comunicadas a todos os servidores, colaboradores e partes interessadas, garantindo que todos estejam cientes das versões mais recentes das políticas e procedimentos.

7.1.2 *Sanções por Descumprimento das Diretrizes:*

O cumprimento das diretrizes estabelecidas neste Guia de Segurança da Informação e Proteção de Dados é mandatório para todos os servidores, colaboradores, estagiários, prestadores de serviços e terceirizados que utilizam os recursos tecnológicos e acessam as informações do IPAM.

- **Consequências:** O descumprimento de qualquer uma das políticas e procedimentos contidos neste guia, intencional ou por negligência, poderá acarretar em sanções disciplinares, administrativas e/ou legais;

- **Graduação das Sanções:** As sanções serão aplicadas de acordo com a gravidade da infração, o impacto gerado, a reincidência e as normas internas do IPAM (Regimento Interno, Código de Conduta, etc.), podendo incluir, mas não se limitar a: advertência verbal, advertência escrita, suspensão, e em casos graves, rescisão do contrato de trabalho ou desligamento do serviço público, sem prejuízo de outras medidas legais cabíveis;

- **Responsabilidade Legal:** É importante ressaltar que 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 LGPD e demais legislações pertinentes.

7. REFERÊNCIAS NORMATIVAS E BIBLIOGRÁFICAS

- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).
- Instruções Normativas do GSI/PR (IN 01/GSI/PR, IN 03/GSI/PR).
- MANUAL DO PRÓ-GESTÃO versão 3.6.
- Lei 886/2022 do IPAM
- Decreto 21.060 JUNHO/2025 do Município de Porto Velho que institui a política de segurança.
- Outras normas internas do IPAM.
- Publicações de referência (CIS, ISO 27001, NIST, ANPD).