

RESOLUÇÃO N.º 001, DE 14 DE JULHO DE 2025

Aprova a **Política de Segurança da Informação** no âmbito do IPREMA

O CONSELHO FISCAL E DELIBERATIVO DO IPREMA, usando das atribuições que lhe são conferidas por lei, e

CONSIDERANDO que Lei Geral de Proteção de dados – LGPD, aprovada pela Lei Federal nº 13.709 de 14 de agosto de 2018 é de observância obrigatória da União, Estados e Município, incluindo-se a administração pública indireta.

CONSIDERANDO que a informação é um ativo essencial da organização e precisa ser protegida quanto a eventuais ameaças, preservando e minimizando os riscos para a continuidade dos serviços prestados pelo RPPS;

CONSIDERANDO que a adoção de procedimentos que garantam a segurança das informações deve ser prioridade constante do RPPS, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;

CONSIDERANDO o disposto no Manual do PRÓ-GESTÃO, aprovado pela Portaria da Secretaria da Previdência nº 3.811/2024;

CONSIDERANDO a deliberação do Conselho Fiscal e Deliberativo, na reunião extraordinária realizada no dia 30 de junho de 2025, às 14:00, na sede administrativa do IPREMA, conforme ATA nº 02/2021 – Reunião Extraordinária do Conselho Fiscal e Deliberativo.

R E S O L V E:

Art. 1º. Fica instituída a Política de Segurança da Informação no âmbito do IPREMA, na forma do Anexo Único desta Resolução.

Art. 2º. Ficam revogadas às disposições da Resolução nº 02, de maio de 2024.

Art. 3º. Esta Resolução entrará em vigor na data de sua publicação.

Araxá, 14 de Julho de 2025

Juliana Guaraldo Diniz
Presidente do Conselho Fiscal e Deliberativo do IPREMA

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

1. INTRODUÇÃO

A Política de Segurança da Informação é o documento que orienta e estabelece as diretrizes corporativas do Instituto de Previdência Municipal de Araxá – IPREMA para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas.

A presente Política de Segurança da Informação está baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

A informação é um ativo de grande valor para Instituto de Previdência Municipal de Araxá – IPREMA, por isso, necessita ser adequadamente protegida.

2. OBJETIVOS

Estabelecer normas, diretrizes e procedimentos que permitam aos servidores e fornecedores do Instituto de Previdência Municipal de Araxá – IPREMA seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades operacionais e de proteção legal da fundação e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do Instituto de Previdência Municipal de Araxá – IPREMA quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3. APLICAÇÕES

As diretrizes estabelecidas deverão ser seguidas por todos os servidores públicos lotados nesta autarquia (efetivos, temporários, comissionados ou cedidos de outros órgãos), bem como os prestadores de serviço e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada servidor e fornecedor de que os ambientes, sistemas, computadores e redes poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

É também obrigação de cada servidor se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de tecnologia de informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional contratada pelo Instituto de Previdência Municipal de Araxá – IPREMA pertence à referida instituição.

As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

O Instituto de Previdência Municipal de Araxá – IPREMA, por meio de sua equipe de tecnologia de informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4. DAS RESPONSABILIDADES ESPECÍFICAS

Dos Servidores e Fornecedores em Geral

Entende-se por servidor toda e qualquer pessoa física, nomeada por concurso público que exerça alguma atividade dentro ou fora da instituição.

Entende-se por fornecedor o prestador de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.



Será de inteira responsabilidade cada servidor ou fornecedor todo prejuízo ou dano que vier a sofrer ou causar no Instituto de Previdência Municipal de Araxá – IPREMA e/ou a terceiros, em decorrência da não obediência às diretrizes e normas referidas.

Dos Servidores em Regime de Exceção (Temporários e Estagiários):

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na Política de Segurança de Informações.

A concessão de acesso poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas nesta política.

Dos Gestores de Pessoas e/ou Processos:

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores sob a sua gestão.

Atribuir aos servidores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação.

Exigir dos servidores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações de Instituto de Previdência Municipal de Araxá – IPREMA.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política.

Da Equipe de Tecnologia da Informação:

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança de Informações.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para Instituto de Previdência Municipal de Araxá – IPREMA.

Quando ocorrer movimentação interna dos ativos de tecnologia de informação, garantir que as informações de um usuário não serão removidas de forma irreversível antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Realizar auditorias periódicas de configurações técnicas e análise de riscos. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de exoneração de servidor, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos do Instituto de Previdência Municipal de Araxá – IPREMA.

Fomentar a conscientização dos servidores acerca da importância da segurança da informação no desempenho das atividades essenciais do Instituto de Previdência Municipal de Araxá (IPREMA), por meio de programas de capacitação periódicos, submetidos anualmente à apreciação da Diretoria. Esses programas deverão ser acompanhados por indicadores de desempenho que atendam às exigências da cláusula 9.1 – Monitoramento, Medição, Análise e Avaliação do ISMS, conforme ISO 27001.”

Indicadores (KPIs, KRIs e KCIs) recomendados:

- **Número de incidentes de segurança relacionados a erro humano – métrica mensal comparando os totais antes e depois da capacitação (risco e tendência, KRI/KPI) ISO 9001 Checklist+15DataGuard+15ISMS.online+15**

- **Tempo médio de detecção e tempo médio de resposta a incidentes – medido em horas ou dias, com meta de redução percentual contínua (eficácia operacional)**
- **Percentual de controles de segurança implementados e validados – proporção dos controles previstos que estão ativos e atuando eficazmente (controle efetivo, KCI) ISACA Alemanha+1Vanta+1**
- **Percentual de servidores com capacitação atualizada – concluída nos últimos 12 meses, segundo registros de participação (treinamento e conscientização)**
- **Percentual de servidores que atingem o nível mínimo de acertos em prova pós-capacitação – aferindo compreensão efetiva dos conteúdos ministrados (qualidade da capacitação)**
- **Tempo médio para endereçamento de vulnerabilidades críticas identificadas – em até 30 dias desde a detecção (eficiência na mitigação de riscos) Vanta**
- **Percentual de avaliações e auditorias internas concluídas dentro do prazo – cumprindo os ciclos planejados de auditoria ISO 27001 (controle e conformidade) CyberZoni.com+2Scytale+2GRCMana+2**
- **Custo médio por incidente de segurança – valor financeiro associado aos incidentes ocorridos, medido periodicamente (impacto e gestão de recursos)**

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

5. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política de Segurança da Informação, o Instituto de Previdência Municipal de Araxá – IPREMA poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e
- outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação dos Diretores;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

Correio eletrônico:

O objetivo é informar aos servidores do Instituto de Previdência Municipal de Araxá – IPREMA quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

A responsabilidade pela utilização do correio eletrônico do Instituto de Previdência Municipal de Araxá – IPREMA recai a todos os seus membros que efetivamente o utilizam, de modo que a averiguação de responsabilidade entre seus membros seja objetiva.

O uso do correio eletrônico do Instituto de Previdência Municipal de Araxá – IPREMA é para fins corporativos e relacionados às atividades do quanto à instituição.

A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso¹, não prejudique o Instituto de Previdência Municipal de Araxá – IPREMA e também não cause impacto no tráfego da rede.

É proibido aos servidores o uso do correio eletrônico do Instituto de Previdência Municipal de Araxá – IPREMA para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

¹ Para os fins desta política e dos procedimentos institucionais, entende-se por bom senso a capacidade do servidor de agir com discernimento, equilíbrio, responsabilidade e respeito às normas internas, mesmo diante de situações não previstas expressamente neste documento.

A aplicação do bom senso envolve:

- Zelar pela imagem institucional do IPREMA nas ações realizadas em nome da entidade;
- Evitar excessos ou condutas abusivas, especialmente no uso de e-mails, internet, equipamentos e redes institucionais;
- Observar princípios éticos, mesmo quando houver margem de interpretação subjetiva sobre determinada conduta;
- Consultar a chefia imediata ou a área de Tecnologia da Informação, sempre que houver dúvidas sobre a adequação de determinada ação frente à Política de Segurança da Informação.

O bom senso, portanto, não substitui as normas, mas atua como elemento complementar na tomada de decisões cotidianas, reforçando a responsabilidade individual de cada servidor com a segurança da informação e o interesse público.

- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Instituto de Previdência Municipal de Araxá – IPREMA ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando o Instituto de Previdência Municipal de Araxá – IPREMA estiver sujeita a algum tipo de investigação;
- Utilizar o endereço de correio eletrônico corporativo para fins de cadastros pessoais e redes sociais;
- produzir, transmitir ou divulgar mensagem que:
 - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Instituto de Previdência Municipal de Araxá – IPREMA;
 - contenha ameaças eletrônicas, como: spam, mail *bombing*, vírus de computador etc.;
 - contenha arquivos com código executável (exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
 - vise obter acesso não autorizado a outro computador, servidor ou rede;

- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- vise burlar qualquer sistema de segurança;
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- contenha anexo(s) superior(es) a 25 MB para envio (interno e internet) e 25 MB para recebimento (internet), exceto com autorização prévia do gestor da área;
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Internet:

Todas as regras atuais do Instituto de Previdência Municipal de Araxá – IPREMA visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede



corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, ao Instituto de Previdência Municipal de Araxá – IPREMA, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Instituto de Previdência Municipal de Araxá – IPREMA, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

O uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os servidores que estão devidamente autorizados a falar em nome do Instituto de Previdência Municipal de Araxá – IPREMA para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os servidores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos, redes sociais ou qualquer outra tecnologia correlata que venha surgir na internet.



Os servidores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades no Instituto de Previdência Municipal de Araxá – IPREMA e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela área de tecnologia de informação.

Os servidores não poderão em hipótese alguma utilizar os recursos do Instituto de Previdência Municipal de Araxá – IPREMA para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Servidores com acesso à internet não poderão efetuar upload de qualquer software licenciado a Instituto de Previdência Municipal de Araxá – IPREMA ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os servidores não poderão utilizar os recursos de Instituto de Previdência Municipal de Araxá – IPREMA para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (SKYPE, WHATSAPP, redes sociais e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor ou a área de tecnologia da informação julgue necessário.

Não é permitido acesso a sites de proxy.

Controle de Acesso à Informação Sensível de Meio Físico:

O objetivo é prevenir o acesso não autorizado as informações sensíveis de meio físico de posse e competência do Instituto de Previdência Municipal de Araxá – IPREMA, evitando danos e interferências.

O acesso à área em que são processadas e armazenadas as informações sensíveis de meio físico são controlados e restrito às pessoas autorizadas. O acesso não autorizado não será permitido.

O controle de retirada e/ ou consulta das informações será controlado por responsável designado que fará monitoramento por meio de emissão de protocolos. As informações contidas no protocolo contam com no mínimo:

- nome e visto do servidor responsável emissor do protocolo;
- nome e visto do servidor interessado ao acesso da informação sensível de meio físico;
- a data e hora da retirada e/ou consulta da informação sensível de meio físico;
- a data e hora da devolução da informação sensível de meio físico e
- Observações Complementares.

A retirada de informações sensíveis de meio físico sem a devida emissão do protocolo não será autorizada.

Toda a informação sensível de meio físico será conferida no ato da devolução, estando sujeito a emissão de ocorrências em caso de desorganização, desleixo ou ausência de documentos.

São considerados os casos de desorganização e desleixo:

- Desordem na numeração das folhas do processo;
- Rasuras, anotações e amassados;
- Sujeiras de alimentos e bebidas.

Não é permitido a retirada de qualquer folha objeto de complemento ao arquivo de informação.

A possibilidade de foto cópia será permitida somente com a emissão do protocolo, onde deverá ser preenchido no item “Observações Complementares” as folhas que foram objeto da foto cópia.

Não é permitido a locomoção de informações sensíveis de meio físico fora as dependências do Instituto de Previdência Municipal de Araxá – IPREMA.

6. IDENTIFICAÇÃO:

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o Instituto de Previdência Municipal de Araxá – IPREMA e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307–falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores.

Todos os dispositivos de identificação utilizados no Instituto de Previdência Municipal de Araxá – IPREMA, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma única pessoa física.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o Instituto de Previdência Municipal de Araxá – IPREMA e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

A área de tecnologia de informação responde pela criação da identidade lógica dos servidores na instituição.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Caso o servidor esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

7. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos servidores são de propriedade da Instituto de Previdência Municipal de Araxá – IPREMA, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um servidor da área de tecnologia de informação, ou de quem este determinar.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes às atividades do Instituto de Previdência Municipal de Araxá – IPREMA não deverão ser copiados movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos servidores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os servidores do Instituto de Previdência Municipal de Araxá – IPREMA e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da área de tecnologia da informação.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Os servidores devem informar qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado pela área de tecnologia de informação ou por terceiros devidamente contratados para o serviço;
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática;
- O servidor deverá manter a configuração do equipamento disponibilizado pelo Instituto de Previdência Municipal de Araxá – IPREMA, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pelo Instituto de Previdência Municipal de Araxá – IPREMA devem ter imediatamente suas senhas padrões (default) alteradas.

Situações em que é proibido o uso de computadores e recursos tecnológicos de Instituto de Previdência Municipal de Araxá – IPREMA:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;

- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

8. PRIVACIDADE DA INFORMAÇÃO

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e/ou beneficiários e que são manipuladas ou armazenadas nos meios às quais o Instituto de Previdência Municipal de Araxá – IPREMA detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais do Instituto de Previdência Municipal de Araxá – IPREMA e reafirmam o seu compromisso com a melhoria contínua desse processo:

- As informações são coletadas de forma ética e legal, com o conhecimento do segurado / beneficiário, para propósitos específicos e devidamente informados;
- As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
- As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados;

- As informações somente são fornecidas a terceiros, mediante autorização prévia da Diretoria-Executiva ou para o atendimento de exigência legal ou regulamentar;
- As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

9. DISPOSITIVOS MÓVEIS

O Instituto de Previdência Municipal de Araxá – IPREMA deseja facilitar a mobilidade e o fluxo de informação entre seus servidores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pela área de tecnologia de informação, como: notebooks, smartphones e pendrives.

O objetivo é estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores que utilizem tais equipamentos.

A Instituto de Previdência Municipal de Araxá – IPREMA, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O servidor, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Instituto de Previdência Municipal de Araxá – IPREMA, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo servidor deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade do Instituto de Previdência Municipal de Araxá – IPREMA e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação, autorização e sem a condução, auxílio ou presença de um servidor da área de tecnologia de informação.

O servidor deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela área de tecnologia de informação.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do servidor, no caso de furto ou roubo de um dispositivo móvel fornecido pelo Instituto de Previdência Municipal de Araxá – IPREMA, notificar imediatamente o seu gestor direto e a área de tecnologia de informação.

O servidor deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar no Instituto de Previdência Municipal de Araxá – IPREMA e/ou a terceiros.

10. DATACENTER

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor da área de tecnologia da informação ou de um servidor autorizado.

11. BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os servidores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do

produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

Os backups imprescindíveis, críticos, para o bom funcionamento das atividades do Instituto de Previdência Municipal de Araxá – IPREMA, exigem uma regra de retenção especial, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade.

Os arquivos de backup devem estar disponíveis em servidores externos de arquivo, como segunda fonte;

12. ATUALIZAÇÕES

A Comissão de Implementação e Controle da Lei Geral de Proteção de Dados se reservam ao direito de revisar, adicionar ou modificar esta Política de Segurança da Informação para aprimorar e garantir o perfeito funcionamento das normas e regras por ele definidas, principalmente aos casos omissos, que deverão ser encaminhados ao Comitê para avaliação e resolução.

As normas e procedimentos acima não se esgotam neste instrumento, sobretudo em razão da constante evolução tecnológica, não consistindo em rol taxativo, motivo pelo qual é obrigação da Comissão acima, bem como dos usuários adotarem todo e qualquer outro procedimento de segurança que esteja ao seu alcance, visando sempre proteger as informações desta Autarquia.

13. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do Instituto de Previdência Municipal de Araxá – IPREMA. Ou seja, qualquer incidente de segurança subte-se como alguém agindo contra a ética e os bons costumes.



Encaminha-se, em anexo, o Plano de Resposta a Incidentes de Segurança da Informação, elaborado conforme as diretrizes da Política de Segurança da Informação do IPREMA e as boas práticas previstas na norma ISO/IEC 27035. O documento visa orientar a atuação preventiva e reativa diante de eventuais eventos de segurança, assegurando a continuidade das atividades institucionais e a proteção dos ativos informacionais.

Esta Política de Segurança da Informação entra em vigor na data de sua publicação e poderá ser alterada a qualquer tempo por decisão do Comitê Gestor de Segurança, sempre que surgirem fatos relevantes, ainda que não contemplados neste documento. Ressalva-se, contudo, a obrigatoriedade de sua revisão anual, cuja versão atualizada deverá ser submetida à validação do Conselho Deliberativo.

ANEXO 1

PLANO DE RESPOSTA A INCIDENTES (PRI)

1. Objetivo

Estabelecer diretrizes e procedimentos padronizados para **identificação, registro, análise, resposta, contenção, erradicação, recuperação e lições aprendidas** de incidentes de segurança da informação, minimizando impactos e promovendo a melhoria contínua dos controles internos.

2. Abrangência

Aplica-se a **todos os sistemas, ativos de informação, colaboradores, prestadores de serviço e unidades organizacionais** da instituição, sempre que houver suspeita ou confirmação de um incidente de segurança da informação.

3. Definições

- **Incidente de Segurança:** Evento adverso real ou potencial que compromete a confidencialidade, integridade ou disponibilidade das informações.
 - **Evento:** Ocorrência observável no ambiente que pode estar relacionada ou não a um incidente.
 - **Responsável pelo Tratamento:** Pessoa ou grupo designado para coordenar a resposta ao incidente.
 - **Stakeholders:** Partes interessadas (usuários, gestores, TI, jurídico, comunicação etc.).
-

4. Classificação dos Incidentes

Os incidentes serão classificados de acordo com sua **severidade e impacto**, conforme matriz abaixo:

4.1 Matriz de Impacto

Impacto	Baixo	Médio	Alto
Criticidade	Ex: vazamento interno de dados sem impacto	Ex: indisponibilidade de sistema por até 2h	de Ex: ataque ransomware, perda de dados sensíveis

4.2 Níveis de Severidade

Nível	Descrição	Tempo Máximo de Resposta
1 – Crítico	Alto impacto, sistemas essenciais afetados	Imediato (até 1h)
2 – Alto	Prejuízo operacional relevante	Até 4h
3 – Médio	Impacto controlável, sem vazamento ou paralisação	Até 1 dia útil
4 – Baixo	Evento sem impacto significativo	Até 3 dias úteis

5. Etapas da Resposta a Incidentes

5.1 Preparação

- Definir equipe responsável pela resposta a incidentes (TI, segurança, jurídico, comunicação, etc.).
- Treinar usuários sobre como identificar e reportar incidentes.
- Manter atualizados os contatos e procedimentos emergenciais.

5.2 Identificação

- Monitoramento contínuo de ativos e redes.
- Recebimento de alerta via canal oficial (e-mail, sistema de helpdesk, telefone).
- Registro inicial no **formulário de incidentes**, contendo:
 - Data e hora;
 - Quem reportou;
 - Descrição do ocorrido;
 - Ativos envolvidos.

5.3 Contenção

- Contenção imediata (ex: desconectar sistema da rede);

- Avaliação do escopo e propagação;
- Decisão conjunta sobre desligamento de sistemas ou bloqueios.

5.4 Erradicação

- Eliminação da causa raiz (ex: remoção de malware, troca de senhas, aplicação de patch);
- Revalidação da segurança do ambiente;
- Atualização de controles de prevenção.

5.5 Recuperação

- Restauração dos serviços com segurança;
- Validação com as áreas envolvidas;
- Monitoramento pós-incidente.

5.6 Lições Aprendidas

- Realização de reunião de análise pós-incidente;
- Identificação de falhas de processo, tecnologia ou treinamento;
- Propostas de melhoria;
- Atualização da PSI e dos controles afetados.

6. Comunicação e Escalonamento

6.1 Canal de Notificação de Incidentes

- E-mail: incidentes@instituicao.gov.br
- Telefone: (xx) xxxx-xxxx
- Sistema de chamados interno (HelpDesk)

6.2 Comunicação Externa

- Envolvimento do jurídico para avaliar impactos legais e regulatórios (ex: LGPD);
- Comunicação pública, se necessário, com apoio da área de comunicação.

7. Indicadores de Desempenho (KPIs)

Indicador	Descrição	Meta
Tempo médio de resposta (MTTR)	Tempo entre a identificação e a contenção do incidente	≤ 4 horas
% de incidentes resolvidos no prazo	Percentual de incidentes tratados conforme SLA	≥ 95%
Incidentes recorrentes	Quantidade de incidentes com causa repetida	Redução contínua
Taxa de reportes de usuários	% de incidentes reportados por colaboradores	≥ 30% do total

8. Responsabilidades

Função	Responsabilidade
Usuários	Identificar e reportar incidentes
Equipe de TI	Executar contenção, erradicação e recuperação
Comitê de Segurança	Avaliar impactos, aprovar ações estratégicas e revisar políticas
Jurídico	Avaliar implicações legais e orientar sobre notificações
Comunicação	Gerenciar comunicação com a mídia ou órgãos externos, se necessário

9. Revisão e Atualização

Este plano deverá ser revisado **anualmente** ou sempre que ocorrerem:

- Alterações significativas nos sistemas ou processos;
 - Novos tipos de ameaças;
 - Incidentes graves com impacto relevante.
-

Data de aprovação: ____/____/____

Revisão prevista: ____/____/____



INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ARAXÁ

Instituto de Previdência Municipal de Araxá – IPREMA
Rua Dr. Franklin de Castro, 160, Centro, CEP 38183 – 120
(34) 3611-2602 / iprema@araxa.mg.gov.br