INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE ARARIPE-CE

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO- PSI

IPREMA
INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ARARIPE

# RESOLUÇÃO IPREMA Nº 002/2026

**DISPÕE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO-PSI DO RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA).**

A Diretoria do IPREMA, no uso de suas atribuições legais conferidas pela Lei Municipal n°. 927/2009 de 23 de Dezembro de 2009, conforme dispõe o art. 28, parágrafo 3° da Lei.

RESOLVE:

Art. 1° - Aprova a Política de Segurança da Informação-PSI do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA), da forma dos anexos desta Resolução, com objetivo de adequação as ações de conformidade para Certificação do Pró-Gestão RPPS.

Art. 2º Esta norma abrange todos os recursos e ambientes computacionais, bem como os documentos, informações e dados produzidos e/ou recebidos e custodiados pelo IPREMA, devendo ser observada por todos os servidores e prestadores de serviços responsáveis pelo tratamento das informações

Art. 3º - Esta resolução entra em vigor na data de sua publicação, revogam-se as disposições em contrário.

Araripe-Ce, 19 de maio de 2026.

**DIRETORIA EXECUTIVA**

João Batista da Silva Neto
Diretor Presidente

Francisco Diógenes Ramos da Silva
Diretor Administrativo e Financeiro

Crislucia de Oliveira Amarante
Diretora de Benefícios

Flávia Juliana da Silva Gomes
Assessoria Jurídica

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA)

A Política da Segurança da Informação - PSI - é uma declaração formal de compromisso da Unidade Gestora do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) com a proteção das informações sob sua guarda. Documento elaborado em atendimento ao disposto no item 3.1.5 do Manual do Pró-Gestão RPPS com objetivo de Certificação inicial e ascensão de Nível.

## 1. INTRODUÇÃO

1.1 No presente documento são estabelecidas as diretrizes corporativas no âmbito da segurança das informações manipuladas e transitadas pela Unidade Gestora do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA)

1.2 A Política de Segurança da Informação (PSI) tem o intuito de garantir, principalmente, que as informações sejam protegidas, tanto no que se refere à confidencialidade quanto à integridade dos dados, garantindo que os mesmos sempre possam estar disponíveis a quem necessita e a quem é de direito.

1.3 A cada vez que uma informação é manipulada, a mesma está sujeita a erros, sejam causados pelas máquinas que a manipulam quanto pelos seres humanos. Desta forma, é importante que haja diretrizes visando à minimização desse tipo de problema, com o principal intuito de proteger a informação corporativa.

## 2. OBJETIVOS e FINALIDADE

2.1 objetivo da PSI apresentada aqui é instruir os servidores do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) e demais pessoas interessadas com procedimentos a serem adotados para que se tenha uma maior segurança dos dados.

2.2 Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional pertence à instituição. As exceções devem ser explícitas e formalizadas. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços e estejam plenamente de acordo com o estabelecido no Código de Ética da instituição.
Qualquer incidente que possa afetar a segurança da informação deverá ser comunicado de imediato ao setor de controle interno do IPREMA, esta encaminhará ao órgão competente da Prefeitura para que as devidas providências sejam tomadas.

2.3 A ideia é alertar aos membros da autarquia quanto às possíveis consequências dos seus atos e o que deve ser feito para melhor tratar as informações de sua competência. Com relação aos interessados externos, o documento informa como as informações do órgão podem ser acessadas. São definidas aqui as responsabilidades e as boas práticas.

**3. PRINCÍPIOS -** Além dos objetivos e finalidades citados, o RPPS, como órgão público, também tem por obrigação seguir os ritos legais propostos pela Lei Geral de Proteção de dados, além de criar a política de segurança da informação, nomear um encarregado pela proteção de dados pessoais, treinar servidores da Unidade Gestora para um adequado tratamento de dados e assim, evitar o vazamento das informações dos beneficiários.
In verbis LGPD

> *"Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público*
> *.....*
> *Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e*

*atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais"*

## 3.1 PRINCIPAIS DEFINIÇÕES:

a) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
b) Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
c) Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
d) Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
e) Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
f) Encarregado: pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados pessoais (ANPD).
g) Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional,

## 4. RESPONSABILIDADES

4.1 Colaboradores

a) É considerado colaborador qualquer pessoa que tenha vínculo empregatício de tempo indeterminado com a autarquia; podem ser funcionários estatutários ou sob outro regime jurídico, incluindo estagiários.

b) Tais pessoas têm responsabilidade sobre todas as informações da qual têm conhecimento e/ou que manipulam em razão do seu serviço, devendo privar pela sua proteção.

4.2 Visitantes

a) Qualquer pessoa que venha até a sede da autarquia é considerada visitante. A mesma também está sujeita à PSI, devendo zelar pelas informações do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) que tem conhecimento em razão do seu trabalho, bem como qualquer eventual uso de equipamento ou infraestrutura.
b) O visitante deve sempre ser supervisionado pela pessoa visitada, a qual é responsável pelos dados aos qual o primeiro tem acesso e também pelos equipamentos utilizados. Além disso, o visitado tem a responsabilidade de avisar ao visitante sobre as normas da PSI ARARIPE-CE IPREMA. Os prestadores de serviço também são caracterizados como visitantes.

4.3 Gestores

a) Qualquer pessoa que possua um colaborador, equipe ou processo sob sua supervisão é considerado gestor. O gestor, além de responsável pelos seus atos, também responde pelos atos de seus subordinados diretos, devendo esse zelar pela proteção da informação manipulada por sua equipe.

b) O gestor deve ser o modelo de conduta na equipe, orientando-a e fiscalizando-a para que incidentes relacionados à PSI não ocorram. Ele também deverá adaptar os processos e procedimentos de sua responsabilidade à política, cuidando para que a mesma não seja infringida.

4.4 Pessoas jurídicas contratadas.

a) Qualquer pessoa jurídica que seja, ou venha a ser, contratada para prestação de serviços na Unidade Gestora do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) é responsável por cuidar das informações da autarquia a que tiver conhecimento, seja mediante contrato ou solicitação de serviço. As pessoas jurídicas também são responsáveis pelos prestadores de serviços enviados, respondendo solidariamente a qualquer incidente ocorrido com os mesmos.
b) A pessoa jurídica que possuir banco de dados com informações de propriedade do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) deve zelar pela sua proteção, em termos de confidencialidade, integridade ou disponibilidade dos dados. Deve estar claro que todos os dados pertencem à autarquia.
c) A premissa apresentada no parágrafo anterior se estende aos equipamentos que porventura sejam submetidos à manutenção e à pessoa jurídica responsável por tal serviço. Os dados fornecidos pelo RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) à pessoa jurídica contratada não devem ser divulgados ou repassados a terceiros sem que haja autorização explícita.

### 4.5 Clientes

a) São considerados clientes da Unidade Gestora do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) todos os segurados e beneficiários do regime que necessitam de qualquer serviço prestado pela referida. A responsabilidade sobre as informações a que o cliente tem direito, ou passa a conhecer, é do colaborador que realizou o contato e do gestor imediato do departamento ao qual o ato ocorreu.

## 5. CORREIO ELETRÔNICO

b) O uso do correio eletrônico do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) é para fins corporativos e relacionados às atividades do colaborador usuário. A utilização desse serviço para fins pessoais é permitida desde que seja feita com bom senso e sem conflito com

qualquer norma do Código de Ética, não prejudique a autarquia e nem cause impacto no tráfego da rede.

5.1 É vedado aos colaboradores da Unidade Gestora do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA):

a) Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição e com ciência da gerência de Cadastro e Sistemas de Informação;
b) Enviar mensagens usando nome de usuário de outra pessoa ou endereço eletrônico que não esteja autorizado a usar;
c) Enviar qualquer e-mail que torne seu remetente e/ou do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) vulneráveis a ações civis ou criminais;
d) Divulgar externamente informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização explícita;
e) Falsificar ou adulterar informações do cabeçalho do e-mail;
f) Produzir, transmitir ou divulgar mensagem que:
g) Conflite com os interesses da autarquia Contenha ameaças eletrônicas, como spam ou vírus;
h) Vise obter acesso não autorizado a outro computador ou servidor;
i) Vise interromper um serviço por meio de método ilícito;
j) Vise burlar qualquer sistema de segurança;
k) Vise vigiar secretamente ou assediar outro usuário;
l) Vise acessar informações confidenciais sem autorização explícita do proprietário;
m) Possua anexo superior a 10MB;
n) Tenha conteúdo considerado impróprio, obsceno ou ilegal;
o) Seja caluniosa, difamatória ou ofensiva;
p) Tenha fins políticos (propaganda);
q) Inclua material protegido por direitos autorais sem a permissão do detentor.

5.2 Toda mensagem enviada pelo correio eletrônico deve possuir uma assinatura que identifique claramente o remetente.

## 6. COMUNICADOR INSTANTÂNEO

(Mensagem instantânea é uma forma de comunicação que permite que pessoas e empresas troquem mensagens em tempo real por meio da internet)

6.1 São vedados os seguintes comportamentos nos comunicadores instantâneos a serviço do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA):

a) Divulgar externamente informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização explícita;
b) Enviar mensagens passando-se por outro usuário;
c) Utilizar conta alheia para envio de mensagens sem autorização explícita e sem identificar-se adequadamente;
d) Enviar mensagens difamatórias, ofensivas, preconceituosas, obscenas, caluniosas ou que tenham fins de propaganda política;
e) Utilizar de avatares ou frases de status que sejam difamatórias, ofensivas, preconceituosas, obscenas, caluniosas ou que tenham fins de propaganda política.

6.2 Caso haja a necessidade de realização de videoconferência com compartilhamento de tela, o usuário responsável pela tela compartilhada deve garantir que nenhuma informação, além da necessária, seja transmitida. O mesmo também deve alertar ao destinatário sobre as consequências do uso indevido das informações que receber.

## 7. INTERNET E VPN.

7.1 Embora a conexão direta e permanente da rede corporativa com a internet ofereça grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos da informação. Todas as regras estabelecidas pela empresa contratada para provimento da internet e administração da rede devem ser seguidas.

7.2 Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA), em total conformidade legal, reserva-se o direito de solicitar monitoria e registro de todos os acessos a ela. A internet disponibilizada pode ser usada com finalidade pessoal, desde que não prejudique a produtividade da unidade e não onere a rede, causando lentidão ou outros problemas. Da mesma forma, seu uso não deve ferir qualquer norma do Código de Ética vigente.

7.3 PROIBIÇÕES

a) É proibida a divulgação de qualquer informação corporativa em redes sociais, listas de discussão, comunidades de relacionamento ou a terceiros via comunicadores eletrônicos ou qualquer outra tecnologia que venha surgir da internet, salvo quando realizado pelas pessoas autorizadas a realizar comunicação externa.

b) É proibido o download e a instalação de softwares que tenham direitos autorais, marca registrada ou patente na internet e que não foram devidamente adquiridos pela autarquia. O mesmo se aplica ao download de mídias e arquivos em geral que não sejam de uso livre, sejam eles imagens, apresentações, planilhas, músicas, entre outros.

c) É proibido expor, armazenar, distribuir, editar, imprimir ou gravar materiais de cunho sexual, obsceno, difamatório, ofensivo, preconceituoso e político (propaganda) por qualquer meio.

d) É proibido o uso de softwares ou serviços de nuvem não homologados - Softwares IT - (Ex: usar um Dropbox pessoal para guardar documentos do IPREMA).

7.4 Transferências de Arquivos

a) Como é possível a transferência de arquivos entre os computadores das redes distintas, devem ser observadas as mesmas regras dispostas no item 12, tomando todas as precauções possíveis para que as informações usadas no trabalho não sejam disponibilizadas a qualquer outra pessoa não competente que possa ter acesso ao mesmo computador do usuário. Assim, recomenda-se que a referida transferência de arquivos seja realizada apenas quando for imprescindível para o trabalho realizado.
b) Também é importante salientar que, mesmo em trabalho remoto, o servidor está sujeito à totalidade desta Política de Segurança das Informações.

## 8. SERVIDOR DE ARQUIVOS.

8.1 O uso deste servidor de arquivos (provido pela Empresa contratada) é permitido a todos os usuários. Entretanto, os diretórios existentes ali estão permissionados de acordo com o organograma vigente na instituição.

8.2 Caso haja alguma necessidade de alteração no permissionamento, esta deverá ser comunicada e justificada à Diretoria Executiva para avaliação e concessão, caso seja aplicável.

8.3 Além dos diretórios correspondentes às coordenadorias e grupos, existem os diretórios de compartilhamentos, nos quais os usuários podem compartilhar arquivos com outros, entre coordenadorias iguais ou distintas.

8.4 Não é permitido armazenar arquivos que não tenham relação com o trabalho realizado, especialmente filmes e músicas, mesmo que isto aparentemente não cause prejuízo à instituição.

8.5 É VEDADO:

a) Armazenar vídeos e músicas;

b) Armazenar conteúdo difamatório, ofensivo, preconceituoso, obsceno, sexual, calunioso ou que tenha fins de propaganda política;
c) Editar ou apagar arquivos de outros usuários sem autorização do mesmo;
d) Fraudar, de qualquer forma, as informações dos arquivos;
e) Instalar ou armazenar programas sem o conhecimento da área de TI;
f) Armazenar conteúdo nocivo, como vírus e malwares;
g) Armazenar conteúdo protegido por direitos autorais ou patentes.
h) Qualquer necessidade de armazenamento de arquivo que se configure como exceção às regras apresentadas deve ser comunicada à área de TI para avaliação, desde que haja justificativa plausível.

## 9. IDENTIFICAÇÃO PESSOAL

9.1 Os dispositivos de identificação (o que inclui CPF's e assinadores digitais) e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) e/ou terceiros.

a) O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

b) Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

9.2 As senhas utilizadas para o acesso aos equipamentos e serviços são de uso pessoal e intransferível, não devendo ser armazenadas em arquivos eletrônicos

compreensíveis por linguagem humana (sem criptografia), bem como baseadas em informações pessoais e padrões óbvios, como “12345”, “654321”, “qwert”, entre outros. Mesmo que o sistema utilizado permita o uso de senhas simples, as seguintes regras devem ser seguidas para a confecção da senha, de forma a tornar mais difícil uma eventual tentativa de fraude:

a) Utilizar ao menos um dígito;
b) Utilizar ao menos uma letra minúscula;
c) Utilizar ao menos uma letra maiúscula;
d) Utilizar ao menos um símbolo especial, como ‘@’, ‘#’, ‘$’ entre outros.
e) Caso haja esquecimento de senha, ou qualquer outro problema de acesso, o colaborador deverá entrar em contato pessoalmente com a área responsável.
f) Fica proibido o uso de "post-it" ou “outro meio” com senhas em lugares de fácil acesso.

## 10. EQUIPAMENTOS

10.1 O colaborador é totalmente responsável por cada equipamento que usa, devendo zelar pelo seu estado de conservação, com especial atenção aos gabinetes de computadores.

a) Há uma relação de todos os equipamentos de informática vinculados a cada usuário, de acordo com o número do patrimônio. Qualquer troca de equipamento deve ser comunicada à administração para atualização desta lista.
b) Caso haja qualquer problema com algum dos equipamentos, o mesmo deve ser comunicado ao setor de controle interno, que comunicará à área de TI para que a manutenção seja providenciada.
c) Caso existam informações que necessitem ser armazenadas no HD da máquina alocado ao usuário, este deve fazê-lo na área protegida do usuário, preferencialmente no diretório “Documentos”, pois isto evita que outros usuários que venham a utilizar o mesmo equipamento tenham acesso a tais dados.

d) Para uso de equipamentos compartilhados, como projetor e notebook, o motivo deve ser apresentado à gerência de Cadastro e Sistemas de Informação, que providenciará os aparelhos, casos disponíveis para o evento requerido.
e) Durante o horário de uso, o responsável pela retirada responderá pelos equipamentos em sua posse.

## 11. COMPORTAMENTO ESPERADO (BOAS PRÁTICAS).

11.1 Espera-se dos usuários das informações do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) comportamento compatível com a PSI apresentada. Desta forma, são dadas a seguir algumas atitudes que devem ser observadas no dia-dia:

a) Política de Mesa Limpa e Tela Limpa (Clean Desk): Ao final do expediente ou em ausências prolongadas, o colaborador deve garantir que documentos físicos contendo dados pessoais ou sensíveis sejam guardados em gavetas ou armários trancados.
b) Da mesma forma, a estação de trabalho (desktop ou notebook) deve ser bloqueada (Windows + L) sempre que o servidor se afastar da mesa."
c) Retirada dos papéis da impressora: toda vez que alguém enviar um documento para impressão, o mesmo deve ser retirado imediatamente após o término da mesma, de forma a evitar que ele fique exposto a terceiros;
d) Descarte de papéis: caso algum papel com informação relevante e/ou confidencial necessite ser descartado, ele deve ser triturado na máquina específica para tal finalidade. Documentos confidenciais ou com dados pessoais de segurados não devem ser utilizados como papel de rascunho, devendo haver o descarte apropriado;
e) Bloqueio da estação de trabalho: ao ausentar-se da frente de sua estação de trabalho sem bloquear a tela do computador, o usuário está aceitando o risco de um terceiro utilizar sua máquina sem autorização. Assim, o bloqueio deve ser feito após qualquer saída de frente da estação de trabalho. A proteção de tela também deve ser configurada para que o micro seja bloqueado após determinado período de inatividade;

f) Conversas em áreas abertas: tal como não se deve divulgar informações da autarquia via internet, sem prévia autorização, também se deve ter o cuidado de não divulgar, mesmo que de maneira não intencional, informações restritas. Desta forma, conversas sobre assuntos do trabalho (especialmente aqueles sensíveis e/ou que envolvem informações pessoais) devem ser evitadas em ambientes que possuam pessoas externas ou que possam comprometer a segurança das informações trocadas;
g) Retirada de documentos da sede: não se devem retirar documentos da sede do RPPS de ARARIPE-CE- IPREMA, pois uma vez fora do prédio não é possível garantir seu correto tratamento. Caso haja a necessidade de locomoção dos documentos para reuniões externas ou viagens, a gerência responsável pela respectiva guarda deve ser informada.

## 12. DISPOSITIVOS MÓVEIS, SEGURANÇA E AFASTAMENTO DE PESSOAL

Considera-se dispositivo móvel qualquer aparelho que tenha atribuições de mobilidade, tal como: notebook, smartphone e pendrive. Comumente, mídias como pendrive são usadas para transferir dados de um computador para outro. Apesar de ser recomendado usar o servidor de arquivos para tal finalidade, esta ação é permitida desde que todos os dados transferidos sejam apagados da mídia.

### 12.1 SEGURANÇA EM CONEXÔES EXTERNAS E TRABALHO REMOTO:

a) Uso de Redes Wi-Fi: É proibido o acesso a sistemas internos ou manipulação de dados institucionais através de redes Wi-Fi públicas ou abertas (como as de shoppings, aeroportos e cafeterias) sem o uso obrigatório da VPN (Virtual Private Network) devidamente configurada pela TI.
b) Retirada de Equipamentos: A utilização de equipamentos (computadores ou notebooks) fora das dependências do IPREMA para fins de trabalho remoto exige a formalização prévia do ato.
c) Fluxo de Autorização: Para que o equipamento seja liberado para uso externo e tenha os acessos de domínio configurados, o servidor deve:

- Abrir um chamado formal (via formulário ou sistema oficial) detalhando a necessidade e o período;
- Anexar a autorização expressa da Presidência da autarquia;
- Aguardar a conferência e liberação técnica da Gerência de TI/Sistemas.
- Responsabilidade: O servidor detentor do equipamento assume total responsabilidade pela integridade física do ativo e pelo cumprimento das normas desta PSI enquanto o dispositivo estiver fora da sede.

**12. 2 GESTÃO DE ACESSOS EM AFASTAMENTOS E ALTERAÇÕES DE VÍNCULO -** Para garantir a integridade dos sistemas e evitar o uso de contas inativas, o IPREMA deve estabelecer o controle rigoroso de acessos durante ausências:

a) Afastamentos Temporários: Em casos de férias, licença-maternidade, licença para tratamento de saúde (doença), licença-funeral (luto) ou qualquer outro afastamento legal, a Gerência de Administração/RH deverá informar à TI para que os acessos aos sistemas e e-mail corporativo sejam temporariamente suspensos ou monitorados, conforme a duração do período.
b) Comunicação Obrigatória: É responsabilidade da Gerência de Administração ou da chefia imediata notificar a Gerência de Cadastro e Sistemas de Informação sobre o início e o término desses períodos de afastamento para a devida gestão das credenciais.
c) Retorno às Atividades: Ao retornar do afastamento, o servidor terá seus acessos reativados mediante confirmação de sua presença física ou via chamado formal à TI.
d) Revogação de Acessos (Offboarding): No caso de desligamento, exoneração, aposentadoria ou transferência do colaborador, a Gerência de Recursos Humanos/Administração deve notificar a TI imediatamente (ou em até 24h) para a revogação de todos os acessos lógicos e recolhimento de ativos físicos.

## 13. BACKUP (CÓPIA DE SEGURANÇA).

### 13.1 RESPONSABILIDADE DO USUÁRIO

a) O usuário tem a responsabilidade de salvar os arquivos nas pastas da rede (servidor) que são cobertas pelo backup automático, garantindo que seus arquivos de trabalho não fiquem perdidos apenas no "Desktop" da máquina local.

b) Para backup dos dados da estação de trabalho foram disponibilizados diretórios no servidor de arquivos para realização das cópias de segurança. Há um diretório para cada usuário e somente este terá acesso às informações ali gravadas.

c) Com relação aos dados no servidor de arquivos, recomenda-se que o usuário, periodicamente, copie-os para sua estação de trabalho, no local de sua preferência. Isto é uma redundância a mais para caso de falha no servidor ou então na rede de intranet. Ressalta-se, entretanto, que todos os arquivos na nuvem provida pela Empresa contratada possuem redundância e backup automático por várias vezes no mesmo dia, sendo possível recuperar de maneira direta backups datados de até 1 (um) mês. Havendo necessidade de recuperação de versões mais antigas dos arquivos, deve-se entrar em contato com a gerência e Cadastro e Sistemas de Informação.

d) Não é permitido realizar backup dos dados em equipamentos ou mídias pessoais. Havendo necessidade de trabalho à distância ou locomoção do colaborador, a área de TI deve ser comunicada para que os procedimentos adequados sejam tomados.

## 14. ASSINATURA E PROCESSO DIGITAL.

14.1 A DIRETORIA DO RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) possuem identificação pessoal certificado, usado para assinaturas digitais de documentos em geral, podendo incluir e-mails. Tal como já apontado na seção 9, seu uso é pessoal e intransferível, sendo vedado qualquer tipo de cessão a outras pessoas.

14.2 A assinatura realizada com o dispositivo tem validade legal e, portanto, sua utilização deve se dar da mesma forma que o uso da assinatura em papel, devendo-se avaliar bem o documento sendo assinado.

14.3 Para assinatura digital, deve-se introduzir o token, leitor ou link na estação de trabalho e, através do software que manipula o documento alvo, realizar os comandos para assinatura, utilizando, quando solicitado, o valor de PIN (senha) dos meios acima citados. Recomenda-se que o valor do PIN seja alterado para que fique diferente da senha padrão fornecida inicialmente. Havendo dúvidas de como proceder nesta operação, a área de TI deve ser consultada.

14.4 A principal utilidade do referido dispositivo é a validação dos documentos e despachos do processo digital implantado na autarquia. Para uso desta funcionalidade, a diretoria deve realizar seu acesso, mantendo suas informações pessoais atualizadas e tramitando os processos de acordo com os respectivos mapeamentos. Da mesma forma, as credenciais de acesso são pessoais e intransferíveis, devendo o usuário zelar pelo seu cuidado, bem como pela integridade de todas as informações ali contidas, seja de processos de próprio interesse ou de processos de terceiros a que venha a ter conhecimento.

## 15. ARQUIVOS DIGITALIZADOS

15.1 A digitalização de documentos para a Unidade Gestora do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) deve seguir o disposto no Decreto Federal nº 10.278, de 18 março de 2020, considerando que a tabela de temporariedade de guarda e classificação de documentos será publicada mediante Portaria específica.

a) O colaborador ou assessoria que for designado para a operação de digitalização dos documentos deve ter conhecimento da sua confidencialidade, zelando para que ninguém mais tenha acesso ao mesmo, se não for pessoa de interesse.

b) A digitalização deve ser realizada mediante o software proprietário provindo da mesma fabricante da máquina digitalizadora. Quando isto não for aplicável, a equipe de TI é a responsável por indicar e instalar eventual software substituto. Os parâmetros utilizados para tal devem ser configurados pelo time de TI no computador do usuário.

15.2 Metadados, ou Metainformação, são dados sobre outros dados.

a) Um item de um metadado pode dizer do que se trata aquele dado, geralmente uma informação inteligível por um computador. Os metadados facilitam o entendimento dos relacionamentos e a utilidade das informações dos dados Os dados e metadados do arquivo gerado são responsabilidade do digitalizador e do detentor do documento. Tais informações devem ser cadastradas através de software próprio para edição de metadados, a ser indicado pela equipe de TI. A transferência do arquivo gerado com os metadados do local de digitalização para o local de armazenamento deve ser realizada dentro da rede protegida, utilizando os diretórios do servidor, visto que tanto o arquivo quanto seus metadados podem possuir informações sigilosas e/ou confidenciais.
b) Todo documento físico que for movido de lugar para a digitalização deve ser retornado à sua origem, quando o procedimento for concluído, para sua devida destinação.

## 16. DA POLÍTICA DE PRIVACIDADE DE DADOS PESSOAIS.

16.1 A RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) deve editar documento conhecido como "Política de Privacidade" que será publicado no site institucional. como Termo de Privacidade. A Estrutura da Política de Privacidade IPREMA - Araripe-CE:

a) Dados Pessoais Coletados: Dados cadastrais, Identificação (CPF, RG), dados funcionais, dados sensíveis (saúde/médicos para perícia e aposentadoria), dados de dependentes (beneficiários).

b) Uso e Processamento: Gestão de benefícios, atualização de cadastro, análise de elegibilidade para aposentadorias/pensões, folha

de pagamento do IPREMA e cumprimento de obrigações legais, conforme a Lei Municipal 927/2009.

c) Medidas de Proteção: Protocolos de segurança física e digital, acesso restrito a dados pessoais, controle de acesso e monitoramento contra vazamentos, alinhado ao Pró-Gestão RPPS.

d) Direitos dos Titulares: Acesso facilitado aos dados, correção de dados incompletos ou inexatos, anonimização, bloqueio ou eliminação de dados desnecessários, e informações sobre compartilhamento.

e) Procedimentos de Solicitação: Definição de canal (ouvidoria/site) para requerer acesso, correção ou exclusão, com prazos claros de resposta.

f) Responsabilidades do IPREMA: Nomeação de Encarregado (DPO), transparência ativa, treinamento de equipe e conformidade com a LGPD.

## 17. PROCEDIMENTOS DE CONTINGÊNCIA (“BACKUP”)

17.1 As orientações supramencionadas no anexo referem-se também a ações de contingência, porém detalhando sobre o serviço de backup que compreende a realização de cópias de segurança dos arquivos com o objetivo de restaurá-los no menor tempo possível caso haja necessidade. Para garantir a segurança da informação, são realizadas cópias de segurança dos arquivos mantidos em servidores, sistemas e respectivos bancos de dados utilizados pelo IPREMA conforme item 13.

a) As rotinas de cópia de segurança são realizadas de forma automatizada, em horários pré-definidos, fora do horário de funcionamento do instituto, denominadas de “Janelas de Backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processamento sendo realizado nos sistemas informatizados.
b) São realizadas verificações periódicas dos backups realizados e testes de restauração com o intuito de averiguar a integridade dos arquivos ou banco de dados, executados aproximadamente a cada

30 ou 60 dias ou período determinado pelo setor de TI, de acordo com a criticidade do backup. Quando identificado erro, seja na execução do backup e/ou no processo de restauração, é realizado um novo backup no primeiro horário disponível, depois de identificado e solucionado o problema.

c) Terceiros e Pessoas Jurídicas Contratadas: No caso de empresas prestadoras de serviço, fornecedores ou consultorias: As sanções são disposta no item 18.

## 18. SANÇÕES E CONFORMIDADE

18.1 A violação das normas da PSI pelos servidores pode acarretar em sanções administrativas, além de responsabilidades civis e penais.

a) Responsabilidade Administrativa: A violação das normas desta PSI por servidores públicos (estatutários, comissionados ou estagiários) constitui infração disciplinar, sujeitando o infrator às sanções previstas no Estatuto dos Servidores Públicos do Município de ARARIPE-CE, que podem incluir, mas não se limitam a:

- Advertência (por escrito);
- Suspensão das atividades;
- Demissão ou destituição de cargo em comissão, após o devido processo administrativo disciplinar (PAD), garantidos o contraditório e a ampla defesa.

b) Terceiros e Pessoas Jurídicas Contratadas: No caso de empresas prestadoras de serviço, fornecedores ou consultorias:

- O descumprimento de qualquer cláusula desta PSI poderá ser considerado infração contratual, ensejando a aplicação de multas, rescisão unilateral do contrato e impedimento de licitar e contratar com a Administração Pública, conforme a Lei de Licitações vigente.

## 19. ADEQUAÇÃO DA LGPD NO IPREMA

a) Adequação do site

b) Inclusão de informações no site (MENUS DE NAVEGAÇÃO) constantes no ANEXOS desta PSI:

**ANEXO I - O QUE É A LGPD?**

**ANEXO II - TERMO DE PRIVACIDADE**

**ANEXO III – Procedimento Operacional Padrão-POP – Governança do Fluxo de compartilhamento de dados dos servidores ativos, inativos e pensionistas e seus dependentes.**

**ANEXO IV - O USO DE COOKIES (Adequação do site do IPREMA com a implementação da Política de cookies)**

**ANEXO V - SOBRE A PROTEÇÃO DE DADOS**

**ANEXO VI - ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS E CANAL DE COMUNICAÇÃO (Nomeação de encarregado pela proteção dos dados pessoais)**

c) Adequação do arquivo físico

d) Elaboração de manual e mapeamento de medidas de contingências.

e) Envio da PSI para empresas terceirizadas e instituições financeiras.

f) Capacitação da Unidade Gestora: https://www.escolavirtual.gov.br/curso/153/

## 20. CONSIDERAÇÕES FINAIS

20.1 Esta PSI guiará as ações de todos os usuários das informações do RPPS DO MUNICÍPIO DE ARARIPE-CE (IPREMA) de forma a zelar, da melhor maneira possível, pelas informações da autarquia.

20.2 Qualquer dano às informações é muito prejudicial a todos que necessitam dela, então é muito importante que todos estejam engajados em protegê-la.

20.3 Este documento deverá ser revisado a cada dois anos e poderá ser alterado no futuro para contemplar fatos e tecnologias não previstas no momento. Neste caso, haverá devida comunicação aos usuários.

ARARIPE-CE, 23 de março de 2026.

# ANEXO I

## O que é a LGPD?

LGPD é a sigla que denomina a Lei Geral de Proteção de Dados no Brasil, que pretende proteger todos os dados pessoais utilizados por pessoas físicas e jurídicas que estejam no território brasileiro e em alguns casos, fora do país, previsto na Lei nº 13.709, de 14 de agosto de 2018. Ela busca proteger os direitos fundamentais de liberdade e privacidade que estão previstos na Constituição Federal, além de trazer regras que devem ser respeitadas acerca do armazenamento, compartilhamento, tratamento e coleta de dados pessoais, discorrendo inclusive sobre as penalidades para quem não obedecer a essas regras. A LGPD entrou em vigor no ano de 2020, contudo as suas sanções só passaram a vigorar a partir do dia 1º de agosto de 2021.

## Quais conceitos são importantes para compreender a LGPD?

Dado pessoal: dado relacionado à pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político; dado referente à saúde, ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento: 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.

Agentes de tratamento: São o Controlador e o Operador.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

Encarregado: pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados pessoais (ANPD). Também denominado Data Protection Officer (DPO).

**Qual a finalidade de tratamento dos dados pessoais pelo IPREMA?**

No uso de suas atribuições, todos os dados, documentos e informações tratados pelo IPREMA vinculam-se exclusivamente à finalidade pública, destinados a subsidiar a prestação do serviço público para o qual o IPREMA foi criado.

**Quais os direitos dos titulares de dados segundo a LGPD?**

Conforme expresso na LGPD, o titular dos dados pessoais possui o direito a obter do Controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

1. Confirmação da existência de tratamento;
2. Acesso aos dados;
3. Correção de dados incompletos, inexatos ou desatualizados;
4. Anonimização, bloqueio ou eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
5. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da ANPD, observados os segredos comercial e industrial;

6. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD;
7. Informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;
8. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
9. Revogação do consentimento, nos termos do §5º do art. 8º da LGPD.
10. Como o IPREMA Garante a Segurança dos dados pessoais?
11. O IPREMA garante a segurança dos dados pessoais através dos procedimentos estabelecidos na Política de Segurança de documentos, informações e proteção de dados pessoais, bem como com a realização de treinamentos e workshops de segurança da informação junto aos seus servidores.
12. O que é a Política de Segurança de Documentos, Informações e Proteção de Dados Pessoais?
13. É um documento contendo um conjunto de regras gerais que direcionam a segurança e privacidade da informação deste Instituto, e são suportadas por normas e procedimentos que devem ser seguidas por toda a organização, orientando a segurança da informação, conforme o ramo de negócio, legislação e normas vigentes, possuindo caráter de documento jurídico.
14. Para fins da elaboração deste documento, foram consideradas as normas ABNT NBR ISO/IEC 27001:2013 – Segurança da Informação e ABNT NBR ISO/IEC 27002:2013 – Código de Prática para controles de segurança da informação, a Lei nº 8.159/1991 – Política Nacional de Arquivos Públicos e Privados, a Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI) e a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

**Como os titulares de dados pessoais podem exercer os direitos previstos na LGPD?**

Nos moldes da Lei de Acesso à Informação, os cidadãos podem efetivar seu direito de acesso pelo canal de ouvidoria do IPREM https://iprema.com.br/institucional/contato/ pelo Sistema de Informações ao

Cidadão (SIC), ou pelo Portal de Transparência do Município de Araripe-CE https://araripe.ce.gov.br/ouvidoria-municipal/

Quanto aos titulares de dados pessoais, a LGPD estabelece que esse poderá solicitar do órgão esclarecimentos acerca da finalidade e forma de tratamento dos dados, os quais estão especificados no teor da Política de Segurança de documentos, informações e proteção de dados pessoais, a qual constará no portal do IPREMA para consulta, além da possibilidade de solicitar informações por meio de requerimento, através do setor “IPREMA-DPO - Departamento de Proteção de Dados”.

# ANEXO II

**TERMO DE PRIVACIDADE - Portal do Instituto de Previdência do Município de Araripe-CE, site mantido pelo IPREMA, desenvolvido e administrado pela empresa terceirizada.**

Esse termo de privacidade tem por finalidade estabelecer as regras para o tratamento de dados pessoais coletados dos usuários, além do registro de suas atividades, de acordo com as leis aplicáveis.

É importante destacar que o Instituto de Previdência do Município de Araripe empreende esforços para proteger a privacidade dos usuários e visitantes deste site, especialmente no que se refere à segurança da informação. Seus dados pessoais são protegidos pela Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018.

## PRINCIPAIS DEFINIÇÕES

Para fins deste Termo de Privacidade, considera-se:

1. Dado pessoal Qualquer informação relacionada à pessoa natural, direta ou indiretamente, identificada ou identificável.
2. Dado sensível Categoria especial de dados pessoais referentes à origem racial ou étnica, convicção religiosa, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, referentes à saúde ou à vida sexual, dados genéticos ou biométricos relativos à pessoa natural.
3. Titular Pessoa natural a quem se referem os dados pessoais, tais como antigos, presentes ou potenciais clientes, colaboradores, contratados, parceiros comerciais e terceiros.
4. Tratamento 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. Anonimização Processo por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, considerados os meios técnicos razoáveis e disponíveis no momento do tratamento.
6. Agentes de tratamento São o Controlador e o Operador.
7. Controlador pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados.
8. Encarregado Geral Pessoa indicada pelo controlador e operador como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
9. Encarregado Setorial Pessoa indicada nos termos do Decreto Municipal nº 9792/2021, assim como ao encarregado geral, com a função de executar a Política Municipal de Proteção de Dados Pessoais.
10. Banco de Dados Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
11. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709/2018 em todo o território nacional.

## USO E ARMAZENAMENTO DE DADOS E INFORMAÇÕES

Os dados são coletados por meio dos requerimentos, cadastros e da pesquisa de satisfação, por conseguinte armazenados nas bases de dados do Instituto, onde:

1. Os requerimentos (aposentadoria, pensão, revisão de benefício e administrativos) são enviados por meio de formulários onde os dados necessários para o atendimento da demanda são coletados e conservados indefinidamente, com o objetivo de controlar e acompanhar os requerimentos e mensagens, tendo em vista minimizar os processos abertos em duplicidade. Em alguns formulários, é possível gerar uma cópia de sua solicitação para visualização e/ou impressão.
2. Cadastros de atualização da base de dados dos segurados e beneficiários

3. A pesquisa de satisfação salva os dados indefinidamente, porém, os dados são anônimos, com a finalidade de obter um histórico da evolução da qualidade do atendimento prestado pelos servidores e/ou serviços avaliados. Esses dados podem subsidiar melhorias no atendimento e serviços ofertados pelo IPREMA.
4. Compartilhamento de dados e informações

## SOBRE OS SISTEMAS UTILIZADOS DE COLETAS DE INFORMAÇÕES DE RECADASTRAMENTO E PROVA DE VIDA

O Instituto de Previdência do Município efetua o compartilhamento de dados com órgãos públicos quando instituído por leis, regulamentos, decretos ou similares, e com entidades privadas quando há necessidade estritamente funcional, vinculado aos contratos ou instrumentos congêneres. Para esse compartilhamento são estabelecidos direitos e deveres das partes, visando impedir a utilização dos dados pessoais de maneira diferente daquela estabelecida pela empresa e/ou que violem as legislações de privacidade aplicáveis. Também é exigido que todos os envolvidos tratem os dados pessoais com segurança e sigilo, e os mantenham apenas por período determinado. Estas obrigações permanecem mesmo após o fim do relacionamento entre as partes.

## ATUALIZAÇÕES DESSE TERMO DE PRIVACIDADE

O IPREMA informa que este documento poderá ser atualizado, a qualquer tempo, sem aviso prévio, razão pela qual se recomenda a sua verificação periódica. Desta maneira, caso este Termo de Privacidade seja alterado, a data ao final do documento será atualizada, constando a última versão. Alterações neste Termo de Privacidade não se aplicam de forma retroativa.

# ANEXO III

## PROCEDIMENTO OPERACIONAL PADRÃO (POP) – COMPARTILHAMENTO DE DADOS

ESTRUTURA DE GOVERNANÇA DE COMPARTILHAMENTO SEGURO DE DADOS DE SERVIDORES E DEPENDENTES

1. Objetivo: Padronizar o compartilhamento de dados de servidores ativos, inativos, pensionistas e dependentes com o Poder Executivo, Ministério Público, Tribunais de Contas e Instituições Financeiras Conveniadas.

2. Abrangência: Diretoria-Executiva e Sistemas de Informação.

3. Base Legal: Artigos 23 e 26 da LGPD (Tratamento e uso compartilhado de dados pelo Poder Público para fins de interesse público e execução de políticas públicas).

4. Fluxo Operacional de Execução:
   Recebimento da Demanda ➔ Análise de Legitimidade ➔ Tratamento e Minimização ➔ Canal Seguro de Envio ➔ Registro em Log

   Passo 1: Recebimento e Triagem da Demanda
   Toda solicitação externa de dados deve ser oficializada por meio de ofício formalizado, e-mail institucional homologado ou requisição via sistema oficial do convênio bancário.

   Passo 2: Análise de Legitimidade e Finalidade
   O setor de cadastro ( RH ou setor designado) e o DPO devem verificar se há previsão em Lei, regulamento, decreto ou contrato ativo para o

compartilhamento.É expressamente proibido repassar informações a terceiros sem justificativa ou autorização explícita.

Passo 3: Minimização dos Dados

Ao extrair o banco de dados dos segurados e pensionistas, o operador do IPREMA deve filtrar apenas os campos estritamente necessários para a finalidade requerida.

Dados financeiros, pessoais, de saúde/perícia médica (sensíveis) ou dados de dependentes menores de idade devem ser tarjados ou retidos, exceto quando indispensáveis à auditoria ou cumprimento de obrigação legal.

Passo 4: Transmissão por Canal Seguro

Regra de Conexão: A transferência dos arquivos digitais deve ser realizada obrigatoriamente dentro da rede protegida do instituto.

Trabalho Remoto/Externo: Se o operador estiver fora da sede, o envio exige o uso mandatório da VPN configurada pela TI.

Vedações de Envio: É terminantemente proibido enviar listagens contendo dados pessoais por e-mails particulares, aplicativos de mensagens instantâneas comuns ou armazená-los em ferramentas de nuvem não homologadas (ex: Dropbox pessoal).

Passo 5: Termo de Compromisso de Terceiros

No envio de dados para instituições financeiras (consignados), exigir formalmente que a entidade trate as informações sob sigilo absoluto, sendo vedada a utilização para marketing de produtos não contratados.

Passo 6: Registro de Log

A Gerência de TI manterá o registro automatizado (log) de quem acessou, editou, exportou ou transmitiu a base de dados, salvaguardando a responsabilidade civil e administrativa da autarquia. O registro em log consiste na gravação automatizada e cronológica de todos os eventos relevantes realizados nos sistemas operacionais, bancos de dados e redes do IPREMA.

# ANEXO IV

## UTILIZAÇÃO DE COOKIES

INCLUIR MENSAGEM AO ACESSAR O SITE:
Termos de privacidade - Este site armazena dados como cookies para habilitar suas funcionalidades, incluindo análises e personalização. Ao usar este site, você aceita automaticamente o uso de cookies ou pode optar em não aceitar e limitar.

### O QUE SÃO COOKIES?

Os cookies são utilizados pelo IPREMA para facilitar e aprimorar a navegação no seu site. Eles são pequenos arquivos que ficam armazenados no seu computador ou no seu dispositivo móvel através do browser e que possibilitam que você tenha uma experiência de visualização mais rápida, prática e individualizada, entre outras coisas. Também utilizamos este tipo de arquivo para reconhecê-lo(a) como um visitante anterior do nosso site ou aplicativo e para preencher formulários de forma automática no site.

### COMO UTILIZAMOS OS COOKIES?

Usamos preferencialmente a ferramenta Google Analytics e Google Tag Manager para inserção dos códigos necessários que usamos para registrar elementos da sua navegação de forma a permitir uma experiência mais apurada e efetiva.

### NOSSAS PÁGINAS UTILIZAM COOKIES PARA REGISTAR:

As suas preferências em termos de visualização, tais como parâmetros relativos ao contraste e à cor ou ao tamanho dos caracteres;
Se você já respondeu a um questionário ou realizou o preenchimento de um formulário em uma janela/página separada em que lhe é perguntado se acha útil ou não o conteúdo da página em questão (para que o mesmo deixe de aparecer se

já respondeu) ou refaça o preenchimento de dados que tenha que ser inseridos em outra visita;
Se você já deu ou não o seu acordo quanto à instalação de cookies;
Se você já fechou ou não um banner em nossa página;
Se você está visitando o site diretamente (digitando o endereço no seu navegador) ou advindo de alguma outra plataforma de redes sociais (como Facebook ou Twitter) ou sistema de busca (como Google, Yahoo ou Bing);
Se um ou mais vídeos inseridos nas nossas páginas foram vistos;
Se um ou mais arquivos .pdf foram baixados;
Se você clicou em algum botão ou link para realizar uma ação específica;

**TIPOS DE COOKIES**

Tipo Descrição Como gerir esse cookie
Cookies de essenciais São os mínimos necessários para que o site funcione minimamente sem te incomodar demais, permitindo navegar no mesmo e utilizar os seus serviços e funcionalidades. Sem estes cookies absolutamente necessários, o site não irá funcionar tão bem como nós gostaríamos, e podemos não ser capazes de fornecer certas experiências ou determinados serviços ou recursos a ele associados. Aceitar / recusar através de configuração do navegador.
Cookies de sessão Esses cookies de sessão são usados para manter o estado da aplicação ativa enquanto você navega, costumam interferir na usabilidade do website. Aceitar / recusar através de configuração do navegador.
Cookies persistentes São utilizados para guardar informações por um prazo maior de tempo como ajustes de interface, popups visualizados, dados de navegação, normalmente não interferem fortemente na utilização do website.

Aceitar / recusar através de configuração do navegador.

Identificação de Usuário Esses cookies de identificação de usuário são usados para garantir que quem está utilizando só veja a sua própria informação. Aceitar / recusar através de configuração do navegador.

Segurança Os cookies de segurança são usados para os controles de segurança e verificações. Aceitar / recusar através de configuração do navegador.

A ativação dos cookies persistentes não é indispensável para que um site de internet funcione, mas facilita a sua navegação. Eles podem ser apagados ou bloqueados no seu navegador, mas se o fizer poderá desativar algumas funcionalidades do site e você acabará recebendo alertas novamente, o que pode tornar sua navegação mais lenta e maçante.

As informações associadas aos cookies não são utilizadas para identificar pessoalmente qualquer visitante, ou seja, ninguém pode identificar você, essa troca de informações só se dá dentro do seu próprio computador, entre o seu navegador e o servidor que mantém as páginas do site.

# ANEXO V

## SOBRE A PROTEÇÃO DE DADOS

O Instituto de Previdência do Município de ARARIPE-CE é autarquia responsável por gerir o Regime Próprio de Previdência Social dos servidores efetivos do município de ARARIPE-CE e conduz suas atividades de forma íntegra e transparente, zelando pela privacidade de seus beneficiários e servidores ativos, conforme nossa Política de Segurança da Informação, de documentos e de proteção de dados pessoais.

É dever do IPREMA garantir a confidencialidade e integridade dos dados pessoais a que tem acesso, utilizando-os exclusivamente para as finalidades específicas e legítimas, franqueando o acesso ao respectivo titular, nos termos da Lei nº 13.709/2018 (LGPD - Lei Geral de Proteção de Dados) e desta Política de Segurança da Informação.

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta política de segurança da informação, tem como objetivo: Estabelecer os procedimentos para utilização correta dos ativos de tecnologia da informação pertencentes ao Instituto de Previdência do Município de ARARIPE-CE (IPREMA), a fim de evitar incidentes que possam: inutilizar, extinguir ou alterar as informações e recursos utilizados no instituto; Promover a conscientização para com a segurança da informação; Prover meios que contribuam para a manutenção dos princípios da segurança da Informação e seus aspectos: Confidencialidade, Integridade e Disponibilidade, Autenticidade e Não repúdio.

## ANEXO VI

**ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS**

NOME DO (A) DESIGNADO(A):

CONTATOS:

E-mail: https://iprema.com.br/institucional/contato/

Fone:

**CANAL DE COMUNICAÇÃO**

Para exercer os seus direitos enquanto titular de dados pessoais, você pode entrar em contato conosco através da nossa Ouvidoria https://iprema.com.br/institucional/contato/