

Política de Proteção de DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÃO *2025*



MÁRCIO GOMES DE LIMA – TC QOBM
Diretor Geral

NÚCLEO DE PROTEÇÃO DE DADOS

GLEYCE DOS SANTOS BARBOSA JOBIM – 1º TEN QCOBM
Representante do Corpo Técnico/ Coordenador do NPD

KÉDIMA PRISCILA MELO DA SILVA – 1º TEN QCOBM
Encarregada do Tratamento de Dados

ELENICE CATAO AMUTARES - 1º TEN QCOBM
Representante do Setor de Informática

ANGELI CRISTIANE VARJÃO DA SILVA – 3º SGT QCPBM
Representante do Setor Pessoal

ELLEN WHITE DA SILVA DIAS – Assistente Social
Representante da Ouvidoria

Manaus, novembro de 2025





CONTROLE DE REVISÕES

[illegible]

<https://www.instagram.com/pggm.am/>
<https://www.instagram.com/bombeiros.cbmam/>
diretoria@poligmestrinho.am.gov.br
 Fone: (92) 99213-8618
 Avenida Getúlio Vargas, 341 - Centro
 Manaus - AM
 CEP: 69020-010

Policlínica
Governador
Gilberto Mestrinho

Corpo de
**Bombeiros Militar
do Amazonas**
Diretoria de Saúde



A autenticidade deste documento pode ser conferida no site
<https://edoc.amazonas.am.gov.br/62E8.77A7.4766.634E/F776C534>
 Código verificador: **62E8.77A7.4766.634E** CRC: **F776C534**

SUMÁRIO

FINALIDADE	5
ABRANGÊNCIA.....	5
CONTATOS.....	6
TERMOS E DEFINIÇÕES.....	7
OBJETIVOS.....	13
PRINCÍPIOS E DIRETRIZES	14
FUNÇÕES E RESPONSABILIDADES	15
2. Compete aos Gestores (gerentes e chefes)	17
3. Compete ao Núcleo Proteção de Dados:	18
4. Compete ao controlador:	20
5. Compete ao encarregado de proteção de dados:.....	21
6. Compete ao setor de informática	23
7. Compete ao setor pessoal.....	24
8. Compete à unidade de controle interno (UCI).....	25
9. Compete à ouvidoria.....	25
10. Compete ao operador	26
TRATAMENTO DE DADOS PESSOAIS E INFORMAÇÕES	27
CONSCIENTIZAÇÃO, CAPACITAÇÃO E SENSIBILIZAÇÃO.....	32
SEGURANÇA E BOAS PRÁTICAS	34
ENSINO E PESQUISA	36
AUDITORIA E CONFORMIDADE	38
CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES.....	39
PENALIDADES	41
DISPOSIÇÕES FINAIS.....	42
REFERÊNCIAS.....	43
ANEXOS	45



FINALIDADE

A Política de Proteção de Dados Pessoais e Segurança da Informação tem por finalidade estabelecer conceitos, objetivos, princípios, diretrizes, responsabilidades e ações que garantam a proteção dos dados pessoais dos titulares e dos ativos de informações da Policlínica Governador Gilberto Mestrinho, visando mitigar riscos às informações e aos dados pessoais tratados na instituição, e no que couber, no relacionamento com outras entidades públicas ou privadas. A aplicação desta Política será pautada pelo dever de boa-fé, ética e observância do disposto na Lei Geral de Proteção de Dados Pessoais (LGPD), na Lei de Acesso à Informação (LAI) e demais outras normas vigentes.

ABRANGÊNCIA

Esta Política regula a proteção de dados pessoais de titulares tratados na Policlínica Governador Gilberto Mestrinho e todos os ativos de informação da mesma, incluindo dados, sistemas, aplicativos, dispositivos e redes. Aplica-se a todos os colaboradores, funcionários, contratados, parceiros, terceiros e pessoas habilitadas pela administração que acessam, processam ou tratam dados pessoais de titulares e informações em nome da Policlínica Governador Gilberto Mestrinho ou nas suas dependências. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela Policlínica Governador Gilberto Mestrinho e entidades subsidiárias.



CONTATOS

Em atendimento aos direitos do titular, relacionados na LGPD, além do atendimento presencial, a PGGM disponibiliza os seguintes canais e atendimento:

Contato institucional: (92) 99213-8618

Ouvidoria: (92) 99303-6352/ ouvidoria@poligmestrinho.am.gov.br

Encarregada de Dados: lgpd@poligmestrinho.am.gov.br



TERMOS E DEFINIÇÕES

AFI – Sistema de Administração Financeira Integrada;

AGENTES DE TRATAMENTO: o controlador e o operador;

AJURI – Sistema de Gestão Material e Patrimônio;

ANPD – Autoridade Nacional de Proteção e Dados;

AUTENTICIDADE - qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

BPA – Boletim de Produção Ambulatorial;

CADSUS – Sistema de Cadastro Nacional de Usuários do SUS;

CBMAM – Corpo de Bombeiros Militar do Amazonas;

CCA – Controle de Concessão de Adiantamento;

CNES – Cadastro Nacional de Estabelecimentos de Saúde;

COMITÊ DE ÉTICA EM PESQUISA (CEP) – colegiado vinculado à instituição que realiza a pesquisa, de natureza pública ou privada, de composição interdisciplinar, constituído de membros das áreas médica, científica e não científica, de caráter consultivo e deliberativo, que atua de forma independente e autônoma, para assegurar a proteção dos direitos, da segurança e do bem-estar dos participantes da pesquisa, antes e no decorrer da pesquisa, mediante análise, revisão e aprovação ética dos protocolos de pesquisa e de suas emendas, bem como dos métodos e materiais a serem usados para obter e documentar o consentimento livre e esclarecido dos participantes da pesquisa;



CONFIDENCIALIDADE – propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

CONSENTIMENTO – manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

CONTROLADOR – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

CSC – Centro de Serviços Compartilhados;

CSC – Centro de Serviços Compartilhados;

DADO ANONIMIZADO – dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

DADO PESSOAL – informação relacionada a pessoa natural identificada ou identificável;

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;

DISPONIBILIDADE – propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

DOCUMENTO - unidade de registro de informações, qualquer que seja o suporte ou formato;



ELIMINAÇÃO – exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

ENCARREGADO – pessoa indicada pelo controlador e operador, para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD);

INFORMAÇÃO – dados processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

INFORMAÇÃO PESSOAL – aquela relacionada à pessoa natural identificada ou identificável;

INFORMAÇÃO SIGILOSA – aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

INTEGRIDADE – propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

LAI - sigla de Lei de Acesso a Informação;

LGPD - sigla de Lei Geral de Proteção de Dados Pessoais;

MESA LIMPA – prática de organização do local de trabalho na qual o colaborador deve armazenar qualquer tipo de material impresso (papéis, lembrete, anotações, documentos em geral) que contenha informações institucionais ou dados pessoais de titulares, visando o resguardo dessas informações durante a ausência do funcionário no seu local e/ou estação de trabalho e a prevenção de acesso não autorizado;

NPD – Núcleo de Proteção de Dados;



OPERADOR – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

PNCP – Portal Nacional de Contratações Públicas;

PRIMARIEDADE – qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações;

PRODAM – Processamento de Dados Amazonas S/A;

REGULA SES – Sistema do Complexo Regulador do Amazonas;

SALUX – sistema digital de gerenciamento de atendimentos atualmente implantado na PGGM;

SAME – Serviço de Arquivo Médico e Estatística;

SEGURANÇA DA INFORMAÇÃO – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

SES/AM – Secretaria de Estado de Saúde do Amazonas;

SGC – Sistema de Gestão de Contratos, instrumento de gestão de contratos do Poder Executivo Estadual do Amazonas;

SIASUS – Sistema de Informação Ambulatorial do SUS;

SICLOM – sistema de controle logístico de medicamentos, sistema digital de atendimento utilizado para dispensação de medicamentos do Componente Estratégico da Assistência Farmacêutica (CESAF) no âmbito do SUS;

SIGED – Sistema Integrado de Gestão Eletrônica de Documentos;



SIGTAP – Sistema de Gerenciamento da Tabela de Procedimento, Medicamentos e OPM do SUS;

SISAIH – Sistema de Informações Hospitalares;

SISMEDEX – sistema digital de atendimento utilizado para dispensação de medicamentos do Componente Especializado da Assistência Farmacêutica (CEAF) no âmbito do SUS;

SISREG – Sistema de Regulação e Marcação de Consultas;

SISREG – Sistema Nacional de Regulação, plataforma digital do Ministério da Saúde do Brasil para gerenciar e organizar o acesso da população a serviços de saúde no SUS;

SISSA – Sistema de Solicitação de Autorização;

SUS – Sistema Único de Saúde;

TABWIN – Sistema de Transferência de arquivos DATASUS;

TELA LIMPA – prática de organização do local de trabalho na qual o colaborador deve desconectar seu usuário de recursos tecnológicos protegidos por senhas individuais sempre que se afastar dos dispositivos, visando a prevenção de acesso não autorizado a informações institucionais e dados pessoais de titulares durante a ausência do funcionário no seu local e/ou estação de trabalho;

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO – documento no qual o indivíduo ou seu representante legal manifesta sua disposição de participar voluntariamente da pesquisa, após ter sido informado e esclarecido sobre todos os aspectos relevantes para a tomada de decisão sobre sua participação;



TERMO DE RESPONSABILIDADE – termo assinado pelo usuário, concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

TITULAR – pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

TRATAMENTO DA INFORMAÇÃO – conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

TRATAMENTO DE DADOS – 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;

UCI – Unidade de Controle Interno, setor da PGGM responsável por supervisionar e aprimorar os controles internos, promovendo a eficiência, a transparência e a conformidade com leis e regulamentos;



OBJETIVOS

- I. estabelecer medidas eficazes para o cumprimento das normas de proteção de dados pessoais, ativos de informação e conhecimentos gerados ou recebidos pela PGGM e demonstrar a eficácia das mesmas;
- II. estabelecer competências e responsabilidades quanto à segurança dos dados pessoais e das informações;
- III. promover o alinhamento das ações de segurança de dados pessoais e informações com as estratégias de planejamento organizacional da PGGM;
- IV. promover a criação de programas de treinamento e conscientização para que os colaboradores entendam suas responsabilidades e procedimentos na proteção de dados pessoais e informações;
- V. estabelecer revisões de processos com o objetivo de aferir a diminuição ou aumento de riscos que envolvem o tratamento de dados pessoais e ativos de informação;
- VI. promover a adequada gestão do tratamento dos dados pessoais e ativos de informação;
- VII. promover a formulação regras de segurança, de boas práticas e de governança com objetivo de definir procedimentos e outras ações referentes a privacidade e proteção de dados pessoais e ativos de informação;



PRINCÍPIOS E DIRETRIZES

O tratamento de dados pessoais e de ativos de informação no âmbito da PGGM será pautado pelo dever de boa-fé, pelas determinações constitucionais e administrativas que norteiam a Administração Pública Estadual, bem como pelos seguintes princípios e diretrizes:

- I. Finalidade, adequação, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas referentes ao tratamento de dados pessoais;
- II. Propriedade, disponibilidade, integridade, confidencialidade, primariedade e autenticidade das informações;
- III. Alinhamento da Política de Proteção de Dados e Segurança da Informação com o planejamento estratégico e a continuidade dos processos e serviços essenciais para o funcionamento da PGGM;
- IV. Responsabilidade do usuário de informação e dos agentes de tratamento de dados pessoais pelos atos inconformes com as normas e legislações aplicáveis;
- V. Respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;
- VI. Observância da publicidade de informações como preceito geral e do sigilo como exceção;
- VII. Educação e comunicação como alicerces fundamentais para o fomento da proteção de dados pessoais e da segurança da informação.



FUNÇÕES E RESPONSABILIDADES

Qualquer pessoa natural ou jurídica de direito público ou privado que tenha interação em qualquer fase do tratamento de dados pessoais de titulares e acesso a informações da PGGM deve assegurar a privacidade e a proteção dos mesmos, inclusive após o término do tratamento, observando as medidas técnicas e administrativas determinadas pela PGGM.

A estrutura da Gestão de Proteção de Dados Pessoais e Segurança da Informação da Policlínica Governador Gilberto Mestrinho é composta pela Alta Administração (Direção e Gestores), Núcleo de Proteção de Dados, Encarregado de Proteção de dados, controlador (papel desempenhado pela alta administração em cooperação com a SES/CBMAM), setor pessoal, setor de tecnologia da informação e operadores/usuários de informação.



1. Compete à Direção

- I. Formalizar, aprovar e zelar pelo cumprimento dessa política fornecendo meios para assegurar o desenvolvimento, implementação e atualização da mesma;
- II. Atender ao disposto nos normativos e publicações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) que disciplinam o tratamento e a governança dos dados pessoais;
- III. Elaborar, quando couber, o Plano de Resposta à Incidentes e Relatório de Impacto de Proteção de Dados Pessoais (RIPD) relacionados às operações de tratamento, e atualizá-lo quando necessário;
- IV. Realizar o desenvolvimento e a atualização das políticas/avisos de privacidade, que tem por finalidade o fornecimento de informações sobre o tratamento de dados pessoais em cada ambiente físico ou virtual, bem como, especificar as medidas de proteção de dados adotadas para salvaguardar esses dados pessoais;
- V. Propor recursos necessários às ações de proteção de dados pessoais de titulares e à segurança da informação;
- VI. Acompanhar os trabalhos do Núcleo de Proteção de Dados;
- VII. Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à proteção de dados pessoais de titulares e à segurança da informação;
- VIII. Autorizar, revisar e revogar os acessos de estudantes e pesquisadores a informações institucionais e dados pessoais de titulares para fins de ensino e pesquisa, mediante assinatura de carta de anuência nos casos necessários;



2. Compete aos Gestores (gerentes e chefes)

- I. Gerenciar os dados pessoais e as informações geradas ou sob a responsabilidade da sua área de gestão durante todo o seu Ciclo de Vida;
- II. Identificar, classificar e rotular as Informações geradas ou sob a responsabilidade da sua área de gestão conforme normas, critérios e procedimentos adotados pela Instituição, com base na LAI, legislações específicas e no guia para classificação de informações em grau de sigilo da secretaria de segurança pública do Amazonas;
- III. Autorizar, revisar e revogar os acessos à recursos tecnológicos, dados pessoais e informações sob sua responsabilidade, mediante assinatura do termo de responsabilidade e comunicação com o setor pessoal e o setor de informática;
- IV. Determinar a participação dos colaboradores da sua área nas ações de capacitação e de profissionalização de recursos humanos em temas relacionados à proteção de dados pessoais de titulares e à segurança da informação;
- V. Zelar pelo cumprimento dessa política por todos os colaboradores de sua área;
- VI. Revisar e propor atualizações à presente Política.



3. Compete ao Núcleo Proteção de Dados:

- I. Implementar, revisar e monitorar a política institucional de proteção de dados pessoais e segurança da informação, assegurando o cumprimento das diretrizes internas relativas à privacidade e à segurança da informação;
- II. Assegurar a conformidade das atividades de tratamento de dados pessoais com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), inclusive por meio da elaboração de registros de tratamento e relatórios de impacto à proteção de dados;
- III. Orientar e capacitar os colaboradores, promovendo ações de sensibilização, treinamentos e atividades educativas relacionadas à proteção de dados pessoais e à segurança da informação;
- IV. Atuar como canal oficial de comunicação com a Autoridade Nacional de Proteção de Dados (ANPD), inclusive no que se refere à notificação de incidentes de segurança e ao atendimento de demandas regulatórias;
- V. Garantir o atendimento às solicitações dos titulares de dados pessoais, assegurando o exercício dos direitos previstos na LGPD, como acesso, retificação, exclusão, oposição e portabilidade de dados;
- VI. Realizar avaliações de impacto à proteção de dados pessoais e informações institucionais, identificando riscos associados e propondo medidas de mitigação;
- VII. Gerenciar incidentes de segurança envolvendo informações institucionais e dados pessoais, adotando providências para sua contenção, mitigação, registro e comunicação às autoridades competentes, quando necessário;
- VIII. Auditar e monitorar continuamente as atividades relacionadas ao ciclo de vida das informações e dados pessoais no âmbito da unidade, com vistas à conformidade com as normas legais e regulamentares aplicáveis;



- IX. Manter atualizados os registros das operações de tratamento de dados pessoais, de forma a evidenciar a conformidade com a legislação vigente;
- X. Acompanhar e analisar alterações legislativas e regulamentares, bem como boas práticas nacionais e internacionais em proteção de dados, recomendando atualizações às políticas e procedimentos internos;
- XI. Avaliar os impactos da legislação e da regulamentação relacionada à privacidade e à proteção de dados pessoais às disposições desta Política e trabalhar em conjunto com as áreas de Tecnologia da Informação para garantir o cumprimento das normas aplicáveis e implementar melhorias nos procedimentos, controles e medidas de segurança, visando à mitigação de riscos às Informações aos Dados Pessoais;

O Núcleo de Proteção de Dados (NPD) será constituído no mínimo por:

- I. o encarregado de dados pessoais;
- II. um representante do corpo técnico;
- III. um representante do setor de informática;
- IV. um representante do setor pessoal
- V. um representante da ouvidoria;

A Coordenação do Núcleo de Proteção de Dados e Segurança da Informação será exercida pelo componente indicado pela Direção.

A responsabilidade pelas decisões relacionadas ao tratamento de dados pessoais e ao sigilo de informações é da Alta Administração da PGGM, em parceria com a SES e CBMAM, que no exercício das atribuições típicas de controlador determinam as medidas necessárias para executar a Política de Proteção de Dados Pessoais e Segurança da Informação dentro de sua estrutura organizacional.



4. Compete ao Controlador:

- I. Observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos no momento de decidir sobre um futuro tratamento ou realizá-lo;
- II. Considerar o preconizado pelos art. 7º, art. 11 e art. 23 antes de realizar o tratamento de dados pessoais;
- III. Cumprir o previsto pelos art. 46 e art. 50 da LGPD buscando à proteção de dados pessoais e sua governança;
- IV. Indicar um encarregado pelo tratamento de dados pessoais, divulgando a identidade e as informações de contato do encarregado de forma clara e objetiva, preferencialmente no sítio institucional;
- V. Elaborar o inventário de dados pessoais a fim de manter registros das operações de tratamento de dados pessoais;
- VI. Reter dados pessoais somente pelo período necessário para o cumprimento da hipótese legal e finalidade utilizadas como justificativa para o tratamento de dados pessoais;
- VII. Criar e manter atualizados os avisos ou políticas de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou virtual, e como os dados pessoais neles tratados são protegidos;
- VIII. Requerer dos operadores a ciência com o termo de confidencialidade para cada tipo serviço acessado, informatizado ou não, que trate dados pessoais de titulares e informações da PGGM;
- IX. Determinar que os colaboradores tenham o menor nível de privilégio e o mínimo de acesso aos recursos necessários para realizar suas tarefas;



- X. Determinar que os contratos de prestação e serviço firmados pela Policlínica Governador Gilberto Mestrinho contenham cláusula específica sobre a obrigatoriedade de atendimento à essa Política de Proteção de Dados Pessoais e Segurança da Informação;

5. Compete ao Encarregado de Proteção de Dados:

- I. Compor o Núcleo de Proteção e Dados;
- II. Receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, inclusive junto à ANPD;
- III. Receber comunicações e requisições da ANPD e adotar providências;
- IV. Orientar os colaboradores da organização a respeito das práticas a serem adotadas em relação à proteção de dados pessoais e informações institucionais;
- V. Conduzir o diagnóstico de privacidade e identificar vulnerabilidades no acesso aos dados pessoais de titulares e às informações da PGGM;
- VI. Fomentar as ações de prevenção à incidentes de segurança da informação;
- VII. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;

O Encarregado de Proteção de Dados prestará assistência e orientação à alta administração na elaboração, definição, e implementação de:



- I. regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da LGPD;
- II. inventário de dados pessoais;
- III. plano de resposta a incidentes;
- IV. relatório de impacto à proteção de dados pessoais;
- V. instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;
- VI. outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.



6. Compete ao Setor de Informática

- I. Compor o Núcleo de Proteção de Dados;
- II. Aplicar a presente Política de forma que a proteção dos dados pessoais e informações estejam alinhados com a carta de serviços da PGGM;
- III. Apoiar a alta administração na seleção de recursos tecnológicos que contemplem as normas de segurança de dados e informações;
- IV. Criar metodologia institucional para identificar e classificar os riscos inerentes à Segurança da Informação da Instituição e Dados Pessoais dos Titulares;
- V. Recomendar e/ou adotar controles que mitiguem os riscos mapeados, inerentes à Segurança da Informação e à Proteção de Dados Pessoais;
- VI. Recomendar e/ou implementar processos de autenticação e controle de acesso seguros para os Recursos Tecnológicos;
- VII. Desenvolver e participar de programas de treinamento para os colaboradores da PGGM de forma a conscientizá-los sobre as responsabilidades de todos relação à Segurança da Informação e dos dados pessoais;
- VIII. Manter atualizado o inventário de Recursos de Tecnologia, com todos os sistemas, aplicativos, softwares, ferramentas de gerenciamento de informações e dados da Instituição;
- IX. Em conjunto com o Encarregado e com o Núcleo Proteção de Dados, gerir, analisar e acompanhar os Incidentes de Segurança da Informação e as suspeitas ou casos de violações dessa Política, definindo as ações de remediação conforme as diretrizes e procedimentos estabelecidos pela Instituição e acompanhando sua implementação pelas áreas responsáveis;
- X. Revisar e propor atualizações à presente Política.



7. Compete ao Setor Pessoal

- I. Compor o Núcleo de Proteção de Dados;
- II. Garantir que, no momento da contratação, o colaborador da PGGM tenha ciência desta Política e assine o termo responsabilidade anexo;
- III. Apoiar as ações de sensibilização, treinamentos e atividades educativas relacionadas à proteção de dados pessoais e à segurança da informação promovidas pelo NPD;
- IV. Informar imediatamente para a área de Tecnologia da Informação todas as contratações, transferências, afastamentos, desligamentos, mudanças de funções, licenças e modificações no quadro de colaboradores sob a sua supervisão;
- V. Informar imediatamente para a área de Tecnologia da Informação todas as autorizações, revisões e revogações de acessos à recursos tecnológicos, dados pessoais e informações determinadas pelos gestores;



8. Compete à Unidade de Controle Interno (UCI)

- I. Colaborar com o NPD para a Implementação, revisão e monitoramento da política institucional de proteção de dados pessoais e segurança da informação;
- II. Apoiar as ações de sensibilização, treinamentos e atividades educativas relacionadas à proteção de dados pessoais e à segurança da informação promovidas pelo NPD;
- III. Colaborar com a alta administração na produção do Plano de Resposta à Incidentes e Relatório de Impacto à Proteção de Dados;
- IV. Oferecer apoio jurídico à Alta Administração e ao Encarregado de Dados em casos de incidentes de segurança da informação e dados pessoais;

9. Compete à Ouvidoria

- I. Compor o Núcleo de Proteção de Dados;
- II. Colaborar com o NPD para a Implementação, revisão e monitoramento da política institucional de proteção de dados pessoais e segurança da informação
- III. Apoiar as ações de sensibilização, treinamentos e atividades educativas relacionadas à proteção de dados pessoais e à segurança da informação promovidas pelo NPD;
- IV. Apoiar o encarregado de dados nas ações de recebimento de reclamações e comunicações dos titulares e da ANPD;



10. Compete ao Operador

- I. Conhecer e fazer cumprir essa política e a demais norma de proteção a dados pessoais de titulares e segurança da informação;
- II. Compreender e assinar o termo de responsabilidade instituído nessa política;
- III. Adotar a conduta e todos os procedimentos necessários para proteger as Informações da Instituição e os dados pessoais dos titulares, incluindo evitar discutir assuntos de trabalho em ambientes públicos ou em áreas expostas;
- IV. Observar os princípios estabelecidos no art. 6º da LGPD e os princípios e diretrizes dessa política, ao realizar tratamento de dados pessoais de titulares e acessar informações da PGGM;
- V. Seguir as diretrizes estabelecidas pelo controlador;
- VI. Verificar se as diretrizes estabelecidas pelo controlador cumprem os requisitos legais presentes nos art. 7º, art. 11 e art. 23 da LGPD, antes de efetuar o tratamento de dados;
- VII. Responsabilizar-se por seus atos durante a etapas do ciclo de vida dos dados pessoais de titulares e informações da PGGM dos quais participar ou tiver acesso;
- VIII. Participar de ações de capacitação e iniciativas relacionadas à proteção de dados e segurança da informação;
- IX. Comunicar formalmente ao Encarregado de Dados qualquer incidente ou ameaça à segurança da informação e à proteção de dados;
- X. Comunicar formalmente à alta administração da PGGM qualquer descumprimento ou violação dessa Política ou demais normas correlatas;



TRATAMENTO DE DADOS PESSOAIS E INFORMAÇÕES

No âmbito a Policlínica Governador Gilberto Mestrinho, o tratamento de dados pessoais e dados pessoais sensíveis será realizado somente nas hipóteses previstas nas seções I e II do capítulo II da LGPD. Da mesma forma, o tratamento de dados pessoais de crianças e adolescentes ocorrerá nos termos da seção III do capítulo II da LGPD.

O uso compartilhado de dados pessoais deverá ocorrer em estrita observância ao art. 26 da LGPD.

A Policlínica Governador Gilberto Mestrinho não realiza transferência internacional de dados pessoais.

Durante a rotina prevista na carta de serviços da unidade serão seguidas as seguintes regras gerais durante o ciclo de vida dados pessoais de titulares:

- I. **Coleta de dados:** será realizada somente por operadores autorizados pela alta administração e signatários do termo de responsabilidade, orientados a coletar apenas informações necessárias à prestação do serviço e adequadas às finalidades do serviço prestado, prezando-se pela qualidade do dado obtido, sendo os dados mais frequentemente coletados: nome completo, nome social, gênero, orientação sexual, idade, endereço, telefone, email, RG, CPF, CNS, cor, etnia, dados biométricos, dados de saúde, prontuário, exames, entre outros;



- II. **Armazenamento:** os dados serão armazenados principalmente em meios digitais, como pastas de rede administradas pela PRODAM, sistemas digitais rastreáveis e com acesso por senha individual (como SALUX, SISREG, SISMEDEX, SICLOM, SIGED, SGC, entre outros), nuvem digital e arquivos físicos sob controle restrito (SAME, Almoxarifado, Setor Pessoal, entre outros), de forma a garantir a segurança contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão acidentais ou ilícitas;
- III. **Compartilhamento:** os dados coletados na PGGM serão compartilhados somente com órgãos de saúde autorizados ou mediante previsão legal.
- IV. **Acesso:** os dados coletados e armazenados no âmbito da PGGM poderão ser consultados, alterados, corrigidos ou excluídos a pedido do titular, de forma gratuita, seguindo-se a normas internas da instituição;
- V. **Descarte/ eliminação:** será realizado o descarte de dados armazenados em arquivo físico ou eliminação de dados armazenados em meios digitais de forma sigilosa, de acordo com prazos legais previstos para cada caso;



No âmbito da PGGM será assegurado o direito fundamental de acesso à informação conforme os princípios básicos da administração pública e seguindo as diretrizes prevista na Lei nº 12527 de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI).

Às informações não sigilosas de interesse público serão, preferencialmente, disponibilizadas no site da instituição.

Quando não estiverem disponíveis no site, tais informações poderão ser formalmente solicitadas, devendo a solicitação ser atendida imediatamente sempre que possível. Não sendo possível conceder o acesso imediato, a solicitação de informação não sigilosa deverá ser atendida em um prazo de até 20 (vinte) dias, podendo ser prorrogado por mais 10 (dez) dias, mediante justificativa expressa, da qual será cientificado o requerente. O fornecimento das informações solicitadas será gratuito e, preferencialmente, por meios digitais.

Os ativos de informações da PGGM considerados sigilosos podem ser não classificados (com restrições de acesso respaldada em legislação específica) ou classificados, com base na LAI, como reservado, secreto e ultrassecreto, tendo prazos máximos de restrição de acesso à informação a partir da data de sua produção de 5 anos, 15 anos e 25 anos, respectivamente. Durante esse período a PGGM pode negar o acesso a tais informações sigilosas, esclarecendo o requerente sobre as possibilidades de recursos previstos na LAI.

Durante a rotina prevista na carta de serviços da unidade serão seguidas as seguintes regras gerais durante o ciclo de vida de informações da PGGM:

- I. **Criação e Captura:** informações serão geradas ou adquiridas por meio de atividades institucionais, coleta de dados de titulares e fontes externas ou importação de dados de outros sistemas;
- II. **Classificação e Categorização:** as informações serão organizadas com base em seu tipo, valor e uso e classificadas pelos gestores com base na



LAI, legislações específicas e no guia para classificação de informações em grau de sigilo da secretaria de segurança pública do Amazonas;

- III. **Armazenamento e Arquivamento:** as informações necessárias aos trabalhos realizados na PGGM ou em razão dela serão armazenadas em sistemas adequados, dependendo de sua classificação, principalmente em meios digitais, como pastas de rede administradas pela PRODAM, sistemas digitais rastreáveis e com acesso por senha individual (como SALUX, SISREG, SISMEDEX, SICLOM, SIGED, SGC, entre outros), nuvem digital e arquivos físicos sob controle restrito (SAME, Almoxarifado, Setor Pessoal, entre outros), de forma a garantir a segurança contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão acidentais ou ilícitas;
- IV. **Acesso e Uso:** o acesso às informações e recursos tecnológicos (internet, e-mail institucional, sistemas, dispositivos, nuvem, entre outros) será realizado somente por colaboradores autorizados pela alta administração e signatários do termo de responsabilidade, orientados a utilizá-los conforme o previsto nessa Política e demais normas aplicáveis para fins estritamente relacionados aos trabalhos realizados na PGGM ou em razão dela;
- V. **Manutenção e Proteção:** para garantir a manutenção e proteção das informações, as pessoas autorizadas e sistemas utilizados devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa. Serão utilizados recursos tecnológicos seguros, preferencialmente institucionais (SISREG, SISMEDEX, SICLOM, SIGED, SGC, e-mail institucional) ou certificados pela ISO 27001:2022 (DETIN/PRODAM), pela Sociedade Brasileira de Informática em Saúde (SBIS) em nível de Garantia de Segurança 2 e pela SAFEWEB (SALUX). Adicionalmente serão adotadas medidas como o bloqueio de sites inseguros ou não relacionados às atividades de trabalho, bem como orientação dos colaboradores a não abrir anexos suspeitos recebidos por e-mail e praticar os conceitos de “mesa limpa” e “tela limpa” nos terminais de trabalho;



- VI. **Descarte:** será realizado o descarte de dados armazenados em arquivos físicos ou eliminação de dados armazenados em meios digitais de forma sigilosa, de acordo com prazos legais previstos para cada caso, de forma definida pelos gestores setoriais. Para arquivos excluídos diretamente no servidor de rede, tanto em ambientes Windows Server quanto Linux Server, não há envio para a Lixeira, dessa forma, a exclusão é considerada permanente;



CONSCIENTIZAÇÃO, CAPACITAÇÃO E SENSIBILIZAÇÃO

Os servidores da Policlínica Governador Gilberto Mestrinho com acesso a informações e dados pessoais devem participar de programas de conscientização, capacitação e sensibilização em matérias de segurança da informação, privacidade e proteção de dados pessoais, objetivando adequar o tema aos seus papéis e responsabilidades. Para tanto serão realizados:

- I. **Capacitação Institucional contínua:** será realizado um treinamento inicial de todos os atuais colaboradores da PGGM no qual os mesmos serão informados sobre os termos da LAI/LGPG, seus papéis, suas responsabilidades, a Política de Proteção de Dados Pessoais e Segurança da Informação e a Política de Privacidade da PGGM. Continuamente, cada colaborador que passar a fazer parte da equipe da PGGM, será esclarecido com essas mesmas informações pelo pessoal de RH e gestores setoriais, com apoio do Núcleo de Proteção de Dados. Eventualmente todos os servidores serão convidados a realizarem cursos *on line* em plataformas digitais gratuitas sobre o tema;
- II. **Campanha “LGPD todo dia”:** serão enviados informativos digitais (textos, fotos e vídeos) sobre a LAI/LGPD, a Política de Proteção de Dados Pessoais e Segurança da Informação e a Política de Privacidade da PGGM semanalmente nos 3 primeiros meses após a publicação desses documentos e, após esse período, mensalmente. Adicionalmente, serão fixados produtos de comunicação visual nos murais da PGGM de forma permanente, atualizando-se quando necessário;



- III. **Semana da LGPD:** será um evento realizado trienalmente, com ampla divulgação e participação dos colaboradores, composto de atividades como educação continuada sobre a LAI/LGPD, Política de Proteção de Dados Pessoais e Segurança da Informação e a Política de Privacidade da PGGM, rodas de conversa, compartilhamento de casos reais, competições e outras atividades propostas a cada edição;



SEGURANÇA E BOAS PRÁTICAS

Considerando a necessidade de mitigar incidentes com informações e dados pessoais, devem ser adotadas as seguintes medidas técnicas e organizacionais de privacidade e proteção de dados:

- I. O acesso aos recursos utilizados na PGGM sempre que possível será realizado por meio do registro de senha pessoal e intransferível após firmados os termos de responsabilidade para cada caso;
- II. Os recursos tecnológicos adquiridos pela PGGM deverão oferecer segurança aos dados pessoais e informações, considerando o conceito de economicidade;
- III. Os colaboradores, sistema e contratados terão o menor nível de privilégio e o mínimo de acesso aos recursos necessários para realizar suas tarefas;
- IV. O acesso aos dados pessoais e às informações deve estar limitado às pessoas que deles necessitem para realizar o trabalho proposto;
- V. O acesso aos dados pessoais e informações registradas e armazenadas em meios físicos serão acessados somente por pessoal autorizado e descartados de forma a não haver possibilidade de acesso indevido;
- VI. Nos postos de trabalho serão adotadas as práticas de mesa limpa e tela limpa, prevenindo acesso a informações e dados pessoais físico e digitais por terceiros não autorizados;
- VII. Todos os dados pessoais devem estar armazenados em ambiente seguro, de modo que terceiros não autorizados não possam acessá-los;



Qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais dos titulares deve ser comunicada a Autoridade Nacional de Proteção de Dados (ANPD) dentro do prazo previsto pela LGPD.

A PGGM mantém uma base de conhecimento com documentos que apresentam condutas e recomendações que melhoram o gerenciamento de risco e orientam na tomada de decisões adequadas em casos de comprometimento de dados pessoais, a saber:

- I. **A Política de Proteção de Dados Pessoais e Segurança da Informação:** cujo conteúdo que deve ser de conhecimento de todos os colaboradores;
- II. **A Política de Privacidade:** cujo conteúdo deve estar disponível para conhecimento de todos os usuários dos serviços;
- III. **O Plano de Resposta a Incidentes:** que está sendo elaborado pelo Núcleo de Proteção de Dados, cujo conteúdo deve ser de conhecimento dos setores de TI, UCI e gestores;
- IV. **O Relatório de Impacto à Proteção de Dados:** que será elaborado, quando necessário, pela Direção juntamente com o Núcleo de Proteção de Dados, cujo conteúdo deve ser de conhecimento dos gestores, ANPD e auditores;



ENSINO E PESQUISA

O uso de dados de titulares tratados na PGGM para fins de pesquisa deverão seguir os preceitos da lei 14.874, de 28 de maio de 2024 e demais legislações aplicáveis.

Os dados pessoais e sensíveis tratados e armazenados no âmbito da PGGM poderão ser utilizados para fins de realização de estudos por órgãos de pesquisa, garantida, sempre que possível a sua anonimização, conforme previsto na LGPD.

Quando anonimizados, é dispensado o fornecimento de consentimento do titular para uso dos dados para essa finalidade. Quando não for possível utilizar os dados anonimizados, indica-se a solicitação de consentimento do titular, quando tratar-se de estudo prospectivo, em caso de estudo retrospectivo, indica-se a solicitação de dispensa de consentimento ao Comitê de Ética em Pesquisa que avaliará o projeto.

Nas hipóteses em que os dados pessoais anonimizados estejam disponíveis para domínio público, será dispensada a solicitação de anuência institucional para uso dos mesmos.

Nas hipóteses em que os dados pessoais não estejam disponíveis para domínio público, será necessária a solicitação da anuência institucional para uso dos mesmos, sendo a resposta da Direção decidida a cada caso considerando-se as legislações pertinentes.

A direção deve responder às solicitações de anuência para acesso a informações institucionais e dados pessoais tratados na instituição em até 30 dias, prorrogáveis por mais 30, mediante justificativa expressa, da qual será cientificado o requerente.

A solicitação de anuência institucional deverá ser encaminhada oficialmente por escrito pelo requerente à Direção contendo, no mínimo, o título, justificativa, objetivos, metodologia e resultados esperados do trabalho, bem como, expressamente relacionados os dados e informações as quais deseja ter acesso. Informações adicionais podem ser solicitadas no ato da solicitação ou posteriormente pela Direção, com apoio do Núcleo de Educação Permanente e Humanização (NEPSHU), Núcleo de Proteção de Dados (NPD) e Unidade de Controle Interno (UCI).



A solicitação de anuência poderá ser feita por meio físico, no apoio à direção, ou digital pelo e-mail: diretoria@poligmestrinho.am.gov.br.

A resposta à solicitação de anuência será dada por meio digital em forma de carta de anuência (anexa a essa política).



AUDITORIA E CONFORMIDADE

O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais e informações e da garantia das cláusulas de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

As atividades e serviços desenvolvidos na PGGM devem observar os requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes para estarem em conformidade.

Será realizada anualmente ação de verificação de conformidade para diagnóstico de problemas, feedbacks e planejamento de ações corretivas por meio de formulários digitais com ampla divulgação e participação dos colaboradores para identificar possíveis falhas no tratamento de dados de titulares, coletar sugestões, reclamações e cases de sucesso. Com base nos resultados obtidos, serão realizadas as ações corretivas necessárias, a serem definidas pelo NPD, em cada caso;

Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação de conformidade.



CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Os contratos, convênios, acordos e instrumentos similares atualmente em vigor, que de alguma forma envolvam o tratamento de dados pessoais, precisam incorporar cláusulas específicas em total conformidade com a presente Política de Proteção de Dados Pessoais e Segurança da Informação e que contemplem minimamente:

- I. requisitos mínimos de segurança da informação;
- II. determinação de que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador;
- III. requisitos de proteção de dados pessoais que os operadores de dados pessoais devem atender;
- IV. condições sob as quais o operador deve permitir acesso, devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador;
- V. diretrizes específicas sobre o uso de subcontratados pelo operador para execução contratual que envolva tratamento de dados pessoais.



A Gerência Administrativa e Financeira (GEAF), em especial o Setor de Contratos, devem estar cientes do conteúdo do Guia de Requisitos e Obrigações quanto à Privacidade e Segurança da Informação da Secretaria de Governo Digital, que orienta a adequação do processo de contratação para contemplar os requisitos mais importantes de privacidade e segurança dos dados.

As unidades organizacionais da PGGM devem adotar medidas rigorosas com o propósito de assegurar que os terceiros e processadores de dados pessoais contratados estejam plenamente em conformidade com as cláusulas contratuais estabelecidas no momento da celebração do acordo entre as partes envolvidas.



PENALIDADES

O não cumprimento desta Política ou de qualquer dos demais padrões institucionais de Proteção de Dados Pessoais e Segurança de Informação, comprovado após a devida apuração, serão passíveis de penalidades, tanto na esfera administrativa (advertências, punições administrativas, demissão ou rescisão contratual, entre outras) quanto na esfera civil e penal (reparação dos danos causados à Instituição e às demais pessoas prejudicadas), conforme a gravidade do ato, nos termos da legislação aplicável,, assegurados aos envolvidos o contraditório e a ampla defesa.

Casos de descumprimento desta Política serão registrados e comunicados à diretoria para ciência e tomada das providências cabíveis.

Entre as penalidades que estarão sujeitos aqueles que infringirem a Política de Proteção de Dados Pessoais e Segurança da Informação relacionam-se: advertência, suspensão, demissão, destituição de cargo, quebra de contrato ou rescisão do vínculo com o poder público, suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a dois anos, declaração de inidoneidade para licitar ou contratar com a administração pública, até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, multa, entre outras penalidades cabíveis, além de responsabilização civil e/ou militar, a depender de cada caso.



DISPOSIÇÕES FINAIS

Essa política encontra-se disponível na pasta de rede e será enviada a todos os colaboradores por meios digitais, poderá ser disponibilizada aos titulares de dados sempre que necessário, ou em caso de indisponibilidade, pode ser solicitada para o encarregado de dados da PGGM.

Os integrantes do Núcleo de Proteção de Dados (NPD) poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos à Proteção de Dados Pessoais alinhados às diretrizes emanadas pelo NPD e aos respectivos Planos Estratégicos Institucionais da PGGM.

Dúvidas e esclarecimentos sobre a Política de Proteção de Dados Pessoais e Segurança da Informação e seus documentos podem esclarecidos junto ao Núcleo de Proteção de Dados, por meio do contato do encarregado de dados.

Esta política será revisada e atualizada em intervalos não superiores a 4 (quatro) anos, a partir do início de sua vigência, ou em caso de atualização necessária à adequação de novas legislações pertinentes. Todas as alterações oriundas de revisão deverão ser registradas.

Os casos omissos serão resolvidos pela Direção Geral da PGGM com apoio do NPD.

Esta política entra em vigor na data de sua publicação.



REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Abril de 2022. Acesso em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso: 08/09/2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08/09/2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso: 08/09/2025.

BRASIL. Lei nº 14.874, de 28 de maio de 2024. Dispõe sobre a pesquisa com seres humanos e institui o Sistema Nacional de Ética em Pesquisa com Seres Humanos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14874.htm. Acesso: 09/09/2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Guia de Requisitos e Obrigações quanto a Privacidade e à Segurança da Informação. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_requisitos_obrigacoes.pdf. Acesso 08/09/2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Modelo de Política de Segurança da Informação. Disponível em:



https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_seguranca_informacao.pdf. Acesso 08/09/2025.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Modelo de Política de Proteção de Dados Pessoais. Disponível em:

https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_ppdp.pdf. Acesso 08/09/2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação. Disponível em:

<https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1>. Acesso em: 08/09/2025.

[GUIA para Classificação de informações em grau de sigilo: classificação, declassificação e transparência. Secretaria de Segurança Pública do Amazonas. 2024. Disponível em:](#)

<https://www.ssp.am.gov.br/wp-content/uploads/2024/12/GUIA-PARA-CLASSIFICACAO-DE-INFORMACOES-EM-GRAU-DE-SIGILO.pdf>. Acesso: 10/09/2025.

POLÍTICA Corporativa de Segurança da Informação e Proteção de Dado Pessoais.

Empresa Brasileira de Correios e Telégrafos. 2022. Disponível em:

<https://www.correios.com.br/aceso-a-informacao/institucional/legislacao/politicas-corporativas/arquivo/politica-corporativa-de-segurancao-informacao>. Acesso: 05/09/2025.

POLÍTICA de Segurança da Informação. ACCAMARGO. 2021. Disponível em:

https://accamargo.org.br/sites/default/files/2021/05/politica-seguranca-informacao-0007_01_0.pdf. Acesso: 10/09/2025.



ANEXOS

- Termo de Responsabilidade;
- Modelo de Carta de Anuência;





TERMO DE RESPONSABILIDADE PARA O TRATAMENTO DOS DADOS E INFORMAÇÕES

NOME:	
MATRÍCULA OU CPF:	SETOR:
TIPO DE VÍNCULO: () MILITAR () CIVIL ESTATUTÁRIO () ESTAGIÁRIO () OUTRO:	

OBSERVAÇÃO: CPF SÓ SERÁ UTILIZADO PARA QUEM NÃO TEM MATRÍCULA

Em observância à Lei de Acesso à informação nº 12.527, de 18 de novembro de 2011 e à Lei Geral de Proteção de Dados nº 13.709 de 14 de agosto de 2018, e alterações dada pela Lei nº13.853, de 08 de julho de 2019, através do presente instrumento, eu SERVIDOR/COLABORADOR acima descrito, reconheço que:

- I. Em razão da utilização das ferramentas tecnológicas/equipamentos médico-hospitalares disponibilizados pela PGGM, poderei ter acesso a diversas informações institucionais e dados pessoais, sensíveis e sigilosos, e me comprometo a tratá-los conforme os preceitos das leis vigentes;
- II. Tenho inequívoco conhecimento de que minhas credenciais de acesso (login e senha) a essas ferramentas são de uso pessoal e intransferível e de conhecimento exclusivo, sendo de minha responsabilidade zelar pela segurança destas credenciais de acesso;
- III. Tenho ciência de que meus dados pessoais utilizados para acesso aos sistemas disponibilizados pela PGGM, serão conservados durante o tempo que estiver vigente a relação contratual, sendo de minha responsabilidade solicitar a exclusão a qualquer tipo de acesso permitido quando for desligado das funções por quaisquer motivos;

Por intermédio do presente TERMO me comprometo:

1. A conhecer e fazer cumprir a Política de Proteção de Dados Pessoais e Segurança da Informação da PGGM;
2. A conhecer e fazer cumprir a Política de Privacidade da PGGM;
3. A não utilizar ou apropriar para mim ou para outrem, de QUALQUER informação, incluindo dado pessoal, dado pessoal sensível e documentos, sigilosos ou não, a que tiver acesso, para uso indevido ou alheio às suas atribuições. No presente ou futuro, ou para o uso de terceiros;
4. A não efetuar nenhuma gravação, fotografia ou cópia de documentação, base de dados, sistemas computacionais, informações ou outras tecnologias a que tiver acesso, sem a devida autorização;
5. A não divulgar de nenhuma maneira ou por qualquer meio as informações, incluindo dados e documentos pessoais, a que tiver acesso;
6. Em cuidar para que as informações confidenciais fiquem restritas ao conhecimento tão somente das pessoas que estejam diretamente envolvidas nos atendimentos;
7. A informar qualquer forma de tratamento de dados pessoais indevidos;
8. A adotar todas as medidas possíveis durante o tratamento de dados, de forma a não permitir o vazamento de dados pessoais, dados pessoais sensíveis e ou informações sigilosas;

Página 46 de 49

<https://www.instagram.com/pggm.am/>
<https://www.instagram.com/bombeiros.cbmam/>
diretoria@poligmestrinho.am.gov.br
 Fone: (92) 98406-1098
 Avenida Getúlio Vargas, 341 - Centro
 Manaus - AM
 CEP: 69020-010

Policlínica
Governador
Gilberto Mestrinho

Corpo de
**Bombeiros Militar
do Amazonas**
Diretoria de Saúde



A autenticidade deste documento pode ser conferida no site
<https://edoc.amazonas.am.gov.br/62E8.77A7.4766.634E/F776C534>
 Código verificador: **62E8.77A7.4766.634E** CRC: **F776C534**



9. Estou ciente enquanto servidor/estagiário que no momento do meu desligamento ou finalização de estágio, devo comparecer ao RH para que sejam cancelados os todos os acessos a programas e arquivos institucionais.

A vigência da obrigação de tratamento de dado adequado, assumida pela minha pessoa por meio deste termo, deverá ser mantida por tempo indeterminado.

Pelo não cumprimento do presente TERMO DE RESPONSABILIDADE PARA O TRATAMENTO DOS DADOS - LGPD, fica o abaixo assinado ciente de todas as sanções administrativas e ou judiciais que poderão advir.

Manaus-AM, _____ de _____ de _____

Assinatura do colaborador

Considerando o termo acima assinado, autorizo o presente colaborador a ser cadastrado para acesso a:

- | | |
|--|--|
| ☐ Rede de internet; | ☐ Pastas de Rede; |
| ☐ Salux; | ☐ Ajuri; |
| ☐ Sismedex; | ☐ SGC; |
| ☐ Siclom; | ☐ Siged; |
| ☐ SisReg; | ☐ _____; |

Manaus-AM, _____ de _____ de _____

Gestor

Página 47 de 49



TERMO DE ANUÊNCIA

Declaramos para os devidos fins que estamos de acordo com a
execução do projeto de pesquisa intitulado
“

_____”, sob a coordenação e a responsabilidade do(a) pesquisador(a)
Prof(a). _____, e assumimos o compromisso de apoiar o
desenvolvimento da referida pesquisa a ser realizada nessa instituição, no
período de ____/____/____ a ____/____/____, após a devida aprovação
no Sistema CEP/CONEP.

Manaus-AM, _____ de _____ de _____

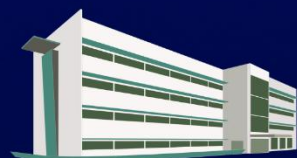
DIRETOR GERAL





GOVERNO DO
AMAZONAS
A FORÇA DA NOSSA GENTE

Secretaria de **Saúde**



POLICLINICA GOVERNADOR
GILBERTO MESTRINHO



A autenticidade deste documento pode ser conferida no site
<https://edoc.amazonas.am.gov.br/62E8.77A7.4766.634E/F776C534>
Código verificador: **62E8.77A7.4766.634E** CRC: **F776C534**