



Política de Segurança da Informação

PARANAGUAPREV

Versão	2.0
Data de vigência	07/07/2026
Elaborado por	Luciana Camargo Franco
Aprovado por	Presidente – Ali El Kadri
Próxima revisão prevista	07/07/2028

Sumário

1. OBJETIVO	3
2. ABRANGÊNCIA.....	3
3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO	3
4. GOVERNANÇA E RESPONSABILIDADES	4
4.1 Alta Administração.....	4
4.2 Responsável pela Segurança da Informação	4
4.3 Infraestrutura de TI	4
4.4 Usuários	5
5. CONTROLE DE ACESSO	5
5.1 Princípios Gerais	5
5.2 Responsável pela Gestão de Acessos	5
5.3 Procedimento de Concessão de Acesso Lógico	5
5.4 Alteração ou Revogação de Acessos	6
5.5 Controle de Acesso Físico.....	6
5.6 Responsabilidades dos Usuários.....	6
6. USO DE INTERNET, E-MAIL E SISTEMAS	6
7. BACKUP, CONTINGÊNCIA E CONTINUIDADE	7
8. INCIDENTES DE SEGURANÇA.....	7
9. TERCEIROS E CONTRATOS	8
10. LGPD E PROTEÇÃO DE DADOS	9
11. TREINAMENTO E CONSCIENTIZAÇÃO	9
12. VIGÊNCIA, REVISÃO E CONTROLE DE VERSÃO	10
13. DISPOSIÇÕES FINAIS.....	10
HISTÓRICO DE VERSÕES	11

1. OBJETIVO

A presente Política de Segurança da Informação (PSI) tem por objetivo estabelecer diretrizes, princípios, responsabilidades e controles mínimos necessários para a proteção das informações sob a guarda da Paranaguá Previdência, assegurando a confidencialidade, a integridade, a disponibilidade, a legalidade e a rastreabilidade das informações, em conformidade com a legislação vigente e com as boas práticas aplicáveis à Administração Pública.

Esta Política visa orientar o uso adequado dos ativos de informação, sejam eles físicos ou digitais, próprios ou terceirizados, prevenindo acessos não autorizados, vazamentos de dados, indisponibilidades de sistemas, perdas de informação e outros incidentes que possam comprometer a continuidade das atividades institucionais, a proteção dos dados pessoais dos segurados, servidores e demais titulares, bem como a imagem e a credibilidade da Paranaguá Previdência.

Considerando a realidade organizacional e tecnológica da entidade, caracterizada pela inexistência de estrutura própria de Tecnologia da Informação e pela utilização predominante de sistemas, serviços e infraestrutura terceirizados, esta Política estabelece controles proporcionais, viáveis e compatíveis com o porte da instituição, atribuindo responsabilidades claras aos usuários internos e aos prestadores de serviços contratados, sem impor exigências técnicas incompatíveis com sua capacidade operacional.

A PSI constitui instrumento fundamental de governança, integrando-se aos processos administrativos, aos contratos firmados com terceiros, às ações de proteção de dados pessoais e às exigências do Programa Pró-Gestão RPPS, servindo como referência obrigatória para a tomada de decisões relacionadas à segurança da informação e à gestão de riscos informacionais no âmbito da Paranaguá Previdência.

Esta Política é complementada por documentos operacionais específicos, especialmente o Manual Simplificado de Contingência e Continuidade, a Matriz de Contingência e Continuidade e os Formulários de Contingência e Revisão Anual, os quais detalham os procedimentos mínimos de continuidade, registro de ocorrências, acionamento de responsáveis e fornecedores, mapeamento de riscos, evidências mínimas e revisão periódica dos controles relacionados à segurança da informação.

2. ABRANGÊNCIA

Aplica-se a:

- Servidores públicos;
- Estagiários;
- Prestadores de serviço;
- Empresas contratadas para fornecimento de sistemas, suporte técnico, hospedagem, e-mail e armazenamento em nuvem;
- Qualquer pessoa que tenha acesso, ainda que eventual, às informações da Paranaguá Previdência.

3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A PSI fundamenta-se nos seguintes princípios:

- Confidencialidade
- Integridade
- Disponibilidade
- Legalidade e Finalidade
- Responsabilização e Prestação de Contas

4. GOVERNANÇA E RESPONSABILIDADES

4.1 Alta Administração

Compete à Presidência:

- Aprovar esta Política;
- Garantir sua divulgação;
- Assegurar cláusulas contratuais de segurança da informação;
- Designar responsável formal pela gestão da PSI.

4.2 Responsável pela Segurança da Informação

A gestão da PSI será exercida por responsável formalmente designado, podendo acumular funções administrativas, não sendo exigida estrutura própria de Tecnologia da Informação.

Compete ao Responsável pela Segurança da Informação:

- Coordenar a aplicação da PSI;
- Interagir com prestadores de serviço;
- Acompanhar incidentes de segurança da informação e respectivas providências;
- Acompanhar as revisões da PSI e dos documentos complementares;
- Manter e revisar o Manual Simplificado de Contingência e Continuidade;
- Manter e revisar a Matriz de Contingência e Continuidade;
- Assegurar a utilização dos Formulários de Contingência e Revisão Anual nos casos aplicáveis;
- Coordenar a revisão anual dos procedimentos de contingência e continuidade, com apoio da Diretoria Administrativa e dos prestadores de serviços, quando necessário;
- Manter registro das ocorrências, revisões, providências adotadas e melhorias identificadas relacionadas à segurança da informação.

4.3 Infraestrutura de TI

A Paranaguá Previdência não possui estrutura própria de Tecnologia da Informação, sendo sua infraestrutura, sistemas e serviços tecnológicos apoiados predominantemente por prestadores de serviços terceirizados.

Nesse contexto:

- A infraestrutura local, incluindo servidor de domínio e arquivos, é administrada por empresa terceirizada;
- O suporte técnico aos usuários é integralmente terceirizado;
- Os sistemas previdenciários e administrativos são fornecidos e mantidos por empresas externas;
- Os serviços de e-mail institucional, hospedagem, site, armazenamento em nuvem, backup e internet dependem de fornecedores contratados ou prestadores responsáveis;
- As responsabilidades técnicas recaem sobre os prestadores contratados, conforme as respectivas cláusulas contratuais, níveis de serviço, canais de atendimento e obrigações de segurança aplicáveis.

Compete à Paranaguá Previdência manter o acompanhamento administrativo desses serviços, registrando os responsáveis internos, prestadores envolvidos, contatos, riscos, impactos, procedimentos de acionamento e evidências mínimas necessárias.

A identificação dos serviços críticos, prestadores envolvidos, responsáveis internos, riscos, procedimentos resumidos e evidências mínimas deverá constar da Matriz de Contingência e Continuidade, mantida como documento complementar a esta Política.

Em situações de falha, indisponibilidade, incidente ou necessidade de continuidade operacional, deverão ser observados, conforme o caso, o Manual Simplificado de Contingência e Continuidade, a Matriz de Contingência e Continuidade e os Formulários de Contingência e Revisão Anual.

4.4 Usuários

Compete aos usuários:

- Utilizar sistemas apenas para fins institucionais;
- Manter sigilo das credenciais;
- Comunicar incidentes;
- Cumprir esta Política.

5. CONTROLE DE ACESSO

O controle de acesso tem como objetivo assegurar que apenas pessoas autorizadas tenham acesso às informações, sistemas e ambientes da Paranaguá Previdência, preservando a confidencialidade, integridade e disponibilidade dos dados institucionais.

Considerando a estrutura organizacional reduzida da entidade e a inexistência de setor próprio de Tecnologia da Informação, o controle de acesso é realizado de forma administrativa, com apoio dos prestadores de serviços responsáveis pelos sistemas utilizados pela instituição.

5.1 Princípios Gerais

O controle de acesso observará os seguintes princípios:

- Utilização de credenciais individuais e intransferíveis;
- Concessão de acesso conforme necessidade funcional (princípio do menor privilégio);
- Registro e rastreabilidade das solicitações de acesso;
- Bloqueio imediato em caso de desligamento ou alteração de função;
- Responsabilidade do usuário pela guarda e sigilo de suas credenciais.

É vedado o compartilhamento de logins ou senhas entre usuários.

5.2 Responsável pela Gestão de Acessos

A gestão administrativa e operacional dos acessos aos sistemas institucionais é exercida pela Diretoria Administrativa, atualmente representada pela servidora Luciana Camargo Franco, que possui perfis administrativos ou de gestão de usuários, quando disponibilizados pelos sistemas utilizados pela instituição.

Compete à responsável:

- Avaliar a necessidade funcional do acesso solicitado;
- Autorizar ou negar solicitações de criação, alteração ou exclusão de acessos;
- Realizar, sempre que possível, a criação, alteração ou bloqueio de usuários diretamente nos sistemas institucionais;
- Solicitar suporte técnico às empresas fornecedoras dos sistemas quando necessário, especialmente em situações que demandem orientação técnica ou intervenção especializada;
- Acompanhar situações de desligamento, afastamento ou mudança de função que exijam revisão dos acessos concedidos.

Os prestadores de serviços de tecnologia atuam exclusivamente em caráter de suporte técnico, não sendo responsáveis pela decisão administrativa de concessão de acessos.

5.3 Procedimento de Concessão de Acesso Lógico

A concessão de acesso aos sistemas institucionais seguirá, sempre que aplicável, as seguintes etapas:

1. O servidor ou setor demandante solicita o acesso necessário para execução de suas atividades institucionais;
2. A solicitação é analisada pela Diretoria Administrativa, que verifica a necessidade funcional do acesso;
3. Uma vez autorizada a solicitação, a responsável realiza a criação ou configuração do acesso diretamente no sistema correspondente, utilizando suas credenciais administrativas;
4. Caso haja necessidade de apoio técnico, poderá ser solicitado suporte ao fornecedor do sistema ou à empresa responsável pelo suporte tecnológico;
5. O usuário recebe suas credenciais de acesso e deverá realizar a troca de senha no primeiro acesso, sempre que o sistema permitir.

Os perfis de acesso deverão refletir exclusivamente as atividades desempenhadas pelo usuário, observando o princípio do menor privilégio.

5.4 Alteração ou Revogação de Acessos

Sempre que ocorrer:

- Mudança de função;
- Afastamento prolongado;
- Desligamento do servidor;
- Encerramento de contrato de prestador de serviço,

a Diretoria Administrativa deverá proceder à alteração, suspensão ou exclusão dos acessos existentes.

Essas medidas serão realizadas diretamente nos sistemas institucionais pela responsável pela gestão de acessos, podendo haver apoio técnico das empresas fornecedoras dos sistemas quando necessário.

5.5 Controle de Acesso Físico

O acesso às dependências administrativas da Paranaguá Previdência é restrito aos servidores, colaboradores autorizados e prestadores de serviço.

Visitantes deverão:

- Identificar-se na recepção ou setor responsável;
- Informar o motivo da visita;
- Permanecer acompanhados por servidor durante a permanência nas dependências da instituição.

Ambientes que contenham equipamentos, documentos ou arquivos institucionais devem permanecer sob responsabilidade dos servidores autorizados.

5.6 Responsabilidades dos Usuários

Todos os usuários que possuam acesso aos sistemas ou informações institucionais devem:

- Manter sigilo sobre suas credenciais;
- Não compartilhar logins ou senhas;
- Bloquear o computador quando se ausentar da estação de trabalho;
- Comunicar imediatamente qualquer suspeita de uso indevido de acesso ou incidente de segurança.

6. USO DE INTERNET, E-MAIL E SISTEMAS

- Uso exclusivamente institucional;
- Vedado compartilhamento de senhas;
- Vedado armazenamento de dados institucionais em nuvens pessoais;
- O e-mail institucional e o site são serviços terceirizados, devendo observar boas práticas de segurança.

7. BACKUP, CONTINGÊNCIA E CONTINUIDADE

A Paranaguá Previdência adotará medidas proporcionais de backup, contingência e continuidade, compatíveis com sua estrutura administrativa reduzida e com a utilização predominante de sistemas, serviços e infraestrutura terceirizados.

O servidor local deverá possuir rotina de backup em nuvem ou solução equivalente, sob responsabilidade do prestador de serviço contratado, cabendo à Paranaguá Previdência manter o acompanhamento administrativo dos responsáveis, contatos, canais de atendimento e evidências disponíveis.

Os sistemas terceirizados utilizados pela entidade deverão manter rotinas próprias de backup, segurança, disponibilidade e recuperação, conforme responsabilidade dos respectivos fornecedores e cláusulas contratuais aplicáveis.

A Paranaguá Previdência manterá mapeamento dos responsáveis internos, prestadores, serviços críticos, riscos, impactos, procedimentos de acionamento e evidências mínimas relacionadas à continuidade das atividades institucionais, sem realizar operação técnica direta dos ambientes terceirizados.

Para apoio à aplicação prática desta Política, serão mantidos como documentos complementares:

- Manual Simplificado de Contingência e Continuidade, contendo os procedimentos mínimos de atuação diante de indisponibilidades, falhas, incidentes, interrupções de serviços, internet, e-mail, arquivos, sistemas, energia ou prestadores de tecnologia;
- Matriz de Contingência e Continuidade, contendo o mapeamento dos processos, sistemas, serviços, riscos, impactos, responsáveis internos, prestadores, procedimentos resumidos e evidências mínimas;
- Formulários de Contingência e Revisão Anual, destinados ao registro de ocorrências, acionamento de responsáveis e fornecedores, providências adotadas, normalização, pendências e revisão anual dos procedimentos.

A Paranaguá Previdência não mantém plano próprio de recuperação de desastres interno complexo, em razão de sua estrutura reduzida e da terceirização dos serviços de tecnologia, devendo adotar procedimentos simplificados, proporcionais e documentados de contingência e continuidade.

Os procedimentos de contingência e continuidade deverão ser revisados anualmente ou sempre que houver alteração relevante de sistemas, contratos, fornecedores, responsáveis, contatos, canais de atendimento, estrutura operacional ou riscos identificados.

8. INCIDENTES DE SEGURANÇA

Considera-se incidente de segurança qualquer evento que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade, legalidade ou rastreabilidade das informações, dados, sistemas, arquivos, e-mails, infraestrutura tecnológica ou serviços utilizados pela Paranaguá Previdência.

Todo incidente deverá:

- ser comunicado imediatamente à chefia, à Diretoria Administrativa ou ao Responsável pela Segurança da Informação;

- ser registrado em formulário próprio;
- indicar o sistema, serviço ou informação afetada;
- registrar responsáveis ou fornecedores acionados;
- conter número de protocolo, quando houver;
- indicar as providências adotadas;
- registrar a data e horário de normalização;
- indicar pendências ou ações posteriores.

O registro deverá ser realizado por meio dos Formulários de Contingência e Revisão Anual, especialmente pelo formulário de registro de ocorrência de contingência.

Quando o incidente envolver dados pessoais, o Encarregado de Dados/LGPD deverá ser comunicado, para avaliação das providências cabíveis conforme a legislação aplicável e as orientações da Administração.

9. TERCEIROS E CONTRATOS

Os contratos firmados com terceiros que tenham acesso a informações, sistemas, dados, infraestrutura tecnológica, serviços digitais ou dados pessoais sob responsabilidade da Paranaguá Previdência deverão conter, sempre que aplicável, cláusulas relacionadas à segurança da informação, proteção de dados, confidencialidade, disponibilidade dos serviços e comunicação de incidentes.

Todos os contratos deverão prever, conforme a natureza do objeto contratado:

- Cláusulas de confidencialidade e sigilo das informações acessadas em razão da prestação dos serviços;
- Obrigações mínimas de segurança da informação;
- Responsabilidade pela proteção dos dados, sistemas, acessos, ambientes ou serviços sob gestão do contratado;
- Comunicação imediata à Paranaguá Previdência em caso de incidente, falha, indisponibilidade, vazamento, acesso indevido, perda de dados ou qualquer evento que possa comprometer a segurança da informação;
- Manutenção de rotinas próprias de backup, disponibilidade e recuperação, quando aplicável ao serviço contratado;
- Indicação de canais de atendimento, suporte, chamado ou protocolo;
- Responsabilidade como operador de dados pessoais, quando aplicável, nos termos da legislação de proteção de dados;
- Apoio técnico à Paranaguá Previdência para apuração, contenção, correção e registro de incidentes relacionados aos serviços prestados.

Os prestadores de serviços relacionados a sistemas, suporte técnico, hospedagem, e-mail institucional, armazenamento em nuvem, internet, site institucional, backup ou infraestrutura tecnológica deverão manter canais de atendimento, contatos e procedimentos de acionamento registrados no Manual Simplificado de Contingência e Continuidade e/ou na Matriz de Contingência e Continuidade.

Sempre que houver alteração de fornecedor, contrato, canal de atendimento, telefone, e-mail, nível de serviço, responsável técnico ou escopo do serviço contratado, os documentos complementares deverão ser atualizados.

A Paranaguá Previdência deverá acompanhar administrativamente o cumprimento das obrigações contratuais relacionadas à segurança da informação, sem prejuízo das responsabilidades técnicas assumidas pelos prestadores contratados.

10. LGPD E PROTEÇÃO DE DADOS

A Paranaguá Previdência atua como controladora dos dados pessoais tratados no âmbito de suas atividades institucionais, sendo responsável pela definição das finalidades e meios de tratamento, observadas as competências legais e administrativas aplicáveis.

Os sistemas, serviços e plataformas terceirizadas utilizados pela entidade poderão atuar como operadores de dados pessoais, quando realizarem tratamento de dados em nome da Paranaguá Previdência, nos termos da legislação aplicável e das cláusulas contratuais firmadas.

A Paranaguá Previdência manterá Encarregado de Dados designado, responsável por atuar como canal de comunicação entre a entidade, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados, sem prejuízo das demais responsabilidades internas relacionadas à segurança da informação.

Os direitos dos titulares de dados pessoais serão assegurados, conforme previsto na legislação de proteção de dados, observadas as hipóteses legais de tratamento, as competências institucionais da entidade e os procedimentos administrativos aplicáveis.

Em caso de incidente de segurança envolvendo dados pessoais, o evento deverá ser comunicado ao Responsável pela Segurança da Informação e ao Encarregado de Dados/LGPD, para avaliação das providências cabíveis.

Os incidentes envolvendo dados pessoais deverão ser registrados em formulário próprio, com indicação, sempre que possível, das medidas de contenção adotadas, avaliação preliminar do impacto, dados ou categorias de dados envolvidos, responsáveis acionados, fornecedores envolvidos, providências adotadas e eventual necessidade de comunicação aos titulares ou à autoridade competente.

O tratamento de incidentes envolvendo dados pessoais deverá observar esta PSI, o Manual Simplificado de Contingência e Continuidade, a Matriz de Contingência e Continuidade, os Formulários de Contingência e Revisão Anual e as normas aplicáveis de proteção de dados pessoais.

Os prestadores de serviços que atuem como operadores de dados deverão adotar medidas de segurança compatíveis com o serviço prestado, comunicar imediatamente incidentes ou suspeitas de incidentes e apoiar a Paranaguá Previdência na apuração, contenção e documentação das providências adotadas.

11. TREINAMENTO E CONSCIENTIZAÇÃO

A Paranaguá Previdência promoverá ações simples e proporcionais de treinamento, orientação e conscientização em segurança da informação, compatíveis com sua estrutura administrativa e operacional.

As ações de treinamento e conscientização poderão ocorrer por meio de orientações internas, reuniões, comunicados, envio de materiais informativos, ciência formal da Política de Segurança da Informação ou outras medidas simples de divulgação.

Deverão ser observadas, no mínimo, as seguintes práticas:

- Orientações básicas sobre segurança da informação na admissão ou início das atividades de servidores, estagiários, colaboradores e demais usuários autorizados;
- Divulgação anual da Política de Segurança da Informação aos servidores e colaboradores;
- Orientação sobre o uso adequado de sistemas, e-mail institucional, internet, arquivos, documentos e credenciais de acesso;
- Reforço quanto à vedação de compartilhamento de senhas e ao dever de comunicação imediata de incidentes, falhas, indisponibilidades ou suspeitas de uso indevido;

- Divulgação da existência e finalidade dos documentos complementares da PSI, especialmente o Manual Simplificado de Contingência e Continuidade, a Matriz de Contingência e Continuidade e os Formulários de Contingência e Revisão Anual;
- Orientação básica sobre a proteção de dados pessoais e a comunicação de incidentes envolvendo dados pessoais ao Responsável pela Segurança da Informação e ao Encarregado de Dados/LGPD.

Em razão da estrutura reduzida da entidade, não há exigência de programas complexos, plataformas especializadas ou ferramentas específicas de treinamento, sendo admitidas ações simplificadas, documentadas e proporcionais à realidade da Paranaguá Previdência.

12. VIGÊNCIA, REVISÃO E CONTROLE DE VERSÃO

Esta Política de Segurança da Informação entra em vigor na data de sua aprovação e deverá ser observada por todos os servidores, estagiários, colaboradores, prestadores de serviço e demais usuários que tenham acesso às informações, sistemas, documentos, ambientes ou serviços da Paranaguá Previdência.

A PSI deverá ser revisada a cada 2 anos ou sempre que houver alteração relevante de legislação, estrutura organizacional, sistemas, contratos, prestadores de serviço, riscos identificados, controles de segurança da informação ou necessidades institucionais.

Os documentos complementares relacionados à contingência e continuidade, especialmente o Manual Simplificado de Contingência e Continuidade, a Matriz de Contingência e Continuidade e os Formulários de Contingência e Revisão Anual, deverão ser revisados anualmente ou sempre que houver alteração relevante de fornecedores, sistemas, responsáveis, contatos, canais de atendimento, estrutura operacional, serviços críticos ou procedimentos de contingência.

A revisão dos documentos complementares deverá gerar registro próprio, ainda que simplificado, por meio dos Formulários de Contingência e Revisão Anual, indicando, quando aplicável, a data da revisão, os participantes, os itens avaliados, os contatos conferidos, a verificação das evidências de backup ou continuidade, as ocorrências analisadas e as melhorias identificadas.

O histórico de versões da PSI deverá ser mantido ao final do documento, contendo, no mínimo, a versão, a data de vigência, o responsável pela elaboração ou revisão, a autoridade aprovadora, a descrição resumida das alterações realizadas e a próxima revisão prevista.

As cópias impressas desta Política são consideradas não controladas, devendo prevalecer a versão eletrônica ou oficialmente aprovada e mantida pela Paranaguá Previdência.

13. DISPOSIÇÕES FINAIS

Esta Política de Segurança da Informação tem por finalidade proteger a Paranaguá Previdência, seus servidores, beneficiários, fornecedores, prestadores de serviços, colaboradores e a sociedade em geral contra riscos relacionados ao uso, tratamento, armazenamento, acesso, compartilhamento, indisponibilidade ou perda de informações.

Todos os usuários, internos ou externos, que tenham acesso às informações, sistemas, documentos, ambientes ou serviços da Paranaguá Previdência possuem responsabilidade pela manutenção de um ambiente seguro, devendo observar as diretrizes desta Política e comunicar imediatamente qualquer suspeita de incidente, falha, indisponibilidade, uso indevido, acesso não autorizado ou violação de segurança da informação.

Integram esta Política, como documentos complementares e operacionais:

- **Manual Simplificado de Contingência e Continuidade;**
- **Matriz de Contingência e Continuidade;**

- **Formulários de Contingência e Revisão Anual.**

O cumprimento desta Política, aliado à cooperação dos usuários e ao apoio contínuo da Administração, contribui para a preservação da confidencialidade, integridade, disponibilidade, legalidade e rastreabilidade das informações, bem como para a proteção dos dados pessoais, a continuidade das atividades institucionais, a confiabilidade dos serviços prestados e a imagem da Paranaguá Previdência.

Paranaguá, 07 de julho de 2026.

HISTÓRICO DE VERSÕES

Versão 01 – 15/01/2026

- Elaboração inicial da Política de Segurança da Informação, adaptada à estrutura organizacional e tecnológica da Paranaguá Previdência.
- **Elaborado por:** Luciana Camargo Franco.
- **Aprovado por:** Presidente – Ali El Kadri.

Versão 02 – 07/07/2026

- Revisão e atualização da Política de Segurança da Informação para inclusão e vinculação dos documentos complementares de segurança da informação: **Manual Simplificado de Contingência e Continuidade, Matriz de Contingência e Continuidade e Formulários de Contingência e Revisão Anual.**
- Também foram realizados ajustes nos itens relacionados a backup, contingência, continuidade, incidentes de segurança, terceiros e contratos, LGPD, treinamento, revisão periódica e controle de versão.
- **Revisado por:** Luciana Camargo Franco.
- **Aprovado por:** Presidente – Ali El Kadri.
- **Próxima revisão prevista:** 07/07/2028, sem prejuízo da revisão anual dos documentos complementares.