

Agência de Previdência Social de Mato Grosso do Sul**POLÍTICA COMPLEMENTAR DE AUDITORIA DE ACESSO LÓGICO, RECUPERAÇÃO DE DESASTRES, BACKUP E RESTAURAÇÃO DA AGEPREV**

PORTARIA AGEPREV Nº 0064, DE 20 DE OUTUBRO DE 2026.

Aprova a Política Complementar de Auditoria de Acesso Lógico, Recuperação de Desastres, Backup e Restauração, no âmbito da Agência de Previdência Social de Mato Grosso do Sul (AGEPREV).

O DIRETOR-PRESIDENTE DA AGÊNCIA DE PREVIDÊNCIA SOCIAL DE MATO GROSSO DO SUL (AGEPREV), no uso de suas atribuições legais,

RESOLVE:

Art. 1º Fica aprovada a Política Complementar de Auditoria de Acesso Lógico, Recuperação de Desastres, Backup e Restauração da Agência de Previdência Social de Mato Grosso do Sul (AGEPREV), na forma do Anexo Único desta Portaria.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Campo Grande-MS, 20 de outubro de 2026.

JORGE OLIVEIRA MARTINS
Diretor-Presidente da AGEPREV

ANEXO ÚNICO DA PORTARIA AGEPREV Nº 0064, DE 20 DE OUTUBRO DE 2026.**POLÍTICA COMPLEMENTAR DE AUDITORIA DE ACESSO LÓGICO, RECUPERAÇÃO DE DESASTRES, BACKUP E RESTAURAÇÃO DA AGEPREV****SUMÁRIO**

1. VINCULAÇÃO NORMATIVA	1
2. OBJETIVO	2
3. ABRANGÊNCIA	2
4. REFERÊNCIAS NORMATIVAS	2
5. PRINCÍPIOS E DIRETRIZES GERAIS	2
6. COMITÊ DE SEGURANÇA DA INFORMAÇÃO	3
6.1 - Finalidade	3
6.2 - Composição	3
6.3 - Competências	3
6.4 - Funcionamento	3
7. GESTOR DE SEGURANÇA DA INFORMAÇÃO	3
8. PROCEDIMENTO DE AUDITORIA DE ACESSO LÓGICO	4
8.1 Objetivo	4
8.2 Periodicidade	4
8.3 Procedimentos	4
8.4 Relatório de Auditoria	4
9. ROTINAS DE RECUPERAÇÃO DE DESASTRES	5
9.1 Objetivo	5
9.2 Situações de Acionamento	5
9.3 Procedimentos para Recuperação	5
9.4 RPO e RTO	5
9.5 Testes das Rotinas de Recuperação	6
10. BACKUP E RESTAURAÇÃO	6

10.1 Objetivo.....	6
10.2 Abrangência.....	6
10.3 Responsabilidade.....	6
10.4 Periodicidade dos Backups.....	7
10.5 Monitoramento.....	7
10.6 Armazenamento.....	7
10.7 Restauração.....	7
10.8 Testes de Restauração.....	7
11. REGISTROS E EVIDÊNCIAS.....	8
12. REVISÃO E ATUALIZAÇÃO DA POLÍTICA.....	8
13. DISPOSIÇÕES FINAIS.....	8

1. VINCULAÇÃO NORMATIVA

A presente Política Complementar de Auditoria de Acesso Lógico, Recuperação de Desastres, Backup e Restauração da Agência de Previdência Social de Mato Grosso do Sul – AGEPREV constitui instrumento subsidiário e complementar à Política de Segurança da Informação do Governo do Estado de Mato Grosso do Sul – PSI, aprovada pela Deliberação CETI nº 02, de 24 de fevereiro de 2022, publicada no Diário Oficial Eletrônico do Estado de Mato Grosso do Sul nº 10.767, de 25 de fevereiro de 2022.

A Política de Segurança da Informação estadual estabelece diretrizes gerais para a proteção dos ativos de informação e aplica-se aos colaboradores, prestadores de serviços, usuários internos e externos e demais pessoas que tenham acesso às informações pertencentes ou custodiadas pelo Governo do Estado de Mato Grosso do Sul.

O presente instrumento não substitui nem afasta as disposições da Política de Segurança da Informação vigente, devendo ser interpretado e aplicado de forma integrada e complementar às normas, políticas e procedimentos de Segurança da Informação adotados pelo Governo do Estado de Mato Grosso do Sul.

Esta Política tem por finalidade detalhar, no âmbito da AGEPREV, os controles relacionados à auditoria de acesso lógico, às rotinas de recuperação de desastres e aos procedimentos de backup e restauração.

Constitui, ainda, instrumento de governança, controle interno e Segurança da Informação destinado ao atendimento dos requisitos aplicáveis ao Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social – Pró-Gestão RPPS, Nível IV.

2. OBJETIVO

A presente Política tem por objetivo estabelecer as diretrizes, responsabilidades, procedimentos e mecanismos de controle relativos à Auditoria de Acesso Lógico, Recuperação de Desastres, Backup e Restauração no âmbito da AGEPREV.

Visa assegurar a proteção dos ativos de informação, a rastreabilidade dos acessos, a continuidade dos serviços e a disponibilidade, integridade e recuperação das informações e dos recursos tecnológicos utilizados pela Autarquia.

3. ABRANGÊNCIA

Esta Política aplica-se a todos os servidores, colaboradores, prestadores de serviços, usuários internos e externos e demais pessoas que tenham acesso autorizado às informações, sistemas, aplicações, bancos de dados, redes, equipamentos ou demais recursos tecnológicos pertencentes, utilizados ou custodiados pela AGEPREV.

Sua aplicação deverá ocorrer de forma integrada à Política de Segurança da Informação do Governo do Estado de Mato Grosso do Sul e às demais normas e procedimentos de Segurança da Informação aplicáveis.

4. REFERÊNCIAS NORMATIVAS

A presente Política observará, especialmente:

- I – a Política de Segurança da Informação do Governo do Estado de Mato Grosso do Sul;
- II – a Política de Controle de Acesso;
- III – a Política de Uso da VPN;

- IV – a Norma de Continuidade de Negócio;
- V – a Política de Backup e Restauração;
- VI – demais normas de Segurança da Informação vigentes no âmbito do Governo do Estado de Mato Grosso do Sul;
- VII – os requisitos aplicáveis do Manual do Pró-Gestão versão vigente.

A PSI estadual também declara alinhamento com as normas ABNT NBR ISO/IEC 27001 e 27002.

5. PRINCÍPIOS E DIRETRIZES GERAIS

A Segurança da Informação deverá ser orientada pela preservação da confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações, conforme estabelecido na Política de Segurança da Informação do Governo do Estado de Mato Grosso do Sul.

Deverão ser observadas as seguintes diretrizes:

- I – concessão de acessos de acordo com a necessidade e as atribuições de cada usuário;
- II – aplicação do princípio do menor privilégio;
- III – utilização de identificação individual e intransferível;
- IV – manutenção de registros que possibilitem a rastreabilidade dos acessos;
- V – proteção das informações contra acessos, alterações, perdas ou divulgações não autorizadas;
- VI – manutenção de cópias de segurança das informações e sistemas relevantes;
- VII – adoção de mecanismos de restauração de dados e recuperação dos serviços;
- VIII – identificação, registro e tratamento de incidentes e não conformidades;
- IX – realização periódica de auditorias e testes;
- X – adoção de medidas voltadas ao aprimoramento contínuo da Segurança da Informação.

6. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

6.1 – Finalidade

O **Comitê de Segurança da Informação da AGEPREV** constitui instância permanente de apoio à governança da Segurança da Informação, com a finalidade de definir e apoiar as estratégias necessárias à implantação, manutenção e aprimoramento da Política de Segurança da Informação.

Compete também ao Comitê acompanhar as ações relacionadas à proteção dos ativos de informação, gestão de riscos, continuidade dos serviços e controles de Segurança da Informação.

6.2 – Composição

O Comitê de Segurança da Informação será composto pelos seguintes membros:

- I – Diretor-Adjunto da AGEPREV, que exercerá a Presidência do Comitê;
- II – 01 (um) representante do Controle Interno da AGEPREV, na qualidade de membro;
- III – Gestor de Segurança da Informação da AGEPREV, na qualidade de membro e responsável pelo acompanhamento das ações de Gestão da Segurança da Informação.

Os membros serão formalmente designados por ato da autoridade competente.

Poderão ser convidados representantes da UTIC, de outras unidades da AGEPREV, de órgãos estaduais, prestadores de serviços ou especialistas para participar das reuniões, sem direito a voto, quando a matéria demandar conhecimento técnico específico.

6.3 – Competências

Compete ao Comitê de Segurança da Informação:

- I – definir e apoiar estratégias para implantação, manutenção e aprimoramento das políticas de Segurança da Informação;
- II – acompanhar o cumprimento das políticas, normas e procedimentos aplicáveis;
- III – acompanhar e avaliar riscos relevantes relacionados à Segurança da Informação;
- IV – acompanhar os resultados das auditorias de acesso lógico;
- V – recomendar providências para tratamento das não conformidades identificadas;
- VI – acompanhar os resultados dos testes de backup, restauração e recuperação de desastres;
- VII – acompanhar incidentes relevantes de Segurança da Informação;
- VIII – apoiar a revisão e atualização das políticas, normas e procedimentos relacionados à Segurança da Informação;
- IX – acompanhar ações de conscientização e capacitação;
- X – propor medidas destinadas ao aperfeiçoamento dos controles;
- XI – acompanhar a implementação das recomendações decorrentes de auditorias, avaliações de riscos,

testes e incidentes;

XII – comunicar à Diretoria da AGEPREV situações que representem risco significativo à Segurança da Informação ou à continuidade dos serviços.

6.4 - Funcionamento

O Comitê reunir-se-á ordinariamente, **no mínimo trimestralmente**, e extraordinariamente sempre que necessário.

As reuniões deverão ser formalizadas por meio de atas contendo, no mínimo, os assuntos tratados, deliberações, recomendações, responsáveis e prazos, quando aplicáveis.

7. GESTOR DE SEGURANÇA DA INFORMAÇÃO

Compete ao Gestor de Segurança da Informação:

- I – prover e manter disponíveis informações relativas à Gestão da Segurança da Informação;
- II – promover a divulgação das políticas e normas de Segurança da Informação;
- III – promover ações de conscientização e orientação;
- IV – propor projetos, controles e iniciativas destinados ao aperfeiçoamento da Segurança da Informação;
- V – acompanhar as ações relacionadas à classificação da informação e à temporalidade de sua guarda;
- VI – apoiar a identificação, avaliação, tratamento e monitoramento de riscos;
- VII – acompanhar os controles destinados à preservação da confidencialidade, integridade e disponibilidade das informações;
- VIII – acompanhar os controles de acesso físico e lógico;
- IX – acompanhar o registro, análise e tratamento dos incidentes de Segurança da Informação;
- X – acompanhar os procedimentos de backup, restauração, continuidade e recuperação de desastres;
- XI – coordenar e acompanhar as auditorias de acesso lógico;
- XII – propor a revisão e atualização das políticas, normas e procedimentos de Segurança da Informação;
- XIII – prestar apoio técnico ao Comitê de Segurança da Informação;
- XIV – comunicar ao Comitê e à Diretoria situações relevantes relacionadas a riscos, incidentes, vulnerabilidades ou não conformidades;
- XV – acompanhar a implementação das ações corretivas;
- XVI – manter ou acompanhar a manutenção dos registros e evidências das ações realizadas.

A PSI estadual já atribui à unidade responsável funções de gestão da Política, divulgação, conscientização, fornecimento de informações e proposição de melhorias.

8. PROCEDIMENTO DE AUDITORIA DE ACESSO LÓGICO

8.1 Objetivo

A Auditoria de Acesso Lógico tem por objetivo verificar periodicamente os acessos aos sistemas, aplicações, bancos de dados, redes e demais recursos tecnológicos utilizados pela AGEPREV.

Busca-se identificar acessos incompatíveis, usuários inativos, privilégios inadequados, acessos não autorizados e outras situações que possam representar riscos à Segurança da Informação.

8.2 Periodicidade

A Auditoria de Acesso Lógico será realizada **trimestralmente**, sem prejuízo de auditorias extraordinárias diante de:

- I – incidente de Segurança da Informação;
- II – suspeita ou indício de acesso indevido;
- III – alteração relevante nos sistemas ou infraestrutura;
- IV – identificação de vulnerabilidade;
- V – determinação da Diretoria, do Gestor ou do Comitê de Segurança da Informação.

8.3 Procedimentos

A Auditoria de Acesso Lógico deverá observar, no mínimo, as seguintes etapas:

- I – Planejamento:** definição dos sistemas, aplicações, bancos de dados e ambientes a serem avaliados;
- II – Levantamento:** obtenção da relação de usuários, perfis, permissões, contas administrativas, acessos remotos e demais registros necessários;
- III – Verificação:** análise da compatibilidade entre os acessos concedidos e as atribuições dos usuários;
- IV – Análise dos registros:** avaliação de logs e registros disponíveis, buscando identificar acessos indevidos, tentativas malsucedidas, comportamentos atípicos e demais ocorrências relevantes;
- V – Revisão de usuários:** identificação de contas pertencentes a servidores ou colaboradores desligados,

afastados, transferidos ou sem necessidade de acesso;

VI – Revisão de privilégios: análise das contas administrativas e dos usuários com privilégios elevados;

VII – Acessos de terceiros e remotos: verificação das permissões concedidas a prestadores de serviços, terceiros e usuários com acesso remoto ou VPN;

VIII – Registro das constatações: formalização dos resultados, riscos, não conformidades e recomendações;

IX – Tratamento: encaminhamento das inconsistências às áreas responsáveis;

X – Acompanhamento: monitoramento das ações corretivas até sua regularização.

A Política Estadual determina aplicação do princípio do menor privilégio e identificação individual dos usuários, permitindo que os registros de acesso sejam utilizados como evidência.

Também estabelece que os acessos aos sistemas operacionais sejam realizados mediante identificação exclusiva, sujeita a registro e auditoria, inclusive para contas administrativas.

8.4 Relatório de Auditoria

Ao final de cada auditoria deverá ser elaborado Relatório de Auditoria de Acesso Lógico, contendo, no mínimo:

- período analisado;
- sistemas e ambientes avaliados;
- usuários e perfis analisados;
- constatações;
- não conformidades identificadas;
- recomendações;
- providências adotadas ou necessárias;
- responsável pela regularização;
- prazo, quando aplicável;
- situação da ocorrência.

As não conformidades deverão ser acompanhadas até sua regularização.

9. ROTINAS DE RECUPERAÇÃO DE DESASTRES

9.5 Objetivo

As Rotinas de Recuperação de Desastres têm por objetivo estabelecer ações para recuperação dos sistemas, dados, informações e recursos tecnológicos utilizados pela AGEPREV diante de incidentes ou desastres que provoquem indisponibilidade total ou parcial dos serviços.

9.6 Situações de Acionamento

As rotinas poderão ser acionadas em caso de:

- I – indisponibilidade de sistemas críticos;
- II – falha de hardware, software ou infraestrutura;
- III – corrupção, perda ou exclusão indevida de dados;
- IV – ataques cibernéticos;
- V – falhas elétricas;
- VI – eventos ambientais ou físicos;
- VII – indisponibilidade do ambiente principal de processamento;
- VIII – demais incidentes capazes de comprometer significativamente a continuidade dos serviços.

A Política Estadual contempla expressamente hipóteses de corrupção de dados, falhas elétricas e de software, exclusão acidental, falha física, intempéries e ataques externos.

9.7 Procedimentos para Recuperação

Na ocorrência de incidente ou desastre deverão ser observadas, conforme sua natureza e criticidade, as seguintes etapas:

I – Identificação e registro: identificar a ocorrência, os sistemas e serviços afetados;

II – Comunicação: comunicar a UTIC, o Gestor de Segurança da Informação e os responsáveis pelos serviços;

III – Avaliação: avaliar a extensão, criticidade e impactos da indisponibilidade;

IV – Priorização: definir a ordem de recuperação dos serviços;

V – Acionamento: mobilizar recursos técnicos, humanos e cópias de segurança;

VI – Recuperação: executar os procedimentos necessários para recuperar dados, sistemas e serviços;

VII – Validação: verificar a integridade dos dados e o funcionamento dos sistemas recuperados;

VIII – Restabelecimento: promover o retorno dos serviços ao ambiente operacional;

IX – Comunicação: informar às áreas envolvidas sobre o restabelecimento;

X – Registro: documentar as ações realizadas, resultados, período de indisponibilidade e eventuais perdas.

A Norma de Continuidade estadual prevê a identificação dos processos críticos, avaliação de impacto, definição do tempo máximo de recuperação e condições para retomada dos serviços e reconciliação dos bancos de dados.

9.8 RPO e RTO

Para os sistemas e serviços considerados críticos deverão ser estabelecidos, quando tecnicamente aplicáveis:

I – RPO – Recovery Point Objective: quantidade máxima de informação cuja perda poderá ser tolerada em razão de uma indisponibilidade;

II – RTO – Recovery Time Objective: período máximo necessário para que determinado serviço ou sistema seja recuperado e volte a estar disponível.

A definição deverá considerar a criticidade e o impacto da indisponibilidade de cada serviço.

Os conceitos de RPO e RTO constam expressamente da Norma de Continuidade estadual.

9.9 Testes das Rotinas de Recuperação

As rotinas de recuperação de desastres deverão ser testadas **no mínimo anualmente**, podendo ser realizados testes extraordinários sempre que houver alterações significativas na infraestrutura, nos sistemas críticos ou nas estratégias de recuperação.

Os testes deverão avaliar, quando aplicável:

- I – capacidade de acionamento das equipes responsáveis;
- II – disponibilidade das cópias de segurança;
- III – recuperação dos sistemas e dados;
- IV – integridade das informações recuperadas;
- V – tempo necessário para restabelecimento;
- VI – falhas e oportunidades de melhoria.

Os resultados deverão ser formalmente registrados.

A Norma Estadual determina a realização de testes e avaliações periódicas ou extraordinárias, incluindo simulações de incidentes e interrupções.

10. BACKUP E RESTAURAÇÃO

10.1 Objetivo

Estabelecer diretrizes para execução, armazenamento, monitoramento, teste e restauração das cópias de segurança dos dados, sistemas e informações utilizados pela AGEPREV.

10.2 Abrangência

As rotinas de backup deverão contemplar, conforme aplicabilidade e criticidade:

- I – bancos de dados;
- II – sistemas e aplicações;
- III – repositórios institucionais de arquivos;
- IV – correio eletrônico;
- V – arquivos de configuração;
- VI – registros e logs;
- VII – infraestrutura e ambientes virtualizados;
- VIII – demais informações necessárias à continuidade das atividades.

A Política Estadual contempla, entre seus domínios, arquitetura, banco de dados, repositório de arquivos, e-mail, hospedagem, infraestrutura, LDAP, plataformas web, sistemas e virtualização.

10.3 Responsabilidade

A UTIC, ou unidade responsável pelos serviços de Tecnologia da Informação aplicáveis à AGEPREV, será responsável pela execução e acompanhamento técnico das rotinas de backup e restauração.

Compete à unidade responsável:

- I – manter os procedimentos de backup e restauração;
- II – criar e manter as cópias de segurança;
- III – executar os procedimentos de restauração;
- IV – monitorar a execução dos backups;
- V – tratar falhas identificadas;
- VI – gerenciar mídias e ambientes de armazenamento;
- VII – realizar testes de restauração;
- VIII – manter registros e relatórios das atividades;
- IX – comunicar falhas e ocorrências relevantes.

Essas atribuições seguem as responsabilidades atribuídas à UTIC na Política Estadual.

10.4 Periodicidade dos Backups

Para as categorias de dados sem especificação própria:

I – Backup Completo: realizado entre os 10 (dez) primeiros dias de cada mês, com armazenamento em dois locais distintos;

II – Backup Incremental: realizado diariamente nos demais dias do mês.

Para os bancos de dados:

I – Backup Completo: realizado semanalmente;

II – Backup Incremental e Diferencial: realizados a cada 12 (doze) horas, de forma intercalada.

Essas periodicidades seguem a Política de Backup e Restauração do Governo do Estado.

10.5 Monitoramento

Os backups deverão ser programados preferencialmente para execução automática em horários de menor utilização dos sistemas e da rede.

A execução deverá ser monitorada, devendo ser mantidos registros que permitam verificar o sucesso ou eventual falha das operações.

Quando identificada falha, deverão ser adotadas medidas para correção e nova execução na primeira janela disponível.

10.6 Armazenamento

As cópias de segurança deverão ser armazenadas de forma a preservar sua confidencialidade, integridade e disponibilidade.

Deverão existir cópias em ambientes distintos, conforme a estratégia aplicável ao serviço.

O backup **off-site** deverá ser armazenado em local diverso daquele onde se encontra o data center de produção, devendo os dados transportados estar criptografados.

10.7 Restauração

A restauração deverá ocorrer mediante solicitação registrada, contendo, quando aplicável:

- I – identificação do solicitante;
- II – unidade ou setor;
- III – identificação dos arquivos ou informações;
- IV – localização dos dados;
- V – versão ou data pretendida;
- VI – justificativa da solicitação.

Após a execução, deverá ser registrada a conclusão da restauração ou eventual impossibilidade de recuperação.

Deverão ser mantidos registros que permitam identificar o solicitante, os dados restaurados, a versão recuperada e as respectivas datas.

10.8 Testes de Restauração

As cópias de segurança deverão ser submetidas a testes mensais de restauração, contemplando diferentes domínios de dados.

Os testes deverão verificar:

- I – a integridade das cópias;
- II – a efetiva possibilidade de restauração;
- III – a suficiência dos dados armazenados;
- IV – o funcionamento dos dados ou serviços após a recuperação;
- V – a necessidade de adequação das rotinas existentes.

Os resultados deverão ser registrados e validados pelo responsável pelo serviço.

A Política Estadual estabelece expressamente testes mensais de restauração, com alternância dos domínios de dados ao longo do exercício.

11. REGISTROS E EVIDÊNCIAS

A execução das ações previstas nesta Política deverá ser formalmente registrada, de modo a assegurar a rastreabilidade e a comprovação das atividades.

Deverão ser mantidos, conforme aplicável:

- I – relatórios de auditoria de acesso lógico;
- II – registros dos usuários, perfis e acessos analisados;
- III – registros das não conformidades e ações corretivas;
- IV – logs e registros de acesso;
- V – relatórios ou registros de execução de backup;
- VI – registros de falhas e respectivas correções;
- VII – solicitações e registros de restauração;
- VIII – evidências dos testes de restauração;
- IX – relatórios de testes de recuperação de desastres;
- X – registros de incidentes e respectivas providências;
- XI – atas das reuniões do Comitê de Segurança da Informação;
- XII – demais documentos necessários à comprovação dos controles estabelecidos.

12. REVISÃO E ATUALIZAÇÃO DA POLÍTICA

A presente Política deverá ser revista periodicamente, no mínimo a cada 4 (quatro) anos, podendo ser revisada em intervalo inferior sempre que necessário, especialmente em razão de alterações legais, normativas, tecnológicas, organizacionais ou da identificação de novos riscos relacionados à Segurança da Informação.

A revisão poderá ainda ocorrer em razão de:

- I – alterações significativas na infraestrutura tecnológica;
- II – implantação ou substituição de sistemas relevantes;
- III – ocorrência de incidentes relevantes de Segurança da Informação;
- IV – resultados de auditorias ou testes que indiquem necessidade de adequação;
- V – alterações nos riscos relacionados à Segurança da Informação;
- VI – recomendações do Gestor ou do Comitê de Segurança da Informação.

As alterações decorrentes da revisão deverão ser formalmente aprovadas e divulgadas aos servidores, colaboradores, prestadores de serviços e demais usuários abrangidos por esta Política.

13. DISPOSIÇÕES FINAIS

A presente Política possui caráter **subsidiário e complementar à Política de Segurança da Informação do Governo do Estado de Mato Grosso do Sul**, devendo suas disposições ser interpretadas de forma integrada com os demais instrumentos normativos de Segurança da Informação vigentes.

A execução das ações previstas deverá observar a integração entre a AGEPREV, o Gestor de Segurança da Informação, o Comitê de Segurança da Informação, a UTIC e as demais unidades responsáveis pelos sistemas, serviços e informações envolvidos.

Os casos omissos ou situações que demandem avaliação específica deverão ser submetidos às unidades competentes, observadas as responsabilidades estabelecidas nesta Política.

O descumprimento de suas disposições sujeitará os responsáveis às medidas administrativas e demais providências cabíveis, observada a legislação vigente.

A presente Política entrará em vigor na data de sua publicação.

Campo Grande-MS, 20 de outubro de 2026.

JORGE OLIVEIRA MARTINS

Diretor-Presidente da Agência de Previdência Social de Mato Grosso do Sul – AGEPREV