POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

63 2111-6350
2111-6356

https://www.palmas.to.gov.br/
previpalmas@palmas.to.gov.br
gabprevipalmas@gmail.com

802 Sul, Avenida NS 02, Alameda 03, APM 15B,
Loteamento Palmas 2a Etapa - Plano Diretor Sul
CEP 77.023-006 – Palmas/TO

APRESENTAÇÃO

A Política de Segurança da Informação (PSI) do Instituto de Previdência Social do Municipio de Palmas tem por finalidade estabelecer diretrizes, responsabilidades e procedimentos voltados à proteção das informações, sistemas e ativos tecnológicos utilizados pelo Instituto, garantindo a confidencialidade, integridade, disponibilidade e autenticidade das informações previdenciárias e administrativas.

Este manual visa assegurar a continuidade dos serviços essenciais, a mitigação de riscos operacionais e a conformidade com a legislação vigente, em especial com os princípios da administração pública, as boas práticas de governança de TI e a Lei Geral de Proteção de Dados Pessoais (LGPD).

A informação constitui ativo essencial às atividades do Instituto de Previdência Social do Municipio de Palmas. A presente Política de Segurança da Informação visa proteger esse patrimônio contra ameaças e vulnerabilidades, garantindo os princípios básicos de:

- **Confidencialidade:** Acesso restrito apenas a pessoas autorizadas.
- **Integridade:** Garantia de que a informação não seja alterada indevidamente.
- **Disponibilidade:** Garantia de acesso sempre que necessário para fins legais e operacionais.

Este instrumento define normas e procedimentos destinados a reduzir riscos de falhas e prejuízos que possam comprometer a missão da autarquia, zelando especialmente pela intimidade dos segurados.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 4

Capítulo I. Disposições Gerais 4
Capítulo II. Agentes Públicos 4
Capítulo III. Princípios 5
Capítulo IV. Objetivos 5
Capítulo V. Autenticação de Acesso aos Sistemas de Gestão 6
Capítulo VI. Uso do Correio Eletrônico e do Acesso à Internet 7
Capítulo VII. Uso da Internet pela Rede Wi-Fi 8
Capítulo VIII. Estações de Trabalho 10
Capítulo IX. Procedimentos Básicos de Segurança 11
Capítulo X. Acesso Remoto 13
Capítulo XI. Penalidades 13
Capítulo XII. Disposições Finais 14

PROCEDIMENTOS DE CONTINGÊNCIA 15

1 DENÚNCIAS 24

1.1 OUVIDORIA DO PREVIPALMAS 24

2 INFORMAÇÕES, CRÍTICAS OU SUGESTÕES 25

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) do PREVIPALMAS. Esta norma estabelece as diretrizes para o manuseio, controle e proteção dos dados sob responsabilidade do Instituto, visando garantir a confidencialidade, integridade e disponibilidade das informações contra acessos não autorizados ou uso indevido, independentemente do suporte utilizado.

Art. 2º Toda informação produzida ou recebida, derivada da atividade profissional pelos usuários, pertence ao PREVIPALMAS, salvo as exceções explícitas e formalizadas previamente em documento entre as partes envolvidas.

CAPÍTULO II
AGENTES PÚBLICOS

Art. 3º Para fins desta Política de Segurança da Informação, considera-se agente público toda pessoa física que exerça, ainda que transitoriamente ou sem remuneração, por qualquer forma de investidura ou vínculo, atividade no PREVIPALMAS, compreendendo:

I. Servidores efetivos, comissionados e cedidos;

II. Estagiários e prestadores de serviço (pessoas físicas ou jurídicas);

III. Membros de conselhos e órgãos colegiados;

IV. Qualquer indivíduo com acesso autorizado aos sistemas ou bases de dados do Instituto.

CAPÍTULO III
PRINCÍPIOS

Art. 4º São princípios da Política de Segurança da Informação, no âmbito do PREVIPALMAS:

I. **Confidencialidade:** Proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas;

II. **Integridade:** Garantia da exatidão das informações e dos métodos de processamento;
III. **Disponibilidade:** Garantia de que os usuários autorizados e os interessados tenham acesso às informações.

IV. **Autenticidade:** Garantia da identidade de quem produz ou envia a informação, assegurando a validade da autoria;

CAPÍTULO IV
OBJETIVOS

Art. 5º São objetivos da Política de Segurança da Informação, no âmbito do PREVIPALMAS:

I. Proteger a informação sob a guarda do Instituto de Previdência Social do Município de Palmas, em qualquer meio ou suporte, de vários tipos de ameaças, para garantir a continuidade das atividades, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;

II. Adotar condutas que observem os preceitos legais, de acordo com aspectos de legitimidade, legalidade e justiça;
III.

IV. Garantir a segurança dos ativos computacionais, instalações prediais e documentos em meio físico abrangendo, também, o controle de acesso de pessoas às instalações do PREVIPALMAS;

V. Garantir a segurança de toda e qualquer informação contida em meio digital, seja em equipamentos, tráfego de informações pela rede, por correio eletrônico ou armazenada em estações de trabalho dos usuários;

VI. Promover a educação e conscientização de cada usuário sobre a responsabilidade para com a segurança da informação, por meio de sugestões e ações educativas;

VII. Promover ampla divulgação da Política de Segurança da Informação a todos os servidores efetivos, cedidos, comissionados, temporários, estagiários, conselheiros, segurados, beneficiários, dependentes e pessoas jurídicas ou físicas contratadas pelo PREVIPALMAS.

CAPÍTULO V
AUTENTICAÇÃO DE ACESSO AOS SISTEMAS DE GESTÃO DO PREVIPALMAS

Art. 6º A autenticação de usuários nos sistemas de gestão do PREVIPALMAS será realizada mediante credenciais individuais e intransferíveis. As senhas devem possuir, no mínimo, 08 (oito) caracteres, contendo obrigatoriamente letras maiúsculas, minúsculas, números e caracteres especiais (símbolos), sendo vedado o compartilhamento ou a utilização de sequências óbvias.

§1º As senhas deverão ser alteradas periodicamente pelos usuários ou sempre que necessário.

§2º Todas as ações executadas por meio do login individual serão de inteira responsabilidade do usuário correspondente.

CAPÍTULO VI
USO DO CORREIO ELETRÔNICO E DO ACESSO À INTERNET

Art. 7º A ferramenta de correio eletrônico corporativo constitui meio de comunicação corporativa do PREVIPALMAS, devendo ser utilizado de acordo com os princípios estabelecimentos na Política de Segurança da Informação.
§1º É vedado o uso de contas particulares de correio eletrônico para fins institucionais.

§2º A autenticação de acesso do usuário ao seu respectivo correio eletrônico corporativo do PREVIPALMAS ocorrerá por meio de login e senha individual.

Art. 8º Os recursos de internet, correio eletrônico corporativo ou qualquer outro existente ou que venha a ser adotado, deverão ser utilizados em consonância com os interesses do PREVIPALMAS.

Art. 9° O acesso à internet deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:

I. Proibição do acesso a sites não confiáveis, impróprios, incluindo aqueles com conteúdo sexual ou preconceituoso, jogos, salas de bate-papo, apostas e assemelhados;

II. Proibição do uso de ferramentas Peer-to-Peer (P2P), para o compartilhamento de serviços e dados;

III. Proibição do uso e instalação de jogos ou do download de arquivos que comprometam o tráfego da rede (vídeos, imagens, músicas, etc.), para fins particulares;

CAPÍTULO VII
USO DA INTERNET PELA REDE WI-FI

Art. 10° O uso da Internet pela rede Wi-fi, no âmbito do PREVIPALMAS, é permitido aos servidores efetivos, cedidos, comissionados, temporários, estagiários e conselheiros, desde que para o uso profissional, condizente com as tarefas do cargo ou função.

§1º Os usuários deverão conhecer as regras de acesso à referida rede, contidas na Política de Uso e estar cientes das penalidades que poderão ocorrer caso haja violação das mesmas.

§2º Para visitantes ou outros usuários não mencionados, será permitido o uso, mediante justificativa, podendo ser acatada ou não pela Gerência, mediante preenchimento e assinatura de formulário com as informações necessárias, onde o usuário declarará ciência e acordo com as normas existentes na Política de Uso.

Art. 11° A Política de Uso da rede Wi-fi, no âmbito do PREVIPALMAS, é constituída pela seguintes regras:

I. Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;

II. Responsabilizar-se pela sua identidade eletrônica, senha ou outro dispositivo de segurança, negando revelá-la a terceiros;

III. Manter seus dispositivos pessoais (notebooks, smartphones, etc.) com softwares e antivírus atualizados;

IV. Não usar a rede para trafegar informações confidenciais e/ou sigilosas, salvo quando utilizado algum meio seguro de transmissão (vpn, conexões cifradas, etc.);

V. Responder pelo mau uso dos recursos computacionais em qualquer circunstância;

VI. Responder por atos que violem as regras de uso dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na política de uso desses recursos.

Art. 12° Considera-se violação à Política de Uso da Rede Wi-Fi e dos recursos computacionais do PREVIPALMAS:

I. Infringir leis ou regulamentos locais, estaduais, nacionais ou internacionais vigentes;

II. Acessar, armazenar ou transmitir conteúdos (textos, imagens ou áudios) de natureza ofensiva, obscena ou abusiva;

III. Utilizar recursos institucionais para constranger, assediar, ameaçar ou perseguir qualquer indivíduo;

IV. Realizar ou tentar realizar acesso não autorizado a sistemas, bases de dados ou recursos computacionais do Instituto;

V. Utilizar a infraestrutura do PREVIPALMAS para invadir, comprometer ou danificar recursos computacionais de outras instituições;

VI. Violar sistemas de segurança, incluindo a tentativa de captura de senhas, engenharia social ou personificação de outros usuários;

VII. Interceptar, monitorar ou tentar capturar tráfego de dados na rede sem autorização expressa;

VIII. Provocar intencionalmente a degradação dos serviços, o congestionamento da rede ou a interrupção de sistemas mediante a inserção de vírus, malwares ou ataques de negação de serviço;

IX. tilizar os recursos para fins comerciais, publicitários ou de propaganda político-partidária, incluindo o envio de mensagens em massa (spam);

X. Veicular ou acessar conteúdos de teor pornográfico, racista, sexista, difamatório ou que promovam discursos de ódio e perfis falsos;

XI. Consumir recursos de rede e processamento de forma deliberadamente improdutiva ou fútil, prejudicando a finalidade pública da instituição.

CAPÍTULO VIII
ESTAÇÕES DE TRABALHO

Art. 13° Cada servidor deverá utilizar uma estação de trabalho determinada, que deverá ser protegida por senha individual e intransferível, sendo esta composta por, no mínimo 08 (oito) caracteres alfanuméricos (letras e números), com letras maiúsculas e minúsculas.

Art. 14° O uso das estações de trabalho deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:

I. Proibição do uso de dispositivos móveis de armazenamento sem aplicação de antivírus;

II. Proibição do armazenamento, edição ou distribuição de qualquer material de cunho sexual, preconceituoso, ou ilegal, incluindo piratarias;

III. Proibição do consumo de alimentos e bebidas nas mesas de trabalho, próximo aos equipamentos eletrônicos e em locais que armazenem informações de forma física;

IV. Proibição do uso indevido de impressoras para fins particulares;

V. Proibição da retirada de equipamentos eletrônicos da sede do PREVIPALMAS, salvo autorização;

VI. Proibição da retirada de arquivos físicos ou digitais da sede do PREVIPALMAS, salvo autorização;

VII. Proibição de instalação de softwares ou hardwares não licenciados sem autorização, ou qualquer outro tipo de pirataria.

Art. 15° Compete ao usuário reportar imediatamente qualquer atividade anômala na estação de trabalho, bem como notificações do sistema ou do software antivírus que possam comprometer a integridade do ambiente computacional.

Art. 16° A retirada de qualquer equipamento pertencente ao parque computacional do PREVIPALMAS fica condicionada à prévia autorização. O procedimento exige o preenchimento de formulário específico, contendo a justificativa da movimentação e as assinaturas da gerência e do servidor responsável pela retirada, que assumirá a guarda e conservação do bem

CAPÍTULO IX
PROCEDIMENTOS BÁSICOS DE SEGURANÇA

Art. 17° O PREVIPALMAS adotará providências no sentido de garantir:

I. Que os equipamentos estejam em bom estado de conservação para atender as demandas do PREVIPALMAS e não comprometam a segurança das informações produzidas;

II. Os sistemas informatizados de gestão, utilizados pelo PREVIPALMAS, deverão atender os seguintes requisitos mínimos:

I. Oferecer serviços de cópias de dados, preferencialmente backup virtual, realizados diariamente;

II. Possibilitar a administração gerenciar os níveis de acesso a cada funcionalidade;

III. Possibilitar a administração gerenciar os perfis e usuários para acesso ao sistema;

IV. Possibilitar a auditoria nos módulos;

V. Possibilitar o registro de login de alterações, com informação do usuário que efetuou a alteração;

VI. Possibilitar o registro de tentativas de acesso sem sucesso, armazenando o endereço IP de origem.

Art. 18° Os usuários de sistemas e serviços de informação do PREVIPALMAS deverão registrar e relatar à Gerência qualquer observação ou suspeita de fragilidade de segurança das informações armazenadas.

Art. 19° As evidências dos incidentes de segurança deverão ser coletadas e armazenadas pela Gerência de Tecnologia, a fim de que sejam tomadas as providências devidas.

Art. 20° A acesso aos documentos armazendos nos arquivos físicos do PREVIPALMAS só poderão ocorrer por servidor público efetivo ou cedido ao PREVIPALMAS, autorizado e designado previamente por esta, madiante o preenchimento dos controles de retirada e devolução dos documentos, nos quais deverão constar o arquivo retirado/devolvido, nome do servidor que acessou o documento, data e horário.

§1º O armazenamento de documentos em arquivos físicos do PREVIPALMAS e o acesso aos mesmos deverão observar regras e princípios básicos de arquivologia e biblioteconomia, e da legislação aplicável, a citar-se, especialmente, a Lei de Acesso à Informação (Lei Federal n.º 12.527, de 18 de novembro de 2011), Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709, de 14 de agosto de 2018), ISO 27002, observadas as garantias legais e constitucionais de sigilo de determinadas informações de cunho pessoal.

Art. 21° Além dos procedimentos básicos descritos no Capítulo VIII, desta Política de Segurança da Informação, os agentes públicos deverão observar integralmente das disposições do Plano de Contingência, descritas no Anexo II, deste instrumento.

CAPÍTULO X
ACESSO REMOTO

Art. 22° O acesso remoto de terceiros à rede do PREVIPALMAS será permitido somente para atender aos interesses da Fundação, mediante autorização prévia e expressa da Gerência.

§1º A ferramenta de conexão remota utilizada poderá ser de uso gratuito, ou da qual o terceiro possua licença de uso.

§2º Os terceiros que tenham acesso remoto à rede deverão observar os seguintes requisitos, sob pena de aplicação das penalidades cabíveis:

I. Manter sigilo das informações às quais tiverem acesso, sendo de sua total e exclusiva responsabilidade qualquer operação realizada sob suas credenciais de uso;

II. Comunicar imediatamente à Gerência Administrativa qualquer situação que coloque em risco o acesso ao ambiente de rede do PREVIPALMAS.

CAPÍTULO XI
PENALIDADES

Art. 23° O não cumprimento dos preceitos da Política de Segurança da Informação implicará na adoção das providências necessárias, mediante provocação ou de ofício, com vistas à aplicação das sanções administrativas.

CAPÍTULO XII
DISPOSIÇÕES FINAIS

Art. 24° Todos os usuários ficam cientes de que os ambientes, sistemas, computadores e redes do PREVIPALMAS poderão ser monitorados e gravados.

Art. 25° É vedado aos usuários de sistemas e serviços de informação aceitar ajuda técnica de pessoas estranhas e não autorizadas, salvo do quadro de colaboradores do Instituto ou da equipe técnica especializada contratada mediante procedimento licitatório adequado.

Art. 26° Fica vedada a divulgação ou reprodução de informações produzidas ou recebidas como resultado de atividade com o PREVIPALMAS, sem a autorização da autoridade competente.

Art. 27° Os usuários deverão ser cientificados da existência da Política de Segurança da Informação e sobre o uso correto dos ativos disponibilizados ao estabelecerem vínculo com o PREVIPALMAS, de forma a minimizar os possíveis riscos de segurança, bem como garantir o conhecimento de suas responsabilidades.

Art. 28° O PREVIPALMAS exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos, serviços e informações, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

Art. 29° O PREVIPALMAS realizará, sempre que julgar necessário, ações preventivas e educativas visando garantir a aplicação da Política de Segurança da Informação .

Art. 30° A Política de Segurança da Informação do PREVIPALMAS será revista sempre que necessário, de ofício ou por provocação do Presidente, mediante aprovação prévia.

Art. 31° Este instrumento entra em vigor na mesma data da publicação.

PROCEDIMENTOS DE CONTINGÊNCIA

Sumário

1. Procedimentos de Contingência
2. Objetivos
3. Aplicação e Área Responsável
4. Pontos Frágeis
5. Procedimentos para Restauração de Servidores
   5.1. Servidor de arquivos
   5.2. Servidor de hospedagem
6. Serviço de Acesso à Internet
7. Serviço de Telefonia
8. Notificações
9. Backup

1. Procedimentos de Contingência

Os procedimentos de contingência em Tecnologia da Informação do Instituto de Previdência Social do Município de Palmas constituem o conjunto de ações estratégicas, previamente estabelecidas, destinadas a mitigar os impactos de eventos adversos. Tais medidas visam assegurar a continuidade operacional, minimizar os períodos de indisponibilidade dos serviços críticos e neutralizar danos financeiros ou institucionais decorrentes de incidentes tecnológicos.

2. Objetivos

Este Plano de Contingência estabelece as diretrizes e protocolos de resposta a incidentes críticos que possam comprometer a integridade e a disponibilidade das informações do PREVIPALMAS. O objetivo é assegurar a continuidade dos serviços essenciais por meio de procedimentos pré-definidos de recuperação, garantindo o restabelecimento da operabilidade técnica, total ou parcial, frente a sinistros ou ameaças externas.

3. Aplicação e Área Responsável

O presente instrumento possui abrangência integral sobre o Instituto de Previdência Social do Município de Palmas, devendo sua execução e fiscalização ser coordenada pela Gerência de Tecnologia.

4. Pontos Frágeis

A relação dos pontos frágeis aponta os possíveis focos de crise das tecnologias utilizadas pelo PREVIPALMAS, destacando-se:

I. Servidor de arquivos;
II. Serviço de acesso à Internet;
III. Serviço de telefonia.

5. Procedimentos para Restauração dos Servidores

Os servidores constituem o cerne da infraestrutura tecnológica do Instituto de Previdência Social do Município de Palmas. Tratam-se de ativos de alto desempenho projetados para o processamento centralizado de aplicações, suporte a múltiplos usuários simultâneos e provimento de serviços críticos de rede.

Sua arquitetura é indispensável para a viabilização das atividades institucionais, englobando funcionalidades vitais como:

Gestão de Dados: Hospedagem de bancos de dados previdenciários e armazenamento estruturado de arquivos;

Comunicação Integrada: Gerenciamento de correio eletrônico institucional;

Colaboração: Compartilhamento de recursos lógicos e físicos;

Segurança e Acesso: Administração centralizada de identidades e suporte a acessos remotos seguros.

Fatores de Risco e Indisponibilidade

A resiliência operacional do PREVIPALMAS pode ser comprometida por diversos vetores de falha que resultam na interrupção de sistemas e serviços de rede. Os principais desencadeadores de incidentes incluem:

Falhas de Hardware: Obsolescência ou defeitos em componentes físicos;

Cibersegurança: Ataques de *malware*, *ransomware* ou acessos não autorizados;

Fator Humano: Erros operacionais ou parametrizações incorretas de sistemas;

Infraestrutura Crítica: Instabilidades na rede lógica ou no suprimento de energia elétrica;

Configuração: Inconsistências em protocolos de rede e atualizações de software.

Monitoramento e Diagnóstico

Para assegurar a prontidão na resposta a incidentes, o instituto adota mecanismos proativos de identificação de falhas, tais como:

Monitoramento de Logs: Análise de alertas emitidos por sistemas operacionais e aplicações de gestão;

Telemetria de Infraestrutura: Supervisão de utilitários de rede e alertas sonoros/visuais de sistemas de energia ininterrupta (*UPS/Nobreaks*);

Testes de Estresse e Redundância: Realização periódica de diagnósticos em dispositivos críticos para validar a integridade da rede.

5.1. Servidor de arquivos

Um servidor de arquivos é um computador conectado a uma rede que tem como objetivo principal proporcionar um local para o armazenamento compartilhado de arquivos de computadores (como documentos, arquivos de som, fotografias, filmes, imagens, bases de dados, etc) que podem ser acessados pelos dispositivos que estão ligados à rede de computadores.

O Servidor seria a 'máquina principal' enquanto os dispositivos ligados ao servidor são chamados de 'clientes'. É projetado principalmente para permitir o armazenamento, compartilhamento e recuperação rápida de dados onde a computação pesada é fornecida pelas estações de trabalho.
Em caso de problemas no servidor de arquivos deve-se adotar o seguinte procedimento:

I. Avisar aos setores os serviços afetados e o prazo para restabelecimento;
II. Providenciar um novo equipamento para instalação;
III. Instalar os drivers e serviços necessários;
IV. Restaurar o backup dos arquivos;
V. Configurar o acesso dos usuários e os serviços;
VI. Testar a autenticação via rede e integridade dos arquivos.

5.2. Servidor de hospedagem

Um servidor de hospedagem possui o armazenamento de um site e disponibiliza o mesmo na internet, ou seja, o serviço de hospedagem possibilita que o site seja visualizado 24h por dia em todo o mundo. Em caso de problemas no servidor de hospedagem deve-se adotar o seguinte procedimento:

I. Avisar aos setores os serviços afetados e o prazo para restabelecimento;
II. Abrir um chamado no sistema de atendimento da empresa contratada para prestação deste serviço;
III. Acompanhar através de e-mail ou telefonema, o andamento do chamado;
IV. Alterar as senhas dos administradores do painel do cliente;
V. Testar as principais funções do servidor de hospedagem.

6. Serviço de Acesso à Internet

O serviço de acesso à internet disponibiliza os meios pelos quais os usuários podem conectar-se à rede mundial de computadores. Em caso de problemas no acesso à internet deve-se adotar o seguinte procedimento:

I. Avisar aos setores os serviços afetados;
II. Checar o cabeamento de rede;
III. Checar a alimentação de energia elétrica dos equipamentos de rede (modem, roteadores e switches);
IV. Analisar se o problema é local ou no provedor de acesso;
V. Contactar o provedor deste serviço para solicitação de reparo;
VI. Avisar aos setores o prazo para restabelecimento.

7. Serviço de Telefonia

Para a disponibilização do serviço de telefonia aos usuários, o PREVIPALMAS utiliza uma linha telefônica fixa. Em caso de problemas no serviço de telefonia deve-se adotar o seguinte procedimento:

I. Checar a alimentação de energia elétrica dos aparelhos (telefonia fixa);

II. Analisar se o problema é local ou na operadora;
III. Contactar a operadora para solicitação de reparo;
IV. Avisar aos setores os serviços afetados e o prazo para restabelecimento.

8. Notificações

As notificações devem ocorrer a todos os usuários afetados quando acontecer qualquer um dos problemas acima citados. Deverá ser notificado o problema ocorrido, causa (quando houver) e informado o prazo estimado para a resolução do mesmo e ações que os usuários devem adotar (quando for o caso).

As notificações deverá ocorrer das seguintes formas:

I. Notificações Internas:
E-mail;
Telefone.
II. Notificações Externas:
E-mail;
Telefone;
Website;

9. Backup

O Backup constitui a salvaguarda dos ativos de informação da instituição. Sua finalidade é mitigar os riscos de perda de dados decorrentes de falhas operacionais, erro humano ou incidentes tecnológicos. A correta execução das cópias de segurança assegura a resiliência do ambiente, permitindo a restauração imediata da operabilidade e a integridade das informações. As rotinas de backup observam as seguintes diretrizes estratégicas. Os Backups são feitos em 2 servidores locais destintos, visando maior segurança dos dados, a política de backup do Previpalmas segue práticas de segurança com as seguintes rotinas:

- Backups incrementais realizados diariamente;
- Backup completo executado semanalmente, às sextas-feiras;
- Replicação e armazenamento de backups externos, visando proteção contra falhas, perda de dados, ataques cibernéticos ou desastres.
- Os procedimentos de backup são monitorados e periodicamente validados quanto à integridade e possibilidade de restauração.

Rotina de Backup: Sistema SPG

Esta documentação estabelece as diretrizes de governança e a arquitetura de proteção de dados do ecossistema SPG. A estratégia visa assegurar a integridade e a alta disponibilidade dos ativos de informação, mitigando riscos de interrupção operacional por meio de protocolos de salvaguarda automatizada e redundância de dados.

Cronograma e Frequência

Os backups são processados de forma totalmente automatizada, sem necessidade de intervenção manual diária.

- **Horário de Execução:** Diariamente às 23:59.
- **Janela de Backup:** Programada para o período de menor tráfego no sistema para evitar impactos na performance.

Retenção de Dados

A política de retenção define por quanto tempo cada arquivo de backup permanece disponível antes de ser removido para otimização de espaço.

- **Prazo de Retenção:** 7 dias.
- **Política:** O sistema mantém o histórico da última semana (D-1 até D-7). Ao atingir o 8º dia, a cópia mais antiga é automaticamente sobrescrita ou excluída.

Arquitetura de Armazenamento

Para garantir a máxima segurança contra falhas críticas de infraestrutura (como desastres no datacenter principal), seguimos o princípio de isolamento geográfico e lógico.

- **Localização:** Armazenamento em nuvem (Cloud Storage).
- **Tipo de Repositório:** Servidor de Objetos.
- **Isolamento:** Os backups residem em uma estrutura totalmente externa aos servidores de aplicação. Isso garante que, em caso de comprometimento total do servidor do SPG, os dados permaneçam intactos e acessíveis para restauração.

Fluxo de Backup

I. **Geração:** O script de backup inicia às 23:59.

II. **Compressão/Criptografia:** Os dados são compactados para reduzir o tempo de transferência.

III. **Transferência Off-site:** O arquivo é enviado via conexão segura para o servidor de objetos na nuvem.

IV. **Validação:** O sistema confirma o sucesso do upload e aplica a regra de rotação (excluindo arquivos com mais de 7 dias).

Rotina de Backup: Sistema SOFTPREV

O backup é o procedimento fundamental de segurança destinado à salvaguarda de dados, informações e ativos digitais do sistema. Sua finalidade é garantir a resiliência institucional diante de falhas técnicas, exclusões indevidas, sinistros ou incidentes que possam comprometer os pilares da integridade, disponibilidade e continuidade da informação.

1. Periodicidade e Execução

A rotina de backup é executada diariamente às 00:00h, sendo processada em servidor físico local dedicado a esta finalidade. Além do cronograma fixo, cópias de segurança complementares poderão ser realizadas em caráter preventivo ou em decorrência de demandas técnicas e operacionais específicas.

2. Armazenamento e Retenção

As cópias de segurança são mantidas em ambiente controlado e seguro, observando-se um período de retenção de até 5 (cinco) anos, conforme os critérios técnicos e a política de armazenamento vigente. Decorrido este prazo, o descarte ou a sobrescrita dos dados seguirá os protocolos de segurança estabelecidos.

3. Conformidade Legal (LGPD)

Todos os processos de custódia, guarda e eventual restauração de dados observam rigorosamente as diretrizes da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). São aplicados controles rígidos para assegurar a confidencialidade e o tratamento adequado das informações sob responsabilidade desta instituição.

4. Responsabilidades e Limitações

O backup constitui uma camada de contingência e não isenta os usuários da observância às boas práticas de gestão e controles de acesso. A restauração (restore) dos dados está estritamente condicionada à existência de uma cópia íntegra e disponível, respeitadas as limitações técnicas do ambiente e os ciclos de retenção adotados.

Denuncias

Aqueles que tiverem conhecimento de violação à Política de Segurança da Informação do Instituto de Previdência Social do Municipio de Palmas, poderão apresentar denúncia através dos seguintes instrumentos:

Ouvidoria

Endereço: INSTITUTO DE PREVIDÊNCIA SOCIAL DO MUNICIPIO DE PALMAS - PREVIPALMAS
Quadra ACSE 80 Avenida NS 2, SN - Plano Diretor Sul CEP: 77023-006, Palmas - TO

Site: <https://previpalmas.to.gov.br/ouvidoria>

Telefone: (63)2111-6363

INFORMAÇÕES, CRÍTICAS OU SUGESTÕES

Para obter maiores informações, realizar críticas ou sugestões ao conteúdo deste publicação, entre em contato com o PREVIPALMAS:

INSTITUTO DE PREVIDÊNCIA SOCIAL DO MUNICIPIO DE PALMAS - PREVIPALMAS

Quadra ACSE 80 Avenida NS 2, SN - Plano Diretor Sul CEP: 77023-006, Palmas - TO

Atendimento de segunda a sexta-feira, das 13h00 às 19h00.

CANAIS DE ATENDIMENTO

E-mail: <previpalmas@palmas.to.gov.br>

Telefone: (63) 2111-6350

Site: <previpalmas.to.gov.br>

PREVIPALMAS
INSTITUTO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE PALMAS

INSTITUTO DE PREVIDÊNCIA SOCIAL DO MUNICIPIO DE PALMAS - PREVIPALMAS
Quadra ACSE 80 Avenida NS 2, SN - Plano Diretor Sul
CEP: 77023-006, Palmas - TO
CNPJ: 05.278.848/0001-09