



PORTARIA ADMINISTRATIVA Nº 48/2023 - MacaíbaPrev

Dispõe sobre a instituição da Política de Segurança da Informação - PSI do Instituto de Previdência dos Servidores do Município de Macaíba, e dá outras providências.

O (A) DIRETOR (A) PRESIDENTE DO MACAÍBAPREV, nos usos de suas atribuições legais, conferida pela Lei Municipal nº 1.695, de 30 de abril de 2014:

CONSIDERANDO que a informação é um ativo essencial da organização e precisa ser protegida quanto a eventuais ameaças, preservando e minimizando os riscos para a continuidade dos serviços prestados pelo MacaíbaPrev;

CONSIDERANDO que a adoção de procedimentos que garantam a segurança das informações deve ser prioridade constante do RPPS, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da Instituição;

CONSIDERANDO que este RPPS busca a certificação em Nível I do Pró-Gestão no Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios (instituída pela Portaria MPS nº 185/2015 e Portaria

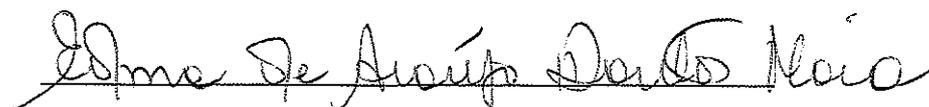
SPREV nº 4.248/2022, com vigência a partir de 02 de janeiro de 2023), de acordo com a seção 3.1.5 – Política de Segurança da Informação;

RESOLVE:

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito do MacaíbaPrev, na forma do Anexo I desta Portaria;

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

Macaíba/RN, 16 de Outubro de 2023.



Edma de Araújo Dantas Maia

Diretora Presidente do MacaíbaPrev



MACAÍBA
PREV

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE MACAÍBA

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Institui a Política de Segurança da Informação - PSI do Instituto de Previdência dos Servidores do Município de Macaíba - MACAÍBAPREV, e dá outras providências.

MACAÍBA/RN

Outubro-2023

Sumário

1. INTRODUÇÃO	5
2. OBJETIVOS	5
3. APLICAÇÕES	6
4. DAS RESPONSABILIDADES ESPECÍFICAS	7
4.1 DOS SERVIDORES EM GERAL	7
4.2 DOS SERVIDORES EM REGIME DE EXCEÇÃO – ESTAGIÁRIOS E TEMPORÁRIOS.....	7
4.3 DOS DIRETORES E GESTORES.....	7
5. O MONITORAMENTO DO AMBIENTE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.....	8
6. IDENTIFICAÇÃO	9
7. COMPUTADORES E RECURSOS TECNOLÓGICOS.....	10
8. PRIVACIDADE DA INFORMAÇÃO	11
9. DISPOSITIVOS MÓVEIS	11
10. PROCEDIMENTOS DE BACKUP.....	12
11. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	12
12. DAS DISPOSIÇÕES FINAIS	13
13. ANEXO II.....	14

1. INTRODUÇÃO

A Política de Segurança da Informação - PSI é um documento que destina orientar e estabelecer diretrizes corporativas do MACAÍBAPREV para a proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários. Devendo, portanto, ser cumprida e aplicada em todas as suas áreas e/ou setores.

A presente Política de Segurança da Informação é uma declaração formal de compromisso do RPPS com a proteção das informações sob sua guarda e a formalização das normas para segurança, baseada no Manual do Pró-Gestão RPPS do Ministério do Trabalho e Previdência – MTP, Secretaria de Previdência – SPREV e da Subsecretaria dos Regimes Próprios de Previdência Social – SRPPS, instituída pela Portaria MPS nº 185/2015 e Portaria SPREV nº 4.248/2022, com vigência a partir de 02 de janeiro de 2023.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos servidores, fornecedores e prestadores de serviços do MACAÍBAPREV seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades operacionais e de proteção legal da instituição e do indivíduo.

Garantir que os recursos computacionais e tecnológicos serão utilizados de maneira adequada e com responsabilidade. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando exposição que possa prejudicar este Instituto, colaboradores e terceiros.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a efetivação de controles e processos para seu atendimento. Assim como, implementar controles para preservar os interesses do MACAÍBAPREV contra danos que possam ser considerados como violação ao uso dos serviços e, portanto, considerados proibidos. Por isso, busca-se atender os seguintes princípios:

- **Confidencialidade:** proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas;
- **Integridade:** garantia da exatidão das informações e dos métodos de processamento;
- **Disponibilidade:** garantia de que os usuários autorizados e os interessados tenham acesso às informações.

No caso dos procedimentos aqui estabelecidos sejam violados pelos usuários, o MACAÍBAPREV tomará as devidas medidas cabíveis.

3. APLICAÇÕES

As diretrizes aqui estabelecidas deverão ser seguidas por todos os servidores, bem como os fornecedores, estagiários, colaboradores e prestadores de serviço que se aplicam à informação em qualquer meio ou suporte. Esta política dá ciência a cada servidor, fornecedor e prestador de serviços de que os ambientes, sistemas, computadores e redes poderão ser monitorados e gravados, conforme previsto nas leis brasileiras vigentes.

É obrigação de cada servidor se manter atualizado em relação a esta política de segurança e aos procedimentos e orientações relacionadas, buscando orientação do seu gestor ou da área de tecnologia de informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional realizada no MACAÍBAPREV pertence à referida instituição. As exceções serão devidamente analisadas por este Instituto e formalizadas entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido dentro dos limites cabíveis, desde que não prejudique o desempenho dos sistemas e serviços. O MACAÍBAPREV poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4. DAS RESPONSABILIDADES ESPECÍFICAS

4.1 DOS SERVIDORES EM GERAL

Entende-se por servidor toda pessoa legalmente investida em cargo ou em emprego público na administração direta, nas autarquias ou nas fundações públicas.

Será de inteira responsabilidade do servidor todo prejuízo ou dano que vier a causar ao MACAÍBAPREV e/ou a terceiros, em decorrência da não obediência às diretrizes e recomendações referidas neste documento.

4.2 DOS SERVIDORES EM REGIME DE EXCEÇÃO – ESTAGIÁRIOS E TEMPORÁRIOS

Devem esses entenderem dentro da sua condição especial de servidores, cumprir rigorosamente o que está previsto nesta Política de Segurança da Informação, assim como, a concessão de acesso poderá ser revogada a qualquer tempo, se for verificado que a justificativa de motivo de negócio não mais atende aos interesses desse Instituto ou se o colaborador não estiver cumprindo as condições definidas nesta PSI.

4.3 DOS DIRETORES E GESTORES

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os demais servidores sob a sua gestão. Atribuir, incentivar e orientar os demais servidores a terem responsabilidades no cumprimento da Política de Segurança da Informação.

Exigir dos servidores a assinatura do Termo de Compromisso e Ciência¹, assumindo o dever de seguir as recomendações e/ou condutas estabelecidas, bem como se comprometendo a manter o sigilo e a confidencialidade, sobre todos os ativos de informações do MACAÍBAPREV.

¹ Documento constante no Anexo II.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política de segurança.

5. O MONITORAMENTO DO AMBIENTE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O monitoramento do ambiente da política de segurança da informação relacionada ao uso da **internet**, do **correio eletrônico**, dos **computadores** e de **outros recursos tecnológicos** do RPPS será supervisionado por profissional da área de TI da unidade gestora e na sua ausência por servidor designado pela direção do Instituto.

O objetivo é prevenir o acesso não autorizado às informações sensíveis de meio físico de posse e competência do MACAÍBAPREV, evitando danos e interferências na sua rotina de atividades.

O acesso à área em que são processadas e armazenadas as informações sensíveis de meio físico são controladas e restritas às pessoas autorizadas.

O controle de retirada e/ ou consulta das informações físicas será controlado pelo responsável designado que fará o monitoramento por meio de emissão de protocolos. Essas informações deverão conter, no mínimo:

- ✓ Identificação (nome) e visto do servidor responsável emissor do protocolo;
- ✓ Identificação (nome) e visto do servidor interessado ao acesso da informação sensível de meio físico;
- ✓ Data e hora da retirada e/ou consulta da informação sensível de meio físico;
- ✓ Data e hora da devolução da informação sensível de meio físico.

A retirada de informações sensíveis de meio físico sem a devida emissão do protocolo não será autorizada. Além disso, toda a informação sensível de meio físico será conferida no ato da devolução, estando sujeito à emissão de ocorrências em caso de desleixo, desorganização ou ausência de documentos.

São considerados casos de desorganização e desleixo de documentos, entre outros:

- ✓ Desordem na numeração das folhas do processo;
- ✓ Rasuras, anotações e amassados;
- ✓ Sujeiras de alimentos e manchas de bebidas.

Não é permitida a retirada de qualquer folha objeto de complemento ao arquivo de informação ou dossiê, exceto para a possibilidade de foto cópia, desde que haja a emissão de protocolo da documentação retirada, com o preenchido/indicação da(s) folha(s) que foram objeto da foto cópia.

Não é permitida a locomoção de informações sensíveis de meio físico fora das dependências do MACAÍBAPREV, exceto quando estritamente necessária à realização da demanda a realizar, acompanhado do devido controle de saída/entrada de documentação.

6. IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o MACAÍBAPREV².

Tal procedimento visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores da unidade gestora.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a Instituição e a legislação brasileira (cível e criminal).

Existindo *login* de uso compartilhado (por mais de um colaborador), a responsabilidade perante o MACAÍBAPREV e a legislação brasileira (cível e criminal) será dos usuários que dele se utilizarem.

² O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro, segundo o art. 307, de falsa identidade.

É proibido o compartilhamento de *login* para funções de administração de sistemas.

A área de tecnologia da informação (TI) responde pela criação da identidade lógica dos servidores no RPPS.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas pelo setor da tecnologia da informação.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos, compreensíveis por linguagem humana (não criptografados).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu *login*/senha.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

7. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os servidores do MACAÍBAPREV deverão zelar pelo uso e manutenção dos equipamentos utilizados, assim como, reportarem possíveis defeitos ou falhas existentes nos equipamentos ao setor responsável por saná-las. Além disso, deverá ter os seguintes cuidados:

- Não baixar arquivos e programas de uso inapropriados;
- Evitar conectar as contas pessoais a menos que sejam indispensáveis a realização do trabalho;
- Criar/reservar uma pasta para arquivos frequentes na área de trabalho ou no servidor da unidade gestora;
- Manter o HD limpo do computador utilizado;
- Fazer backups regulares no computador utilizado;
- Atualizar, sempre que necessário e/ou recomendado, o sistema operacional utilizado.

8. PRIVACIDADE DA INFORMAÇÃO

A proteção da privacidade das informações é aquelas que pertencem aos seus segurados e/ou beneficiários e que são manipuladas ou armazenadas nos meios às quais o MACAÍBAPREV detém total controle administrativo, físico, lógico e legal.

Adiante são expostos os compromissos a serem seguidos pelo MACAÍBAPREV, na busca pela melhoria contínua dos processos da Política de Segurança da Informação:

- ✓ As informações são coletadas de forma ética e legal, com o conhecimento do segurado/beneficiário, para propósitos específicos e devidamente informados;
- ✓ As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
- ✓ As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido dessas, o cumprimento de nossa política de segurança e privacidade de dados;
- ✓ As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

9. DISPOSITIVOS MÓVEIS

Os servidores do MACAÍBAPREV deverão zelar pelo uso e manutenção dos dispositivos móveis utilizados, assim como, reportarem possíveis defeitos ou falhas existentes ao setor responsável por saná-las. Além disso, deverá ter os seguintes cuidados:

- ✓ Usar uma senha forte de acesso;
- ✓ Desativar as informações de localização das fotos tiradas;
- ✓ Desativar a funcionalidade Bluetooth quando essa não estiver em uso;
- ✓ Usar uma rede privada virtual - VPN;

- ✓ Não esquecer de ativar suas funcionalidades de segurança;
- ✓ Tomar cuidado com permissões a aplicativos.

10. PROCEDIMENTOS DE BACKUP

Os servidores do MACAÍBAPREV deverão manter as principais práticas recomendadas ao uso de backup nos seus equipamentos de uso profissional da unidade, a fim de mitigar a perda de dados e desastres operacionais. Recomenda-se as boas práticas de backup, entre outras:

- ✓ Manter a constância dos backups;
- ✓ Não fazer backup dos arquivos no mesmo disco rígido em que o Windows está instalado;
- ✓ Sempre que possível, remover os arquivos duplicados e armazenar os arquivos na nuvem.

11. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Inicialmente com a supervisão e/ou orientação de profissional da área de segurança da informação será recomendada a criação de pôsteres ou cartilhas, com o intuito de divulgar e conscientizar os servidores e demais colaboradores sobre a política de segurança da informação a ser seguida por todos no MACAÍBAPREV³.

Já quando for detectada uma violação da PSI, a primeira coisa a ser feita é determinar a sua razão, ou seja, verificar se a violação ocorreu por desconhecimento da PSI vigente, negligência ou acidente por parte do servidor ou colaborador.

E, caso seja necessário advertir o servidor ou colaborador pelo não cumprimento das recomendações estabelecidas neste documento, esses devem ser informados e encaminhados ao departamento de Gestão de Pessoas (Recursos Humanos) do MACAÍBAPREV, a fim de registrar a devida sanção, no caso de comprovada a irregularidade.

³ A PSI deverá fazer parte do programa de integração de novos servidores.

É assegurado tanto ao servidor quanto ao colaborador o pleno direito de contestação e de defesa.

12. DAS DISPOSIÇÕES FINAIS

A Política de Segurança da Informação deve ser entendida como parte fundamental da cultura interna do MACAÍBAPREV e qualquer incidente relacionado a esse tema subentende-se como alguém agindo contra a ética e os bons costumes.

Sua criação e revisão deverão ser precedidas de aprovação por toda diretoria do MACAÍBAPREV, devidamente registrada em ata e divulgadas obrigatoriamente pelo próprio ente aos servidores e colaboradores da sua estrutura organizacional. As recomendações aqui descritas deverão sofrer alterações sempre que necessário.

Os requisitos estabelecidos nesta PSI se fazem obrigatórios, devendo ser seguido por todos os servidores ou colaboradores que acessem informações do MACAÍBAPREV.

Macaíba/RN, 16 de Outubro de 2023.

Edma de Araújo Dantas Maia
Diretora-Presidente do MacaíbaPrev

13. ANEXO II

TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO MACAÍBAPREV

Declaro que recebi e li a Política de Segurança da Informação - PSI do MACAÍBAPREV, estando ciente de seu conteúdo e da sua importância para o bom exercício funcional desse RPPS.

A assinatura do presente termo representa a manifestação da minha concordância e do meu compromisso em cumpri-lo.

Macaíba/RN, _____ de _____ de 20 ____.

Nome:

Matrícula: