RESOLUÇÃO DO PREVMMAR Nº 008/2020 DE 15 DE OUTUBRO DE 2020.

"Dispõe sobre aprovação da Politica de Segurança do PREVMMAR – Serviço de Previdência dos Servidores Municipais de Maracaju-MS e dá outras providências."
CONSIDERANDO, o artigo 29, §3º e artigo 31, I e artigo 32, § 9º, I da lei 1.892, de 16 de outubro de 2017, bem como as alterações da Lei 1.982 de 11 de agosto de 2020, aprova a Politica de Segurança do PREVMMAR, deliberado em Ata nº 017/2020, de 15.10.2020;

RESOLVEM:

Art. 1º. Fica aprovado a Politica de Segurança do PREVMMAR – Serviço de Previdência dos Servidores Municipais de Maracaju/MS, na forma do Anexo Único desta Resolução.

Art. 2º. Este Resolução entrará em vigor na data de sua publicação, revogadas as disposições em contrário.

Maracaju-MS, aos 15 dias do mês de outubro do ano de dois mil e vinte.

Roseli Bauer
Presidente do PREVMMAR

Marilene Tesser
Presidente Conselho Curador
Representante do SIMTREMA

Clementino Serafim de Oliveira
Representante do SISPMMA

Jorge Carlos Heller Netto
Representante do Executivo

Neli Terezinha Bairros
Representante dos Aposentados/Pensionistas

Mayara Ferreira Maris
Representante do Legislativo

ANEXO UNICO DA RESOLUÇÃO PREVMMAR Nº 008/2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO PREVMMAR

A Política de Segurança da Informação, no SERVIÇO DE PREVIDENCIA DOS SERVIDORES MUNICIAPIS DE MARACAJU-MS - PREVMMAR, aplica-se a todos os servidores públicos, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento do PREVMMAR, ou acesso às informações pertencentes ao Serviço de Previdencia dos Servidores Muncipais de Maracaju.

Todo e qualquer servidor que utilize de recursos computadorizados do PREVMMAR, ou que detenha o banco de dados do PREVMMAR em seus programas, tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

A violação desta política de segurança é qualquer ato que:

- Exponha o PREVMMAR a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou informações ou ainda da perda de equipamento;
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos governamentais;
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer Lei, regulamento ou qualquer outro dispositivo governamental.

MISSÃO DO SETOR DE INFORMÁTICA DO PREVMMAR

Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade, será nomeado um servidor que em conjunto com a Equipe de Informatica do Muncipio de Maracaju-MS, desenvolverá a função.

OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO PREVMMAR

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização das atividades do PREVMMAR.

Para os efeitos e aplicações, são adotadas as seguintes definições técnicas:

a) Hardware: Componente ou conjunto de componentes físicos de um computador ou de seus periféricos;

b) Software: Conjunto dos componentes que não fazem parte do equipamento físico propriamente dito e que incluem as instruções e programas, bem como os dados a eles associados, empregados durante a utilização do sistema;

c) Internet: Conjunto de computadores interligados em uma rede de abrangência mundial, que se comunicam utilizando o protocolo TCP/IP;

d) Intranet: Conjunto de computadores e outros equipamentos de uma instituição que formam uma rede utilizando o protocolo TCP/IP e são ligados à Internet usualmente através de um sistema de proteção (Firewall); sendo que realizamos a instalação do servidor e até dezembro de 2020 será instalado no PREVMMAR o sistema de proteção (Firewall).

e) Correio eletrônico (e-mail): Serviço que possibilita a troca assíncrona e ubíqua de mensagens através de recursos da Internet;

f) Site: Conjunto de documentos apresentados ou disponibilizados na rede mundial (web) por um indivíduo, empresa ou instituição, que pode ser acessado em um endereço específico da rede Internet (URL - UniformResourceLocator), podendo

ser subdividido em páginas com endereços específicos e próprios;

g) Download: Obtenção de cópia, em máquina local, de um arquivo originalmente armazenado em máquina remota ou em rede.

h) Upload: Armazenamento de Arquivos em Serviços de Nuvem.

i) Administradores: Técnicos de Manutenção e Suporte do setor de Informática responsável pelos Sistemas e pela Rede. Acesso especial dos administradores a senhas, informações ou outros privilégios só poderá ser usado com a finalidade de manutenção corretiva e/ou preventiva dos equipamentos e somente dentro dos limites necessários para execução das atividades necessárias. Qualquer informação obtida por meio de direitos especiais e privilégios deve ser tratada como privativa e confidencial pelos administradores da rede, sendo que estes poderão responder administrativamente por qualquer uso indevido de senhas ou informações dos usuários

j) Usuário: utilizador do equipamento de informática que fará uso do mesmo para realização de suas tarefas e atribuições.

k) Backup: Cópia de Segurança dos Sistemas e Arquivos para recuperação em casos de desastres. Essas Cópias deverão estar em Ambiente Interno e Externo corretamente armazenadas e protegidas

É DEVER DE TODOS OS SERVIDORES DO PREVMMAR:

Considerar a informação como sendo um bem da entidade, um dos recursos críticos para a realização das atividades, que possui grande valor para o PREVMMAR e deve sempre ser tratada profissionalmente.

1. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do diretor-presidente do PREVMMAR estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias), de acordo com a tabela abaixo:

1. Pública
2. Interna

3. Confidencial
4. Restrita

CONCEITOS:

Informação Pública: É toda informação que pode ser acessada por servidores da entidade, usuários, fornecedores, prestadores de serviços e público em geral;

Informação Interna: E toda informação que só pode ser acessada por servidores do PREVMMAR. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da entidade.

Informação Confidencial: É toda informação que pode ser acessada por servidores e parceiros e parceiros da entidade. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao serviço da entidade ou ao negócio do parceiro.

Informação Restrita: E toda informação que pode ser acessada apenas por servidores da entidade, explicitamente indicado pelo nome. A divulgação não autorizada dessa informação pode causar sérios danos a entidade e/ou comprometer a estratégia da organização.

O diretor-presidente deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras e mídias locais de fácil acesso, tendo sempre em mente o conceito de “mesa limpa”, ou seja, ao terminar o trabalho, não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

2. DADOS PESSOAIS DOS SERVIDORES DO PREVMMAR

2.1 O PREVMMAR se compromete em não acumular ou manter intencionalmente dados pessoais de servidores, além daqueles relevantes na condução de suas atividades.

2.2 Todos os dados pessoais de servidores e assegurados serão considerados dados essenciais.

2.3 Dados pessoais de servidores sob a responsabilidade do PREVMMAR não serão usados para fins diferentes daqueles para os quais foram coletados.

2.4 Dados pessoais de servidores não serão transferidos para terceiros, exceto quando exigido pelo exercício da atividade da instituição e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso, a lista de endereços eletrônicos (e-mails) usados pelos servidores do PREVMMAR.

3. PROGRAMAS ILEGAIS

3.1 A instalação de softwares somente poderá ser realizada pelos administradores da rede e dos equipamentos, seguindo os requisitos técnicos de segurança, sendo em nenhuma hipótese instalado pelos usuários dos equipamentos. Caberá ainda aos administradores, a manutenção preventiva e corretiva nos hardwares dos equipamentos.

3.2 Periodicamente, o setor de informática fará verificações nos dados dos servidores e/ou nos computadores dos servidores, visando garantir a correta aplicação desta diretriz.

4. PERMISSÕES E SENHAS

4.1 Quando da necessidade de cadastramento de um novo servidor para a utilização da rede, sistemas ou equipamentos de informática do PREVMMAR, o setor de origem do novo servidor deverá comunicar esta necessidade ao setor de informática, por meio de comando interno ou e-mail, informando a que tipo de rotinas e programas o novo servidor terá direito de acesso e quais serão restritos. A informática fará o recadastramento e informará ao novo servidor qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada 45 (quarenta e cinco) dias;

4.2 Por segurança, a informática recomenda que as senhas tenham sempre um mínimo de 8 (oito) caracteres alfanuméricos, caractéres especiais e diferenciação de letras maiúsculas e minusculas.

4.3 Todos os servidores responsáveis pela aprovação eletrônica de documentos (pedidos de compra, licitações, etc.) deverão comunicar ao setor de informática qual será o seu substituto quando de sua ausência do PREVMMAR, para que as permissões possam ser alteradas (delegadas a outro servidor).

5. COMPARTILHAMENTO DE PASTAS E DADOS

5.1 É de obrigação dos servidores rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos.

6. CÓPIA DE SEGURANÇA (BACKUP) DO SISTEMA INTEGRADO E SERVIDORES DE REDE DO PREVMMAR COM O MUNICIPIO DE MARACAJU

6.1 Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da informática e deverão ser feitas diariamente.

7. SEGURANÇA E INTEGRIDADE DO BANCO DE DADOS DO PREVMMAR

7.1 O gerenciamento do banco de dados é de responsabilidade dos terceiros contratados, nos sitemas de concessão de beneficios, folha de pagamentos, e contabilidade, sendo o setor de informática e do servidor delegado para esta área, responsaveis pela manutenção, alteração e atualização de equipamentos e programas do PREVMMAR.

8. ADMISSÃO/DEMISSÃO DE SERVIDORES EFETIVOS

8.1 O diretor-presidente do PREVMMAR deverá comunicar o setor de informática toda e qualquer movimentação de servidores, para que os mesmos possam ser cadastrados ou excluídos no sistema do PREVMMAR.

8.2 Cabe ao diretor-presidente a comunicação ao setor de informática sobre as rotinas a que o novo servidor terá acesso, para que na data de seu desligamento/exoneração possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.

8.3 Cabe ao diretor-presidente do PREVMMAR dar conhecimento e obter as devidas assinaturas de concordância dos novos servidores em relação à Política de

Segurança da Informação do PREVMMAR.

8.4 Nenhum servidor poderá ser cedido ao PREVMMAR sem ter expressamente concordado com esta política.

9. TRANSFERÊNCIA DE SERVIDORES

9.1 Quando um servidor for transferido de função/atribuição, o diretor-presidente deverá comunicar o fato ao setor de informática, para que sejam feitas as adequações necessárias para o acesso do referido servidor aos sistemas informatizados do PREVMMAR.

10. CÓPIA DE SEGURANÇA DE ARQUIVOS INDIVIDUAIS DO PREVMMAR

10.1 É de responsabilidade dos próprios servidores, a elaboração de cópias de segurança (“backups”) de textos, planilhas, mensagens eletrónicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos servidores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos trabalhos do PREVMMAR.

10.2 No caso das informações consideradas de fundamental importância para a continuidade dos trabalhos do PREVMMAR, o setor de informática disponibilizará um espaço no servidor onde cada funcionário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup de informática.

11. PROPRIEDADE INTELECTUAL DO PREVMMAR

11.1 É de propriedade do PREVMMAR, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer servidor durante o curso de seu vínculo com o PREVMMAR.

12. USO DO AMBIENTE WEB(Internet) DO PREVMMAR

12.1 O acesso à internet será autorizado para os servidores que necessitam da mesma para o desempenho das suas atividades profissionais no PREVMMAR. Sites que não contenham informações que agreguem conhecimento profissional e/ou para as atividades do PREVMMAR não devem ser acessados.

12.2 O uso da internet será monitorado pelo setor de informática, inclusive através

de “logs” (arquivos gerados no servidor) que informam qual servidor está conectado, o tempo que usou a internet e qual a página que acessou. Quando da instalação do FIREWALL .

12.3 A definição dos servidores que terão permissão para uso (navegação) da internet é atribuição do diretor-presidente do PREVMMAR, com base em recomendação do setor de informática.

12.4 Não é permitido instalar programas provenientes da internet nos microcomputadores do PREVMMAR, sem expressa anuência do setor de informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e municipais.

12.5 Os servidores devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licenças de uso ou patentes de terceiros.

12.6 Quando navegando na internet, é proibida a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionadas a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados das atividades do PREVMMAR;
- Que promovam discussão pública sobre as atividades do PREVMMAR, a menos que seja autorizado pelo diretor-presidente;
- Que possibilitem a distribuição de informações de nível “confidencial”;
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais;

TODOS ESSE QUESITOS SERÃO POSSÍVEIS COM A IMPLANTAÇÃO DO FIREWALL.

13. USO DE CORREIO ELETRÓNICO (EMAIL) INSTITUCIONAL DO PREVMMAR

13.1 O correio eletrônico fornecido pelo PREVMMAR é um instrumento de comunicação interna e externa para a realização das atividades do PREVMMAR.

13.2 As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do PREVMMAR, não podem ser contrárias à legislação vigente e nem aos princípios éticos do PREVMMAR.

13.3 O uso do correio eletrônico é coletivo e cada servidor deve se identificar e se responsabilizar nas mensagens enviadas.

13.4 É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem do PREVMMAR;
- Possam prejudicar a imagem de outras entidades ou empresas;
- Sejam incoerentes com as políticas do PREVMMAR.

13.5 A utilização do “e-mail” deve ser criteriosa, evitando que o sistema fique congestionado.

13.6 O setor de informática poderá, visando evitar a entrada de vírus no PREVMMAR, bloquear o recebimento de e-mails provenientes de sites gratuitos (propagandas, vendas, etc.).

14. NECESSIDADES DE NOVOS SISTEMAS, APLICATIVOS E/OU EQUIPAMENTOS PARA O PREVMMAR

14.1 O setor de informática é responsável pela aplicação da Política do PREVMMAR, em relação a definição de compra e substituição de “software” e “hardware”.

14.2 Qualquer necessidade de aquisição de novos programas ou equipamentos deverá ser discutida com o responsável pelo setor de informática.

14.3. Não é permitida a compra ou o desenvolvimento de software ou hardware diretamente pelos servidores.

15. USO DE COMPUTADORES PESSOAIS (LAPTOP) DE PROPRIEDADE DO PREVMMAR

15.1 Os servidores que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou outro qualquer equipamento de informática, de propriedade do PREVMMAR, devem estar cientes de que:

- Os recursos da tecnologia da informação, disponibilizados para os servidores,

tem como objetivo a realização de atividades profissionais;

- A proteção do recurso computacional de uso individual é de responsabilidade do próprio servidor;
- É de responsabilidade de cada servidor assegurar a integridade de cada equipamento, bem como a confidencialidade e disponibilidade de informação contida no mesmo;
- O servidor não deve alterar configurações no equipamento disponibilizado.

15.2 Em caso de furto:

- Registrar Boletim de Ocorrência em uma delegacia de polícia;
- Comunicar o diretor-presidente do PREVMMAR;
- Enviar cópia do B. O. para o setor de informática.

16. RESPONSABILIDADES DO DIRETOR-PRESIDENTE DO PREVMMAR

16.1 O diretor-presidente do PREVMMAR é responsável pela definição dos direitos de acesso dos servidores aos sistemas de informações do PREVMMAR, cabendo a ele ou ela, verificar se os mesmos estão acessando exatamente as rotinas compatíveis com suas respectivas funções, usando e conservando adequadamente os equipamentos e mantendo as cópias de segurança de seus arquivos individuais, conforme estabelecido nesta Política.

16.2 O setor de informática fará auditorias periódicas do acesso dos servidores às informações, verificando:

- Que tipo de informação o servidor pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e/ou informação;
- Quem autorizou o servidor a ter permissão de acesso à determinada rotina e/ou informação;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

17. SISTEMA DE TELECOMUNICAÇÕES DO PREVMMAR

17.1. O controle de uso, concessão de permissão e a aplicação de restrições em relação aos ramais eletrônicos do PREVMMAR, assim como o uso de eventuais ramais

virtuais instalados nos computadores, é de responsabilidade do setor de informática, de acordo com as definições da diretoria executiva do PREVMMAR.

18. USO DE ANTIVÍRUS

18.1 Todo arquivo em mídia proveniente de entidade externa deve ser verificado por programa antivírus.

18.2 Todo arquivo recebido/obtido através do ambiente da internet deve ser verificado por programa antivírus.

18.3 Todas as estações de trabalho devem ter um antivírus instalado. A autorização do antivírus será automática, agendada pelo setor de informática, via rede.

18.4 O servidor e os profissionais que prestam serviço de suporte e manutenção aos sistemas terceirizados, não podem em hipótese alguma, desabilitar o programa antivírus, instalado nas estações de trabalho, sem autoização expressa da Presidente do PREVMMAR.

19. PENALIDADES

19.1. O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, abertura de processo administrativo e disciplinar passível de exoneração, rescisão de contrato de serviço, outras ações disciplinares e/ou processo civil e criminal.

20. Esta política entra em vigor na data de sua publicação.

Maracaju, MS, 07 de outubro de 2020.

Roseli Bauer
Presidente do PREVMMAR

Marilene Tesser
Presidente Conselho Curador
Representante do SINTREMA

Clementino Serafim de Oliveira
Representante do SSPMM

Jorge Carlos Heller Netto
Representante do Executivo

Neli Terezinha Bairros
Representante dos Aposentados/Pensionistas

Mayara Ferreira Maris
Representante do Legislativo