DECRETO Nº. 2.808, de 23 de Junho de 2021.

Institui a Política de Segurança da Informação no âmbito do Instituto de Previdência Social dos Servidores Municipais de Nova Andradina – MS - PREVINA.

O PREFEITO MUNICIPAL DE NOVA ANDRADINA, Estado de Mato Grosso do Sul, no uso das atribuições que lhe são conferidas no inciso III do art. 72 da Lei Orgânica do Município;

CONSIDERANDO a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito do Instituto de Previdência Social dos Servidores Municipais de Nova Andradina – MS - PREVINA, de forma a atender aos princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

CONSIDERANDO que os agentes públicos devem zelar pelas informações que lhes são confiadas no exercício de suas funções;

CONSIDERANDO que as ações de Segurança da Informação reduzem custos e riscos e aumentam os benefícios prestados aos segurados, ao permitir a oferta de processos, produtos e serviços suportados por sistemas de informações mais seguros;

CONSIDERANDO – O disposto pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº. 13.709, de 14 de agosto de 2018.

DECRETA:

Art. 1º - Fica instituída a Política de Segurança da Informação no âmbito do Instituto de Previdência Social dos Servidores Municipais de Nova Andradina – MS - PREVINA.

§ 1º Para aplicar a Política de Segurança da Informação do PREVINA fica criado o Anexo I deste Decreto - Plano de Segurança da Informação do PREVINA – PSIPREV.

§ 2º O PSIPREV constitui um conjunto de ações e diretrizes que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas pelo PREVINA.

§ 3º Fica autorizada a Secretaria Municipal de Finanças e Gestão através do Setor de Tecnologia de Informação subsidiar, no limite de suas competências, a aplicação do disposto neste Decreto.

Art. 2º Constituem objetivos da Política de Segurança da Informação do PREVINA:

I - dotar os órgãos e setores do PREVINA de instrumentos jurídicos, normativos e institucionais que os capacitem técnica, tecnológica e administrativamente, com vistas a assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sigilosas do PREVINA;

II - estabelecer e controlar os níveis de acesso de fornecedores externos aos sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em Segurança da Informação;

IV - assegurar a interoperabilidade entre os sistemas de Segurança da Informação.

V – promover a segurança física e a proteção de dados organizacionais, e procedimentos de contingência (backups, controle de acesso).

Art. 3º Para os fins deste Decreto, ficam estabelecidos os seguintes conceitos:

I - ativo: todo elemento tangível ou intangível que compõe o processo de comunicação, abrangendo a informação, o respectivo emissor e meio de transmissão, até o receptor;

II - autenticidade: garantia de que uma informação, produto ou documento origina-se do autor a quem se atribui;

III - Central de Serviços: ponto único de contato do usuário com a área de Tecnologia da Informação e Comunicação da Administração Municipal, responsável pelo registro, análise e acompanhamento das requisições de serviços, bem como pela conclusão do atendimento;

IV - confidencialidade: garantia do sigilo da informação, de forma que o seu acesso seja obtido somente quando autorizado;

V - disponibilidade: propriedade do ativo, o qual deve estar acessível e utilizável sob demanda por uma entidade autorizada, quando solicitado;

VI - gestor de informação: pessoa detentora de competência institucional para autorizar ou negar o acesso à determinado sistema de informação ou recurso tecnológico ao usuário;

a) A função de Gestor de Informação será exercida pelo Diretor Financeiro do PREVINA.

VII - incidente de segurança: evento adverso, confirmado ou sob suspeita, que comprometa a integridade, a autenticidade, a conformidade ou a disponibilidade de qualquer ativo do PREVINA;

VIII - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

IX - integridade: salvaguarda da exatidão e da totalidade da informação e dos métodos de processamento;

X - legalidade: conformidade das ações realizadas no âmbito da Política de Segurança da Informação com o arcabouço normativo vigente;

XI - não repúdio: garantia de que um usuário não consiga negar (dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação;

XII - Segurança da Informação: conjunto de medidas que tem como objetivo o estabelecimento de controles necessários à proteção das informações durante sua criação, aquisição, uso, transporte, guarda e eliminação, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou intencionais, garantindo a continuidade dos serviços e a preservação de seus aspectos básicos, quais sejam, confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

XIII - Tecnologia da Informação e Comunicação: solução ou conjunto de soluções sistematizadas baseadas no uso de recursos tecnológicos que visam resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, bem como subsidiar processos que convertam dados em informação;

XIV - usuário: aquele que atua em órgão ou setor do PREVINA, seja servidor público, estagiário, contratado ou terceirizado, ou que, de alguma forma, encontre-se exercendo atividade junto ao PREVINA, desde que autorizado.

Art. 4º A Política de Segurança da Informação instituída neste Decreto reger-se-á pelos seguintes princípios:

I - tratamento da informação como patrimônio, tendo em vista que a divulgação das informações estratégicas de qualquer natureza pertencentes à Administração deve ser protegida de forma adequada, com vistas a evitar alterações, acessos ou destruição indevidos;

II - classificação da informação, garantindo-lhe o adequado nível de proteção, considerando:

a) a avaliação da necessidade e do tipo de acesso pelo usuário, adotando-se como parâmetro o grau de confidencialidade da informação;

b) a definição da confidencialidade da informação será definida em consonância com as atividades desempenhadas pelo usuário, com vistas a garantir a adequada autorização de acesso pelo gestor de informação, que deverá conter os limites de acesso, tais como leitura, atualização, criação e remoção, entre outros;

III - controle de acesso às informações, tendo como orientação a classificação definida no inciso II do *caput* deste artigo, respeitando a legislação vigente e considerando, ainda, que:

a) o acesso e o uso de qualquer informação, pelo usuário, devem se restringir ao necessário para o desempenho de suas atividades;

b) no caso de acesso a sistemas informatizados, deverão ser utilizados sistemas e tecnologias autorizados pelo PREVINA, por meio de identificador único e senha, ambos pessoais e intransferíveis;

c) o acesso, a divulgação e o tratamento da informação classificada como sigilosa, ficarão restritos às pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas pelas autoridades competentes.

IV - continuidade do uso da informação, sendo necessária, para o funcionamento dos sistemas, pelo menos uma cópia de segurança atualizada e guardada em local remoto, com o nível de proteção equivalente ao nível de proteção da informação original, observadas as seguintes regras:

a) para a definição das cópias de segurança devem ser considerados os aspectos legais, históricos, de auditoria e de recuperação de ambiente;

b) os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação devem ter controle de acesso físico, condições ambientais adequadas e ser protegidos contra situações de indisponibilidade causadas por desastres ou contingências;

c) definição do nível de disponibilidade para cada serviço prestado pelos sistemas de informação, nas situações mencionadas na alínea "b" deste inciso;

V - educação em Segurança da Informação, devendo ser observada pelo usuário a correta utilização das informações e dos recursos computacionais disponibilizados.

Art. 5º As medidas a serem adotadas para fins de proteção da informação deverão considerar:

I - os níveis adequados de integridade, confidencialidade e disponibilidade da informação;

II - as instruções e os procedimentos pertinentes, assim como a legislação vigente;

III - a compatibilidade entre a medida de proteção e o valor do ativo protegido;

IV - o alinhamento com as diretrizes estratégicas da Administração Municipal;

V - as melhores práticas para a gestão da Segurança da Informação;

VI - os aspectos comportamentais e tecnológicos apropriados.

Art. 6º Compete ao Gestor de Informação do PREVINA e ao Setor de Tecnologia da Informação da Prefeitura de Nova Andradina através do Plano de Segurança da Informação - PSIPREV

I - assegurar que a implementação da Política de Segurança da Informação tenha uma coordenação e que suas ações permeiem o PREVINA;

II - autorizar o emprego dos recursos necessários à implementação da Política de Segurança da Informação instituída neste Decreto;

III - estabelecer a estrutura necessária para a gestão de Segurança da Informação.

IV - elaborar e revisar continuamente os procedimentos e a normatização relacionada ao processo de gestão da Segurança da Informação;

V - avaliar propostas de modificação da Política de Segurança da Informação encaminhadas pelo PREVINA;

VI - garantir que os registros de auditoria de eventos de Segurança da Informação sejam produzidos e mantidos em conformidade com as normas vigentes;

VII - planejar, elaborar e propor estratégias e ações para a institucionalização da política, normas e procedimentos relativos à Segurança da Informação;

VIII - subsidiar a compatibilização de estratégias, planos e ações desenvolvidos no âmbito do PREVINA relativos à Segurança da Informação;

IX - realizar análise de riscos de processos, em consonância com os objetivos e ações estratégicas estabelecidas pelo PREVINA, e atualizá-la periodicamente;

X - promover estudos e projetos visando estimular o aperfeiçoamento tecnológico e científico em Segurança da Informação;

XI - avaliar a eficácia dos procedimentos relacionados à Segurança da Informação, propondo e implementando medidas que visem a melhoria do processo de Gestão de Segurança da Informação no âmbito do PREVINA;

XII - recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

XIII - relatar os incidentes de Segurança da Informação ao Diretor Presidente do PREVINA e ao Secretário Municipal de Finanças e Gestão, para que sejam tomadas as devidas providências;

XIV - apurar os incidentes de segurança críticos e dar o encaminhamento adequado;

XV - promover a conscientização, o treinamento e a educação em Segurança da Informação.

XVI – Criar, alterar ou excluir usuários para acesso aos diferentes sistemas de informação e/ou recursos tecnológicos sob sua guarda.

a) Em caso de sistemas terceirizados deverá tomar as providências necessárias para a criação alteração ou exclusão de acesso para os usuários.

b) A criação, alteração ou exclusão mencionadas neste inciso deverão ser feitas em estrito cumprimento ao Anexo I deste Decreto – Termo de Autorização para a Criação, Alteração ou Exclusão de Usuário.

Art. 8º É dever do usuário, em consonância com a Política de Segurança da Informação estabelecida neste Decreto:

I - responsabilizar-se, no âmbito de sua atuação, pela proteção e segurança da informação que lhe é confiada, devendo conhecer, entender e cumprir a Política estabelecida neste Decreto, bem como as diretrizes e instruções correlatas, zelando por sua correta aplicação;

II - fazer uso correto e responsável dos recursos tecnológicos, pautando-se pela legalidade e conduta ética, sempre em conformidade com os princípios da Segurança da Informação;

III - comunicar ao seu superior hierárquico qualquer incidente de segurança ou situação de risco no âmbito de sua atuação, que deverá cientificar o setor de Tecnologia da Informação para as devidas providências.

IV - guardar sigilo funcional sobre as informações que venha a ter conhecimento através dos sistemas que tenha acesso.

V – observar e cumprir o disposto pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº. 13.709, de 14 de agosto de 2018.

Art. 9º A não observância da Política de Segurança da Informação pelos usuários configura descumprimento de dever funcional, indisciplina ou insubordinação, conforme o caso, sujeitando o infrator à incidência das sanções cabíveis, nos termos da legislação vigente.

Art. 10 Os procedimentos relacionados à Segurança da Informação serão detalhados no Plano de Segurança da Informação – PSIPREV, que passa a integrar a Política de Segurança da Informação do PREVINA instituída neste Decreto.

Art. 11 Fica criado o Anexo II deste Decreto – Termo de Autorização para a Criação, Alteração ou Exclusão de Usuário.

§ 1º O Termo o qual se refere este artigo deverá ser preenchido pelo Gestor de Informação.

§ 2º O Termo de Compromisso e Responsabilidade, que acompanha o Anexo I deste Decreto deverá ser assinado pelo Servidor que utilizará os sistemas/recursos tecnológicos autorizados.

Art. 12 Este Decreto entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

Nova Andradina-MS, 23 de junho de 2021.

José Gilberto Garcia
PREFEITO MUNICIPAL

PUBLICADO
DIÁRIO OFICIAL DO MUNICÍPIO
Edição nº 1125
Data 24 / 06 / 21

ANEXO I AO DECRETO Nº 2.808, DE 23 DE JUNHO DE 2021

PLANO DE SEGURANÇA DA INFORMAÇÃO DO PREVINA – PSIPREV

Nº	AÇÃO	RESPONSÁVEL	PRAZO
01	Mapear todos os equipamentos e recursos tecnológicos utilizados no âmbito do PREVINA, classificando-os por usuários e responsáveis pela manutenção e/ou guarda, também serão detalhados o estado de conservação e se atendem sua necessidade, providenciando reparos, alterações ou sua substituição se necessário.	Gestor de Informação	31 de outubro de 2021.
02	Mapear todos os sistemas utilizados no âmbito do PREVINA, classificando-os por usuários e responsáveis pelo suporte e/ou criação/alteração/exclusão do acesso.	Gestor de Informação	31 de outubro de 2021
03	Excluir/inativar, nos termos do do anexo II deste decreto, todos os usuários identificados na ação 02 que não o utilizem mais ou que não integrem mais o quadro de servidores vinculados ao PREVINA.	Gestor de Informação e Responsável por cada Sistema.	31 de dezembro de 2021
04	Criar usuários para todos os servidores vinculados ao PREVINA, nos termos do anexo II deste decreto, conforme mapeamento realizado na ação 02.	Gestor de Informação e Responsável por cada Sistema.	31 de dezembro de 2021
05	Catalogar os procedimentos de segurança e backups existentes nos sistemas locais utilizados. Realizar análise de riscos.	Gestor de Informação e Responsável por cada Sistema.	31 de dezembro de 2021
06	Condensar as informações acima em um único documento que conterá todas as informações executadas nas ações anteriores: Catalogo de Equipamentos e recursos e seus usuários e responsáveis, Sistemas utilizados, usuários dos sistemas inclusive com a autorização de uso e ciência do usuário de seus diretos e deveres, catalogo dos procedimentos de segurança e backups adotados. Este documento deverá abordar ainda todas as ações e ocorrências descritas nas alíneas do Art. 06 deste decreto.	Gestor de Informação e Responsável por cada Sistema.	31 de janeiro de 2022
07	Adotar anualmente as ações 01 a 05, a fim de atualizar periodicamente o documento produzido na ação 06.	Gestor de Informação e Responsável por cada Sistema.	Anualmente

ANEXO II AO DECRETO Nº 2.808, DE 23 DE JUNHO DE 2021.

ESTADO DE MATO GROSSO DO SUL
PREFEITURA MUNICIPAL DE NOVA ANDRADINA

TERMO DE AUTORIZAÇÃO

CRIAÇÃO, ALTERAÇÃO OU EXCLUSÃO DE USUÁRIO PARA ACESSO A SISTEMAS DE INFORMAÇÃO E/OU RECURSOS TECNOLOGICOS NO ÂMBITO DO PREVINA.

NOME:	MATRICULA:
EMAIL:	TELEFONE:
UNIDADE:	CARGO:
GESTOR DE INFORMAÇÃO:	

PREENCHIMENTO EXCLUSIVO DO GESTOR DE INFORMAÇÃO DA UNIDADE

Na qualidade de Gestor de Informação de minha unidade, **SOLICITO** para o servidor acima descrito:

- ☐ Criação de Usuário
- ☐ Alteração de Usuário
- ☐ Exclusão de Usuário

Na qualidade de Gestor de Informação de minha unidade, **SOLICITO** para o servidor acima descrito os seguintes acessos:

- ☐ Internet
- ☐ Intranet
- ☐ Impressora
- ☐ Sistemas Bancários
- ☐ CADPREV
- ☐ PROGETEC
- ☐ CJUR
- ☐ Sistema Contábil
- ☐ Sistema de Folha
- ☐ Sistema de Protocolo
- ☐ Sistema de Compras
- ☐ Sistema de Licitações
- ☐ Sistema Tributário
- ☐ Sistema de Patrimônio
- ☐ Sistema de Estoque
- ☐ Sistema de Frotas
- ☐ Outros Sistemas

Especificar:_____

Observações:_____

**O perfil de usuário será o necessário para as atribuições do Cargo acima descrito ou conforme o campo observações.*

PREENCHIMENTO EXCLUSIVO DO SERVIDOR USUÁRIO

TERMO DE COMPROMISSO E RESPONSABILIDADE DO USUÁRIO

1-Utilizarei os sistemas corporativos do PREVINA unicamente para desempenhar minhas atribuições e atividades diárias no interesse da organização;
2-Não utilizarei a estrutura tecnológica do PREVINA para obter, fazer, executar ou distribuir copias não autorizadas de arquivos e informações;
3-Comprometo-me em manter total sigilo sobre dados ou informações que venha a ter conhecimento em razão do acesso aos sistemas/recursos tecnológicos.
4-Jamais utilizarei os sistemas/recursos tecnológicos sem a devida autorização do Gestor de Informação;

CÓDIGO PENAL

Art. 153 Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: Pena – Detenção, de 1 a 6 meses, ou multa. § 1º. A divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em Lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção de 1(um) a 4(quatro) anos e multa.

Art. 313-A Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão de 2(dois) a 12(doze) anos e multa.

Art. 313-B. Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção de 3(três) meses a 2(dois) anos e multa. Parágrafo único: As penas são aumentadas de um terço até a metade se a modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Art. 299 – Omitir, em documento público ou particular, declaração que dele deva constituir, ou nele inserir, fazer inserir declaração falsa ou diversa da que deva ser escrita, com fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Pena – Reclusão de 01 (um) a 05 (cinco) anos e multa se o documento é público, e reclusão de 01 (um) a 03 (três) anos e multa se o documento é particular. Parágrafo único – Se o agente é funcionário público e comete o crime prevalecendo-se do cargo ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena da sexta parte.

Art. 325 – Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena: detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.

DECLARAÇÃO

Declaro, sob as penas da lei, verdadeiras as informações neste ato prestadas, fazendo parte integrante dos registros e arquivos do PREVINA, tendo ciência do que estabelecem os artigos 153, 313-A, 313-B, 299, 325 e 327 do Código Penal Brasileiro, a legislação aplicada e demais normas complementares, aquiescendo com todas as responsabilidades inerentes ao uso dos sistemas/recursos tecnológicos, bem como das implicações e sanções administrativas, civis e penais decorrentes do seu uso indevido, seja qual for a circunstância, constituindo o usuário e senha disponibilizados para acesso, propriedade do PREVINA e portanto, sujeitos ao monitoramento e controle das ações realizadas em seu âmbito.

Declaro ainda que, estou ciente que o usuário e senha para acesso aos sistemas de informação/recursos tecnológicos são pessoais e intransferíveis, sendo única e exclusiva a responsabilidade de seu uso por minha parte.

Nova Andradina - MS, _____/_____/_____ _____

Local **Data** **Assinatura do Servidor**

AUTORIZAÇÃO DO GESTOR DE INFORMAÇÃO

Autorizo o servidor supramencionado.

(carimbo e assinatura)

Para uso exclusivo do setor responsável.

Usuário criado por: _____ **em**____/____/_____