ipms INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE SUZANO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE SUZANO

SUMÁRIO:

1 – INTRODUÇÃO 4

2 – NORMA ABNT NBRISO/IEC 27002:2005 E DEFINIÇÕES 5

3 – OBJETIVO 7

4 - INSTRUMENTOS NORMATIVOS 7

5 - DO ACESSO A INFORMAÇÃO E DA SUA DIVULGAÇÃO 9

6 - DA APROVAÇÃO E REVISÃO DA PSI 10

7 - DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO 10

8 - CLASSIFICAÇÃO DA INFORMAÇÃO 10

9 - PROTEÇÃO DA INFORMAÇÃO 12

10 - PRIVACIDADE DA INFORMAÇÃO 13

11 - TRANSFERÊNCIAS DE SERVIDORES 14

12 - CÓPIAS DE SEGURANÇA – BACKUP 14

13 - USO DO AMBIENTE WEB (Internet) 15

14 - USO DO CORREIO ELETRÔNICO – (E-mail) 16

15 - SISTEMAS, APLICATIVOS E EQUIPAMENTOS DO IPMS 17

16 - USO DE COMPUTADORES E EQUIPAMENTOS DO IPMS 17

17 - PAPÉIS E RESPONSABILIDADES 18

17.1. SERVIDORES, SEGURADOS, ESTAGIÁRIOS E PRESTADORES DE SERVIÇOS. 18

18 - SUPERINTENDÊNCIA DO IPMS 19

19 - DIRETORIA ADMINISTRATIVA E FINANCEIRA 19

20 - DIRETORIA DE BENEFÍCIOS E GESTÃO DE PESSOAS 20

21 - PROCURADORIA JURÍDICA 21

22 - GESTOR DA INFORMAÇÃO 21
23 – AUDITORIA 22
24 - VIOLAÇÕES E SANÇÕES 22
24.1 - VIOLAÇÕES 22
24.2 - SANÇÕES 23
25 - LEGISLAÇÃO APLICÁVEL 23

1 – INTRODUÇÃO

Como a informação é um dos principais ativos das organizações. É atraves dela que as instituições gerenciam seus produtos e ou serviços e traçam suas estrategias, tornando os sistemas de informações ativos criticos que necessitam serem protegidos contra ameças que podem explorar as vulnerabilidades do sistema. Estas violações na segurança podem causar a perda da confidencialidade, integridade, e disponibilidade das informações, podendo gerar prejuizos financeiros e afetando sua reputação perante a sociedade.

Visando assegurar que as informações do IPMS não estejam com pessoas desautorizadas, não sejam corrompidas ou mesmo inacessíveis, faz-se necessário a implementação desta Politica de Segurança da Informação - P.S.I para garantir a confidencialidade, integridade e disponibilidade, que são os pilares da segurança da informação.

O propósito é formalizar o direcionamento estratégico da gestão de segurança da informação, estabelecendo as diretrizes a serem seguidas para a implantação e manutenção de uma politica de segurança da informação, guiando-se, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000.

O presente documento constitui uma declaração formal do IPMS – Instituto de Previdência do Município de Suzano, a acerca de seu compromisso com a proteção dos dados e das informações de sua propriedade ou sob sua custódia, devendo ser obedecido por todos os seus dirigentes, conselheiros, servidores, segurados, servidores dos órgãos reguladores e fiscalizadores e dos prestadores de serviços deste Regime Prório de Previdência Social.

O gerenciamento dos riscos é um dos pricipais processsos da gestão da segurança, pois visa identificar, analisar, avaliar e controlar os riscos inerentes à segurança da informação. Para isso, a conscientização de todos os envolvidos é imprescindível para a prevenção de incidentes e, esta política de segurança da informação deve ser seguida pelos usuários do IPMS como uma ferramenta de trabalho que serve para ajudá-los em suas rotinas operacionais.

É dever de todos do IPMS – Instituto de Previdência do Município de Suzano, seguir as normas e as diretrizes estabelecidas nesta Politica de Segurança da Informação - P.S.I.

2 – NORMA ABNT NBRISO/IEC 27002:2005 E DEFINIÇÕES

A ABNT NBR ISO/IEC 27002:2005, define a segurança da informação como sendo a "preservação da confidencialidade, da integridade e da disponibilidade da informação". Nesse contexto, a segurança da informação é a garantia de que as informações da organização serão protegidas de acordo com os três pilares:

Confidencialidade: pode ser definida como a garantia de que as informações serão acessadas apenas pelas pessoas que tem autorização para acessá-las;

Integridade: é a garantia de que as informações são corretas e completas e;

Disponibilidade: é a garantia de que as informações estarão disponíveis para serem acessadas pelas pessoas que tem autorização para vê-las quando forem necessárias.

Destaca ainda que a *"*Segurança da informação" é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."

Ainda de acordo com a norma ABNT BR ISO/IEC27002:2005, *"A* segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio."

Mediante tal embasamento e considerando o disposto na adesão ao Pró Gestão, o INSTITUTO DE PREVIDENCIA DO MUNICÍPIO DE SUZANO - IPMS resolve implantar a Politica de Segurança da Informação (P.S.I.), cuja estrutura e diretrizes são expressas neste documento. Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

Colaborador: Funcionários de quaisquer cargo, estagiários e prestadores de serviços;

Confidencialidade: Informação acessível ou divulgada somente às pessoas autorizadas;
Disponibilidade: Pessoas autorizadas com acesso à informação sempre que necessário;

Integridade: Informações mantidas integras em seu formato original;
Normas de Segurança da Informação: Especificam os processos e controles que devem ser implementados para o alcance dos objetivos de segurança da informação definidos nesta política;

Prestadores de serviços: Pessoa jurídica ou física que mantenha contrato de prestação de serviço com o IPMS.

Segurança da Informação: É o conjunto de controles que visam garantir a preservação dos aspectos de confidencialidade, integridade e disponibilidade das informações; Termos de ciência de Segurança: Declaração onde o colaborador atesta a ciência sobre todos os termos tratados nessa PSI, normas a ela vinculadas e a sua estrutura de funcionamento;

Visitante: Todo indivíduo que não mantenha qualquer vínculo formal com o IPMS, ou seja, aqueles que não se enquadram na definição de Colaborador, conforme acima.

Ativo: É tudo aquilo que tenha valor para a organização. [ISO/IEC 13335- 1:2004]

Ativo de Informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou a instituição. [ISO/IEC 13335-1:2004].

Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. [ABNT NBR ISO/IEC 27002:2005].

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004].

Incidente de segurança da informação: indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004].

Informação: agrupamento de dados que contenham algum significado.

Risco: combinação da probabilidade de um evento e de suas consequências [ABNT NBR ISO/IEC Guia 73:2005].

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. [ABNT NBR ISO/IEC 27002:2005].

3 – OBJETIVO

Foi elaborada esta PSI - Política de Segurança da Informação para orienta na criação de normas mais específicas e procedimentos para o tratamento seguro das informações e de outros ativos organizacionais que processam ou armazenam dados e informações, além de auxiliar também na identificação e classificação das informações e dos demais ativos quanto à sua importância para este Regime Próprio de Previdência Social do Município de Suzano - IPMS.

Esta norma a ser implementada define uma série de controles para proteção desses ativos e informações, como a análise crítica e manutenção da própria Política de Segurança da Informação, a atribuição de responsabilidades relativas à segurança da informação, a elaboração de contratos e acordos de confidencialidade entre instituições prevendo a preservação da segurança da informação, a execução de inventários de ativos, a contratação de mão de obra, termo de responsabilidade e sigilo da informação, termo de uso dos sistemas de informação e os controles de acesso físico às dependências do IPMS.

O objetivo da PSI – Política da Segurança da Informação é garantir a segurança dos ativos desta autarquia previdenciária municipal que busca prevenir e mitigar os riscos e incidentes na operacionalização das uas atribuiçoes institucional. Por definição, um ativo é tudo aquilo que pode ser transformado em valor para a empresa. Assim, quando falamos em informação, ela só tem valor se os três pilares da segurança que são: Confidencialidade, Integridade e Disponibilidade também conhecida pela sigla CID forem alcançados.

4 - INSTRUMENTOS NORMATIVOS

A preocupação com segurança da informação na Administração Pública Federal vem sendo demonstrada através de diferentes instrumentos normativos. Podemos destacar os seguintes ordenamentos juridicos:

Código Penal (Decreto-lei nº 2.848, de 07 de dezembro de 1940), preve estabelece, no art. 153 e art. 325 que se deve guardar o sigilo necessário da informação. O mesmo código preve ainda, as penalidades nos termos da legislação para a divulgação de segredo; invasão de dispositivo informático; falsidade ideológica; inserção de dados falsos em sistema de informações; modificação ou alteração não autorizada de sistema de informações e violação de sigilo funcional.

Lei nº 8.159/1991 diz que é "dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação".

A Lei nº 9.983/2000 altera o Código Penal, incluindo uma preocupação com a integridade e confiabilidade das informações armazenadas em sistemas computacionais ao tipificar a alteração desses dados.

O Decreto nº 9.637/2018 que revogou o Decreto nº 3.505/2000 institui a Política de Naciona de Segurança da Informação e dispõe sobre a governança da segurança da informação, destacando que um dos pressupostos básicos é a conscientização dos órgãos e entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco de suas vulnerabilidades.

Já o Decreto nº 7.845/2012, regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo Federal, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Por último, temos em vigor desde o último dia 18 de setembro de 2020, a Lei Nº 13.709/2018, de 14 de agosto de 2018, que é a Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e tem como objetivo regulamentar a política de proteção de dados pessoais e, modifica alguns dos artigos do Marco Civil da Internet e impacta outras normas como as alterações no cadastro positivo, transformando drasticamente a maneira como empresas e órgãos públicos tratam a privacidade e a segurança das informações de usuários e clientes.

A LGPD prevê a utilização de medidas técnicas e administrativas aptas a proteger os dados, tornando necessária haver a Governança dos Dados, identificando onde residem, qual seu fluxo, classificando seu nível (dados pessoais, sensíveis ou não), gerenciando seu uso e ciclo de vida, protegendo de possíveis vazamentos ou deleções indevidas e monitorando sua utilização.

Este documento que compõem a estrutura normativa está dividido em três categorias:

a) Política (nível estratégico): constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o IPMS decidiu incorporar à sua gestão de acordo com a visão estratégica e serve como base para que as normas e os procedimentos sejam criados e detalhados;

b) Normas (nível tático): especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da política da politica de seguranca da informação;

c) Procedimentos (nível operacional): instrumentalizam o dispo to nas normas e na política, permitindo a direta aplicação nas atividades do IPMS.

5 - DO ACESSO A INFORMAÇÃO E DA SUA DIVULGAÇÃO

Caberá ser observadas as normas e procedimentos específicos aplicáveis, visando assegurar a:

I - Gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;

II - Proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade e;

III- Proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Os documentos integrantes da estrutura desta P.S.I. devem ser divulgados a todos os servidores, conselheiros, segurados, estagiários e prestadores de serviços do IPMS quando de sua admissão, bem como, através dos meios oficiais de divulgação interna do IPMS e, também, publicadas no site da instituição, de maneira que seu conteúdo possa ser consultado a qualquer momento.

6 - DA APROVAÇÃO E REVISÃO DA PSI.

Os documentos integrantes da estrutura normativa da Segurança da Informação do IPMS deverão ser aprovados e revisados conforme critérios descritos abaixo:

a) Política

Nível de aprovação: Conselho Deliberativo

Periodicidade da revisão: anual

b) Normas

Nível de aprovação: Conselho Deliberativo

Periodicidade da revisão: anual

c) Procedimentos

Nível de aprovação: Diretoria responsável pela área envolvida.

Periodicidade da revisão: semestral.

Durante o primeiro ano de vigência de cada documento, considerado a partir da data de sua publicação, a periodicidade das revisões poderá ser igual à metade dos períodos acima definidos.

7 - DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, apresentamos as diretrizes da política de segurança da informação do IPMS que constituem os principais pilares do sistema de segurança da informação da instituição, norteando a elaboração das normas e procedimentos:

8 - CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação das informações é o processo de identificar e definir niveis e critérios de proteção adequada para as informações, objetivando garantir a segurança das mesmas. Uma organização precisa ser capaz de identificar os valores de suas informações para garantir sua confidencialidade, integridade e disponibilidades. O objetivo principal desta classificação está em priorizar recursos, focando os investimentos nas informações mais importantes para a organização. São exemplos de informações:

Dados: Base de dados e arquivos, documentação de sistemas, informações armazenadas, procedimentos de suportes ou operação;

Software: Aplicativos, sistemas ferramentas de desenvolvimento e utilitários;

Ativos fisicos: equipamentos computacionais (processadores, monitores e impressoras), equipamentos de comunicação (roteadores, hub), pen drive e midias magnéticas (fitas, discos), estaçoes de trabalho (mesas e cadeiras);

Serviços: serviço de operadora de telecomunicação, dados e internet, serviço de energia eletrica, água e etc..

Define-se como necessária a classificação de toda a informação de propriedade do IPMS de maneira proporcional ao seu valor para a instituição, para possibilitar o controle adequado da mesma, devendo ser utilizados os seguintes níveis de classificação:

a) **Pública**: É uma informação do IPMS ou de seus segurados com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo. É destinada ao
público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

b) **Interna**: É uma informação do IPMS na qual não tem interesse em divulgar, mas cujo acesso por parte de indivíduos externos ao IPMS deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da instituição, porém, não com a mesma magnitude de uma informação confidencial ou restrita. Pode ser acessada sem restrições por todos os segurados e prestadores de serviços do IPMS.

c) **Confidencial**: É uma informação crítica para o IPMS ou de seus segurados. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem institucional, operacional ou, ainda, sanções administrativas, civis e criminais aos seus servidores e segurados. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por servidores, conselheiros, segurados e/ou prestadores de serviços.

d) **Informação Restrita**: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A

divulgação não autorizada dessa informação pode causar sérios danos à organização e/ou comprometer a estratégia da organização.

Todas as diretorias devem orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

9 - PROTEÇÃO DA INFORMAÇÃO

Define-se como necessária a proteção das informações da instituição ou sob sua custódia como fator primordial nas atividades profissionais de cada servidor, conselheiro, segurado, estagiário ou prestador de serviços do IPMS, sendo que:

a) Os servidores devem assumir uma postura proativa no que diz respeito à proteção das informações do IPMS e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade do IPMS;

b) As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;

c) Assuntos confidenciais não devem ser expostos publicamente;

d) Senhas, chaves, token e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;

e) Somente softwares homologados podem ser utilizados no ambiente computacional do IPMS;

f) Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;

g) Deverá ser garantido que o acesso à rede de computadores do IPMS seja individualizado, onde cada usuário, para poder acessar dados da rede de computadores do IPMS, deverá possuir um código de acesso atrelado à uma senha previamente cadastrada, sendo esta pessoal e intransferível, ficando vedada a utilização de códigos de acesso genéricos ou comunitários e o compartilhamento de senha de acesso;

h) É vedado o compartilhamento de informações através de pastas compartilhadas

nos computadores locais da instituição. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

i) Deverão ser criados permissões de acesso aplicáveis para todos os dados que sejam compartilhados através dos servidores do IPMS;

j) Todos os dados considerados como imprescindíveis aos objetivos do IPMS devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo estas cópias serem submetidos à testes periódicos de recuperação.

10 - PRIVACIDADE DA INFORMAÇÃO

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e que são manipuladas ou armazenadas nos meios às quais o IPMS detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais do IPMS e reafirmam o seu compromisso com a melhoria contínua desse processo, em consonância com a Lei Geral de Proteção de Dados (LGPD):

a) As informações são coletadas de forma ética e legal, com o conhecimento do segurado, para propósitos específicos e devidamente informados;

b) As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;

c) As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados; Tais informações fornecidas por força de elaboração de trabalhos tecnicos ou contida em banco de dados de sistemas de fornecedores são permanentemente proibidas de serem repassadas a terceiros.

d) As informações somente são fornecidas a terceiros, mediante autorização prévia da superintendência ou para o atendimento de exigência legal;

e) As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só poderão ser fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

11 - TRANSFERÊNCIAS DE SERVIDORES

Quando houver na gestão de pessoal a movimentação de transferencia de seção ou de setor de servidores, a Diretoria na qual o servidor está lotado deverá comunicar o fato ao setor responsável pela Tecnologia da Informação, para que sejam realizadas as adequações necessárias para o acesso do referido servidor ao sistema informatizado do IPMS.

12 - CÓPIAS DE SEGURANÇA – BACKUP

Todas as cópias de segurança serão gerenciadas e executadas por sistemas de agendamento automatizado, para que sejam executadas diariamente após o horario de expediente.

Deverá ser criado setor de Tecnologia da Informação o qual será responsável pela gestão dos sistemas de backup e deverá realizar testes de restauração das cópias para certificar a integridade dos dados, identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, estatística de crecimento dos dados entre outros.

Todo backup deve ser devidamente identificado e datado para efetivo controle. O tempo de vida e uso das mídias utilizadas para backup deve ser monitorado, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante. Testes de restauração (restore) de backup devem ser executados, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios do IPMS, o setor de Tecnologia da Informação disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Tais informações serão incluídas na rotina diária de backup.

13 - USO DO AMBIENTE WEB (Internet)

O acesso à Internet será autorizado para os usuários que o necessitarem para o desempenho das suas funções e atividades profissionais vinculadas ao IPMS. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o instituto não devem ser acessados. Não deverá ser permitido instalar programas provenientes da Internet nos microcomputadores do IPMS, devendo toda instalação ser realizada pelo setor de Tecnologia da Informação.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Não baixar e executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De conteúdo pornográfico ou relacionado a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito;
- Que promovam a participação em salas de discussão de assuntos não relacionados institucionalmente ao IPMS;
- Que possibilitem a distribuição de informações de nível “Confidencial”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

14 - USO DO CORREIO ELETRÔNICO – (E-mail)

O correio eletrônico fornecido pelo IPMS é um instrumento de comunicação interna e externa do instituto. As mensagens devem ser escrita com zelo profissional, não devem comprometer a imagem do IPMS, não podem ser contrárias à legislação vigente e nem aos princípios éticos e morais. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas e ao IPMS;
- Sejam hostis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem e a reputação do IPMS;
- Possam prejudicar a imagem de outras empresas ou órgãos públicos do município;
- Sejam incoerentes com as políticas do IPMS.

Para incluir um novo usuário no correio eletrônico, a respectiva Diretoria deverá fazer um pedido formal ao setor de Tecnologia da informação, que providenciará a inclusão do mesmo.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem do IPMS perante seus servidores e a comunidade em geral e que possam causar prejuízos à imagem institucional e financeira ao IPMS.

Evitar a utilização do e-mail institucional para assuntos pessoais.

Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para as atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo

corrente, aviso de vírus, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, fakenews, etc.

15 - SISTEMAS, APLICATIVOS E EQUIPAMENTOS DO IPMS.

O IPMS deverá implementar uma área responsável pelo setor de Tecnologia da informação, que será responsável pela aplicação da Política de Segurança da Informação do IPMS e pela definição de configuração visando a aquisição e atualização de "software", "hardware" e dispositivos eletrônicos. Quando da necessidade de novas aquisições de programas ("softwares") ou de equipamentos de informática (hardware) deverá ser discutida técnico pelo setor de Tecnologia da informação.

16 - USO DE COMPUTADORES E EQUIPAMENTOS DO IPMS

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

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido.

<u>Os cuidados a serem observados:</u>

Ambiente Externo ao IPMS:

- O equipamento deverá estar sempre em posse do servidor designado para o seu uso;
- Deverá ser dada especial atenção em ambientes públicos com grande movimentação de pessoas, como hall de hotéis, aeroportos, aviões, táxi, carros de aplicativos e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta- malas ou

lugar não visível;

- Redobrar à atenção ao transportar o equipamento na rua.

Em caso de furto ou roubo

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao setor de Tecnologia da informação;
- Envie uma cópia da ocorrência para o IPMS, aos cuidados do superior responsável, que encaminhará para o setor de Tecnologia de Informação

17 - PAPÉIS E RESPONSABILIDADES

17.1. SERVIDORES, SEGURADOS, ESTAGIÁRIOS E PRESTADORES DE SERVIÇOS.

Todo arquivo em mídia proveniente de entidade externa ao IPMS deve ser verificado por programa antivírus, bem como todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. As configurações do antivírus serão definidas pelo setor responsável pela Tecnologia de Informação, sendo vedado ao usuário alterá-las. O usuário tampouco não poderá em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Cabe a todos os servidores, estagiários e prestadores de serviços do IPMS cumprir com as seguintes obrigações:

a) Assinar o Termo de Responsabilidade e Sigilo da Informação;

b) Assinar o Termo de Uso dos Sistemas de Informação;

c) Zelar continuamente pela proteção das informações da instituição ou de seus segurados contra acesso, modificação, destruição ou divulgação não autorizada;

d) Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Instituição;

e) Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;

f) Comunicar imediatamente ao superior responsável, que dará conhecimento ao setor de Tecnologia da informação qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação; e

g) A pessoa física ou entidade privada que, em razão de qualquer vínculo com o IPMS,

executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Política de Segurança da Informação.

18 - SUPERINTENDÊNCIA DO IPMS

18.1 - Cabe à Superintendência:

a) Aprovar a política e as normas de segurança da informação e suas revisões;
b) Nomear o gestor da informação;
c) Receber, por intermédio do setor de Tecnologia da Informação, relatórios de violações da política e das normas de segurança da informação, quando aplicáveis;
d) Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas do setor de Tecnologia da informação.

19 - DIRETORIA ADMINISTRATIVA E FINANCEIRA

19.1 - Cabe à diretoria Administrativa e Financeira:

a) Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;
b) Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;
c) Sugerir ao superintendente, de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;
d) Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados às suas áreas, quando solicitado pelo superintendente;
e) Comunicar imediatamente ao gestor eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação;
f) Manter e preservar as instalações fisicas e o controle e o gerenciamento de portaria na segurança e vigilância física e dos sistemas de monitoramento seja atraves de alarmes e ou CFTV, além de projetos de segurança na prevenção e combate a incendio nas dependencias do IPMS;
g) Criar mecanismos para informar, antecipadamente aos fatos, alterações no quadro de

servidores do IPMS.

h) Fazer a gestão dos documentos, bancos de dados e informações que deram suporte às avaliações atuariais do RPPS e aos demais estudos técnicos previstos na Portaria nº 464 de 19/11/18, visando atender a exigencia para que deverão permanecer arquivados na unidade gestora do RPPS todo conjunto de informações à sua disposição pelo prazo de 10 (dez) anos;

i) Manter a guarda e o controle de todos os arquivos gerados para o preenchimento de todos os demonstrativos que são exigidos para a alimentação dos sistemas gerenciais da SPREV, tais como: o Sistema de Informações Gerenciais dos Regimes Próprios de Previdência Social (SIG- RPPS), o Cadastro Nacional de Informações Sociais (CNIS); Siprev Gestão; CADPREV WEB e CADPREV LOCAL e GESCON. Tais arquivos estão nos diversos formatos para atender as finalidades institucionais desta autarquia previdenciária;

20 - DIRETORIA DE BENEFÍCIOS E GESTÃO DE PESSOAS

20.1 - Cabe à Diretoria de Benefícios e Gestão de Pessoas:

j) Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;

k) Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;

l) Sugerir ao superintendente, de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;

m) Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados às suas áreas, quando solicitado pelo superintendente;

n) Coordenar o registro e atualização dos assentamentos dos segurados e pensionistas, e da documentação e arquivo dos respectivos processos;

o) Manter atualizado o cadastro dos funcionários segurados ativos e inativos, e de seus dependentes, tanto da Prefeitura, da Câmara Municipal e demais órgãos empregadores municipais vinculados ao IPMS;

p) Gerenciar os arquivos bancarios quando do processamento da folha de pagamento dos benefícios previdenciários; e

q) Comunicar imediatamente ao superintendente eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

21 - PROCURADORIA JURÍDICA

21.1 - Cabe, adicionalmente, à procuradoria Jurídica:

a) Incluir na análise e elaboração de contratos, obrigatoriamente, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses do IPMS, em especial a devolução das informações e do banco de dados que povoam o sistema de gestão quando da finalização de contrato com prestadoras de serviços;
b) Manter o superintendente e as diretorias do IPMS informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;
c) Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

22 - GESTOR DA INFORMAÇÃO

O Gestor da Informação poderá ser um servidor especializado em TI ou empresa contratada especificamente para o gerenciamento da Tecnologia de Informação, sendo designado pela Diretoria como responsável por determinado ativo de informação. Este gestor deve dominar todas as regras de negócio necessárias à criação, manutenção e atualização de medidas de segurança relacionadas ao ativo de informação sob sua responsabilidade, seja este de propriedade do IPMS. O Gestor da Informação é o responsável final proteção das informações do IPMS.

22.1 - Compete ao Gestor da Informação:

a) Classificar a informação sob sua responsabilidade, inclusive aquela gerada por servidores, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;
b) Inventariar todos os ativos de informação sob sua responsabilidade;
c) Enviar à diretoria administrativa, quando solicitado, relatórios sobre as informações e ativos de informação sob sua responsabilidade. Os modelos de relatórios serão definidos pelo Gestor de TI e aprovados pela Diretoria administrativa;
d) Sugerir procedimentos para proteger os ativos de informação, conforme a classificação realizada, além da estabelecida pela Política de Segurança da Informação e pelas Normas de Segurança da Informação;

e) Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma. Tal política deve definir quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso;

f) Reavaliar, periodicamente, as autorizações dos usuários que acessam as informações sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;

g) Participar da investigação dos incidentes de segurança relacionados às informações sob sua responsabilidade.

23 – AUDITORIA

Todo ativo de informação sob responsabilidade do setor de Tecnologia da Informação é passível de auditoria em data e horários determinados pelo Superintendente, podendo esta, também, ocorrer sem aviso prévio. A realização de uma auditoria deverá ser obrigatoriamente aprovada pela Superintendencia e, durante a sua execução, deverão ser resguardados os direitos quanto a privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade do IPMS.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, o setor de Tecnologia da Informação poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e das informações obtidas.

Em ambos os casos, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

24 - VIOLAÇÕES E SANÇÕES

24.1 - VIOLAÇÕES

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

a) Quaisquer ações ou situações que possam expor o IPMS ou seus segurados à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

b) Utilização indevida de dados da Instituição, divulgação não autorizada de informações,

sem a permissão expressa do Gestor da Informação;

c) Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do IPMS ou de seus segurados;

d) A não comunicação imediata à área de Gerencia da Informação de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um servidor, segurado, estagiário ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

24.2 - SANÇÕES

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação do IPMS são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

25 - LEGISLAÇÃO APLICÁVEL

Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);

LEI N° 4.583/12 Institui o Regime Próprio de Previdência Social, cria o Instituto de Previdência do Município de Suzano – IPMS

Lei Complementar Municipal nº 190, de 08 de julho de 2010, que dispõe sobre o Estatuto dos Servidores Públicos do Município de Suzano;

Lei Federal nº 8.159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

Lei Federal 10.406, de 10 de janeiro de 2002 (Institui o Código Civil);

Lei Federal 9.983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias);

Lei Federal nº 12.527, de 18 de novembro de 2011. (Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências);

Lei nº 9.717, de 27 de novembro de 1998, que dispõe sobre regras gerais para a organização e o funcionamento dos regimes próprios de previdência social dos servidores públicos da União, dos Estados, do Distrito Federal e dos Municípios, dos militares dos Estados e do Distrito Federal e dá outras providências;

Lei Nº 13.709/2018, de 14 de agosto de 2018, já está em vigor desde 18 de setembro é a Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado;

Portaria Nº 20.532, de 8 de Setembro de 2020, dispoe sobre à aprovação da Versão 3.1 do Manual do Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios - Pró-Gestão RPPS (Processo nº 10133.101343/2019-57).

PLANO DE CONTINGÊNCIA

1- PROPÓSITO 3

2 - SERVIDORES ENVOLVIDOS 3

3 - RESPONSABILIDADES 3

4 - RESTAURAÇÕES DE SERVIDORES EM CASO DE DESASTRES 4

4.1 - Firewall (12 horas) 4

4.2 - Servidores de Banco de Dados e WEB (12 horas) 4

4.3 - Servidor de Aplicação (12 horas) 5

4.4 - Servidores Controlador de domínio / Armazenamento de arquivos (24 horas) 5

4.5 - Servidor de E-mail e Controlador de Domínio secundário (24hs) 6

4.6 - Servidor de hospedagem das VM'S (24 horas) 7

4.7 - Servidor de gerenciamento do Hyper-V (6 horas) 7

4.8 - Serviço de acesso à internet (12 horas) 8

5 - ÁREAS AFETADAS 8

6 – NOTIFICAÇÕES INTERNA (TELEFONE / E-MAIL) 8

7 - NOTIFICAÇÕES EXTERNA (TELEFONE / E-MAIL) 9

8 - BACKUPS 9

1- PROPÓSITO

Estabelecer um plano para a recuperação dos serviços de tecnologia da informação após a ocorrência de eventos que possam causar a interrupção não programada de suas atividades. Este plano visa assegurar o pronto restabelecimento dos serviços de tecnologia, reduzindo o tempo para a normalização da infraestrutura tecnológica do IPMS – Instituto de Previdência do Município de Suzano.

Para isso, ele plano de contingência constitui de um conjunto de procedimentos definidos e estruturados para serem adotados quando da inoperância de um recurso técnico (sistemas, comunicações, componentes, etc.), objetivando a sua recuperação após o evento indesejado.

2 – DO SETOR DE TECNOLOGIA DE INFORMAÇÃO

O IPMS deverá implementar Setor de Tecnologia de Informação com Servidores especializados em TI ou, alternativatimente, contratar empresa especializada que será responsável pela área de Tecnologia e Segurança da Informação do Instituto de Previdência do Município de Suzano, devendo reportar o andamento da implementação do Plano de Contingência para a Superintendência e a Diretoria Administrativa e Financeira do IPMS.

3 - RESPONSABILIDADES

Setor de Tecnologia da Informação:

- Firewall;
- Servidor de Banco de Dados;
- Servidor de Aplicação;
- Servidor de Autenticação/Controlador de Domínio/Arquivos;
- Servidor de E-mail;
- Serviço de acesso à internet;
- Serviço de Backup; e
- Serviço de impressão.

4 - RESTAURAÇÕES DE SERVIDORES EM CASO DE DESASTRES

4.1 - Firewall (12 horas)

Abrangência:

Abriga o serviço de Firewall e funciona como gateway da rede.

Procedimento:

- Comunicar a Superintendência e a todas as diretorias sobre os serviços afetados e o prazo para restauração;
- Entrar em contato com suporte técnico do Firewall;

- Configurar e testar todos os serviços.

4.2 - Servidores de Banco de Dados e WEB (12 horas)

Abrangência:

Abriga o banco de dados e o site do IPMS.

Procedimento:

- Comunicar a Superintendência e a todas as diretorias sobre os serviços afetados e o prazo para restauração;
- Providenciar um novo servidor (casonecessário) parainstalação das aplicações e serviços;
- Proceder com a instalação e configuração do Servidor;
- Instalar o banco de dados;
- Restaurar a base de dados no novo servidor;
- Configurar e testar o banco de dados.

4.3 - Servidor de Aplicação (12 horas)

Abrangência:

Abriga todas as aplicações utilizadas no IPMS.

Procedimento:

- Comunicar a Superintendência e a todas as diretorias sobre os serviços afetados e o prazo para restauração;
- Providenciar um novo servidor (caso necessário) para instalação das aplicações e serviços;
- Proceder com a instalação e configuração do Servidor;
- Restauraras aplicações e serviços;
- Configurar o acesso ao banco de dados;
- Configurar e testar todos os serviços.

4.4 - Servidores Controlador de domínio / Armazenamento de arquivos (24 horas)

Abrangência:

Abriga os dados do diretório e gerencia a comunicação entre usuários e domínios, incluindo os processos de logon do usuário, a autenticação, as pesquisas em diretório e as configurações de diretivas de grupos. Fornece, também, serviços de compartilhamento e armazenamento de arquivos em rede.

Procedimento:

• Comunicar a Superintendência e a todas as diretorias sobre os serviços afetados e o prazo para restauração;
• Providenciar um novo servidor (caso necessário) para instalação das aplicações e serviços;
• Proceder com a instalação e configuração do Servidor;
• Ativar os serviços necessários para o funcionamento do servidor;
• Restaurar os dados do compartilhamento de arquivos;
• Restaurar as configurações de diretivas de grupos;
• Restaurar as configurações de impressoras;
• Configurar e testar todos os serviços.

4.5 - Servidor de E-mail e Controlador de Domínio secundário (24hs)

Abrangência:

Tem como função fornecer um serviço centralizado de e-mail coorporativo e exercer o papel de controlador de domínio secundário, realizando a autenticação do usuário na rede e a distribuição de DNS.

Procedimento:

- Comunicar todas as diretorias sobre os serviços afetados e o prazo para restauração;
- Providenciar um novo servidor (caso necessário) para instalação das aplicações e serviços;
- Proceder com a instalação e configuração do Servidor;
- Instalar os serviços necessários para o funcionamento do e-mail institucional;
- Restaurar as funções e serviços;
- Configurar e testar todos os serviços

4.8 - Serviço de acesso à internet (12 horas)

Abrangência:

Abrange toda a infraestrutura de rede, física e lógica no IPMS.

Procedimento:

- Verificar a alimentação dos ativos de rede (Modens, Switches, Roteadores, etc.);
- Identificar se o problema é local ou na operadora do serviço de Internet;
- Caso seja nos serviços da operadora, entrar em contato com a operadora para solicitar reparo;

- Comunicar todas as diretorias sobre os serviços afetados e o prazo para restauração;

5 – ÁREAS AFETADAS

- Superintendência;
- Diretoria Administrativa e Financeira;
- Diretoria de Benefícios e Gestão de Pessoas; e
- Procuradoria Jurídica.

6 – NOTIFICAÇÕES INTERNA (TELEFONE / E-MAIL):

- Superintendência;
- Diretoria Administrativa e Financeira;
- Diretoria de Benefícios e Gestão de Pessoas; e
- Procuradoria Jurídica.

7- NOTIFICAÇÕES EXTERNA (TELEFONE / E-MAIL)

- PMS – Prefeitura Municipal de Suzano;
- CMS – Câmara Municipal de Suzano; e

8 - BACKUPS

- Arquivos em rede
- Servidor de Banco de Dados / WEB
- Servidor de E-mail
- Servidor de Aplicações
- Servidor de Firewall
- Servidores Controladores de Domínio
- Servidor Gerenciador

ANEXO I

Termo de Responsabilidade e Sigilo da Informação

Eu,----------, RG nº ----------, CPF nº ----------, pertencente ao setor, ----------, cargo:----------, sob a matrícula funcional nº ----------,

Nos termos da Política de Segurança da Informação do IPMS – Instituto de Previdência do Município de Suzano declaro que tenho pleno conhecimento de minhas responsabilidades no que concerne ao sigilo que deve ser mantido em relação aos ativos e informações sigilosas das quais tenha tido acesso ou possa vir a acessar ou ter conhecimento, em decorrência das atividades funcionais desempenhadas no exercício do cargo, função ou da prestação de serviço no âmbito do **IPMS**, ou fora do ambiente do mesmo.

Comprometo-me a guardar o sigilo necessário a que sou obrigado, estando ciente das penalidades nos termos da legislação vigente, especialmente dos art. 153 e art. 325 do Código Penal (Decreto-lei nº 2.848, de 07 de dezembro de 1940) e demais legislações constantes do verso deste anexo I, bem como de quaisquer sanções administrativas que poderão advir.

A vigência da obrigação de sigilo, assumida pela minha pessoa por meio deste termo, terá validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa ou entidade, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

Neste Termo, as seguintes expressões serão assim definidas:
Informação Sigilosa significará toda informação, apresentada sob forma escrita, verbal ou por quaisquer outros meios, que possui restrição de acesso público em razão de sua criticidade para a segurança do **IPMS**, da sociedade e do município.

Informação sigilosa inclui, mas não se limita à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, sistemas, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos e questões relativas ao desempenho das atividades laborais.

Suzano,_____ de _____de 2020.

(Assinatura do Usuário)

(ANEXO I – VERSO)

COMPROMISSO LEGAL

CÓDIGO PENAL BRASILEIRO

DIVULGAÇÃO DE SEGREDO - Art. 153 § 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.

INVASÃO DE DISPOSITIVO INFORMÁTICO - Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (Lei 12.737/2012).

FALSIDADE IDEOLÓGICA - 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.

INSERÇÃO DE DADOS FALSOS EM SISTEMA DE INFORMAÇÕES - 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.

MODIFICAÇÃO OU ALTERAÇÃO NÃO AUTORIZADA DE SISTEMA DE INFORMAÇÕES - 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 em dano para a Administração Pública ou para o administrado.

VIOLAÇÃO DE SIGILO FUNCIONAL - 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.

§ 1º Nas mesmas penas deste artigo incorre quem:

I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas à sistema de informações ou banco de dados da Administração Pública, II - se utiliza, indevidamente, do acesso restrito.

§ 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa.

FUNCIONÁRIO PÚBLICO - Art. 327 - Considera-se funcionário público para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública.

§ 1º Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal e quem trabalha para empresa prestadora de serviço contratada ou conveniada para execução de atividade típica da Administração Pública.

§ 2º A pena será aumentada da terça parte quando os autores dos crimes previstos neste capítulo forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público.

ANEXO II

Termo de Uso dos Sistemas de Informação

Eu,_____ RG nº_____,

CPF nº_____, pertencente a(o) setor_____,

Cargo_____, sob a matrícula funcional nº _____.

CONSIDERANDO que o IPMS – Instituto de Previdência do Município de Suzano:

a) Disponibiliza a infraestrutura tecnológica, como ferramenta de trabalho para o pleno desenvolvimento das atividades profissionais;

b) Detém a exclusiva propriedade da infraestrutura tecnológica disponibilizada;

c) Torna explícito que não há expectativa de privacidade sobre os ativos, informações e recursos institucionais, tendo em vista que os mesmos são destinados para fins profissionais;

d) Pode haver prejuízos pela má utilização dos recursos disponibilizados;

DECLARO estar ciente e ter pleno conhecimento:

a) Da Política de Segurança da Informação – PSI apresentada quando do ato da admissão e disponibilizada de inteiro teor no site do IPMS;

b) Da realização do monitoramento dos recursos tecnológicos disponibilizados, indispensável para a manutenção do nível de segurança adequado desta Autarquia Previdenciária;

c) Que o Instituto de Previdência do Município de Suzano- **IPMS** pode realizar auditoria interna sobre os recursos de hardware e software disponibilizados para as atividades profissionais e;

d) Que o descumprimento desta Política de Segurança da Informação está sujeito às sanções previstas no Estatuto dos Servidores Públicos do Município de Suzano, cláusulas contratuais e demais legislações vigentes, sem prejuízo das ações penal, civil e administrativa, previstas em legislação específica, respeitados os princípios constitucionais do contraditório e da ampla defesa.

Suzano, _____de _____de 2022.

(Assinatura do usuário)

ANEXO III

MINUTA DE RESOLUÇÃO

RESOLUÇÃO N.º ____, DE ___DE AGOSTO DE 2022

Aprova a Política de Segurança da Informação no âmbito do IPMS - Instituto de Previdência do Município de Suzano.

O CONSELHO DELIBERATIVO DO IPMS - Instituto de Previdência do Município de Suzano, usando das atribuições que lhe são conferidas por lei, e

CONSIDERANDO a adesão ao Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios Pró-Gestão RPPS;

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 por este RPPS;

CONSIDERANDO que as adoções de procedimentos que garantam a segurança das informações devem ser prioridade constante do IPMS, visando reduzir os riscos de falhas, danos e prejuízos que possam comprometer os objetivos desta Autarquia Previdenciária;

CONSIDERANDO o disposto no Manual do PRÓ-GESTÃO, versão 3.1, aprovado pela Portaria da Secretaria da Previdência nº 20.532, de 08 de setembro de 2020;

CONSIDERANDO a deliberação do Conselho Deliberativo pela aprovação da Política de Segurança da Informação, ocorrida na reunião realizada em ____de _____de 2022.

R E S O L V E: Art. 1º. Fica instituída a Política de Segurança da Informação no âmbito do Instituto de Previdência do Município de Suzano, conforme documento anexo, parte integrante desta Resolução.

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

Suzano, ____de _____ de 2022.

Joel Barros Bittencourt

Superintendente do IPMS