POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE OSASCO
IPMO

SUMÁRIO

1 INTRODUÇÃO

No intuito de fazer com que as organizações desenvolvam mecanismos para lidar com os riscos de segurança da informação, algumas normas foram criadas para orientar no desenvolvimento dos processos de segurança, dentre elas a norma NBR ISO/IEC 27005:2008 que trata sobre gestão de riscos de segurança da informação. Seu 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 política de segurança da informação, guiando-se, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000.

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

Considerar que a informação, sendo um bem da organização é um dos recursos críticos para a realização do negócio e que possui grande valor para a instituição, este bem deve sempre ser adequadamente tratado para garantir a sua conformidade.

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

O presente documento constitui uma declaração formal do IPMO – Instituto de Previdência dos Servidores Públicos do Município de Osasco, 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 Próprio de Previdência Social.

O gerenciamento dos riscos é um dos principais processos 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 IPMO como uma ferramenta de trabalho que serve para ajudá-los em suas rotinas operacionais.

É dever de todos do IPMO – Instituto de Previdência dos Servidores Públicos do Município de Osasco, seguir as normas e as diretrizes estabelecidas nesta Política de Segurança da Informação - P.S.I.

2 NORMAS E DEFINIÇÕES

A ABNT NBR ISO/IEC 27002:2005, define que *"A informação é um ativo essencial para os negócios de uma organização e, conseqüentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. "*

A norma define a segurança da informação como sendo a "preservação da confidencialidade, da integridade e da disponibilidade da informação". Nesse contexto, confidencialidade pode ser definida como a garantia de que as informações serão acessadas apenas pelas pessoas que têm 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 têm autorização para vê-las, quando forem necessárias. Em outras palavras, segurança da informação é a garantia de que as informações da organização serão protegidas de três maneiras: serão acessadas apenas pelas pessoas que devem ter acesso a elas, estarão corretas e completas e estarão disponíveis sempre que seus usuários precisarem, conforme a norma NBR ISO/IEC 27002:2005, ou "Código de prática para a gestão da segurança da informação" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

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. "

Os pilares da segurança da informação abrangem, obrigatoriamente, os seguintes aspectos:

Confidencialidade

A confidencialidade é o pilar que garante que as informações sejam visualizadas apenas por quem tem esse direito. Compreende a proteção de dados transmitidos contra ataques passivos, isto é, contra acessos não autorizados, envolvendo medidas como controle de acesso. A perda da confidencialidade ocorre quando há uma quebra de sigilo de uma determinada informação (exemplo: a senha de um usuário ou administrador de sistema)

permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários;

Integridade

Já a integridade diz respeito ao nível de confiança sobre a veracidade das informações. A informação deve ser entregue corretamente a todos os usuários que precisam recebê-la. Assim, a segurança da informação busca garantir que os dados institucionais estejam íntegros e confiáveis. Trata da garantia contra ataques ativos por meio de alterações ou remoções não autorizadas. A integridade também é um pré-requisito para outros serviços de segurança. Por exemplo, se a integridade de um sistema de controle de acesso a um sistema operacional for violada, também será violada a confidencialidade de seus arquivos. A perda de integridade surge no momento em que uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário da informação;

Disponibilidade

Por fim, a informação precisa estar disponível sempre quando ela for demandada para as pessoas devidamente autorizadas. Se, por exemplo, seu servidor fica sem energia e você não tem um equipamento para mantê-lo ligado, a disponibilidade da sua informação está comprometida.

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 em seu Plano de Ação IPMO-2020, o INSTITUTO DE PREVIDENCIA DO MUNICÍPIO DE OSASCO resolve implantar a Política 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:

Ativo: É tudo aquilo que tenha valor para a organização. [ISO/IEC 13 335- 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 conseqüências. [ABNT ISO/IEC Guia 73:2005].

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

3 OBJETIVO

Foi elaborada a Política de Segurança da Informação para orientar 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 esta Autarquia Previdenciária.

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 IPMO.

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 suas atribuições 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 também é conhecida pela sigla CID forem alcançados. São eles: Confidencialidade, Integridade e Disponibilidade.

4 INSTRUMENTOS NORMATIVOS

A preocupação com segurança da informação na Administração Pública Federal vem sendo demonstrada através de diferentes instrumentos normativos. A 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".

Código Penal (Decreto - Lei de nº 2.848, de 07 de dezembro de 1940), estabelece, no art. 153 e art. 325 que se deve guardar o sigilo necessário da informação. O mesmo código prevê 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.

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 Nacional 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.

No âmbito municipal, a Lei complementar nº 138, de 17 de novembro de 2005, dispõe sobre os deveres e proibições dos servidores públicos da administração municipal, sobre o processo administrativo para apuração e punição de infrações disciplinares e dá outras providências e, no seu Art. 3º define dentre outros, os seguintes deveres dos servidores: observar as normas legais e regulamentares; atender com presteza ao público em geral, prestando às informações requeridas, ressalvadas as protegidas por sigilo e guardar sigilo sobre assunto da repartição.

Em vigor desde o 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 em 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.

Os documentos que compõem a estrutura normativa são divididos em três categorias:

a) Política (nível estratégico): constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o IPMO 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 de segurança da informação;
c) Procedimentos (nível operacional): instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades do IPMO.

4.1. DO ACESSO À INFORMAÇÃO E DA SUA DIVULGAÇÃO

Caberá ser observadas as normas e procedimentos específicos aplicáveis, 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 IPMO quando de sua admissão, bem como através dos meios oficiais de divulgação interna do IPMO e,

também, publicadas no site da instituição, de maneira que seu conteúdo possa ser consultado a qualquer momento.

4.2. APROVAÇÃO E REVISÃO

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

a) Política

Nível de aprovação: Diretoria Executiva

Periodicidade da revisão: anual

b) Normas

Nível de aprovação: Diretoria Executiva

Periodicidade da revisão: semestral

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.

5 DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, são apresentadas as diretrizes da política de segurança da informação do IPMO que constituem os principais pilares do sistema de segurança da informação da instituição, norteando a elaboração das normas e procedimentos.

5.1 CLASSIFICAÇÃO DA INFORMAÇÃO

Define-se como necessária a classificação de toda a informação de propriedade do IPMO, 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 IPMO 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 IPMO na qual não tem interesse em divulgar, mas cujo acesso por parte de indivíduos externos ao IPMO 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 IPMO.

c) Confidencial: É uma informação crítica para o IPMO 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.

5.2 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 IPMO, sendo que:

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

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

Assuntos confidenciais não devem ser expostos publicamente;

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

d) Somente softwares homologados ou de domínio público podem ser utilizados no ambiente computacional do IPMO;

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

f) Todo usuário, para poder acessar dados da rede de computadores do IPMO, deverá possuir um código de acesso atrelado à uma senha previamente cadastrada, sendo este pessoal e intransferível, ficando vedada a utilização de códigos de acesso genéricos ou comunitários;

g) Não é permitido o compartilhamento de pastas nos computadores de servidores da instituição. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

h) Todos os dados considerados como imprescindíveis aos objetivos do IPMO devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo estas cópias serem submetidas a testes periódicos de recuperação;

5.3 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 IPMO detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais do IPMO e reafirmam o seu compromisso com a melhoria contínua desse processo:

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 técnicos 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 diretoria executiva 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.

6 TRANSFERÊNCIAS DE SERVIDORES

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

7 CÓPIAS DE SEGURANÇA – BACKUP

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

O setor de Tecnologia da Informação será responsável pela gestão dos sistemas de backup e deverá realizar rotineiramente testes de restauração das cópias tantos físicos quanto nas nuvens para certificar a integridade dos dados, proceder com pesquisas freqüentes para 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 crescimento dos dados entre outros.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado, 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 um a simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup. As mídias de backups históricos ou especiais deverão ser armazenadas além das nuvens, em instalações seguras, preferencialmente com estrutura de sala-cofre, distante das instalações do IPMO.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios do IPMO, 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.

8 USO DO AMBIENTE WEB (Internet)

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas funções e atividades profissionais vinculadas ao IPMO. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o instituto não devem ser acessados.

Não é permitido instalar programas provenientes da Internet nos microcomputadores do IPMO, sem expressa anuência do setor de Tecnologia da Informação, mesmo os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais devem ser solicitados ao setor de TI.

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 aos negócios do IPMO;
- Que possibilitem a distribuição de informações de nível “Confidencial”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

9 USO DO CORREIO ELETRÔNICO – (E-mail)

O correio eletrônico fornecido pelo IPMO é um instrumento de comunicação interna e externa do instituto. As mensagens devem ser escritas com zelo profissional, não devem comprometer a imagem do IPMO, 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 IPMO;
- Sejam hostis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem e a reputação do IPMO;
- Possam prejudicar a imagem de outras empresas ou órgãos públicos;
- Sejam incoerentes com as políticas do IPMO.

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 IPMO perante seus servidores e a com unidade em geral e que possam causar prejuízos à imagem institucional e financeira ao IPMO.

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. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e.com, ou de quaisquer outros formatos alertados pela área de Tecnologia da Informação. 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, avisos da Microsoft/Symantec, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, fakenews e etc.

10 NECESSIDADES DE SISTEMAS, APLICATIVOS E/O U EQUIPUIPAMENTOS.

O setor de Tecnologia da informação, por força de suas atribuições é responsável pela aplicação da Política de Segurança da Informação do IPMO e pela definição de configuração visando a aquisição e atualização de “software”, “hardware” e dispositivos eletrônicos. A necessidade de novas aquisições de programas ("softwares") ou de equipamentos de informática (hardware) deverá ser discutida com o responsável técnico pelo setor de Tecnologia da informação.

11 USO DE COMPUTADORES E EQUIPAMENTOS DO IPMO

Os servidores que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade do IPMO, 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.

Os cuidados a serem observados:

Ambiente Externo ao IPMO:

- Mantenha o equipamento sempre com você;
- Atenção em 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;
- Redobre a 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 setor de Tecnologia da informação do IPMO.

12 PAPÉIS E RESPONSABILIDADES

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

Todo arquivo em mídia proveniente de entidade externa ao IPMO 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 software de antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Tecnologia da informação, via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Cabe a todos os servidores, estagiários e prestadores de serviços do IPMO 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 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 IPMO, 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 In formação.

12.2. GESTOR DA INFORMAÇÃO

O Gestor da Informação é um servidor de TI, 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 IPMO.

O Gestor da Informação mesmo delegando a sua autoridade sobre o ativo de informação continua sendo dele a responsabilidade final pela sua proteção.

Compete ao Gestor da Informação:

h) 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;

i) Inventariar todos os ativos de informação sob sua responsabilidade;

j) 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;

k) 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;

l) 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;

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

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

12.3. PRESIDÊNCIA

Cabe à Presidência:

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.

12.4. DIRETORIA ADMINISTRATIVA

Cabe à diretoria Administrativa:

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 gestor, 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 gestor;

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 físicas e o controle e o gerenciamento de toda a segurança e vigilância física e dos sistemas de monitoramento CFTV, além de projetos de segurança na prevenção e combate a incêndio nas dependências do IPMO;

12.5. DIRETORIA DE BENEFÍCIOS

Cabe à Diretoria de Benefícios:

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 gestor, 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 gestor; e

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

12.6. DIRETORIA TÉCNICA

Cabe à Diretoria Técnica:

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

b) Assegurar-se de que os servidores e estagiários comprovem, por escrito, estarem cientes da estrutura normativa de segurança e dos documentos que as compõem;

c) Criar mecanismos para informar, antecipadamente aos fatos, alterações no quadro de servidores do IPMO.

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

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

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

g) Comunicar imediatamente ao gestor eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação;

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 1 9/11/18, visando atender a exigência para que deverão permanecer arquivados na unidade gestora do RPPS todo conjunto de informações à sua disposição pelo prazo de 10 (dez) anos;

i) Como compete a esta diretoria o gerenciamento de todas as ações junto à Secretaria de Previdência, se faz necessário 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 In formações Sociais (CNIS); Siprev Gestão; CADPREV WEB e CADPREV LOCAL e GESCON. Tais arquivos estão em diversos formatos para atender as finalidades institucionais desta autarquia previdenciária; e

j) Gerenciar os arquivos bancários quando do processamento da folha de pagamento dos benefícios previdenciários;

12.7. DIRETORIA FINANCEIRA

Cabe à Diretoria 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 Gestor, 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 Gestor;

e) Comunicar imediatamente ao Gestor eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação; e

f) Disponibilizar no site informações pertinentes a Diretoria Financeira.

12.8. ASSESSORIA JURÍDICA

Cabe, adicionalmente, à Assessoria 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 IPMO, em especial a devolução das informações e do banco de dados que povoam o sistema de gestão quando da finalização de contrato com empresas prestadora de serviços;

b) Manter as diretorias do IPMO 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.

13 AUDITORIA

Todo ativo de informação sob responsabilidade do setor de Tecnologia da Informação é passível de auditoria em data e horários determinados pelo Gestor, podendo esta, também, ocorrer sem aviso prévio.

A realização de uma auditoria deverá ser obrigatoriamente aprovada pela Diretoria e, durante a sua execução, deverão ser resguardados os direitos quanto à privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade do IPMO.

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.

14 VIOLAÇÕES E SANÇÕES

14.1 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 IPMO 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 IPMO 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.

14.2. 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 IPMO são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

15 LEGISLAÇÃO APLICÁVEL

Decreto-Lei 2848, de 07 de dezembro de 1940 (Institui o Código Penal);

Lei Complementar 647/1967 – Criação do Instituto de Previdência do Município de Osasco.

Lei Complementar nº 138, de 17 de novembro de 2005 - Dispõe sobre os deveres e proibições dos servidores públicos da administração municipal, sobre o processo administrativo para apuração e punição de infrações disciplinares e dá outras providências.

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 2.84 8, de 7 de dezembro de 1940 - Código Penal e dá outras providências);

Lei Federal nº 12.527, de 1 8 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 - 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 - Aprova a 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);