POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

IPMV

Instituto de Previdência Municipal de Vilhena

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IPMV.

Atualmente, são frequentes as inúmeras ameaças à integridade da informação, seja no âmbito virtual, ou não, nas repartições públicas e privadas.

Assim, surge a necessidade da criação no Instituto de Previdência Municipal de Vilhena – IPMV de uma Política de Segurança da informação que proteja e ao mesmo blinde, qualquer tipo de iniciativa que coloque em risco a segurança e idoneidade desta autarquia. Para tanto, faz-se necessário viabilizar a implementação efetiva de controles de segurança interna no IPMV.

Este processo deve considerar o incentivo à definição de políticas compreendendo o gerenciamento de riscos, baseando-se em análises quantitativa e qualitativa, análises de custo versus benefício e programas de conscientização de todos os agentes envolvidos diretamente na plena funcionabilidade do Instituto de Previdência.

A gestão da segurança da informação inicia-se com a definição de políticas, procedimentos. guias e padrões Essas políticas devem estar colocadas no mais alto nível de documentação da segurança da informação . Nos demais nlveis, encontram-se os níveis complementares, não significando que as politicas sejam mais importantes que os demais. O fato e que as políticas devem ser definidas em primeiro plano por razões estratégicas, enquanto os dem is níveis/documentos seguem as políticas, de forma consequente, como elementos táticos e operacionais.

Portanto, as políticas, como documento base, devem conter o comprometimento da hierarquia administrativa do IPMV, explicitando de forma clara e abrangente, a importância da segurança da informação, bem como dos recursos computacionais, para a missão institucional. Constitui assim, uma declaração que fundamenta a segurança da informação e comunicações na totalidade da instituição. Deve-se, ainda, conter as necessárias autorizações para a definição dos procedimentos, guias e padrões de segurança da informação determinados.

Distinguem-se as políticas de alertas e as políticas informativas. As politicas de alerta não são mandatárias em si mesmas, mas são fortemente incentivadas que, normalmente, incluirão as consequências da não conformidade com as mesmas. As políticas informativas são as que simplesmente informam aos usuários sobre um determinado ambiente. Não implicam necessariamente em requisitos específicos e seu público-alvo pode ser somente determinado ou, inclusive, parceiros externos ou terceiros. Como tem caráter genérico, podem ser distribuídas para parceiros externos ou terceiros que acessam as redes de informação da instituição (Site e Portal), sem que isso acarrete o comprometimento da informação interna.

Os regulamentos de segurança são aqueles que a instituição deve implementar em conformidade com legislação em vigor, garantindo aderência à padrões e procedimentos básicos de setores específicos. Os padrões especificam o uso uniforme de determinadas tecnologias. Normalmente são mandatórios e implementados através de toda a instituição, objetivando maiores benefícios gerais. Os fundamentos ou princípios são semelhantes aos padrões, com pequena diferença. Uma vez que um conjunto consistente de fundamentos seja definido, a arquitetura de segurança de uma instituição pode ser planejada e os

padrões podem ser definidos. Os fundamentos devem levar em conta as diferenças entre as plataformas existentes, para garantir que a segurança seja implementada uniformemente em toda a 1nstituição. Quando adotados, são mandatórios. Os guias consideram a natureza distinta de cada sistema de informação e são similares aos padrões, embora pouco mais flexíveis. Eles se referem, normalmente, a metodologias para os sistemas de segurança, contendo apenas ações recomendadas e não mandatórias. Podem e devem ser usados para especificar a maneira pela qual os padrões devem ser desenvolvidos, como quando indicam a conformidade com determinados princípios da segurança da informação. Os procedimentos contêm os passos detalhados que devem ser seguidos para a execução de tarefas específicas. São ações detalhadas que devem ser seguidas. São considerados como inseridos no mais baixo nivel em uma cadeia de políticas. Assim, seu propósito é fornecer os passos detalhados para a implementação das políticas, padrões e guias, também chamados de boas práticas. As responsabilidades devem estar relacionadas com o perfil de cada um que esteja envolvido no processo. Estes são exemplos:

- **Diretores, Controladores e Gerentes** – Estão envolvidos com toda a responsabilidade da segurança da informação. Podem delegar a função de segurança, mas são vistos como o principal foco quando são considerados os eventos relacionados com a segurança;

- **Profissionais de segurança dos sistemas de informação** – Recebem a responsabilidade pela implementação e manutenção da segurança. Estão sob sua responsabilidade o projeto, a implementação, o gerenciamento e a revisão das políticas, padrões, guias e procedimentos;

- **Possuidores de dados** – São responsáveis pela classificação da informação. Podem também ser responsabilizados pela exatidão e integridade das informações;

- **Usuários** - Devem aderir às determinações definidas pelos

profissionais de segurança da informação.

A segurança compreende, assim, a proteção das informações em relação aos diversos tipos de ameaças para:

- garantir a continuidade das ações junto ao segurado e que atenda o controle interno do RPPS;
- minimizar todo e qualquer risco ao segurado e às atividades do IPMV;
- maximizar a garantia do bom atendimento e a seguridade do servidor;
- ampliar o retorno sobre os investimentos das contribuições dos servidores segurados.

Assim estabelecido, este documento descreve as Pollticas de Segurança da Informação no âmbito do Instituto de Previdência Municipal de Vilhena, estando em vigor após sua aprovação. Ele deve ser publicado e comunicado para todos os servidores da Instituição e para as partes externas relevantes.

Este documento deve sofrer revisões periódicas, devendo manter-se alinhado com a legislação pertinente, com as normas e padronizações brasileiras e com os objetivos essenciais do RPPS.

As garantias que devem ser conferidas às informações, aos sistemas e aos ativos (qualquer coisa que tenha valor para a instituição) como:

- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- Integridade: propriedade de salvaguarda da exatidão e completeza de ativos. A informação não pode ser alterada ou destruída sem a autorização adequada do responsável pela autarquia;

- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;

- Autenticidade: propriedade que assegura que a informação é realmente da fonte que se declara ser;

- Não repúdio: propriedade que assegura que nem o emissor nem o receptor de uma informação possam negar o fato. a autoria e a responsabilidade.

Quanto à confidencialidade, deve-se garantir: Que o acesso aos dados e informações fiquem restritos às entidades devidamente autorizadas.

a) A proteção em todas as fases: armazenamento, transmissão e processamento. A ausência dessas garantias pode resultar na quebra do sigilo.

Quanto à integridade deve-se garantir:

a) A alteração de dados e informações apenas por usuários devidamente autorizados.

b) o armazenamento , processamento e transmissão dos dados e informações de forma a preservar a exatidão e completeza dos registros.A ausência dessas garantias pode gerar perda ou falsificação de dados/informações.

Quanto à disponibilidade, deve-se garantir o acesso aos usuários autorizados sempre que necessário. A ausência dessa garantia pode gerar situações de negação de serviço, prejuízo em situações de urgência e danos à imagem da instituição.

Quanto à autenticidade, esta implica na certeza de que os dados/informações provêm das fontes anunciadas.

Quanto ao não-repúdio ou irretratabilídade, estes implicam na impossibilidade de negar a autoria, a responsabilização. A ausência dessa garantia pode resultar no uso de informações falsas.

Levando em conta a grande quantidade e variedade das ameaças à segurança da informação, evidencia-se, entre outras, a necessidade de:

- normas específicas para a segurança física de instalações;
- de acesso de colaboradores, usuários e visitantes;
- de criação e manutenção de contas e senhas;
- de instalação e configuração de aplicações;
- de uso de redes, Internet, correio eletrônico e relativas a privacidade, etc.

Todas estas necessidades deverão ser englobadas em uma política de segurança da informação e, cujas diretrizes são estabelecidas por este documento.

Observando o acima estabelecido, o Artigo 2 do Decreto Presidencial nº 3.505 de 13 de Junho de 2000, define: Segurança da Informação é proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, as áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. Ainda, de acordo com o Decreto 3.505/2000, devem ser objetivos de uma Política de Segurança de Informação:

a- Dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o nãorepúdio e a disponibilidade dos dados e das

informações tratadas, classificadas e sensíveis;

b- Eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação.

c- Promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação.

d- Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação.

e- Promover as ações necessárias à implementação e manutenção da segurança da informação.

f- Promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação.

g- Promover a capacitação industrial do País com vistas à sua autonomia

no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação.

h- Assegurar a interoperabilidade entre os sistemas de segurança da informação. Este documento trata da segurança da informação de forma ampla, incluindo todas as formas de armazenamento. eletrônicas ou não.

Este documento deve servir de base para resoluções funcionais e administrativas que implementem as políticas nele contidas, inclusive as regras de uso geral e as Normativas Complementares.

Em síntese, este documento institui diretrizes e princípios de Segurança da Informação (PSI) no âmbito do Instituto de Previdência Municipal de Vilhena, com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade (CIDA) das informações que suportam os objetivos estratégicos deste Instituto. Esta PSI e suas Normativas Complementares aplicam-se a todos setores vinculados ao IPMV, bem como aos seus servidores, conselheiros. prestadores de serviço, colaboradores, estagiários/bolsistas, consultores externos e a quem de alguma forma tenha acesso aos ativos deste Instituto.

ATENÇÃO:

USO DE ANTIVÍRUS

Todo arquivo em mídia proveniente de entidade externa ao IPMV deve ser verificado por programa antivírus. Todo arquivo recebido /obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão ou outra ação disciplinar e/ou processo civil ou criminal.

Vilhena, 24 de novembro de 2020

Helena Fernandes Rosa dos R. Almeida
Presidente do IPMV
Portaria nº. 001/2018/CAF/IPMV

Elaborado por:
José Ribamar Araújo de Sousa
Gerente de Mídia, Informática e Ouvidoria