Política de Segurança da Informação

IPMU/211/2020

Sumário

1. Introdução

Um programa de conscientização sobre **Segurança da Informação** tem como objetivo principal influenciar os servidores a mudarem seus hábitos, bem como criar a consciência de que todos são corresponsáveis pela segurança da informação.

Esse processo de conscientização deve ser contínuo, para manter os usuários alertas e para prepará-los para os novos riscos e ameaças que surgem a cada dia.

Os riscos à vulnerabilidade nos sistemas informativos vêm crescendo em uma velocidade proporcional e muitas vezes superior ao avanço tecnológico, dessa forma, faz-se necessário programar uma Política de Segurança da Informação.

Essa Política de Segurança da Informação do **Instituto de Previdência Municipal de Ubatuba – IPMU** defini normas, diretrizes e procedimentos que visem minimizar os riscos com perdas e violações de qualquer um de seus bens, restringe-se à defesa das informações, sistemas e demais periféricos informatizados do IPMU.

2. Política de Segurança da Informação

A Política de Segurança da Informação é necessária para garantir a proteção das informações do IPMU, assegurando que nenhuma informação seja alterada ou utilizada indevidamente.

A Política de Segurança da Informação tem como objetivo estruturar, elaborar, administrar e manter uma política de segurança da informação, por intermédio da utilização dos ativos e recursos de informática do IPMU e pelo desenvolvimento do comportamento ético e profissional de seus usuários.

A violação desta política de segurança é qualquer ato que:

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

3. Objetivos

O presente documento constitui uma declaração formal do IPMU acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua custódia, devendo ser observado por todos os seus servidores, segurados, estagiários e prestadores de serviços.

Seu propósito é formalizar o direcionamento estratégico acerca da gestão de segurança da informação no IPMU, estabelecendo as diretrizes a serem seguidas para implantação e manutenção de segurança.

O objetivo da Política de Segurança da Informação é estabelecer diretrizes que permitam aos usuários

do IPMU seguirem padrões de comportamento relacionados à segurança, adequados às necessidades da entidade, bem como a implementação de controle e processos para seus atendimentos.

Todos os mecanismos utilizados para a segurança da informação devem ser mantidos para preservar a continuidade das funções institucionais. Por mais eficiente que sejam os softwares e a segurança de todo um sistema, nunca estaremos totalmente a salvo de ameaças virtuais, a preocupação e cuidado com a Segurança das Informações tem que ser uma constante no dia a dia dos participantes do IPMU.

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou seus dispositivos periféricos. É um requisito essencial para o funcionamento confiável dos sistemas de informação. A crescente dependência do uso da informática em todos os setores da atividade humana, aliada à facilidade de acesso aos sistemas de informação através da Internet, trouxe à tona muitos problemas e desafios para a operação segura desses sistemas.

O gerenciamento dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

É de competência da Diretoria Executiva do IPMU promover a cultura de segurança da informação e comunicação e o acompanhamento de investigações e avaliações de danos decorrentes de quebras de segurança.

Os objetivos genéricos da Política de Segurança da Informação para o Instituto de Previdência Municipal de Ubatuba são:

a) Assegurar que os Princípios da Segurança da Informação sejam seguidos.
b) Atestar e assegurar segurança com contato externo em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;
c) Difundir a conscientização a todos servidores visando a compreensão e o manuseio de situações relacionadas à segurança da informação;
d) Impulsionar ações necessárias à implementação e manutenção da segurança da informação;

4. Alçada

A Política de Segurança da Informação do IPMU se destina aos servidores efetivos, cedidos e conselheiros. Também se estende a empresa terceirizada que prestam serviços de manutenção das máquinas, rede do IPMU, de sistemas informatizados e empresas que manipulam informações de identificação pessoal como consultoria atuarial, bancos e etc.

Quando necessário será contratada empresa especializada para estudo das vulnerabilidades, e se existirem serão realizadas ações para saná-las.

5. Responsável

O Diretor Financeiro do IPMU é o responsável pela Gestão da Segurança da Informação.

6. Princípios da Segurança da Informação

Os Princípios da Segurança da Informação são as bases para as ações ou linhas de conduta de segurança que atuam como guia para a implementação e a gestão da Segurança da Informação.

a) A Confidencialidade garante que a informação somente seja acessada por pessoas autorizadas. A principal forma de garantir a confidencialidade é por meio do controle de acesso, ou seja, autenticação por senha, isso já garante que o conteúdo protegido, somente será acessado por pessoas autorizadas. Ela se dá justamente quando se impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem ou documento. Refere-se à proteção da informação contra divulgação não permitida. A perda da confidencialidade se dá quando alguém não autorizado obtém acesso a recursos e informações.

b) A Disponibilidade garante que a informação estará disponível para acesso no momento desejado. Diz a respeito à eficácia do sistema, ao correto funcionamento da rede para que quando a informação for necessária ela poderá ser acessada. A perda de disponibilidade se dá quando se tenta acessar uma informação e não se consegue o acesso esperado.

c) A Integridade garante que o conteúdo da mensagem não foi alterado ou violado indevidamente. Ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade. Há perda de integridade quando a informação é alterada indevidamente ou quando não se pode garantir que a informação é a mais atualizada.

d) A Autenticidade garante a identidade de quem está enviando a informação, ou seja, gera o não-repúdio, que se dá quando há garantia de que o emissor não poderá se esquivar da autoria da mensagem (Irretratabilidade). É através da autenticidade que se garante que a informação é proveniente da fonte anunciada, ou seja, não sofreu nenhuma alteração durante o processo.

7. Classificação da Informação

O IPMU é o proprietário das informações custodiadas pela Diretoria Executiva e administradas pelo Gestor de Segurança da Informação. As Informações custodiadas pela Diretoria Executiva utilizam os seguintes níveis de Classificação:

a) Confidencial: Dados de autenticação como: senhas, PINs, chaves privadas de criptografia, informações sobre: o Patrimônio do IPMU, Segurados e Servidores do IPMU; qualquer Informação que o Gestor da Segurança do IPMU determinar ter o potencial de ocasionar prejuízos ao erário público, ou que viole dados pessoais dos envolvidos.

b) Interna: Informação que é normalmente compartilhada dentro do Instituto de Previdência Municipal de Ubatuba, não é classificada como RESTRITA ou CONFIDENCIAL.

c) Pública: Informação que é livremente disponível fora do Instituto de Previdência Municipal de Ubatuba, corroborando com o Princípio da Transparência das Entidades Públicas e da Lei de acesso à informação.

8. Definições Básicas

Em toda Política de Segurança da Informação faz-se necessário ter uma ideia clara daquilo que se quer defender, contra quem queremos defender e quais os entraves que essa política oferece para funcionamento normal do sistema.

A Política de Segurança da Informação do IPMU define as normas e procedimentos que melhor atendam ao propósito, minimizando os riscos com perdas e violações de qualquer um dos seus bens.

A Política de Segurança da Informação não define procedimentos específicos de manipulação e proteção da informação, mas atribuem direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação.

A implantação da Política de Segurança da Informação baseia-se na aplicação de regras que limitam o acesso às informações e recursos com base na comparação do seu nível de autorização relativo a essa informação ou recurso, na designação da sensibilidade da informação ou recurso e na forma de acesso empregada.

Esta Política de Segurança da Informação norteará a implementação de medidas de proteção de dados que deverão ser aplicadas a toda e qualquer informação, com vistas ao resguardo da imagem e das finalidades institucionais do IPMU. As normativas devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos para que a informação tenha o grau de confidencialidade, integridade e segurança exigidos.

A Política de Segurança da Informação foi organizada com o objetivo de atender aos seguintes critérios de segurança:

a) Estrutura física: Relacionada à segurança dos ativos computacionais, instalações prediais e documentos em meio físico abrangendo, também, o controle de acesso de pessoas às instalações do IPMU;
b) Estrutura lógica: Relacionada a toda e qualquer informação em meio digital, seja em equipamentos, tráfego de informações pela rede, por correio eletrônico ou armazenado em estações de trabalho dos usuários;
c) Recursos humanos: Relacionada à educação e conscientização de cada usuário sobre a responsabilidade para com a segurança da informação, por meio de sugestões e ações educativas.

Para os fins dessa Política de Segurança da Informação, considera-se:

a) Acesso lógico: acesso a rede de computadores, sistemas e estações de trabalho por meio de autenticação;
b) Acesso remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
c) Agente responsável: servidor público ocupante de cargo efetivo ou em comissão no IPMU, direta ou indiretamente incumbido de chefiar e gerenciar os funcionários que sejam usuários das informações no âmbito da autarquia;
d) Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

e) Análise/avaliação de riscos: processo completo de análise e avaliação de riscos;
f) Ativo: qualquer bem que o IPMU possua e que tenha valor para a organização;
g) Ativo da informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles tem acesso;
h) Ativo sigiloso: qualquer bem que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos ao IPMU e seus segurados;
i) Banco de dados: é um sistema de armazenamento de dados que tem como objetivo organizar e guardar as informações;
j) Auditoria: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir ou eliminar fraudes, erros, práticas ineficientes ou ineficazes;
k) Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
l) Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;
m) Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;
n) Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;
o) Download: baixar copiar arquivos de um servidor/site na internet para um computador pessoal;
p) Informação Pública: é toda informação que pode ser acessada por servidores do IPMU, usuários, fornecedores, prestadores de serviços e público em geral;
q) Informação Interna: é toda informação que pode só pode ser acessada por servidores do IPMU. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da entidade;
r) Informação Confidencial: é toda informação que pode ser acessada por servidores do IPMU e parceiros do IPMU. A divulgação não autorizada dessas informações pode causar impacto aos serviços e aos negócios dos parceiros;
s) Informação Restrita: é toda informação que pode ser acessada por servidores do IPMU expressamente indicado pelo responsável da área. A divulgação não autorizada dessas informações pode causar sérios danos ao IPMU ou comprometer a estratégia da entidade.
t) Internet: rede mundial de computadores;
u) Logon: Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;
v) Protocolo: convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;
w) Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e as comunicações;
x) Servidor de Rede: recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
y) Software: são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;
z) Site: conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

aa) Usuários: devem aderir às determinações definidas pelos profissionais de segurança da informação.

9. Orientações sobre a Política de Segurança da Informação

Esta Política define os rumos para a Segurança da Informação, visando preservar os princípios da segurança das informações sob a gestão do IPMU. Descreve a conduta a ser considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente, em consonância com o Código de Ética do Instituto:

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos usuários quando na utilização dos recursos de processamento da informação do IPMU:

a) A identificação do usuário por meio de senha é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela;
b) Ao Gestor do Sistema de Informações se reserva o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet e o uso do Correio Eletrônico;
c) É vedado o manuseio de pessoas não autorizadas da rede do IPMU;
d) O acesso à internet é feito com tecnologia fornecida por operadora especializada;
e) O acesso de visitantes à Área Técnica ou às áreas internas do IPMU deverá ser supervisionado pela Diretoria Executiva do IPMU;
f) O cumprimento da Política de Segurança, pelos usuários, poderá ser auditado periodicamente pelo CONTROLE INTERNO do IPMU;
g) O IPMU possui uma rede integrada de computadores com servidores e um microcomputador para cada usuário;
h) Os acessos aos diretórios dos servidores e aos sistemas corporativos possuem senha de entrada com registro de log e sistema de backup automático;
i) Os usuários deverão proteger o acesso a seus computadores através de tela de bloqueio a ser liberada mediante senha, quando os mesmos não estiverem em uso.

Toda informação que é acessada, transmitida, recebida ou produzida com recursos tecnológicos oferecidos pelo IPMU, está sujeita a monitoramento que podem envolver inspeção física de equipamentos e registro de acessos à internet.

A internet disponibilizada aos servidores não deve ser utilizada para a exposição de conteúdo íntimo ou de vida privada, tampouco vexatório, lembrando que o ambiente está sujeito a monitoramento.

Na hipótese do uso indevido dos recursos disponibilizados, o usuário ficará ciente de que o conteúdo poderá ser retirado dos equipamentos independentemente de aviso prévio.

Como os equipamentos, tecnologias e serviços fornecidos para o acesso à internet e ao e-mail são propriedades do IPMU, ele tem o direito de monitorar, inspecionar e bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, que estejam em disco local na estação ou em áreas privadas da rede.

O uso indevido de qualquer recurso para atividades ilícitas ou que cause danos a terceiros será considerado violação às regras internas e terá as consequências previstas na legislação civil e criminal. Nesses casos, o IPMU cooperará ativamente com as autoridades competentes.

REGRAS GERAIS

a) A utilização de equipamentos de informática particulares na rede, só será liberada mediante autorização e vistoria no equipamento para saber se o mesmo atende aos requisitos mínimos de segurança exigidos;
b) É proibida a instalação ou remoção de softwares que não forem devidamente acompanhados pelo Diretor Financeiro e/ou responsável pelo setor de informática;
c) É proibida a manutenção de equipamentos de informática particulares dentro das dependências do IPMU; e
d) Não são permitidas alterações das configurações da rede de inicialização das máquinas bem como as modificações que possam trazer algum problema futuro;
e) O uso e manuseio, alteração, reposição de equipamento defeituoso será executado unicamente pelo responsável pelo setor da informática;
f) Quando ocorrer a nomeação/contratação/exoneração/ demissão do servidor, a Diretoria Administrativa deverá providenciar a ativação ou desativação dos acessos do usuário a qualquer recurso da rede do IPMU;
g) Todo arquivo em mídia proveniente de entidade externa ao IPMU deve ser verificado por programas antivírus. Todo arquivo recebido/obtido através do ambiente da internet deve ser verificado por programa antivírus. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

10. Do acesso à internet e Correio Eletrônico

O acesso à rede mundial de computadores e seus serviços utilizando os recursos do IPMU ficam sujeito as seguintes regras abaixo:

- Caso necessário, haverá bloqueios dos acessos que comprometam o bom desempenho da rede ou perturbem o andamento dos trabalhos, domínios que comprometam o uso de banda e ofereçam riscos à segurança da rede;
- Ficam estritamente proibidos os sites que contenham material pornográfico, pedofilia, material que faça apologia as atividades criminosas e demais conteúdos semelhantes que afronte os bons costumes; e
- O acesso à Internet é proibido a pessoas que não pertençam ao quadro de servidores do IPMU, salvo os autorizados.

O correio eletrônico fornecido pelo IPMU é um instrumento de comunicação interna e externa para a realização do negócio do IPMU. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do IPMU, não podem ser contrárias à legislação vigente e nem aos princípios éticos do IPMU. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

Os servidores poderão utilizar o correio eletrônico desde que essa ferramenta não seja utilizada de modo indevido, ilegal ou antiético.

Os servidores NÃO poderão utilizar o serviço de correio eletrônico para:

a) Difamar, ofender, perseguir ou ameaçar ou de qualquer outra forma violar os direitos de terceiros;
b) Enviar arquivos que contenham vírus, arquivos corrompidos ou quaisquer outros softwares ou programas semelhantes que possam danificar a operação de outros computadores ou a propriedade de terceiros;
c) Modificar arquivos ou assumir, sem autorização, a identidade de outro usuário;
d) O Correio Eletrônico do IPMU deve ser utilizado sempre baseado no bom senso e de acordo com os preceitos legais;
e) Prejudicar intencionalmente usuários da internet, através do envio de programas e de acesso não autorizados a computadores, ou de alterações de arquivos de programas;
f) Utilizar o serviço de correio eletrônico de qualquer forma a participar em atividades de pesquisa comercial correntes, lixo eletrônico ou quaisquer mensagens periódicas ou não solicitadas (SPAM);
g) Utilizar-se do serviço de propriedade do IPMU, desvirtuando sua finalidade com o intuito de cometer fraude;
h) Vedado o acesso não autorizado às caixas postais de terceiros e as tentativas de acesso deverão ser registradas em log, inclusive acessos feitos indevidamente por administradores de sistemas;
i) Vedado o envio de informações críticas para pessoas ou organizações não autorizadas observando quando for o caso, orientações para o tratamento de informações classificadas; e
j) Vedado o envio de material obsceno, ilegal ou não ético, envio de propaganda, mensagem do tipo corrente e de entretenimento, relacionadas com nacionalidade, raça, orientação sexual, religiosa, convicção política ou qualquer outro assunto que possa vir a difamar o usuário como cidadão e que não tenha relação com o serviço a que o usuário é destinado no ambiente do TI do IPMU.

ACESSO À INTERNET

a) As contas podem ser monitoradas pela Diretoria responsável, com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.
b) É obrigatório armazenar os arquivos inerentes ao IPMU no servidor de arquivos para garantir a cópia de segurança do mesmo;
c) É proibido o uso do servidor de arquivos para armazenar informações de cunho pessoal;
d) Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento da estrutura tecnológica;
e) Não é permitido instalar programas provenientes da Internet nos microcomputadores do IPMU, sem expressa anuência do gestor do sistema de informação, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.
f) O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais no IPMU. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o instituto não devem ser acessados.

g) O servidor do IPMU deve ser utilizado seguindo as seguintes normas:
h) O usuário deve fazer manutenções periódicas no diretório pessoal, evitando acumulo de arquivos desnecessários;
i) Os arquivos gravados em diretórios temporários e públicos do servidor e das estações de trabalho podem ser acessados por todos os usuários que utilizarem a rede, portanto não se pode garantir sua integridade e disponibilidade;
j) Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar; e
k) Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.
l) São de responsabilidade do usuário as informações em seu diretório pessoal, sendo que o mesmo deve evitar o acumulo de arquivos desnecessários.

11. Utilização do Sistema de Telefonia

Esse tópico defini as normas de utilização do sistema de Telefonia que engloba ramais e linhas diretas.

a) O uso indevido do telefone para ligações particulares ou abusivas é passível de procedimento administrativo, bem como restituição financeira aos cofres do IPMU;
b) Os sistemas de telefonia passam a ser 100% passíveis de monitoramento, de maneira aleatória ou definitiva, dependendo da necessidade;
c) Usar o telefone o mínimo necessário. Procure usar o mensageiro eletrônico do IPMU bem como o correio eletrônico;
d) Zelar pelo bom funcionamento do sistema procurando não danificar equipamentos e cabeamento. Caso o usuário note algum problema, comunicar a chefia imediata.

12. Dispositivos Móveis

Entende-se por "dispositivo móvel" qualquer equipamento eletrônico com atribuições de mobilidade de propriedade do IPMU, ou aprovado e permitido por sua Gerência de Sistemas, como: notebooks, smartphones, pendrives, HD externos e/ou quaisquer tipo de dispositivo de armazenamento físico.

O IPMU, na qualidade de proprietário dos equipamentos fornecidos, através da Diretoria Executiva, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O servidor assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no IPMU, mesmo depois de terminado o vínculo mantido com o Instituto.
Todo servidor deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade do IPMU e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição. Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização do Gestor da Segurança da Informação e sem a condução, auxílio ou presença de um técnico responsável designado pelo Gestor.

O Servidor deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico designado pelo Gestor do Sistema de Informações do IPMU.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

O servidor que desempenhe suas funções no todo ou em parte fora das dependências do IPMU é permitido o uso de rede banda larga de locais conhecidos pelo como: sua casa (home-office, hotéis, locais de eventos de capacitação e fornecedores).

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo IPMU, notificar imediatamente o Gestor do Sistema. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O servidor deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao Instituto de Previdência Municipal de Ubatuba.

O Servidor que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do IPMU deverá submeter previamente tais equipamentos ao processo de autorização do Gestor do Sistema de Informações do IPMU.

13. Usuários

Cada usuário deverá utilizar uma estação de trabalho determinada, com códigos internos que permitam a sua identificação na rede interna.

Somente poderão ser mantidos na estação de trabalho arquivos supérfluos ou pessoais, sendo que todos os dados referentes ao IPMU deverão ser mantidos no servidor, com sistema de backup diário.

É proibida a instalação de softwares ou hardwares sem autorização do Gestor da Segurança da Informação, bem como a utilização ou armazenagem de MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria.

O programa que protege o computador de "malwares", também denominado antí-vírus, deverá estar sempre atualizado.

Os usuários deverão reportar as atitudes suspeitas em sua estação de trabalho para o Gestor de Segurança da Informação, o qual acionará um técnico, de forma que possíveis vírus sejam identificados no menor espaço de tempo possível.

Todas as ações executadas serão de inteira responsabilidade do usuário.

a) Antes de ausentar-se do local de trabalho, o usuário deverá fechar todos os programas em uso, efetuar o logoff da rede ou fazer o bloqueio do computador, evitando o uso dos recursos de TI por pessoas não autorizadas.
b) É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos servidores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do IPMU.
c) No caso das informações consideradas de fundamental importância para a continuidade dos negócios do IPMU, o Setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.
d) O acesso a quaisquer outros serviços ou sistemas providos pelo IPMU ou por outros órgãos da administração direta deverá ser solicitado à chefia imediata;
e) O usuário é o único responsável pelo uso da sua identificação (login e senha), quaisquer ações praticadas durante a utilização desta identificação será de sua inteira responsabilidade;
f) O usuário não deverá compartilhar sua senha com outros usuários. Caso, o usuário perceba que outro usuário possa estar utilizando seu login de acesso, o mesmo deverá informar imediatamente à chefia imediata, para efetuar a troca da senha e auditoria das atividades executadas com este login e,
g) Todo servidor do IPMU terá direito a uma senha de acesso a rede corporativa e uma conta de e-mail do IPMU.

14. Recomendações para o uso seguro dos recursos de TI

O envolvimento do usuário é importante no processo da segurança dos recursos de TI, pois é na adequada utilização destes recursos, como instrumento de trabalho, que se inicia a formação de uma cultura de segurança da informação. Desta forma, recomenda-se aos usuários a adoção das seguintes práticas:

a) Certificar que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação;
b) Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;
c) Não abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus.

15. Recomendações sobre atividades permitidas

a) Utilizar programas de computador licenciados para uso pelo IPMU, de acordo com as disposições específicas previstas em contrato.
b) A instalação de programas e sistemas homologados é atribuição da administração de sistemas e TI;
c) Criar, transmitir, distribuir, disponibilizar e armazenar documentos, desde que respeite às leis e regulamentações, notadamente aquelas referentes aos crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade;
d) Fazer cópia de documentos e ou programas de computador a fim de salvaguardá-los, respeitada a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos do IPMU, exigindo-se autorização para aqueles protegidos pelos direitos autorais, inclusive músicas, textos, documentos digitalizados e qualquer conteúdo encontrado em revistas, livros ou quaisquer outras fontes protegidas por direitos autorais.

16. 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, segurado, estagiário ou prestador de serviços do IPMU, sendo que:

a) As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;
b) Assuntos confidenciais não devem ser expostos publicamente, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade do IPMU;
c) Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;
d) 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;
e) Os servidores devem assumir uma postura proativa no que diz respeito à proteção das informações do IPMU e devem estar atentos a ameaças externas,
f) Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
g) Somente softwares homologados podem ser utilizados no ambiente computacional do IPMU;
h) Todos os dados considerados como imprescindíveis aos objetivos do IPMU devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos a testes periódicos de recuperação.

17. Privacidade da Informação

a) Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e que são manipuladas ou armazenadas nos diversos meios, os quais o IPMU detém total controle administrativo, físico, lógico e legal.
b) As diretivas abaixo refletem os valores institucionais do IPMU e reafirmam o seu compromisso com a melhoria contínua desse processo:

c) As informações são coletadas de forma ética e legal, com o conhecimento do segurado, para propósitos específicos e devidamente informados;
d) As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
e) 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;
f) As informações somente são fornecidas a terceiros, mediante autorização prévia da diretoria executiva ou para o atendimento de exigência legal ou regulamentar;
g) As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

18. Recomendações sobre atividades NÃO permitidas

a) Alterar registro de evento dos sistemas de TI;
b) Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;
c) Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente.
d) Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;
e) Introduzir códigos maliciosos nos sistemas de TI;
f) Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;
g) Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;
h) Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;
i) Violar medida de segurança ou de autenticação, sem autorização de autoridade competente.

19. Recomendação para a Utilização de Aplicações Corporativas e Software de Terceiros

a) A classificação ou reclassificação da informação deve seguir as orientações da legislação vigente;
b) As configurações e atribuição de parâmetros em todos os computadores conectados à rede do IPMU devem estar de acordo com as políticas e normas de gerenciamento internas.
c) Deve ser vedado aos usuários o acesso, modificação, a remoção ou a cópia de arquivos que pertençam a outro usuário sem a permissão expressa do mesmo;
d) Deve ser vedado aos usuários que fazem uso de sistemas de informação o acesso não autorizado a qualquer outro sistema que não possua permissão de uso, assim como a danificação, a alteração a interrupção da operação de qualquer sistema do ambiente de TI. Da mesma maneira deve ser vedado aos usuários a obtenção indevida de senhas de acesso, chaves criptográficas ou qualquer outro mecanismo de controle de acesso que possa possibilitar o

acesso não autorizado a recursos informacionais;

e) É vedada a utilização de dispositivos de armazenamento de origem externa, nas estações de trabalho do IPMU ou nos servidores de rede antes de serem submetidos a um software antivírus.
f) É vedada a utilização de software da Internet ou de qualquer outro sistema externo ao IPMU. Esta proibição é necessária porque tal software pode conter vírus que podem comprometer o ambiente de TI.
g) O usuário do ambiente de TI do IPMU não deve executar ou desenvolver qualquer tipo de programa ou processo externo às suas atividades.
h) Os usuários não devem desenvolver, gerar, compilar, copiar, coletar, propagar, executar ou tentar introduzir qualquer código projetado para se auto-replicar, danificar ou de outra maneira obstruir o acesso ou afetar o desempenho de qualquer computador, rede ou sistema de TI do IPMU.
i) Quando do desligamento do usuário, seus arquivos armazenados em estação de trabalho ou em qualquer servidor de rede do IPMU e, também, seus documentos em papel devem ser imediatamente revisados pela chefia imediata para determinar quem tornar-se-á curador das informações relacionadas, assim como nos casos devidos, identificar o método mais adequado para a eliminação das mesmas, levando-se em conta as orientações sobre a eliminação de informações classificadas contidas na legislação vigente.
j) Todas as atividades dos usuários que podem afetar os sistemas de informação do IPMU devem ser possíveis de reconstituição a partir dos logs de maneira a evitar ou dissuadir o comportamento incorreto. Estes procedimentos devem contar inclusive com mecanismos de responsabilização claros e amplamente divulgados nos meios de comunicação internos.
k) Todos os softwares e arquivos transferidos de fontes que não sejam do próprio IPMU via Internet (ou qualquer outra rede Pública) devem ser examinados com o software de detecção de vírus utilizado pelo IPMU. Este exame deve acontecer antes que o seja executado ou aberto por um outro programa, como por exemplo, por um processador de texto e também, antes e depois que o material tenha sido descompactado.

20. Responsabilidades

É de responsabilidade dos próprios servidores do IPMU salvar cópias de segurança, de textos, planilhas, mensagens eletrônicas e outros arquivos ou documentos, desenvolvidos pelos mesmos em suas estações de trabalho, além de salvar em suas pastas pessoais no Servidor do Instituto.

Todo arquivo em mídia proveniente de entidade externa ao IPMU 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.

Cabe aos servidores, estagiários e prestadores de serviços do IPMU cumprir com as seguintes

obrigações:

a) A responsabilidade referente à segurança da informação é atribuição do Diretor Financeiro responsável pelo setor de Informática do IPMU, devendo comunicar ao Presidente e ao Controlador Interno ao constatar qualquer irregularidade.
b) Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Instituição;
c) Comunicar imediatamente à área de Sistema da Informação qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.
d) Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos; e
e) Zelar continuamente pela proteção das informações da instituição ou de seus segurados contra acesso, modificação, destruição ou divulgação não autorizada.

21. Penalidades

O não cumprimento, pelos servidores, deste documento, seja isolada ou cumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

a) Comunicação de Descumprimento: será encaminhado ao funcionário, por e-mail, notificação informando o descumprimento da norma, com a indicação precisa da violação praticada e, em caso de reincidência, será enviada também, uma cópia para a respectiva chefia.
b) Advertência ou Suspensão: a pena de advertência ou suspensão será aplicada nos casos legais e após regular apreciação através de processo administrativo disciplinar.

Toda informação produzida ou recebida derivada da atividade profissional pelos usuários pertence ao IPMU. As exceções deverão ser explícitas e formalizadas previamente em documento entre as partes envolvidas.

Fica vedada a divulgação ou reprodução de informações produzidas ou recebidas como resultado de atividade com o IPMU, sem a autorização da autoridade competente.

Os usuários deverão ser cientificados da existência da Política de Segurança e sobre o uso correto dos ativos disponibilizados ao estabelecerem vínculo com o Instituto, de forma a minimizar os possíveis riscos de segurança, bem como garantir o conhecimento de suas responsabilidades.

Os equipamentos de informática, comunicação, sistemas, correio eletrônico e informações deverão ser utilizados exclusivamente para as atividades de interesse do IPMU, sendo vedado:

a) A duplicação de softwares;
b) A retirada de equipamentos eletrônicos ou arquivos físicos da sede do IPMU sem a autorização da autoridade competente.
c) O acesso a redes sociais, "salas de bate-papo", sites de vídeos ou similares, para fins particulares;
d) O acesso a sites não confiáveis, impróprios ou que não estejam relacionados ao desempenho de atividades-fim do Instituto;
e) O acesso, armazenamento, edição ou distribuição de qualquer material de cunho sexual ou preconceituoso;
f) O armazenamento de arquivos pessoais e/ou não pertinentes às atividades-fim do IPMU nos

computadores e na rede de dados do Instituto;

g) O uso de contas particulares de correio eletrônico para fins institucionais;
h) Os servidores efetivos, cedidos, comissionados e estagiários ficam cientes de que os ambientes, sistemas, computadores e redes do IPMU poderão ser monitorados e gravados, mediante prévia informação.

Os e-mails encaminhados pelo correio eletrônico institucional deverão adotar assinatura padrão com as seguintes informações:

a) Nome completo do servidor;
b) Cargo, registro no órgão fiscalizador da profissão, setor e certificações (se houver);
c) Nome do Instituto, por extenso;
d) Telefones do IPMU;
e) Endereço do site e correio eletrônico do IPMU.

22. Verificação da utilização da Política de Utilização da Rede

Para garantir as regras mencionadas acima, o IPMU, se reserva no direito de verificar, sem prejuízo de outras medidas legais, o cumprimento destas medidas:

a) A divulgação não autorizada de dados ou informações confidenciais através da internet, deliberada ou inadvertidamente, pode ensejar a aplicação das penalidades previstas nos regulamentos e procedimentos internos e/ou na forma da lei;
b) É expressamente proibida a desativação ou a modificação não autorizada, de forma deliberada ou não, da configuração e/ou parâmetros dos programas antivírus, "firewall", "proxy" e similares instalados nos computadores públicos, ou em equipamentos para a proteção da rede interna e garantia da integridade de dados, ou similares;
c) É expressamente proibida a exposição, o armazenamento, a distribuição, a edição e/ou a manipulação de material sexualmente explícito através da infraestrutura tecnológica do IPMU, inclusive recursos informáticos e de rede;
d) É expressamente proibido o acesso a web sites contendo material sexualmente explícito, nudez parcial ou total, que não possuam caráter educacional ou relacionado à saúde ou artigos de caráter sexual, publicações eróticas e outras que apresentam ou discutem assuntos relacionados a sexo, próximas à pornografia, o acesso a sites de empresas cujos negócios são de caráter sexual, como boates, serviços de acompanhante, sites com senha/verificação, incluindo sites nos quais se podem adquirir tais produtos e serviços online;
e) É proibida a utilização dos recursos informáticos e de rede do IPMU para a promoção de assédio ou para a realização de condutas de perturbação de outrem,
f) É proibida a utilização dos recursos informáticos e de rede do Poder Público para a propagação deliberada de qualquer tipo de vírus, "worms", cavalos de troia, ou programas de controle de outros computadores (Back Oriffice, Netbus, etc.).
g) Em casos excepcionais (Ex: vírus na rede), a Seção de Informática pode interromper toda rede, trechos de rede, computadores ou qualquer ativo que por algum motivo seja considerado um risco para a infraestrutura física e lógica sem prévio aviso.
h) Implantar softwares e sistemas que podem monitorar e gravar toda a utilização na Internet, impressoras, etc., através da rede e das estações de trabalho do IPMU;
i) Inspecionar qualquer arquivo armazenado na rede estejam no disco local da estação ou nas

áreas privadas da rede, visando assegurar o rígido cumprimento desta Política de Segurança da Informação;

j) Instalar uma série de softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a primeira, mas não a única barreira entre a rede interna e a Internet.

23. Procedimentos de Contingência

Com o intuito de garantir a segurança da informação, deverão ser realizadas cópias de segurança dos sistemas e respectivos bancos de dados utilizados pelo IPMU.

a) Rotineiramente as de cópias de segurança deverão, sempre que possível, ser realizadas de forma automatizada, em horários pré-definidos, devendo ainda ser realizadas verificações periódicas da sua execução e integridade.

b) A guarda das cópias de segurança deverá ter planejamento de forma que impeça o acesso às pessoas não autorizadas.

24. Conscientização dos Servidores

A Política de Segurança da Informação será disponibilizada na página do IPMU, www.ipmu.com.br, na "internet" e "intranet" para acesso e conhecimento de seu inteiro teor aos usuários.

a) Serão desenvolvidos cursos, os quais ficarão disponíveis aos usuários, internamente, para o desenvolvimento da importância da cultura da segurança da informação no IPMU.

25. Das Disposições Finais

O IPMU adotará providências no sentido de garantir:

a) Que os equipamentos estejam em bom estado de conservação para atender as demandas do Instituto e não comprometam a segurança das informações produzidas;

b) O backup das informações armazenadas em seus computadores de forma periódica, preferencialmente, em servidor que esteja localizado fisicamente em local distinto da sede do Instituto e após o horário comercial (períodos em que não houver nenhum ou pouco acesso de usuários aos equipamentos).

O IPMU exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos, serviços e informações, reservando-se o direto de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

O usuário que tomar conhecimento de qualquer irregularidade sobre essa Política de Segurança deverá comunicar, imediatamente, a autoridade competente do IPMU.

O descumprimento dos requisitos previstos nesta Política de Segurança sujeitará o usuário às medidas administrativas e legais cabíveis previstos no Estatuto dos Servidores Públicos de Ubatuba.

O IPMU realizará, sempre que julgar necessário, ações preventivas e educativas visando garantir a

aplicação da Política de Segurança.

O uso de qualquer recurso da instituição para atividades não profissionais pode ensejar a apuração de responsabilidades através do competente processo administrativo, sendo que o IPMU cooperará ativamente com quaisquer outras autoridades, sempre que necessário.

É facultado aos servidores o uso de sítios ou serviços de notícias, desde que não comprometa o desempenho dos recursos, nem perturbe o bom andamento dos trabalhos.

O acesso à internet pela rede sem fio em equipamentos pessoais deverá ser solicitada e justificada; a liberação será realizada após autorização do responsável pela gestão de segurança da informações do IPMU.

É parte integrante desta Política de Segurança da Informação, o Anexo I – Termo de Ciência das normas de utilização que regulamenta a utilização dos computadores, e-mail e software em geral.

A Política de Segurança da Informação será divulgada através do site (www.ipmu.com.br), de maneira que seu conteúdo possa ser consultado a qualquer momento.

Esta Política de Segurança da Informação poderá ser revisada e atualizada periodicamente no mínimo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata, observando a lei nº 13.709/2018 (LGPD) e suas atualizações.

Os casos omissos e as dúvidas com relação a essa Política de Segurança da Informação serão submetidos ao Conselho de Administração do IPMU.

Ubatuba, 05 de fevereiro de 2021

Fernando Augusto Matsumoto
Diretor Financeiro
Instituto de Previdência Municipal de Ubatuba

Sirleide da Silva
Presidente do Instituto de Previdência Municipal de Ubatuba

Ireni Tereza Clarinda da Silva
Diretora de Seguridade e Benefícios Instituto de Previdência Municipal de Ubatuba

Márcia Conceição Fernandes Famadas Rolim
Diretora Administrativa
Instituto de Previdência Municipal de Ubatuba

Wellington Diniz
Controlador Interno do Instituto de Previdência Municipal de Ubatuba

ANEXO I – TERMO DE CIÊNCIA DAS NORMAS DE UTILIZAÇÃO DOS COMPUTADORES, E-MAIL E SOFTWARE EM GERAL.

Pela presente, comunicamos as regras básicas de uso dos computadores no IPMU e apresentamos diretrizes presentes na Política de Segurança a Informação dos ativos físicos e virtuais (Informática e Telefonia) do IPMU, localizados no site do IPMU, enviado por e-mail, na intranet e fixados nos quadros de aviso é dado ciência através do presente.

O seu e-mail é nome@ipmu.com.br (se necessário será incluído "ultimosobrenome" no corpo de email); a senha para uso desta conta de e-mail é pessoal e intransferível. Mais detalhes para configurar esta conta em sua estação de trabalho vejam também na intranet.

Sobre a conta de e-mail devem ser observadas as seguintes regras:

a) Esta conta de e-mail é de uso exclusivo do Instituto; tem a finalidade de servir como meio de correspondência com nossos segurados, fornecedores, servidores e demais interessados em manter contato com o IPMU. Não poderá ser usada para fins pessoais ou particulares sob nenhum pretexto.
b) Esta conta de e-mail expira com a aposentadoria/exoneração de trabalho ou a critério do IPMU, sem prévio aviso e, sob nenhum pretexto, você poderá usar esta conta de e-mail após a rescisão. A critério do IPMU, a conta de e-mail poderá ser mantida para recebimento de mensagens com bloqueio para envio de mensagens por esta conta.
c) Não será permitido o uso de contas de e-mail pessoais nas dependências do IPMU, salvo com autorização, com a devida justificativa e mediante autorização por escrito dos superiores hierárquicos e Seção de Informática.

Sobre o uso dos computadores e softwares:

a) Somente o gestor da segurança da informação poderá fazer download e disponibilizar programas para instalação nas estações, como também autorizar alterações nas configurações das estações e instalação de programas especiais, plug-ins e etc.
b) Os usuários não podem instalar programas nas estações de trabalho. Caso desejem, a solicitação deverá ser feita por escrito ou por e-mail interno ao o gestor da segurança da informação, que avaliará a real necessidade de instalação e encaminhará à Presidência com manifestação conclusiva.
c) Fica expressamente proibido instalar qualquer tipo de software, manipular qualquer tipo de documento ou material ilegal, enviar e receber mensagens ou qualquer outro procedimento que não atenda às necessidades de trabalho e interesses do IPMU, ou seja, considerado ilegal, ofensivo, antissocial, antiético ou imoral.

Ubatuba, XX de XXXXXX de 2021.

_____
Servidor/Diretor

_____
Presidente do IPMU