IPMU
Instituto de Previdência Municipal de Ubatuba

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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.
Além dos aspectos gerais de Segurança da Informação, cada área deve ter um treinamento adequado a sua realidade.
As políticas podem ser gerais, aplicadas a todos, ou específicas, aplicadas nas situações em que é necessária a existência de políticas e treinamentos específicos para determinados cargos ou grupos distintos dentro do IPMU.

2. Para que serve?

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 Segurança da Informação é garantida por meio da preservação de dos cinco pilares básicos:

- **Confidencialidade:** É a garantia de que somente pessoas autorizadas terão acesso à informação;
- **Integridade**: É a garantia de que a informação mantém as características originais estabelecidas por seu proprietário, ou seja, de que não foi modificada ou alterada de forma indevida;
- **Disponibilidade**: É a garantia de que a informação estará pronta para o uso (por pessoas autorizadas) quando for necessária;
- **Autenticidade:** É a garantia de que a informação vem da fonte anunciada, ou seja, de que o autor da informação é realmente quem diz ser e,
- **Não repúdio:** É a garantia de que a pessoa não negue ter assinado ou criado a informação.

3. Fundamentos e Conceitos

A Política de Segurança da Informação tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações de conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação.
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 as necessidades de negócio da informação, bem como a implementação de controle e processos para seus atendimentos.
A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos do IPMU, com vista à garantia de integridade, disponibilidade, conformidade e confiabilidade.
Todos os mecanismos utilizados para a segurança da informação devem ser mantidos para preservar a continuidade das funções institucionais.

O gerenciamento dos ativos de informações, deverão 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.
Comete a 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.

4. DEFINIÇÕES BÁSICAS

Para os fins dessa Política de Segurança da Informação, considera-se:
Acesso lógico: acesso a rede de computadores, sistemas e estações de trabalho por meio de autenticação;
Acesso remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
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;
Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
Análise/avaliação de riscos: processo completo de análise e avaliação de riscos;
Ativo: qualquer bem que o IPMU possua e que tenha valor para a organização;
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 a eles tem acesso;
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;
Banco de dados: é um sistema de armazenamento de dados que tem como objetivo organizar e guardar as informações;
Auditoria: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir ou eliminar fraudes, erros, práticas ineficientes ou ineficazes;
Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;
Chefe de mais alto nível: está envolvido com toda a responsabilidade da segurança da informação. Pode delegar a função de segurança, mas é visto como o principal ponto quando são consideradas as responsabilizações por eventos relacionados com a segurança;
Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;
Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;
Confidencialidade: propriedade de que a inflação não esteja disponível ou revelada a pessoa física ou jurídica, sistema, órgão ou entidade não autorizada;
Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;
Download: baixar copiar arquivos de um servidor/site na internet para um computador pessoal;
Internet: rede mundial de computadores;
Log: é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado.

Logon: Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;
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;
Possuidores de dados: são responsáveis pela classificação da informação. Podem também ser responsabilizados pela exatidão e integridade das informações;
Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e as comunicações;
Servidor de Rede: recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
Servidor: pessoa legalmente investida em cargo público;
Software: são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;
Site: conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;
Usuários: devem aderir às determinações definidas pelos profissionais de segurança da informação.

5. DAS ORIENTAÇÕES

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.
Como os equipamentos, tecnologias e serviços fornecidos para o acesso à internet e ao e-mail são propriedade 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 privada 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.
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.

Internet:

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

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

Correio Eletrônico

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:

- Modificar arquivos ou assumir, sem autorização, a identidade de outro usuário;
- Prejudicar intencionalmente usuários da internet, através do envio de programas e de acesso não autorizados a computadores, ou de alterações de arquivos de programas;
- Utilizar-se do serviço de propriedade do IPMU, desvirtuando sua finalidade com o intuito de cometer fraude;
- 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);
- Difamar, ofender, perseguir ou ameaçar ou de qualquer outra forma violar os direitos de terceiros;
- 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;
- 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;
- Vedado o envio de informações críticas para pessoas ou organizações não autorizadas observando quando for o caso, orientações para o tratamento de informações classificadas;
- 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;
- O Correio Eletrônico do IPMU deve ser utilizado sempre baseado no bom senso e de acordo com os preceitos legais.

Acesso à Rede

O servidor do IPMU deve ser utilizado seguindo as seguintes normas:

- Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.
- É obrigatório armazenar os arquivos inerentes ao IPMU no servidor de arquivos para garantir a cópia de segurança do mesmo;
- É proibido o uso do servidor de arquivos para armazenar informações de cunho pessoal;
- 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;
- 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;
- O usuário deve fazer manutenções periódicas no diretório pessoal, evitando acumulo de arquivos desnecessários;
- São de responsabilidade do usuário as informações em seu diretório pessoal, sendo que o mesmo deve evitar o acumulo de arquivos desnecessários e,
- As contas podem ser monitoradas pela Diretoria responsável, com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

Regras Gerais

- Não são permitidas alterações das configurações da rede de inicialização das maquinas bem como as modificações que possam trazer algum problema futuro;
- 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;

- 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;
- É proibida a instalação ou remoção de softwares que não forem devidamente acompanhados pelo Diretor Administrativo e/ou responsável pelo setor de informática;
- O uso e manuseio, alteração, reposição de equipamento defeituoso será executado unicamente pelo responsável pelo setor da informática;
- É proibida a manutenção de equipamentos de informática particulares dentro das dependências do IPMU, e
- 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.

Usuários

- Todo servidor do IPMU terá direito a uma senha de acesso a rede corporativa e uma conta de e-mail do IPMU;
- O acesso a quaisquer outros serviços ou sistemas providos pelo IPMU ou por outros órgãos da administração direta deverá ser solicitado a chefia imediata;
- 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;
- 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 a chefia imediata, para efetuar a troca da senha e auditoria das atividades executadas com este login e,
- 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.

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:

- Fazer regularmente cópias de segurança de seus dados;
- Manter registro das cópias de segurança;
- Guardar as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original;
- Alterar periodicamente suas senhas;
- Certificar que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação;
- Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;
- Não abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus.

Recomendações sobre atividades permitidas

Utilizar programas de computador licenciados para uso pelo IPMU, de acordo com as disposições específicas previstas em contrato.

- A instalação de programas e sistemas homologados é atribuição da administração de sistemas e TI;

- 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;
- 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.

Recomendações sobre atividades NÃO permitidas

- Introduzir códigos maliciosos nos sistemas de TI;
- 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;
- Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;
- Alterar registro de evento dos sistemas de TI;
- Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;
- Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;
- Violar medida de segurança ou de autenticação, sem autorização de autoridade competente;
- Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;
- Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente.

Recomendação para a Utilização de Aplicações Corporativas e Software de Terceiros

- 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;
- A classificação ou reclassificação da informação deve seguir as orientações da legislação vigente;
- 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;
- 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- O usuário do ambiente de TI do IPMU não deve executar ou desenvolver qualquer tipo de programa ou processo externo às suas atividades.
- 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.

Responsabilidade:

A responsabilidade referente a segurança da informação é atribuição do Diretor Administrativo, juntamente com o servidor responsável pelo setor de Informática do IPMU, devendo comunicar ao Presidente e ao Controlador Interno ao constatar qualquer irregularidade.

Penalidades:

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

- Comunicação de Descumprimento: será encaminhado ao funcionário, por email, 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.
- Advertência ou Suspensão: a pena de advertência ou suspensão será aplicada nos casos legais e após regular apreciação através de processo administrativo disciplinar.

6. DAS DISPOSIÇÕES FINAIS

Esta Política de Segurança da Informação deve ser revisada e atualizada periodicamente no mínimo a cada 3 (tês) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.
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 janeiro de 2017

Flávio Bellard Gomes
Presidente do Instituto de Previdência
Municipal de Ubatuba