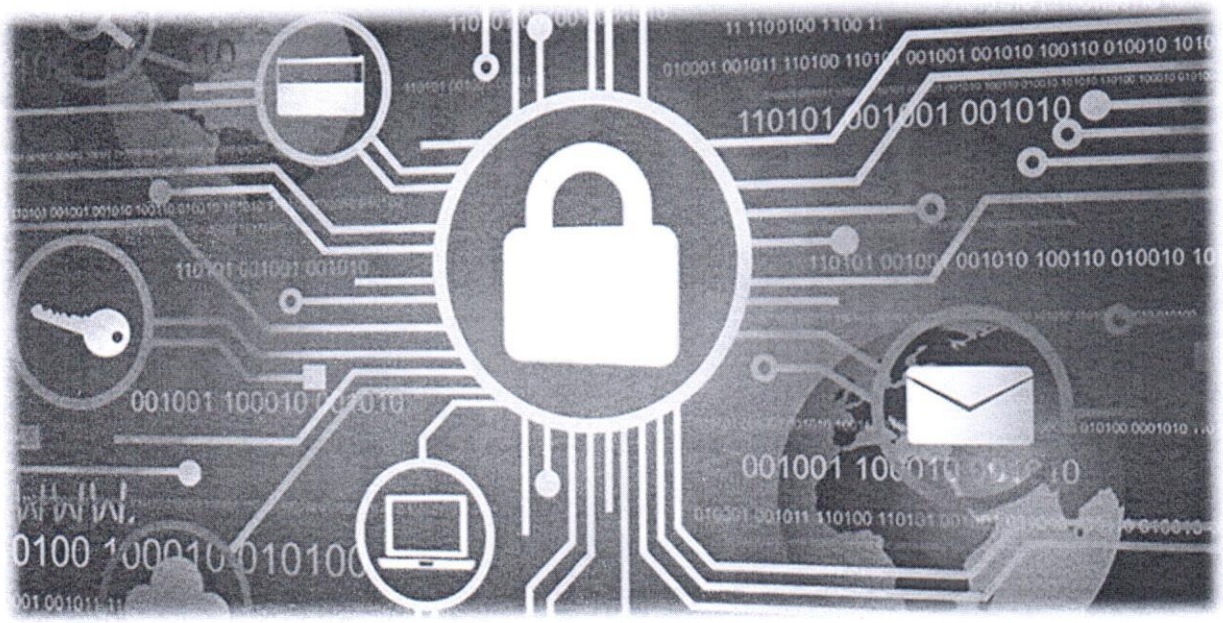
Instituto de Previdência dos Servidores Municipais de São Vicente

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



Instituto de Previdência dos Servidores Municipais de São Vicente

Política de Segurança da Informação do IPRESV

Instituto de Previdência dos Servidores Municipais de São Vicente

Rubens Romão Fagundes
Superintendente

Paolo Brígido da Fonseca
Coordenador do Pró-Gestão RPPS

Josivaldo Junior Nery Sena Santos
Gestor de Tecnologia da Informação

Equipe de Elaboração e Revisão

Josivaldo Junior Nery Sena Santos

Paolo Brígido da Fonseca

Maythe Valéria Giangiulio de Lima

Camila Silva Barcellos

Carolina Michele de Souza Carolo

Instituto de Previdência dos Servidores Municipais de São Vicente

Este documento tem por objetivo divulgar, no ambiente interno do IPRESV, boas práticas em Segurança da Informação (SI), buscando orientar os usuários para uma utilização segura dos recursos de tecnologia da informação disponibilizados pela instituição em conformidade com a Política de Segurança da Informação do Manual do Pró-Gestão RPPS item 3.1.5. 1.

1. Introdução

O termo tecnologia da informação (TI) pode ser definido como o conjunto de recursos tecnológicos e computacionais para geração e uso da informação, abrangendo todas as atividades desenvolvidas na sociedade pelos recursos da informática. Recursos relacionados à TI, como Internet, correio eletrônico, redes sem fio, entre outros, são atualmente ferramentas de trabalho indispensáveis no desempenho das mais diversas atividades. Porém, tais recursos podem ser explorados para fins ilícitos, como roubo de informações, disseminação de vírus, envio de spam, etc.

Diante deste cenário, esta cartilha foi elaborada visando orientar os usuários para uma utilização segura dos recursos de tecnologia da informação disponibilizados pela instituição, em conformidade com a Política de Segurança da Informação do Manual do Pró-Gestão RPPS item 3.1.5.

Nos próximos tópicos, serão apresentadas orientações sobre:

- Senhas;
- Certificado digital;
- Internet;
- Correio eletrônico;
- Estações de trabalho;
- Rede local.

2. Senhas

Via de regra, o acesso aos diversos serviços de informática, como sistemas, e-mail, rede local, entre outros, ocorre mediante autenticação do usuário através de seu nome de usuário (login) e senha (password). Tal processo visa garantir que o acesso à informação seja obtido apenas por pessoas autorizadas (garantia de confidencialidade).

Cada usuário é responsável pela escolha de suas senhas pessoais. Algumas recomendações importantes:

Selecione senhas de boa qualidade. Uma senha bem elaborada reduz as chances de ser comprometida. Algumas recomendações para elaboração de senhas:

- Utilize senhas com pelo menos 6 caracteres;
- Não elabore senhas baseadas em informações pessoais, como nomes, sobrenomes, número de documentos, placas de carros, telefones e datas;
- Não elabore senhas baseadas em palavras que constem no dicionário de qualquer idioma;
- Não elabore senhas com caracteres repetidos ou sequenciais. Ex.: aa22, abcde, ab123;
- Não elabore senhas com caracteres seguidos no teclado do computador. Ex.: qwer, zxcv;

Nunca divulgue ou compartilhe senhas pessoais. As senhas são utilizadas no processo de identificação do usuário perante os serviços de informática. Sua confidencialidade é importante, de forma a evitar que terceiros acessem informações sensíveis, como e-mails e arquivos pessoais, documentos sigilosos, etc. Cada usuário possui logins e senhas individuais, não sendo necessário divulgar ou compartilhar tais dados;

Altere as senhas periodicamente, com o objetivo de assegurar a confidencialidade das mesmas. É recomendável que as senhas sejam alteradas a cada dois ou três meses no máximo;

Quando possível, não utilize senhas iguais para serviços diferentes. Ex.: Utilize senhas distintas para a estação de trabalho e o e-mail;

Evite registrar senhas em locais inseguros, como anotações em papel, embaixo do teclado, adesivos colados no monitor, etc. O recomendável é apenas memorizar a senha;

Sempre altere as senhas temporárias no primeiro acesso. Ex.: Alterar a senha inicial do acesso a estação de trabalho no primeiro acesso;

Não digite senhas quando estiver sendo observado por alguém, evitando assim que outras pessoas descubram suas senhas;

Sempre altere uma senha quando suspeitar que a mesma tenha sido descoberta.

3. Certificado digital

Certificado digital é um documento eletrônico que identifica pessoas e instituições, provando sua identidade e permitindo acessar serviços informatizados com a garantia de autenticidade, integridade e não repúdio, assim como assinar digitalmente documentos. O certificado digital destina-se a qualquer pessoa, física ou jurídica, sendo emitido por uma Autoridade Certificadora (AC). Cada usuário é responsável pela guarda e utilização de seu certificado digital. Algumas recomendações importantes:

Nunca forneça o certificado digital a terceiros. O certificado digital é um documento pessoal e intransferível. Assim como outros documentos pessoais, como CPF, RG e passaporte, não deve ser fornecido a terceiros por questões de segurança;

Aplique as recomendações descritas no item 2. Senhas para as senhas do certificado digital. Um certificado digital possui duas senhas: PIN e PUK. O PIN (Personal Identification Number) é fornecido pelo usuário na utilização do certificado, como por exemplo para assinar um documento eletrônico. O PUK (Personal Unblocking Key) é utilizado pelo usuário para alterar o seu PIN em caso de necessidade.

4. Internet

O acesso à Internet no IPRESV está disponível para os usuários a partir das estações de trabalho conectadas à rede local da instituição. Algumas recomendações quanto à utilização da Internet:

- No IPRESV, utilize somente os meios de acesso Internet que são a rede local e a rede sem fio da instituição;
- Não acesse sites e serviços Internet suspeitos, como os relacionados à pornografia, software ilegal, spam, etc. Tais sites costumam ser utilizados para disseminação de vírus e roubo de informações pessoais;
- Não acesse sites e serviços Internet sem relação com as atividades desempenhadas pela instituição, como sites de jogos, fóruns não profissionais, comunidades de relacionamento pessoal, bate-papo, áudio e vídeo, dentre outros, evitando assim que o desempenho do acesso Internet e serviços relacionados sejam afetados;
- Somente envie informações pessoais através de sites seguros. Informações pessoais, como senhas e números de cartões de crédito, devem ser fornecidas somente em sites considerados seguros. Para identificar se um site é seguro, verifique se o endereço do mesmo (URL) é iniciado por https:// e se o navegador (Ex.: Internet Explorer, Firefox) exibe a figura de um cadeado fechado;
- Somente acesse sites de instituições financeiras e públicas digitando o endereço diretamente no navegador, nunca clicando em outro site ou em um e-mail recebido, evitando assim que dados pessoais sejam furtados através de sites fraudulentos;

5. Correio eletrônico

O serviço de correio eletrônico institucional está disponível para os usuários a partir de qualquer estação com acesso à Internet. Algumas recomendações quanto à utilização do serviço de correio eletrônico:

- Não abra e-mails e anexos considerados suspeitos, como os relacionados à pornografia, propagandas, correntes, arquivos executáveis, remetentes desconhecidos, dentre outros. Tais e-mails e anexos costumam ser utilizados para disseminação de vírus e roubo de informações pessoais. Caso considere um e-mail ou anexo suspeito, apague o mesmo de sua caixa postal;
- Limpe periodicamente sua caixa postal, apagando e-mails antigos, spams, etc. Tal procedimento previne o não recebimento de e-mails devido ao "estouro" do limite da caixa postal;
- Evite enviar e-mails para um grande número de destinatários, pois tal atitude compromete o desempenho da rede local e do serviço de correio eletrônico;
- Utilize o serviço de correio eletrônico somente para fins profissionais, pois o envio de e-mails sem relação com as atividades desempenhadas pela instituição compromete o desempenho da rede local e do serviço de correio eletrônico;
- Divulgue seu e-mail do IPRESV somente para fins profissionais, evitando informar o mesmo em sites e serviços Internet não seguros. Tal procedimento reduz o recebimento de spams e de outras mensagens indesejadas;

6. Estações de Trabalho

Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do IPRESV e utilizados pelos usuários no desempenho de suas atividades funcionais. Algumas recomendações quanto à utilização das estações de trabalho:

- Não instale softwares sem a autorização. Somente softwares devidamente licenciados para utilização no IPRESV podem ser utilizados nas estações de trabalho.
- Não instale, remova ou modifique qualquer software ou hardware sem a autorização, pois tal atitude pode comprometer a segurança e o desempenho da estação de trabalho;
- Utilize a estação de trabalho somente para fins profissionais.

7. Rede local

O acesso à rede local do IPRESV está disponível para os usuários a partir das estações de trabalho. Algumas recomendações importantes:

Não utilize computadores pessoais na rede local do IPRESV, ou seja, somente acesse a rede local através de computadores e notebooks registrados como patrimônio da instituição, salvo seja solicitado e autorizado por seu superior;

Armazene na rede somente arquivos relacionados com suas atividades funcionais, ou seja, não utilize a rede para armazenar arquivos pessoais, como fotos, músicas, vídeos ou

qualquer tipo de arquivo sem relação com as atividades do IPRESV. A má utilização do espaço disponível para armazenamento de arquivos afeta a performance de serviços essenciais;

No IPRESV, nunca utilize redes sem fio de terceiros. Caso seja necessário acesso sem fio, utilize somente a rede local sem fio disponibilizada pela instituição, evitando assim que informações sensíveis sejam interceptadas por terceiros.

8. Das Responsabilidades e Atribuições

8.1 Servidores, estagiários e prestadores de serviços

Cabe a todos funcionários cumprir fielmente a Política de Segurança da Informação.

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.

Comunicar imediatamente ao setor de Informática qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

8.2 Gestor da Tecnologia da Informação

O Gestor da Informação é um servidor sugerido pelas Coordenadorias e designado pelo Superintendente como responsável.

Compete ao Gestor da Informação:

a) Classificar a informação sob sua responsabilidade, inclusive aquela gerada por servidores, estagiários e prestadores externos.

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

c) Enviar ao Coordenador, quando solicitado, relatórios sobre as informações. Os modelos de relatórios serão definidos pelas Coordenadorias e aprovados pelo Superintendente;

d) Sugerir procedimentos aos Coordenadores para proteger os ativos de informação, estabelecida pela Política de Segurança da Informação e pelas Normas de Segurança da Informação;

8.3 Coordenadorias

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

b) Assegurar que suas Diretorias 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

8.4 Assessoria Jurídica

a) Manter as áreas do IPRESV informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;

b) Incluir na análise e elaboração de contratos, sempre que necessárias, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses do IPRESV;

c) Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

8.5 Diretoria de Recursos Humanos

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

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

9. Considerações Finais

Diante das recomendações e informações apresentadas neste manual, pode-se assimilar a necessidade de implementar as políticas de segurança de informação com a finalidade de proteção da integridade, confiabilidade, confidencialidade e disponibilidade das informações deste órgão, proporcionando um ambiente de trabalho seguro e estável. Assim, se forem tomadas as medidas corretas com relação às boas práticas de segurança da informação, os recursos relacionados à TI, tais como as estações de trabalho, Internet, correio eletrônico, redes sem fio, entre outros, estarão devidamente protegidos.

São Vicente, 29 de janeiro de 2021

Rubens Romão Fagundes
Superintendente