Políticas de Segurança
Da Informação

INSTITUTO DE PREVIDÊNCIA
VILA VELHA

Cartilha

Índice

GLOSSÁRIO

- **Active Directory:** Serviço de diretório do Windows que permite o controle de autenticação de usuários de forma integrada. Dentre outras funções, gerencia os logins, senhas e grupos.

- **Anti-malwares:** ferramentas de bloqueio de conteúdo indesejado (como códigos maliciosos – malwares, programas de propaganda indesejada – adwares, programas de coleta de dados – spywares, etc.), podendo agir apenas em alguns tipos específicos de malwares, como os antivírus, por exemplo.

- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

- **Eliminação de dados:** exclusão de forma permanente e irrecuperável de dado armazenado em equipamento eletrônico, via destruição da mídia ou sobreposição da informação armazenada.

- **login:** identificação de usuário dentro do sistema. Deve ser único para cada usuário do sistema.

- **Usuários:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome da pessoa jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

- **Servers:** “servidores” – equipamentos de informática que disponibilizam serviços pela rede. Neste documento foi utilizado o termo servers para não haver confusão o termo ‘servidor’ se referindo a servidores públicos.

- **Estação de Trabalho:** equipamentos com capacidade de se conectar à rede através do protocolo TCP/IP (computadores, impressoras, switches, etc.). Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- **Certificado Digital:** equipamento utilizado para armazenar a chave privada do usuário, certificado privado do usuário, realizar a assinatura digital do usuário, ou fornecer código de acesso específico, visando a autenticação de um usuário no sistema.

- **Vazamento:** termo utilizado para indicar que uma determinada informação de conteúdo sigiloso teve seu sigilo violado.

Sobre IPVV

O Regime Próprio de Previdência Social do Município de Vila Velha foi instituído após a publicação da Lei Municipal nº 2.318, de 19/12/1986 que assegurava a concessão do benefício de pensão e morte dos dependentes dos servidores do Município. Embora anteriormente a Lei municipal nº 1.507 de 26/10/1973 já assegurasse os benefícios de aposentadoria aos servidores dos municipais, o benefício de pensão por morte, como benefício previdenciário estendido a todos os servidores, só foi disciplinado a partir da Lei Municipal nº 2.318/1986, sendo esse o marco inicial do RPPS, nos termos do Parecer CJ/MPS nº 3.165 de 29/10/2003.

Posteriormente, publicou-se a Lei Municipal nº 3.169, de 22/03/1996, disciplinando conjuntamente a assistência à saúde, o regime próprio recebe contornos de regime previdenciário, prescrevendo a criação do IPVV como entidade autárquica, para ser a unidade gestora do regime. Na continuidade, publicou-se a Lei Municipal Complementar nº 007 de 14/12/2004, no sentido de reorganizar o Regime Próprio de Previdência Social dos Servidores Públicos do Município de Vila Velha, embora observa-se que foi efetuada uma "segregação de regime previdenciário", uma vez que a referida lei manteve vinculada ao RPPS/IPVV somente os servidores titulares de cargos efetivos, admitidos até 31/12/2003, os inativos e os pensionistas (art.55). De outra parte, definiu a lei que os servidores admitidos por concurso público a partir de 31/12/2003 seriam vinculados ao RGPS/INSS (art.57).

Neste sentido constatou-se com clareza que o município passou a conviver com "regimes previdenciários distintos" para servidores que se encontravam na mesma situação jurídico-funcional, necessitando assim a correção através da publicação de uma nova Lei Municipal Complementar nº 022/2012, instituindo o Sistema de Seguridade Social dos Servidores Públicos Ativos e Inativos e dos Pensionistas do Município de Vila Velha, proporcionando os benefícios decorrentes do plano de programa único de previdência.

Apresentação

Este documento tem por objetivo divulgar, no ambiente interno do IPVV, as Políticas de Segurança da Informação (PSI), buscando orientar os usuários para uma utilização segura dos recursos de tecnologia da informação disponibilizados pela instituição do IPVV

1. **Introdução**

Atualmente, a tecnologia é elemento-chave em qualquer setor empresarial sendo que, independentemente do porte ou da área de atuação das empresas, os grandes destaques operam em seus principais sistemas em computadores e com grande dependência da conectividade. Esse é um dos motivos que justificam a necessidade de uma política de segurança da informação nas empresas.

Nas últimas décadas, houve um significativo aumento da quantidade de informações sensíveis circulando de um ponto a outro tanto dentro da organização como dela para o mundo todo, via internet. E por mais que a proliferação dos dispositivos móveis e dos serviços de nuvem e/ou Internet das Coisas (IOT) sejam aspectos mais recentes, também vêm impulsionando os investimentos em ambientes de TI seguros.

Já é questão de primeira necessidade ter políticas que, documentadas, detalhem procedimentos e diretrizes para eliminar a subjetividade ao lidar com informações sensíveis. Assim, as empresas podem gerenciar os riscos por meio de controles bem definidos, que ainda fornecem referências para auditorias e ações corretivas.

Diante disso, 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 servidores para uma utilização segura dos recursos de tecnologia da informação disponibilizados pela instituição.

2. **Aplicação**

As políticas de segurança da informação de que trata esse manual aplicam-se a todos os servidores, prestadores de serviços, parceiros e usuários que utilizem o ambiente informacional do IPVV, ou acesso às informações pertencentes ao Instituto. As políticas de segurança da informação aqui tratadas observam o cumprimento das normas constantes no manual. O descumprimento dessas normas, a exemplo de fraudes e invasão ou violação da integridade dos dados e informações do Instituto, ficará submetido à legislação nacional em vigor.

Aplica-se ainda ao gerenciamento de quaisquer equipamentos, programas, meios físicos de tráfegos e sistemas de armazenamento digital de dados e informações incluindo notebooks, tablets, unidades móveis de armazenamento (discos rígidos-HDs), smartphones, impressoras, além das estações de trabalho, inseridos nas dependências do IPVV.

3. Objetivo da Política de Segurança da Informação:

A informação é um ativo essencial da organização e precisa ser adequadamente protegida. Conforme definição da Associação Brasileira de Normas Técnicas - ABNT (ISO 27002), "Segurança da informação é a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

A adoção de procedimentos que garantam a segurança das informações deve ser prioridade constante, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição.

A política de segurança da informação visa a garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição. Deve observar os seguintes princípios básicos:

Confidencialidade: Proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas.

Integridade: Garantia da exatidão das informações e dos métodos de processamento.

Disponibilidade: Garantia de que os usuários autorizados e os interessados tenham acesso às Informações.

A Política de Segurança da Informação em parceria com o Pro-Gestão RPPS atende os seguintes requisitos:

Nível I: Deve abranger todos os servidores e prestadores de serviço que acessem informações do RPPS, indicando a responsabilidade de cada um quanto à segurança da informação.

Nível II: adicionalmente aos requisitos do Nível I :

a) Indicar regras normativas quanto ao uso da Internet, do correio eletrônico e dos computadores e outros recursos tecnológicos do RPPS.

b) Definir procedimentos de contingência, que determinem a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados, o controle de acesso (Físico e lógico) e a área responsável por elas, estando estes procedimentos mapeados e manualizados.

Nível III: Adicionalmente aos requisitos do Nível II, deverá contar com servidor ou área de Gestão da Segurança da Informação, no âmbito do ente federativo ou do RPPS, com a responsabilidade de:

a) Prover todas as informações de Gestão de Segurança da Informação solicitadas pela Diretoria Executiva.

b) Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os servidores e prestadores de serviços.

c) Promover ações de conscientização sobre Segurança da Informação para os servidores e prestadores de serviços.

d) Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação.

e) Elaborar e manter política de classificação da informação, com temporalidade para guarda.

4. Usuários:

O usuário que utiliza os recursos informacionais deve:

- Cuidar adequadamente do equipamento.
- Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pelo profissional de TI da instituição.
- O usuário tem a responsabilidade de transferir para o servidor designado as informações que estão no computador e que precisam possuir cópias de segurança.

4.1 - A Responsabilidade e Forma de Uso:

O usuário que utiliza acesso à internet:

É responsável por todo acesso realizado com a sua identificação/autenticação.

Não é permitido acessar locais virtuais (sites) que:

Possam violar direitos de autor, marcas, licenças de programas ou patentes existentes.

Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.

Contenham informações que não colaborem para o alcance dos objetivos do IPVV.

Defendam atividades ilegais.

Menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.

Que não tenham relação direta com atividade profissional desempenhada pelo usuário.

Não deve retirar (copiar) dos endereços acessados, material que não seja para o uso profissional no IPVV. Nesses casos, o usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pelo gestor da sua área.

Não é permitido o uso de serviços de mensagem instantânea através dos computadores do IPVV, exceto em eventuais situações de uso profissional autorizado pela Presidência.

Não é permitido o uso de serviços de rádio, download de vídeos, filmes e músicas, através dos computadores do IPVV, exceto em eventuais situações de uso profissional autorizado.

5- 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 e senha. Tal processo visa garantir que o acesso à informação seja obtido apenas por pessoas autorizadas.

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 8 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*;

Procure elaborar senhas baseadas em frases. Desse modo, basta lembrar a frase para lembrar a senha.

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 servidor possui login e senha individual, não sendo necessário divulgar ou compartilhar tais dados;

Altere periodicamente as senhas, 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 o Zoom, Microsoft Teams, e-mail e outros;

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 e-mail no primeiro acesso;

Não digite senhas quando observado por outros, evitando assim que outras pessoas descubram suas senhas;

Sempre altere uma senha quando suspeitar que a mesma foi descoberta.

6- 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). Os certificados utilizados no IPVV são emitidos pela Caixa Econômica Federal.

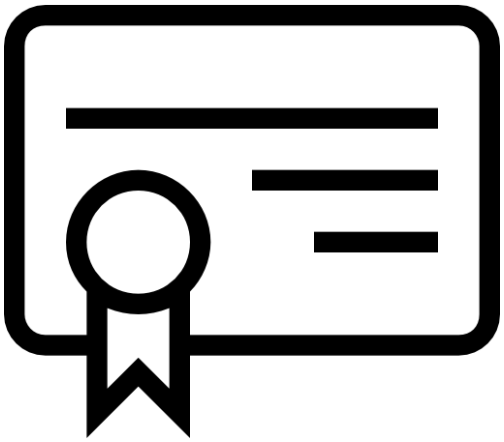
Cada usuário é responsável pela guarda e utilização de seu certificado digital. Algumas recomendações importantes:

Nunca forneça o certificado digital a terceiros. O certificado digital é um documento pessoal e intransferível. Assim como outros documentos pessoais, como CPF, RG (Carteira de Identidade), CNH (Carteira Nacional de Habilitação) 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.



7- Internet:

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

Não acesse sites e serviços de 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 de Internet que não tenha 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 a Internet e serviços relacionados sejam afetados;

Não utilize softwares e serviços de Internet não homologados pelo profissional de TI, como aqueles relacionados a compartilhamento de arquivos, troca de mensagens em tempo real, evitando assim que a segurança e o desempenho da rede institucional 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.: Chrome, 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;

Não utilize computadores públicos ou compartilhados, como terminais em aeroportos, cafés e shopping centers, para acessar serviços disponibilizados no site do IPVV, webmail, etc.

Computadores compartilhados são ambientes inseguros, onde informações sigilosas podem ser obtidas por terceiros.

8- Correio Eletrônico:

O serviço de correio eletrônico institucional está disponível para servidores 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 IPVV somente para fins profissionais, evitando informar o mesmo em sites e serviços de Internet não seguros. Tal procedimento reduz o recebimento de spams e de outras mensagens indesejadas;

O usuário que utiliza um endereço de correio eletrônico:

É responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.

Pode enviar mensagens necessárias para o seu desempenho profissional no Instituto.

Não é permitido criar, copiar ou encaminhar mensagens ou imagens que: contenham declarações difamatórias ou linguagem ofensiva; façam parte de correntes de mensagens, independentemente de serem legais ou não e repassem propagandas ou mensagens de alerta sobre quaisquer assuntos.

9- Estação de Trabalho

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

Não instale softwares sem a autorização do profissional de TI. Somente softwares devidamente licenciados para utilização no IPVV e homologados pelo profissional de TI podem ser utilizados nas estações de trabalho. A utilização de software não licenciado ou considerado "pirata" constitui infração prevista na Lei no 9.609/1998 (http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm);

Não instale, remova ou modifique qualquer software ou hardware sem a autorização do profissional de TI, pois tal atitude pode comprometer a segurança e o desempenho estação de trabalho;

Acesse a estação de trabalho somente com sua conta de usuário, ou seja, nunca utilize uma estação de trabalho através do nome de usuário e senha de outra pessoa.

Tal procedimento visa garantir a confidencialidade das informações processadas;

Ao se afastar da estação de trabalho, efetue o bloqueio ou "logoff' da mesma, evitando assim que outra pessoa acesse a estação de trabalho através do seu nome de usuário e senha;

Utilize a estação de trabalho somente para fins profissionais.

Mantenha a área de trabalho da estação com a menor quantidade possível de ícones, melhorando assim o desempenho do computador

10- Rede Local:

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

Para acesso devido, todo usuário tem cadastro no Active Directory, onde permite o controle de autenticação de usuários de forma integrada. Dentre outras funções, gerencia os logins, senhas, grupos e permissões de acesso em pastas compartilhadas.

Não utilize computadores pessoais na rede local do IPVV, ou seja, somente acesse a rede local através de computadores e notebooks registrados como patrimônio da instituição.

Computadores pessoais conectados à rede do IPVV representam uma das principais portas de entrada de vírus e outras ameaças à segurança da informação;

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 IPVV. A má utilização do espaço disponível para armazenamento de arquivos afeta o desempenho de serviços essenciais;

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