ITA PREV

INSTITUTO DE PREVIDENCIA DOS SERVIDORES PUBLICOS DO MUNICIPIO DE ITAOCARA

30 ANOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SOBRE O INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DE ITAOCARA – ITAPREV

O Instituto de Previdência dos Servidores Municipais de Itaocara é uma entidade autárquica, sem fins lucrativos, com personalidade jurídica de direito público, com autonomia administrativa, patrimônio e gestão financeira própria. Foi criado para cumprir o que determina o artigo 40 da Constituição Federal, que assegura a todos os servidores em cargo efetivo um regime próprio de Previdência. O ITAPREV foi criado em 30 de dezembro de 1994, pela Lei n.º 346 de 1994, seu compromisso é atender as necessidades e prestar serviços ao servidor municipal em situação de incapacidade, idade avançada, tempo de contribuição, reclusão e morte.

Para isso, conta com a contribuição dos Servidores Municipais Efetivos, da Prefeitura e Câmara Municipal de Itaocara.

APRESENTAÇÃO

Este documento tem por objetivo divulgar, no ambiente interno do ITAPREV – ITAOCARA, as Políticas de Segurança da Informação, buscando orientar os usuários para utilização segura dos recursos de tecnologia da informação assegurados pela empresa especializada em sistemas informatizados para gestão de dados de contabilidade pública, tesouraria, recursos humanos, almoxarifado e bens patrimoniais do ITAPREV – ITAOCARA.

Sumário

1. INTRODUÇÃO

A principal justificativa para a existência de uma política de segurança da informação nas instituições e empresa, decorre da crescente dependência da tecnologia em todos os setores da sociedade, independentemente do porte ou área de atuação. As organizações utilizam sistemas informatizados e a conectividade em suas operações, o que torna a segurança da informação um aspecto essencial para garantir a integridade, a confidencialidade e a disponibilidade dos dados.

Em um contexto em que a circulação de informações ocorre constantemente, tanto internamente quanto externamente, através da internet, a necessidade de políticas eficazes e detalhadas que abordem os riscos relacionados ao acesso não autorizado e ao uso indevido de informações sensíveis torna-se ainda mais evidente.

Neste cenário, a política de segurança da informação deve garantir, por meio de controles bem definidos, a proteção de dados pessoais e informações confidenciais, em conformidade com a Lei Geral de Proteção de Dados (LGPD). A LGPD estabelece diretrizes para o tratamento de dados pessoais e exige das organizações um compromisso com a transparência, a segurança e os direitos dos titulares de dados. A criação e a implementação dessa política visam, portanto, não apenas mitigar riscos cibernéticos, mas também assegurar que as práticas de segurança atendam às exigências legais e protejam a privacidade dos indivíduos.

O termo "tecnologia da informação" (TI) abrange o conjunto de recursos tecnológicos e computacionais usados para a geração e o uso da informação, incluindo Internet, correio eletrônico e redes sem fio. Embora esses recursos sejam essenciais para o funcionamento de qualquer organização, é importante destacar que também podem ser explorados de forma indevida, como em casos de roubo de informações pessoais, disseminação de vírus e ataques cibernéticos.

Diante deste cenário, a criação deste documento tem como objetivo orientar todos os colaboradores e usuários sobre as melhores práticas para garantir uma utilização segura dos recursos de TI, assegurando que a proteção de dados pessoais e a conformidade com a LGPD sejam respeitadas em todos os níveis da organização.

2. APLICAÇÃO

Este documento, que aborda a **Política de Segurança da Informação**, destina-se à aplicação por todos os **servidores**, **prestadores de serviços**, **parceiros** e **usuários** que utilizam os recursos informacionais do ITAPREV. As ações e diretrizes aqui estabelecidas visam garantir o cumprimento das normas de segurança da informação e proteção de dados pessoais, conforme exigido pela **Lei Geral de Proteção de Dados (LGPD)** e outras legislações aplicáveis.

O **descumprimento das normas**, incluindo fraudes, invasão de sistemas e violação da integridade dos dados, sujeitará o infrator às penalidades previstas pela legislação nacional em vigor, podendo resultar em **sanções administrativas, cíveis ou criminais**, conforme o caso.

Cabe destacar que esta **Política de Segurança da Informação** se aplica ao gerenciamento e à proteção de todos os **equipamentos**, **programas**, **sistemas de armazenamento digital de dados e informações**, incluindo **notebooks**, **impressoras**, e

servidores inseridos nas dependências do ITAPREV, bem como a qualquer outro recurso tecnológico utilizado para a execução das atividades institucionais.

3. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação tem como objetivo garantir a instituição, diretrizes e estratégias que garantam a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como uma ação adequada para uso, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos armazenados, sob guarda e seguros quanto ameaças e vulnerabilidade e assim minimizar os riscos de acesso.

Dessa forma, a segurança da informação está em conformidade com as disposições constitucionais, legais e regimentais vigentes. Destaca-se ainda, que a política de segurança à informação abrange todos os servidores e prestadores de serviço que acessem informações, indicando a responsabilidade de cada um quanto à segurança da informação.

4. USUÁRIOS

A utilização dos recursos informacionais no ITAPREV deve obedecer por parte dos usuários da seguinte forma:

- **Cuidar adequadamente dos equipamentos**: Os usuários devem tratar todos os dispositivos e recursos tecnológicos com atenção, garantindo que não sofram danos que possam comprometer a segurança ou a integridade dos dados.

- **Responsabilidade no tratamento de dados pessoais**: O usuário deve assegurar que qualquer dado pessoal armazenado ou processado nos sistemas da organização seja tratado de acordo com a LGPD. Isso inclui a responsabilidade de garantir a confidencialidade e a privacidade das informações, evitando o acesso não autorizado ou o uso inadequado.

- **Backup e segurança da informação**: O usuário tem a responsabilidade de transferir para o servidor designado todos os dados relevantes que precisam ser armazenados com cópias de segurança, garantindo que informações essenciais estejam protegidas contra perdas acidentais ou falhas no sistema.

- **Respeitar as normas de uso**: Utilizar os recursos tecnológicos da instituição exclusivamente para fins profissionais, evitando o uso para atividades pessoais que possam representar riscos à segurança, como o acesso a sites não seguros, o envio de informações sensíveis sem criptografia, ou a instalação de softwares não autorizados.

- **Notificação de incidentes de segurança**: O usuário deve comunicar imediatamente ao departamento de TI ou à equipe responsável sobre quaisquer incidentes de segurança, como suspeitas de vazamento de dados ou acessos não autorizados a sistemas ou informações sensíveis.

- **Conscientização e boas práticas de privacidade**: Os usuários devem ser proativos em sua conscientização sobre a privacidade e segurança da informação, incluindo a adoção

de práticas como o uso de senhas fortes, autenticação de dois fatores, e a não divulgação de credenciais a terceiros.

4.1. RESPONSABILIDADE E FORMA DE USO

O usuário que utiliza os recursos de acesso à internet e os sistemas do ITAPREV tem a responsabilidade de garantir o uso adequado e seguro dos mesmos, observando as seguintes diretrizes:

- **Responsabilidade pelo acesso**: O usuário é integralmente responsável por todas as atividades realizadas com sua identificação/autenticação. Isso inclui garantir que suas credenciais de acesso (login e senha) sejam mantidas em sigilo e não sejam compartilhadas com terceiros.

- **Acesso a sites e conteúdos proibidos**: Não é permitido acessar locais virtuais (sites) que possam comprometer a integridade da instituição ou violar direitos, como:

    - Sites que violam direitos de autor, marcas, licenças de programas ou patentes existentes;

    - Conteúdos pornográficos, relacionados ao sexo, exploração infantil ou crimes de pedofilia;

    - Sites que defendem ou promovem atividades ilegais;

    - Conteúdos que incitem preconceito ou discriminação em relação a sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física;

    - Sites que não tenham relação direta com as atividades profissionais desempenhadas pelo usuário no ITAPREV.

- **Uso profissional do material acessado**: Não é permitido retirar (copiar) material de sites acessados, exceto quando for para uso profissional autorizado pelo ITAPREV. O uso de materiais protegidos por direitos autorais sem a devida permissão pode resultar em sanções legais.

- **Uso de serviços de mensagens instantâneas**: O uso de serviços de mensagens instantâneas, como chats e aplicativos de comunicação, não é permitido nos computadores e dispositivos do ITAPREV, salvo quando expressamente autorizado pela Presidência ou pela área responsável. O uso indevido desses serviços pode acarretar riscos de segurança, como o vazamento de dados sensíveis.

- **Proteção de dados pessoais e confidenciais**: Ao acessar informações e utilizar recursos da internet, o usuário deve garantir a proteção de dados pessoais e confidenciais de terceiros, de acordo com a LGPD. Não é permitido o compartilhamento ou o uso

inadequado de dados pessoais de colaboradores, clientes ou qualquer outro titular de dados.

- **Prevenção de incidentes de segurança**: O usuário deve adotar medidas para evitar o acesso não autorizado a sistemas e dados sensíveis, como a utilização de senhas fortes e seguras. Caso identifique algum incidente de segurança, como acessos não autorizados ou vazamento de dados, deve comunicar imediatamente à equipe de TI ou à área responsável.

5. GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Todos os mecanismos de proteção utilizados pela segurança da informação no ITAPREV devem ser mantidos com o objetivo de garantir a continuidade das atividades executadas pelo Instituto de Previdência dos Servidores Públicos do Município de Itaocara. Os requisitos de segurança da informação e comunicação devem ser explicitados em termos de compromisso, celebrados entre a instituição e terceiros, para garantir o conhecimento das diretrizes desta Política e o compromisso com a confidencialidade e proteção dos dados pessoais, em conformidade com a LGPD.

5.1. SENHAS

O acesso aos diversos serviços de informática, como sistemas, e-mails, rede local, entre outros, ocorre mediante autenticação do usuário por meio denome de usuário e senha. Esse processo visa garantir que o acesso às informações seja obtido apenas por pessoas autorizadas e que, em caso de incidentes de segurança, a responsabilidade possa ser claramente atribuída. As senhas devem ser fortes (combinando letras, números e caracteres especiais) e mantidas emsigilo. Além disso, recomenda-se a autenticação de dois fatores sempre que disponível, para aumentar a segurança do acesso.

5.2. CERTIFICADO DIGITAL

O certificadodigital é um documento eletrônico que identifica pessoas e instituições, garantindo a autenticidade, integridade e não repúdio, e permitindo a assinatura digital de documentos. Ele é utilizado para acessar serviços informatizados de forma segura.

Cada usuário é responsável pela guardae usoadequado de seu certificado digital. A perda ou uso indevido do certificado pode resultar em comprometimento da segurança da informação e violação de dados pessoais, o que deve ser imediatamente comunicado ao departamento de TI.

5.3. INTERNET

O acesso à internet no ITAPREV está disponível para os servidores a partir das estações conectadas à rede local da instituição. Esse acesso deve seguir as normas específicas de segurança, respeitando a legislação vigente e as diretrizes desta política. O uso da internet para acessar informações não relacionadas às atividades profissionais pode comprometer a segurança e a confidencialidade dos dados processados.

5.4. CORREIO ELETRÔNICO

O serviço de Correio Eletrônico Institucional está à disposição para os servidores, podendo ser acessado de qualquer estação com acesso à internet. O usuário é responsável por todo o acesso, conteúdo, mensagens e uso do seu e-mail institucional. As seguintes determinações devem ser seguidas:

- **Ambiente Profissional:**O envio de mensagens deve ser restrito às necessidades profissionais no âmbito do ITAPREV.
- **Proibição de mensagens difamatórias**: Não é permitido encaminhar, copiar ou criar mensagens e imagens que contenham declarações ofensivas, ou que façam parte de correntes de mensagens, independentemente de serem legais ou não.
- **Confidencialidade dos dados**: Os usuários devem garantir que informações sensíveis, como dados pessoais de servidores e beneficiários, não sejam enviadas por e-mail sem o devido cuidado e proteção, como a criptografiade dados.

5.5. ESTAÇÕES DE TRABALHO

As estações de trabalho no ITAPREV incluem computadores e notebooks registrados como patrimônio da instituição e utilizados pelos servidores para o desempenho de suas atividades. Algumas regras de segurança são imprescindíveis para garantir a proteção das informações:

- **Instalação de softwares**: Não é permitido instalar softwares sem a autorização da diretoria de TI. A instalação não autorizada pode comprometer a segurança dos sistemas e dados.
- **Bloqueio de estação de trabalho**: Ao se afastar da estação, o usuário deve **bloquear a tela** ou **encerrar a sessão** para evitar o acesso não autorizado.
- **Uso exclusivo para fins profissionais**: A estação de trabalho deve ser utilizada apenas para atividades diretamente relacionadas ao desempenho das funções do servidor no ITAPREV.

5.6. REDE LOCAL

O acesso à rede local do ITAPREV deve ser feito exclusivamente a partir de estação de trabalho registrada como patrimônio da instituição**.** Além disso, é proibido o uso de redes sem fio de terceiros para acessar a rede local. Caso seja necessário o uso de redes sem fio disponibilizadas pela instituição, as seguintes recomendações devem ser seguidas:

- **Uso de redes sem fio**: O acesso via redes sem fio externas não é permitido, pois pode comprometer a **segurança e integridade** das informações e dados pessoais.
- **Conexões seguras**: Sempre que possível, utilizar conexões VPN (Virtual Private Network) para garantir que os dados transmitidos pela rede estejam protegidos.

5.7. CONSCIENTIZAÇÃO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO

O ITAPREV promoverá, de forma contínua, a capacitação dos usuários da instituição sobre a aplicação de boas práticas de segurança da informação e comunicação. A conscientização dos servidores sobre o uso adequado dos recursos de TI, o cumprimento das diretrizes desta política e a proteção dos dados pessoais será fundamental para criar uma cultura de segurança dentro da instituição. A capacitação também abordará a LGPD, garantindo que todos os servidores estejam cientes dos seus papéis na proteção da privacidade e segurança dos dados pessoais.

DIRETORIA EXECUTIVA DO ITAPREV

Membros	**Cargo/função**
PRISCILLA SOARES CURTY	Diretora Presidente
LAENE FARIA CORREA PIRES	Diretora Financeira e Administrativa
VERÔNICA BASTOS MEIRELES	Diretora Previdenciária e Benefícios

APROVAÇÃO DO CONSELHO DELIBERATIVO			
DATA	22/01/2022	**ATA Nº**	001/2024