INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE JOAÇABA – IMPRES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Joaçaba/SC, outubro de 2021.

Avenida XV de Novembro, nº 378, Centro – Joaçaba/SC – CEP: 89600-000 –
Fone: (49) 3527-8810 Site: www.impres.sc.gov.br /E-mail: contato@impres.sc.gov.br

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE JOAÇABA – IMPRES

1 INTRODUÇÃO

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005, "A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios ou atividades de uma Organização ou Instituição e, conseqüentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, [...]. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente."

De acordo com a mesma norma, "Segurança da informação é a proteção da informação de vários tipos de ameaças que visa: garantir a continuidade das atividades, minimizar o risco das atividades e maximizar o retorno sobre os investimentos e as oportunidades surgidas."

As informações do Instituto possuem grande importância, por isso devem ser protegidas, cuidadas e gerenciadas adequadamente com o objetivo de garantir sua disponibilidade, integridade, confidencialidade, autenticidade e irretratabilidade, independentemente do meio de armazenamento, processamento ou transmissão que se utiliza.

A Política de Segurança da Informação - PSI é uma importante ferramenta para combater ameaças aos processos operacionais do Instituto, assim sua implementação, contendo diretrizes, orientações e procedimentos servirão para conscientizar e nortear os servidores, diretores e conselheiros quanto o uso seguro dos processos operacionais.

2 OBJETIVOS

a) Registrar os princípios e as diretrizes de segurança adotados pelo Instituto, a serem observados por todos os usuários e aplicados à todos os sistemas de informação e processos operacionais.

b) Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente tecnológico.

c) Preservar os sistemas de informação do Instituto quanto a:

- Confidencialidade: propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal.
- Integridade: propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital.
- Disponibilidade: propriedade que garante que as informações estejam acessíveis somente às pessoas e aos processos autorizados, no momento requerido.
- Autenticidade: propriedade que confirma a identidade dos usuários antes de permitir o acesso aos sistemas.
- Irretratabilidade: propriedade que impede a negação da autoria de uma informação fornecida.

3 JUSTIFICATIVA

A Segurança da Informação não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de proteção de informações e dados.

A Política de Segurança da Informação - PSI do Instituto de Previdência dos Servidores Públicos do Município de Joaçaba - IMPRES foi elaborada, com o intuito de padronizar, normatizar e disciplinar a utilização dos processos operacionais e recursos de informática do Instituto, visando o comportamento ético e profissional dos usuários.

O referido documento aplicar-se-á às informações em qualquer meio ou suporte e destina-se aos seguintes usuários: servidores efetivos, cedidos, comissionados, estagiários, conselheiros, diretores, segurados ativos, aposentados, pensionistas, e pessoas físicas ou jurídicas contratadas pelo Instituto.

A PSI norteará a implementação de medidas de proteção que deverão ser aplicadas à toda e qualquer informação, independentemente de onde ela se encontre, com vistas ao resguardo da imagem e dos objetivos institucionais do IMPRES. Suas orientações devem ser lidas, estudadas, entendidas e seguidas por todos os envolvidos, para que a informação tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

Toda informação produzida ou recebida como resultado da atividade profissional pelos envolvidos, pertence ao Instituto de Previdência dos Servidores Públicos do Município de Joaçaba - IMPRES. As exceções deverão ser explicitadas e formalizadas previamente em documento entre as partes envolvidas.

Os equipamentos de informática, comunicação, sistemas, correio eletrônico, internet, extranet e informações deverão ser utilizados exclusivamente para as atividades de interesse do Instituto.

4 DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4.1 Da Segurança Física

Refere-se a segurança dos ativos computacionais, instalações prediais e documentos em meio físico abrangendo também, o controle de acesso de pessoas às instalações do Instituto.

Quanto aos documentos impressos e arquivos contendo informações importantes deve-se armazená-los em local seguro e protegido, mas de fácil acesso.

4.1.1 DO ACESSO AO ESPAÇO FÍSICO OU EQUIPAMENTOS

Qualquer pessoa poderá entrar no espaço físico do Instituto desde que identificada e autorizada pelos servidores e deverá respeitar os limites de acesso. Já, o contato ou acesso direto às informações físicas de dados ou processos só poderá ser efetivado por pessoas autorizadas.

- Será disponibilizado chave de entrada da sede, aos servidores efetivos ou cedidos pela municipalidade e aos membros da diretoria;

- As chaves não poderão ser repassadas à outras pessoas que não as citadas;
- Membros dos conselhos deliberativo e fiscal e do comitê de investimentos somente terão acesso a sala, quando houver pessoa autorizada para abri-la;
- Os armários e arquivos com documentos serão acessados somente pelos servidores, exceto os arquivos destinados aos órgãos colegiados que poderão ser acessados por seus membros, esses armários possuirão porta com chave.
- Cada servidor efetivo ou cedido terá um computador, que preferencialmente só será acessado por ele;
- Será disponibilizado computador exclusivo à diretoria e aos membros dos conselhos deliberativos, fiscal ou do comitê de investimentos, que possuirá impressora e webcam instalados e terá senha para acesso as informações e pastas salvas na área restrita à cada colegiado;

4.1.2 DO ARMAZENAMENTO DOS DOCUMENTOS FÍSICOS

Os documentos em formato físico são aqueles que possuem assinaturas, como: processos de concessão de benefícios, pareceres, portarias, resoluções, cálculos atuariais, política de investimentos, APRs, pareceres dos colegiados, atas dos colegiados, declarações, contratos, e outros registros de importância. Todos os envolvidos serão orientados a proceder de forma a:
- Manter os documentos físicos em pastas ou arquivos, bem ordenados e conservados para facilitar o acesso, quando necessário;
- Indicar nas pastas e arquivos o tipo de documento nelas guardados;
- Esvaziar as pastas anualmente e transferir os documentos para arquivo morto;
- Arquivar os documentos necessários para processo de aposentadoria e/ou pensão dos servidores em pastas individualizadas e armazená-las de forma a facilitar o acesso, quando necessário;
- Guardar no arquivo morto a pasta do processo quando findado o benefício, por ocasião do falecimento do segurado e/ou dependentes, podendo ser destruída após transcorrer o tempo de guarda, definido em legislação;

- Conservar em pastas de arquivo morto os documentos físicos digitalizados, podendo ser destruído após transcorrer o tempo de guarda definido em legislação.

4.1.3 DA RETIRADA DE DOCUMENTOS

O acesso irrestrito pode ser visto como uma falha potencial na gestão de documentos, por isso, definiu-se regras que limita quem poderá acessar os documentos, prazos para devolução, entre outras diretrizes. Assim, a retirada de documentos ou processos deverá seguir as normas aqui estabelecidas e o servidor responsável deverá:

- Registrar os documentos físicos, de relevante importância em livro de protocolo, quando forem retirados e devolvidos da sede, pelos usuários;
- Demais pessoas deverão preencher solicitação padrão, onde será especificado o tipo de documento/processo pretendido e o motivo do requerimento; constará espaço para registrar: a quantidade de folhas do documento solicitado, a data da retirada, a assinatura legível de quem retirou, a data de devolução, nome de quem devolveu e de quem recebeu;
- O servidor responsável, no momento da devolução do documento/processo, deverá verificar se o mesmo está completo, conforme quando foi retirado.

4.1.4 DO DESCARTE DE DOCUMENTOS

A eliminação de documentos é uma ação que deve ser realizada criteriosamente, uma vez que os documentos produzidos possuem caráter público. A eliminação não pode ocorrer sem que uma avaliação prévia dos documentos, identificando-se quais poderão ser eliminados, quais deverão ser preservados por mais tempo, e quais deverão ser preservados indefinidamente, visto seu valor permanente e histórico.

É importante salientar que a eliminação de documentos de valor permanente é crime, uma vez que a proteção à documentação pública e a gestão da mesma está prevista em legislação. Assim, é necessário que a eliminação seja feita de maneira criteriosa, sempre seguindo o que a legislação preconiza sobre o descarte.

Com relação ao descarte de papéis/documentos, os servidores deverão:

- Descartar no lixo somente após torná-los ilegíveis;

- Utilizar preferencialmente um triturador de papel para esmigalhar o documento;
- Destinar sempre que possível para a reciclagem;
- Descartar documento físico após digitalizar, ressalvando aqueles de relevada importância e que apresentem conteúdo de valor permanente ou histórico;
- Verificar a possibilidade de descarte junto a diretoria e buscar anuência do conselho deliberativo antes de realizar o descarte de documentos armazenados no arquivo morto;
- Criar tabela eletrônica para registrar todos os documentos do arquivo morto que forem descartados, onde deverá ser anotado informações básicas como: de quem era, à quem foi encaminhado/recebido, data que foi elaborado/recebido, breve relato do conteúdo, data de descarte e porquê foi descartado.

4.2 Da Segurança Lógica

Refere-se a toda e qualquer informação em meio digital, seja em equipamentos de informática, tráfego de informações pela rede, por correio eletrônico ou armazenado em estações de trabalho dos usuários.

4.2.1 DA AUTENTICAÇÃO

A autenticação é um processo que busca verificar a identidade digital do usuário de um determinado ambiente, no momento em que ele requisita um login (acesso) em um programa ou computador. O processo é realizado por meio de comparação das credenciais apresentadas pelo usuário com outra já pré definida no sistema.

A autenticação nos ambientes digitais será baseada em uma senha. Esse meio é muito utilizado por sua facilidade de implantação e manutenção e por seu baixo custo.

4.2.2 DAS SENHAS

O primeiro estágio para proteger os diversos ambientes de trabalho (e-mail, contas, sistemas...) será criar senha de proteção. Todos os envolvidos deverão criar senhas para os diversos ambientes de trabalho, de forma coerente, observando sempre a política de senhas:

- Criar uma seqüencia forte, misturando caracteres de letras minúsculas, maiúsculas e números, para dificultar o acesso indevido ou não autorizado no ambiente de trabalho;
- A senha é pessoal e intransferível, não deverá ser passada à ninguém;
- Tomar precauções para manter a senha secreta;
- Alterar a senha sempre que desconfiar que está havendo algo diferente na estação de trabalho;
- Tudo que for executado com determinada senha, em qualquer ambiente de trabalho, será de inteira responsabilidade do seu detentor;
- Quando houver mudança de diretores ou dos presidentes dos colegiados, o detentor de senha(s) repassará ao sucessor que realizará a alteração da(s) mesma(s), para acessar os diferentes ambientes de trabalho.

4.2.3 DOS DOCUMENTOS ARMAZENADOS DIGITALMENTE

Documentos como: atas dos colegiados, pareceres, relatórios, planejamentos, notícias, fichas de cadastro, resoluções, ofícios e outros, deverão ser armazenados por todos os envolvidos, também em formato digital, uma vez que garantirá a durabilidade e o fácil acesso.

- Criar rotina de digitalização**,** estabelecendo local e prazo para os usuários deixarem os documentos a serem digitalizados**,** ao servidor que executará a tarefa;
- Armazenar em pastas digitais, devidamente identificadas, cópias de documentos digitalizados ou enviados eletronicamente;
- Fazer backup de dados, periodicamente, como medida de segurança**,** mantendo os arquivos em um banco de dados a parte para garantir a sua proteção, evitando a perda dos arquivos;
- Criar padrões de títulos para nomear documentos gerados nos arquivos digitais, visando facilitar a identificação e a busca pelo documento pesquisado. Todos os usuários deverão utilizar o mesmo padrão para nomear arquivos e documentos, facilitando assim a organização.

4.2.4 DOS E-MAILS

O Correio eletrônico, ou e-mail é uma ferramenta que permite compor, enviar e receber mensagens, textos, figuras e outros arquivos através da Internet. É um importante canal de relacionamento de via dupla, para enviar e receber informações.

O e-mail institucional proporciona mais credibilidade para o endereço eletrônico, demonstrando comprometimento com a qualidade da comunicação, tanto para quem entra em contato, como para quem recebe as mensagens.

Ele requer ações de proteção para a segurança dos seus conteúdos. As informações contidas nos e-mails podem ser sigilosas, por isso os passos a seguir deverão ser seguidos por todos os servidores, diretoria e membros colegiados:

- Ter instalado, utilizar e atualizar constantemente antivírus no computador de seu uso;
- Ter filtro anti-spam ativado nas configurações do serviço de e-mail;
- Evitar mensagens que alertam para vírus, porque normalmente visam a apropriação de endereços de e-mail para posterior uso em spam;
- Denunciar e bloquear spams;
- Evitar executar programas de origem desconhecida, verificar o assunto antes de abrir o e-mail, não abrir se não conhecer o remetente ou se o assunto parecer não confiável;
- Não responder mensagens de desconhecidos;
- Não enviar dados ou informação de caráter pessoal/institucional, por e-mail, sem ter segurança no endereço do destinatário;
- Se considerar a possibilidade do computador estar infectado com algum tipo de vírus, não enviar e-mails sem antes passar antivírus atualizado;
- Não utilizar o e-mail do Instituto para assuntos pessoais;
- Evitar anexos muito grandes;
- Todos os presidentes dos colegiados deverão utilizar e-mail institucional para comunicação do Instituto;
- Quando houver mudança de diretores ou dos presidentes dos colegiados, o detentor da senha repassará ao sucessor que realizará a alteração da mesma;
- Mensagens consideradas importantes não deverão ser deletadas da caixa de e-mail, caso a caixa encher, deverá armazená-las em local específico, retirando da caixa sempre a mais antiga;

- As mensagens de correio eletrônico deverão incluir assinatura com o seguinte formato:

Nome do servidor/diretor/conselheiro

Colegiado ou setor que representa

Nome do Instituto

Telefone(s)

Whatsapp.

4.2.5 DO ACESSO A INTERNET

Em primeiro lugar, todo servidor que utiliza a internet no ambiente de trabalho deve ter bom senso para saber que durante o expediente não deve realizar atividades pessoais. Porém, caso o servidor precise checar algum tipo de e-mail ou rede social, é importante que o faça com parcimônia.

A melhor forma de resguardar ambas as partes é contar com a elaboração de uma política transparente e bem divulgada. Assim, todos os usuários deverão adotar as normas a seguir, para evitar transtornos.

- Proteger a rede e o uso da internet, restringindo acessos a sites específicos;
- Bloquear site de jogos; locais na internet que dão espaço a violência e a pornografia;
- Atualizar os sistemas operacionais com periodicidade;
- Possuir antivírus;
- Deixar os navegadores dos computadores sempre atualizados;
- Evitar o uso recreativo da internet;
- É proibido o uso de ferramentas P2P.

4.2.6 DO USO DA ESTAÇÃO DE TRABALHO

Cada estação de trabalho tem códigos internos que permitem a identificação na rede, isso significa que tudo que for executado nela, acarretará em responsabilidade por parte da pessoa que a utiliza. Por isso, deverá ser prática de todos os envolvidos:

- Efetuar logoff ou travar o console sempre que sair da frente da estação de trabalho;
- Não instalar nenhum tipo de software/hardware sem autorização;

- Não ter MP3, filmes, fotos e softwares sem direitos autorais ou qualquer outro tipo de pirataria;
- Manter na estação de trabalho, somente o que for supérfluo ou pessoal. Todos os dados relativos ao Instituto deverão ser mantidos, onde existe um sistema de backup diário e confiável;
- Criar políticas de backup diário ou semanal preferencialmente em servidor que esteja localizado fisicamente em local distinto da sede do Instituto.

4.2.7 DA ASSINATURA DIGITAL

O certificado digital é uma assinatura com validade jurídica que garante as transações eletrônicas e outros serviços realizados pela internet. Essa assinatura permite que o Instituto e pessoas que o represente sejam identificadas digitalmente de qualquer lugar, de forma inequívoca e segura. Ele possui o nome, um número público que é exclusivo (denominada chave pública) e outras informações que comprovam e identificam o seu dono para o sistema.

No Instituto a assinatura eletrônica será utilizada pelos diretores, contador, presidente do conselho deliberativo e prefeito para:
- Assinar e enviar documentos através da internet;
- Logar-se em sites seguros;
- Realizar transações bancárias;
- Assinar escriturações fiscais e contábeis;
- A assinatura eletrônica é pessoal e intransferível, devendo os diretores:

Criar uma senha forte;

Não passar a senha para outro diretor;

Utilizar o Smart Card, Token ou Nuvem;

Cuidar com a validade.

A assinatura digital reduz custos com emissão e armazenamento de documentos, diminui os arquivos físicos que poderão ser substituídos por sistemas de Gerenciamento Eletrônico de Documentos; minimiza risco de fraudes, já que o certificado digital confirma a autenticidade das partes envolvidas com a assinatura do documento e ainda

otimiza tempo e custos com processos de impressão, assinatura, transporte e registro em cartório.

4.2.8 DOS VÍRUS E CÓDIGOS MALICIOSOS

Os vírus de computador são uma das formas mais antigas de malware; são softwares maliciosos criados para causar danos e pela capacidade de evitar a detecção e se replicar, sempre serão motivo de preocupação. Assim, entender o que um vírus é capaz de fazer no computador é o primeiro passo para protegê-lo de ataques. Por isso é importante:

- Manter o anti vírus atualizado;
- Suspeitar de softwares que “você clica e não acontece nada”;
- Optar por uma estrutura de nuvem, seja ela pública, privada ou híbrida;
- Utilizar pendrive ou CDs de fora do Instituto somente no computador determinado para esse uso.

4.3 DA SEGURANÇA DOS RECURSOS HUMANOS

Refere-se a educação e conscientização dos interesses de cada usuário sobre a responsabilidade para com a segurança da informação, por meio de recomendações e ações educativas.

4.3.1 Da Política Social

Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando se discorre sobre segurança, isso é uma desvantagem. Por isso, os usuários deverão observar os seguintes tópicos:

- Não falar sobre a política de segurança do Instituto com terceiros ou em locais públicos;
- Não passar a senha para outra pessoa;
- Evitar digitar as senhas ou usuários em máquinas de terceiros, especialmente fora do Instituto;

- Somente aceitar ajuda técnica, de técnico previamente identificado;
- Evitar executar procedimentos técnicos quando as instruções forem recebidas por e-mail;
- Relatar aos colegas ou superiores pedidos externos ou internos que venham a discordar dos tópicos anteriores.

4.3.2 Da Capacitação dos Envolvidos

Toda vez que uma nova ferramenta ou sistema for inserida na rotina do Instituto, será oferecido capacitação/treinamento para os envolvidos terem conhecimento e poderem utilizá-la da melhor forma possível, visando garantir eficiência, segurança e coesão.

5 DOS ENVOLVIDOS

De nada adianta uma informação segura se a mesma estiver indisponível para quem necessitar. Por isso, segue relação dos envolvidos com as informações relativas ao Instituto.

Nome	Função	e-mail	Fone fixo (ramal) e celular
Ivone Zanatta	Diretora Presidente	ivone_zanatta@yahoo.com.br	998112812
Johnny George Oliveira de Carvalho	Diretor Financeiro /presidente comitê de Investimentos	diretoriafinanceira@impres.sc.gov.br	999286203
Tiago Giumbelli	Diretor Jurídico	dupont.tiago@gmail.com	999123940
Fernanda Braga	Contadora	fernandab.jba@gmail.com	998013300
Daniela Aparecida Mattos	Secretária	contato@impres.sc.gov.br	35278810
Juliana Kusnier	Presidente Conselho Deliberativo	julianakusnier@hotmail.com	999844356
Eliane Aparecida Ceron Vier	Presidente Conselho Fiscal	elianec.vier@gmail.com	998136158

6 CONSIDERAÇÕES FINAIS

Todas as normas aqui estabelecidas serão seguidas a risca por todos os usuários. Ao tomar conhecimento da Política de Segurança da Informação, comprometer-se-ão a

respeitar todos os tópicos nela abordados e estarão cientes que seus ambientes de trabalho, tanto virtual como físico poderão estar sendo monitorados.

A violação à política, às normas ou aos procedimentos ou a não aderência da Política de Segurança da Informação do Instituto de Previdência dos Servidores Públicos do Município de Joaçaba - IMPRES, sujeitará os envolvidos as medidas administrativas cabíveis e penalidades previstas em Lei, garantindo sempre o processo de defesa amplo e contraditório, que poderá acarretar no desligamento do usuário de acordo com a gravidade da ocorrência.

A presente PSI será revista e atualizada periodicamente, sempre que ocorrer falhas de segurança ou algum evento que motive sua revisão.

Joaçaba, outubro de 2021.

Ivone Zanatta
Diretora Presidente
IMPRES - Joaçaba - SC