Política de Segurança da Informação (PSI)

INSTITUTO MUNICIPAL DE PREVIDÊNCIA SOCIAL DE JALES

Julho de 2.021.

Sumário

1. Introdução 3
2. Objetivos 4
3. Abrangência 4
4. Dispositivos 5
   - 4.1 Dados dos servidores:. 5
   - 4.2 Dados pessoais de servidores. 6
   - 4.3 Equipamentos: 6
   - 4.4 Admissão e demissão de servidores/ estagiários: 6
   - 4.5 Programas ilegais: 6
   - 4.6 Instalação de sofware: 7
   - 4.7 Permissões e senhas: 7
   - 4.8 Compartilhamento de dados: 7
   - 4.9 Cópias de segurança de arquivos em desktops: 8
   - 4.10 Segurança e integridade dos dados:. 8
   - 4.11 Propriedade intelectual: 8
   - 4.12 Acesso internet:. 8
   - 4.13 Uso do correio eletrônico (e-mail): 9
   - 4.14 Necessidade de novos sistemas, aplicativos e equipamentos: 10
   - 4.15 Uso de notebook no impsjales: 10
   - 4.16 Responsabilidade dos superiores hierarquicos:. 10
   - 4.17 Uso de antivírus: 11
   - 4.18 Penalidades: 11

1. Introdução

As políticas, normas e procedimentos que visem garantir a segurança da informação devem ser prioridades constantes do Instituto Municipal de Previdência Social de Jales (IMPSJALES).

Assim, busca-se reduzir os riscos de falhas, danos e prejuízos que possam comprometer a imagem e os objetivos do Instituto.

A Política de Segurança da Informação (PSI), define as diretrizes, os limites e o direcionamento que o IMPSJALES deseja para os controles que serão implantados na proteção de suas informações e responsabilidades legais para todos os servidores e usuários, devendo ser cumprida e aplicada em todas as áreas do Instituto.

Esta PSI está baseada nas recomendações propostas pela norma técnica ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está em conformidade com as leis vigentes em nosso país.

Para os efeitos deste regulamento da Política de Segurança da Informação (PSI) entende-se por:

I – IMPSJALES ou instituto: Instituto Municipal de Previdência Social de Jales.

I - Superintendência: Órgão de direção executiva do IMPS JALES;

II – Empresa Contratada: Empresa contratada, responsável pelo armazenamento e processamento de informações de diversos segmentos do IMPSJALES, inclusive por meio de Data Centers, devendo processar e disponibilizar essas informações adequadamente e protegê-las contra ameaças e riscos.

III – Área de TI: Servidor (es) responsáveis designados pelas áreas de tecnologia de Informação do IMPSJALES.

IV – Usuário: Todos os servidores, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou acesso a informações pertencentes ao instituto.

2. Objetivos

Os objetivos genéricos da Política de Segurança da Informação para o IMPSJALES são:

I. Certificar e garantir segurança com contato externo em relação a sistemas, equipamentos, dispositivos e atividades vinculadas a segurança dos sistemas de informação;

II. Promover a conscientização de todos servidores visando a compreensão e o manuseio de situações relacionadas à segurança da informação;

III. Promover as ações necessárias à implementação e manutenção da segurança da informação

Preservar as informações quanto à:

- Confidencialidade: toda informação, até que se torne pública, deve ser acessada por quem de direito e assegurar que informações confidenciais e críticas não sejam subtraídas dos sistemas organizacionais por meio de ciberataques, espionagem, entre outras práticas.

- Integridade: preservação da precisão, consistência e confiabilidade das informações e sistemas.

- Disponibilidade: Garantia de acesso à informação durante o ciclo de sua existência.

- Conformidade: Toda informação deve estar em conformidade com os padrões, regras e, especialmente, com a legislação vigente.

- Auditabilidade: Configuração de sistemas e bases de dados de forma a possibilitar o rastreamento de atividades físicas e lógicas.

3. Abrangência

A Política de segurança da informação do IMPSJALES, aplica-se a todos os servidores, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou acesso a informações pertencentes ao IMPSJALES. Todo e qualquer usuário de recursos computadorizados do instituto tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

•. Exponha o IMPSJALES a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.

•. Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

•. Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

4. Dispositivos

•. É DEVER DE TODOS no IMPSJALES considerar a informação como sendo um bem da Autarquia, um dos recursos críticos para a realização dos objetivos do Instituto, que possui grande valor para o instituto e deve sempre ser tratada profissionalmente.

• A CLASSIFICAÇÃO DA INFORMAÇÃO É de responsabilidade do Chefe/Diretor de cada área que deverão estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

1 – Pública

2 – Confidencial

Toda informação do IMPSJALES deve ser regida pelo princípio da ‘Publicidade’, todavia no ciclo de sua existência é obrigação do Ente Público tratá-la com sigilo e confidencialidade, segundo a Legislação vigente.

Nos casos de processos administrativos disciplinares ou sindicâncias que resultem em punições ou mesmo desligamentos, resguardado o direito ao contraditório, o setor de Recursos Humanos, comunicará o fato o mais rapidamente possível à empresa contratada ou Área de TI, para que o servidor demitido/afastado/suspenso seja bloqueado nos sistemas e acessos que exijam esse procedimento.

4.1 DADOS DOS SERVIDORES: A direção do IMPSJALES não acumulará ou manterá intencionalmente Dados Pessoais de Servidores além daqueles relevantes e exigidos na forma da lei.

4.2 Dados Pessoais de Servidores não serão transferidos para terceiros, exceto quando exigido pela legislação vigente, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos Servidores.

4.3 EQUIPAMENTOS: Os Servidores, por meio de declaração escrita, deverão se comprometer a não armazenar dados pessoais nas instalações dos equipamentos de informática do IMPSJALES, salvo com prévia e expressa autorização por parte da superintendência do Instituto.

Mesmo que seja autorizado o armazenamento destes dados, o IMPSJALES não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos Servidores do IMPSJALES, e jamais poderão fazer parte da rotina de backup.

4.4 ADMISSÃO E DEMISSÃO DE SERVIDORES/ ESTAGIÁRIOS: O setor de Recursos Humanos do IMPSJALES, informará à empresa contratada, ou Área de TI toda e qualquer movimentação de estagiários, admissão/demissão/movimentação de Servidores, para que os mesmos possam ser cadastrados ou excluídos no sistema do IMPSJALES, inclusive o fornecimento de senha ("password") e registro do nome como usuário no sistema (userid), pela empresa contratada, ou Área de TI, ou ainda pelos administradores de sistemas específicos do IMPSJALES.

O IMPSJALES, por meio de seu representante indicado pela superintendência, comunicará à Empresa contratada ou Área de TI sobre as rotinas a que o novo contratado terá direito de acesso. No caso de estagiários informará o tempo em que os mesmos prestarão serviços, para que na data de desligamento possam ser encerradas as atividades relacionadas ao acesso ao sistema.

O setor de Recursos Humanos dará conhecimento e obterá as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação do IMPSJALES.

4.5 PROGRAMAS ILEGAIS: O IMPSJALES respeita os direitos autorais dos programas que usa, não permitindo o uso de programas não licenciados.

4.6 INSTALAÇÃO DE SOFWARE: Os usuários não podem, salvo autorização da superintendência para programas licenciados, instalar "software" (programa) nos equipamentos do IMPSJALES. Periodicamente, a empresa contratada deverá fazer verificações nos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, a superintendência do IMPSJALES deverá ser notificada para as providências necessárias.

A responsabilidade é objetiva e pessoal para aqueles que instalarem em seus computadores de trabalho programas não autorizados e serão responsabilizados por quaisquer problemas ou prejuízos causados, estado sujeitos os sansões previstas neste documento e a sanções previstas no estatuto do servidor municipal.

4.7 PERMISSÕES E SENHAS: Todo usuário para acessar os dados da rede do IMPSJALES, possuirá login e senha previamente cadastrados pela empresa contratada ou Área de TI.

O IMPSJALES indicará a empresa contratada ou Área de TI, por meio de memorando ou e-mail, informando a que tipo de rotinas, acesso a sistemas e programas que os usuários terão direito de acesso.

A empresa contratada ou Área de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro login e após isso a cada 45 (quarenta e cinco) dias. Por segurança, as senhas deverão ter critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

4.8 COMPARTILHAMENTO DE DADOS: Em locais que possuam servidor de rede, não será permitido o compartilhamento de pastas e arquivos através dos computadores e desktops do IMPSJALES. Todos os dados deverão ser armazenados nos servidores da rede.

Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso. Não são permitidos no IMPSJALES o compartilhamento de pastas e arquivos na rede através de dispositivos móveis tais como pendrivers e outros. A exceção são as disponibilizações de cópias digitais de processos aos seus devidos interessados, antecipadas de requerimento próprio ou em cota no processo.

4.9 CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS: Não é política do IMPSJALES o armazenamento de dados inerente as atividades profissionais em desktops individuais. Entretanto, existem alguns programas que não permitem o armazenamento em rede, nestes e em outros casos, a empresa contratada ou Área de TI alertará ao usuário que ele deve fazer backup dos dados de sua máquina periodicamente. (Ex. Outlook).

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos servidores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade da operação do IMPSJALES.

No caso das informações consideradas de fundamental importância para a continuidade dos objetivos do IMPSJALES, a empresa contratada ou Área de TI disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações, mediante análise técnica, econômica e financeira. Estas informações serão incluídas na rotina diária de backup da Informática.

4.10 SEGURANÇA E INTEGRIDADE DOS DADOS: O gerenciamento do(s) banco(s) de dados administrados pela empresa contratada ou Área de TI deverão ter segurança e integridade, assim como a manutenção, alteração e atualização de equipamentos e programas mantidos pelas mesmas.

4.11 PROPRIEDADE INTELECTUAL: É de propriedade do IMPSJALES, todos os “designs”, imagens, criações ou procedimentos desenvolvidos por qualquer servidor durante o curso de seu vínculo empregatício com o Instituto.

4.12 ACESSO INTERNET: será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais no IMPSJALES. Sites que não contenham informações que agreguem conhecimento profissional e/ou para operação das atividades inerentes às funções não devem ser acessados. O uso da Internet deverá ser monitorado pela empresa contratada ou Área de TI, inclusive através de “logs” (arquivos gerados no servidor).
A definição dos Servidores que terão permissão para uso (navegação) da Internet é atribuição da Autarquia. Não será permitido instalar programas provenientes da Internet nos microcomputadores IMPSJALES, sem expressa anuência da empresa contratada ou Área de TI.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando

navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

•. De conteúdo pornográfico ou relacionados a sexo;

•. Que defendam atividades ilegais;

•. Que menosprezem, depreciem ou incitem ao racismo, ao preconceito e a violência;

•. Que veiculem ideologias, filosofias e crenças;

•. Que promovam a participação em salas de discussão de assuntos não relacionados ao IMPSJALES;

•. Que promovam discussão pública sobre assuntos internos do IMPSJALES, a menos que autorizado pela superintendência;

• Que possibilitem a distribuição de informações de nível “Confidencial”;

•. Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

4.13 USO DO CORREIO ELETRÔNICO (E-MAIL): O correio eletrônico fornecido pelo IMPSJALES é um instrumento de comunicação interna e externa para a realização das atividades relativas à Autarquia. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do instituto, não podem ser contrárias à legislação vigente e nem aos princípios éticos do IMPSJALES.
O uso do correio eletrônico é de caráter pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

• . Contenham declarações difamatórias e linguagem ofensiva;

•. Possam trazer prejuízos a outras pessoas;

•. Sejam hostis e inúteis;

• Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;

• . Possam prejudicar a imagem da organização;

•. Possam prejudicar a imagem de outras empresas;

•. Sejam incoerentes com as políticas do IMPSJALES.

Para incluir um novo usuário no correio eletrônico, o IMPSJALES encaminhará pedido formal à empresa contratada ou Área de TI, que providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Visando evitar congestionamento no Sistema de correio eletrônico a empresa contratada ou Área de TI fará auditorias nas estatísticas de uso.

A Empresa contratada ou Área de TI poderá, visando evitar a entrada de vírus no IMPSJALES, bloquear o recebimento de e-mails provenientes de sites gratuitos ou mensagens detectadas como SPAM e/ou MALWARE e outras definições para mensagens que possam prejudicar o funcionamento dos sistemas do IMPSJALES.

4.14 NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS: A empresa contratada ou Área de TI é responsável pela aplicação da Política do IMPSJALES auxiliará na definição de compra e substituição de “software” e “hardware”, de acordo com a disponibilidade e cronograma orçamentária do IMPS JALES.

4.15 USO DE NOTEBOOK NO IMPSJALES: Os usuários que tiverem direito ao uso de computadores pessoais (notebook), ou qualquer outro equipamento computacional, de propriedade do IMPSJALES devem estar cientes de que:

•. Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.

• A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.

• É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

• O usuário não deve alterar a configuração do equipamento recebido e não instalar programas para compartilhamento de arquivos;

•. Em casos onde o equipamento é de propriedade do servidor este deve respeitar esta política de segurança, caso contrário a equipe de TI terá permissão para bloquear o acesso deste equipamento.

•. Em caso de furto, deverá ser registrada a ocorrência em uma delegacia de polícia;

•. Comunique ao seu superior imediato e à empresa contratada ou Área de TI;

•. Envie uma cópia da ocorrência para a empresa contratada ou Área de TI.

4.16 RESPONSABILIDADE DOS SUPERIORES HIERARQUICOS: Os encarregados, chefes de cessões, são responsáveis pelas definições dos direitos de acesso de seus servidores aos sistemas e informações do IMPSJALES, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política. Será definida a hierarquia necessária para realização desta tarefa em cada secretaria.

A empresa contratada ou Área de TI fará auditorias periódicas do acesso dos usuários às informações, verificando:

•. Que tipo de informação o usuário pode acessar;

•. Quem está autorizado a acessar determinada rotina e/ou informação;

•. Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;

4.17 USO DE ANTIVÍRUS: Todo arquivo em mídia proveniente de entidade externa ao IMPSJALES deve ser verificado por programa antivírus. 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, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

4.18 PENALIDADES: O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar em: advertência formal, suspensão, rescisão do contrato de estágio, exoneração, outra ação disciplinar e/ou processo civil ou criminal, tendo como parâmetro o estatuto do servidor, a legislação municipal e demais leis pertinentes.

Jales-SP, 17 de Julho de 2.021.

Claudir Balestreiro

Superintendente

ANEXO I

CIÊNCIA DOS SERVIDORES

Nome: Identidade: CPF: Cargo: Função:	Assinatura

Nome: Identidade: CPF: Cargo: Função:	Assinatura