Manual do Procedimento de Política de Segurança da Informação

001/ 2025

Mapeamento e Manualização de Processos

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ILHA SOLTEIRA – SÃO PAULO

SUMÁRIO

1 INTRODUÇÃO **4**

2 OBJETIVOS **5**

3 NORMAS APLICÁVEIS **5**

4 HABILITAÇÃO **6**

5 DIRETRIZES **6**

5.1 Da política de segurança da informação 7

5.1.1 Divulgação 7

5.1.2 Atualização e Revisão 8

5.1.3 Propriedade Intelectual 8

6 BOAS PRÁTICAS **8**

6.1 Impressão de Documentos 8

6.2 Da Comunicação Verbal e Institucional 9

7 DA SEGURANÇA **9**

7.1 Ambiente Físico 9

7.2 Ambiente Computacional 10

7.2.1 Do Acesso 10

7.2.2 Das Credenciais 11

7.2.3 Da Execução de Programas e Instalação de Softwares 11

7.2.4 Da Navegação na Internet 12

7.2.5 Do Acesso Remoto 13

7.2.6 Da Conexão Wireless Fidelity (Wi-Fi) 13

7.2.7 Do Acesso ao Web E-mail 13

8 PLANO DE CONTINGÊNCIA **15**

8.1.1 Servidor 15

8.1.2 Memória RAM e Backup 16

8.1.3 Acesso à Internet e Rede Interna 16

8.1.4 Alimentação – Energia Elétrica 17

9 VIOLAÇÕES **17**

10 SANÇÕES **17**

11 CONCLUSÃO **18**

REFERÊNCIAS **19**

1. INTRODUÇÃO

A crescente utilização de tecnologias da informação no âmbito da administração pública tem ampliado significativamente a produção, o armazenamento e o tratamento de dados, especialmente aqueles de natureza pessoal e sensível. No contexto dos regimes próprios de previdência social, essa realidade torna-se ainda mais crítica, considerando a responsabilidade institucional na guarda de informações cadastrais, financeiras e funcionais de servidores ativos, aposentados e pensionistas. Diante desse cenário, a segurança da informação configura-se como um elemento estratégico para a continuidade dos serviços, a confiabilidade institucional e o cumprimento das obrigações legais.

A Política de Segurança da Informação (PSI) constitui um conjunto de diretrizes, normas e procedimentos voltados à proteção dos ativos informacionais de uma organização, assegurando os princípios da confidencialidade, integridade e disponibilidade das informações. De acordo com normas internacionais amplamente adotadas, a formalização dessas diretrizes é essencial para estabelecer responsabilidades, orientar comportamentos e reduzir riscos relacionados a acessos não autorizados, vazamentos de dados e falhas operacionais (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2022).

No setor público, a manualização da Política de Segurança da Informação assume papel fundamental ao padronizar práticas, garantir transparência administrativa e promover a conformidade com a legislação vigente. No Brasil, a promulgação da Lei Geral de Proteção de Dados Pessoais reforçou a necessidade de adoção de mecanismos institucionais capazes de proteger dados pessoais tratados por entes públicos, exigindo a implementação de políticas claras, procedimentos documentados e medidas técnicas e administrativas adequadas (BRASIL, 2018).

Nesse sentido, a elaboração de um manual de Política de Segurança da Informação para o Instituto de Previdência Municipal de Ilha Solteira surge como instrumento essencial para orientar servidores, colaboradores e prestadores de serviço quanto ao uso adequado dos recursos tecnológicos e ao tratamento

responsável das informações institucionais. A manualização permite consolidar normas internas, definir níveis de acesso, estabelecer protocolos de resposta a incidentes e fomentar uma cultura organizacional voltada à segurança da informação.

Além disso, a existência de um documento formalizado contribui para o fortalecimento da governança institucional, auxiliando na prevenção de riscos operacionais, jurídicos e reputacionais. Conforme destacam estudos na área de governança de tecnologia da informação, políticas bem estruturadas e devidamente difundidas reduzem vulnerabilidades, aumentam a eficiência administrativa e favorecem a tomada de decisões baseadas em critérios técnicos e normativos (FERNANDES; ABREU, 2014).

Dessa forma, este trabalho tem como objetivo apresentar a manualização da Política de Segurança da Informação no Instituto de Previdência Municipal de Ilha Solteira (IPREM-ISA), evidenciando sua importância como ferramenta de gestão, conformidade legal e proteção dos ativos informacionais, em consonância com as boas práticas recomendadas por normas técnicas e pela legislação brasileira.

2. OBJETIVOS

O presente documento tem como objetivo estabelecer e formalizar a manualização da Política de Segurança da Informação no Instituto de Previdência Municipal de Ilha Solteira, visando à proteção dos ativos informacionais, à garantia da confidencialidade, integridade e disponibilidade das informações, bem como ao atendimento das exigências legais e normativas aplicáveis à administração pública.

3. NORMAS APLICÁVEIS

A seguir, são elencados os principais dispositivos legais que fundamentam e orientam os procedimentos de política e segurança da informação.

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.
- Lei nº 12.527/2011 – Lei de Acesso à Informação.
- Lei nº 8.429/1992 – Lei de Improbidade Administrativa.

- Decreto nº 10.222/2020 – Institui a Estratégia Nacional de Segurança Cibernética.
- ABNT NBR ISO/IEC 27001:2022.
- ABNT NBR ISO/IEC 27002:2022.
- Tribunal de Contas do Estado de São Paulo – Diretrizes e recomendações aplicáveis à administração pública.
- Secretaria de Governo Digital – Normas e orientações de governança digital e segurança da informação.

4. HABILITAÇÃO

Todos os servidores, prestadores de serviços, consultores, auditores, trabalhadores temporários, fornecedores, parceiros institucionais e demais profissionais contratados que atuem em nome do Instituto de Previdência Municipal de Ilha Solteira e que tenham acesso ou façam uso de seus ativos corporativos.

É dever de todos os usuários cumprir integralmente a Política de Segurança da Informação vigente, buscar orientação junto ao responsável pela área de Tecnologia da Informação sempre que houver dúvidas relacionadas à segurança da informação, proteger as informações contra acessos, alterações, destruição ou divulgação não autorizadas, assegurar que os recursos tecnológicos disponibilizados sejam utilizados exclusivamente para as finalidades previamente autorizadas, observar e cumprir a legislação e as normas aplicáveis aos direitos de propriedade intelectual, bem como comunicar imediatamente ao Instituto de Previdência Municipal de Ilha Solteira.

5. DIRETRIZES

As diretrizes da Segurança da Informação no Instituto de Previdência Municipal de Ilha Solteira têm por finalidade assegurar a proteção dos ativos informacionais, observando, de forma prioritária, os princípios da confidencialidade, da integridade e da disponibilidade das informações. A confidencialidade garante que as informações sejam acessadas exclusivamente por usuários devidamente autorizados; a integridade assegura que os dados sejam mantidos íntegros, completos e protegidos contra alterações indevidas; e a disponibilidade visa garantir que as informações

estejam acessíveis sempre que necessárias ao desempenho das atividades institucionais.

O acesso às informações e aos sistemas informatizados deve ser restrito a usuários autorizados, em conformidade com o princípio do menor privilégio e com as atribuições funcionais de cada agente. O uso dos recursos de tecnologia da informação e comunicação deve ocorrer de forma adequada, ética e responsável, sendo vedada a utilização para fins estranhos às atividades institucionais.

A instituição deve adotar medidas técnicas e administrativas destinadas à proteção dos dados pessoais e sensíveis tratados em seus sistemas, em consonância com a legislação vigente, especialmente no que se refere à proteção de dados pessoais. Devem ser estabelecidos procedimentos para a prevenção, a detecção, o registro e o tratamento de incidentes de segurança da informação, garantindo respostas adequadas às ocorrências identificadas.

As responsabilidades relacionadas à segurança da informação devem ser claramente definidas e observadas por servidores, colaboradores e prestadores de serviço, os quais devem atuar em conformidade com as normas internas e com os princípios que regem a administração pública. A instituição deve promover ações contínuas de conscientização e capacitação dos usuários, visando à disseminação das boas práticas de segurança da informação.

Devem ser observados critérios para o armazenamento, o compartilhamento, a transmissão e o descarte seguro das informações, assegurando a rastreabilidade e o monitoramento das ações realizadas nos sistemas institucionais. Além disso, devem ser adotadas medidas que garantam a continuidade dos serviços e a recuperação das informações em situações de falhas, incidentes ou desastres.

Por fim, todas as diretrizes devem estar alinhadas às normas técnicas, aos dispositivos legais vigentes e às orientações dos órgãos de controle, contribuindo para o fortalecimento da governança institucional e para a mitigação de riscos operacionais, legais e reputacionais.

5.1 DA POLITICA DE SEGURANÇA DA INFORMAÇÃO

5.1.1. DIVULGAÇÃO

É responsabilidade da Superintendência assegurar a ampla divulgação da Política de Segurança da Informação no âmbito do Instituto de Previdência Municipal

de Ilha Solteira, de modo a garantir seu conhecimento e cumprimento por todos os servidores e colaboradores. Eventuais ocorrências ou suspeitas de violação da segurança da informação devem ser comunicadas de forma imediata aos responsáveis designados, sem prejuízo da aplicação das penalidades cabíveis, conforme a legislação vigente.

5.1.2. ATUALIZAÇÃO E REVISÃO

Compete à Superintendência, com o apoio da Procuradoria Jurídica, a responsabilidade pelos ajustes, melhorias, aprimoramentos e modificações desta Política, a qual deverá ser revisada sempre que necessário, mediante demanda específica, devendo todas as alterações realizadas ser devidamente registradas.

5.1.3. PRORIEDADE INTELECTUAL

Pertencem ao Instituto de Previdência Municipal de Ilha Solteira todos os materiais, produtos, subprodutos, designs, criações, métodos ou procedimentos desenvolvidos por qualquer servidor no exercício de suas atividades e durante a vigência de seu vínculo institucional com o IPREM-ISA.

6. BOAS PRÁTICAS

6.1. IMPRESSÃO DE DOCUMENTOS

Os documentos impressos que contenham informações institucionais, dados pessoais ou informações sensíveis devem ser manuseados com cautela, evitando-se o acesso por pessoas não autorizadas. Recomenda-se que a retirada de impressões seja imediata, não devendo documentos permanecerem expostos em impressoras, mesas ou locais de circulação comum. Os equipamentos de impressão devem ser utilizados de forma consciente, evitando desperdícios de papel, tinta ou toner, contribuindo para a sustentabilidade ambiental e para a redução de custos operacionais.

Documentos impressos que perderem sua finalidade administrativa ou que não necessitem mais de guarda devem ser descartados de forma segura, preferencialmente por meio de fragmentação ou outro método que impeça a reconstrução das informações. O descarte inadequado de documentos que

contenham dados institucionais ou pessoais configura falha de segurança da informação e poderá ensejar a aplicação de medidas administrativas cabíveis.

6.2. DA COMUNICAÇÃO VERBAL E INSTITUCIONAL

A comunicação verbal e institucional no Instituto de Previdência Municipal de Ilha Solteira deve observar os princípios da ética, da responsabilidade e da segurança da informação, assegurando que as informações institucionais sejam compartilhadas apenas com pessoas autorizadas e por meio de canais oficiais, quando aplicável.

- As informações institucionais devem ser transmitidas de forma clara, objetiva e restrita aos interlocutores autorizados.
- É vedada a divulgação de informações institucionais, pessoais ou sensíveis em locais públicos ou a pessoas não autorizadas.
- Comunicações verbais devem ser realizadas com cautela, evitando-se o compartilhamento de informações sigilosas por meios informais ou inseguros.
- A comunicação institucional deve ocorrer exclusivamente por meio dos canais oficiais da instituição e para fins relacionados às atividades institucionais.
- A divulgação de informações ao público externo ou à imprensa deve ocorrer somente mediante autorização da Superintendência ou da autoridade competente conforme a legislação vigente.
- O uso dos meios institucionais para fins particulares é vedado.
- O compartilhamento indevido de informações poderá ensejar a aplicação das penalidades cabíveis, conforme a legislação vigente.

7. DA SEGURANÇA

7.1. AMBIENTE FÍSICO

O ambiente físico destinado à infraestrutura de tecnologia da informação do IPREM é devidamente protegido e consiste em Data Center localizado na sede do Instituto, entendido como o espaço físico controlado e seguro destinado à instalação e operação de servidores e demais equipamentos responsáveis pelo armazenamento, processamento e funcionamento dos sistemas institucionais, sendo esse ambiente

protegido por sistema de monitoramento contínuo e submetido a controles específicos de acesso, permitidos exclusivamente a pessoas previamente autorizadas.

O ingresso de visitantes, prestadores de serviços, terceiros ou servidores sem autorização formal para acesso às áreas restritas somente ocorrerá mediante acompanhamento permanente de pessoa devidamente autorizada, devendo ser rigorosamente respeitadas as áreas de acesso restrito, sendo vedada qualquer tentativa de acesso não autorizado, bem como a utilização de equipamentos ou recursos tecnológicos em desacordo com as permissões estabelecidas para cada categoria de colaboradores.

7.2. AMBIENTE COMPUTACIONAL

Todo o acesso às informações, bem como ao ambiente computacional e aos sistemas de informação, deve ser devidamente controlado, de forma a assegurar que somente pessoas previamente autorizadas possam utilizá-los, devendo as autorizações concedidas ser objeto de revisão contínua e periódica.

Os dados, as informações e os sistemas de informação do IPREM ISA devem ser protegidos contra ameaças e ações não autorizadas, sejam elas intencionais ou acidentais, com o objetivo de reduzir riscos e garantir a integridade, a confidencialidade e a disponibilidade desses ativos informacionais.

7.2.1 DO ACESSO

Qualquer usuário poderá utilizar as estações de trabalho do IPREM mediante autenticação com credenciais próprias, sendo-lhe assegurado acesso exclusivamente aos recursos e permissões previamente concedidos pelo controlador de domínio, de forma individualizada e em conformidade com suas atribuições funcionais. O acesso à estação de trabalho deverá ser encerrado ao final do expediente, mediante o desligamento do equipamento. Durante ausências temporárias do posto de trabalho, o usuário deverá bloquear a estação de trabalho, sendo obrigatória a digitação da senha de acesso para o desbloqueio e retomada das atividades.

As estações de trabalho constituem ferramentas corporativas e, portanto, devem ser utilizadas exclusivamente para fins profissionais e no desempenho das atividades institucionais. Estas não possuem cópias de segurança, não se responsabilizando o

IPREM por eventuais perdas de informações de natureza não corporativa nelas armazenadas.

7.2.2 DAS CREDENCIAIS

As permissões de acesso aos sistemas e recursos computacionais devem ser concedidas de acordo com o princípio do menor privilégio, assegurando que cada usuário disponha apenas das autorizações estritamente necessárias para o desempenho de suas atribuições.

É vedado o compartilhamento de login e senha entre colaboradores, sendo o uso de credenciais de terceiros prática expressamente proibida e passível de responsabilização, nos termos do Código Penal Brasileiro, especialmente o art. 307, que trata do crime de falsa identidade. É proibido o compartilhamento de credenciais com privilégios de administração de rede, computadores ou sistemas, bem como a concessão de tais privilégios a contas de usuários comuns, salvo quando formalmente autorizado e justificado.

Como boa prática de segurança da informação, recomenda-se que, no primeiro acesso ao ambiente de rede local, o usuário seja imediatamente direcionado à alteração de sua senha inicial. A guarda, a confidencialidade e a memorização da senha, bem como a proteção dos dispositivos de identificação eventualmente designados, como tokens, são de responsabilidade exclusiva do usuário. Os usuários poderão alterar sua própria senha a qualquer tempo e deverão fazê-lo sempre que houver suspeita de comprometimento ou acesso indevido às suas credenciais. Na hipótese de esquecimento da senha, o usuário deverá solicitar formalmente a geração de uma senha provisória ao respectivo provedor de *software*, a qual deverá ser obrigatoriamente redefinida no primeiro acesso ao sistema.

7.2.3 DA EXECUÇÃO DE PROGRAMAS E INSTALAÇÃO DE *SOFTWARES*

É vedada a execução de programas destinados à decodificação de senhas, ao monitoramento indevido da rede, à leitura não autorizada de dados de terceiros, à propagação de códigos maliciosos, bem como à destruição, total ou parcial, de arquivos ou à indisponibilidade de serviços.

Também é proibido executar programas, instalar equipamentos, armazenar arquivos ou praticar quaisquer ações que possam facilitar o acesso de usuários não autorizados à rede corporativa do IPREM.

O IPREM observa e respeita os direitos autorais dos *softwares* utilizados em seu ambiente computacional, sendo vedado o uso de programas não licenciados nos computadores institucionais. É terminantemente proibida a utilização de softwares ilegais ou sem o devido licenciamento, sendo permitida exclusivamente a instalação e o uso de softwares previamente autorizados e destinados à execução das atividades laborais correspondentes a cada cargo ou função.

7.2.4 DA NAVEGAÇÃO NA INTERNET

É expressamente proibida a divulgação, o compartilhamento ou a exposição indevida de informações sigilosas ou institucionais em listas de discussão, fóruns, aplicativos de mensagens instantâneas ou salas de bate-papo. O download de arquivos provenientes da Internet somente será permitido quando estritamente necessário ao desempenho das atividades profissionais, devendo ser observados os termos de licenciamento, uso e registro dos respectivos softwares.

Os usuários deverão utilizar a Internet de forma adequada, responsável e diligente, em conformidade com a legislação vigente, a moral, os bons costumes e a ordem pública, sendo vedada sua utilização como meio ou finalidade para a prática de atos ilícitos, proibidos por lei ou por esta Política, bem como de atos que possam causar prejuízo ao IPREM ou a terceiros, ou que possam danificar, inutilizar, sobrecarregar ou deteriorar recursos tecnológicos, sistemas, documentos ou arquivos, próprios ou de terceiros.

Cada usuário é pessoalmente responsável por todas as atividades realizadas mediante suas credenciais de acesso, sendo expressamente proibida a utilização de softwares de compartilhamento de arquivos do tipo peer-to-peer (P2P), tais como Torrent, Kazaa, Emule ou similares, bem como o acesso a sítios eletrônicos que disponibilizem conteúdos obscenos, pornográficos, eróticos, racistas, nazistas ou qualquer outro que viole a legislação vigente.

7.2.5 DO ACESSO REMOTO

O acesso remoto aos sistemas e recursos computacionais do IPREM é restrito e, quando houver necessidade de sua utilização por servidores ou terceiros, deverá ser previamente com a devida justificativa, a identificação do equipamento a ser acessado e o período pretendido para o acesso, cabendo à área competente a avaliação e a autorização ou não da solicitação. Em nenhuma hipótese o acesso remoto será concedido ou mantido em caráter permanente, devendo sempre observar prazo determinado e finalidade específica.

7.2.6 DA CONEXÃO *WIRELESS FIDELITY (WI-FI)*

O acesso à rede *Wi-Fi* institucional do IPREM é restrito e destinado exclusivamente a usuários previamente autorizados e devidamente autenticados. A concessão de acesso deverá observar critérios de segurança definidos, sendo vedado o compartilhamento de senhas ou a conexão de dispositivos não autorizados.

7.2.7 DO ACESSO AO *WEB E-MAIL*

O acesso a serviços de correio eletrônico externos, gratuitos ou pagos, que possibilitem o envio e o recebimento de mensagens por meio da tecnologia webmail, deverá ser realizado com extrema cautela e de forma moderada, considerando que tais acessos podem representar riscos à segurança das informações institucionais do IPREM ISA. Considerando que os acessos a contas de e-mail pessoais, quando realizados por meio da infraestrutura tecnológica do IPREM ISA, utilizam conexão à internet pertencente à Instituição, cujo endereço IP estará vinculado ao Instituto, o uso inadequado desses serviços poderá acarretar responsabilidades institucionais, justificando-se, assim, a necessidade de cautela por parte dos usuários;

- Na hipótese de o acesso a contas de e-mail pessoais ocasionar qualquer tipo de dano ao IPREM ISA, o usuário será integralmente responsabilizado por seus atos, respondendo nas esferas civil e criminal, nos termos da legislação vigente;
- É expressamente vedado o envio, por meio de contas de e-mail pessoais, de informações, dados ou arquivos que estejam direta ou indiretamente relacionados aos interesses institucionais do IPREM ISA;

- O correio eletrônico constitui a ferramenta oficial de comunicação institucional do IPREM ISA, sendo destinado à formalização das comunicações internas e externas, devendo seu uso ocorrer prioritariamente em benefício do serviço público e no interesse institucional;
- Todos os usuários do IPREM ISA deverão utilizar o serviço de correio eletrônico com conduta ética, responsável e profissional, observando as normas internas e a finalidade institucional do recurso;
- As contas de correio eletrônico possuem titularidade individual, sendo cada usuário diretamente responsável pelas mensagens enviadas e recebidas por intermédio de seu endereço eletrônico institucional;
- O correio eletrônico deverá ser utilizado de forma diligente, adequada e compatível com os objetivos institucionais, sendo vedada qualquer utilização que extrapole os limites do interesse funcional;
- É proibido o acesso não autorizado à caixa postal de outro usuário, bem como qualquer tentativa de violação da confidencialidade das comunicações eletrônicas institucionais;
- É vedado o envio, armazenamento ou manuseio de conteúdos que contrariem a legislação vigente, a moral, os bons costumes ou a ordem pública;
- Não será permitida a utilização do correio eletrônico para a divulgação, incentivo ou prática de atos ilícitos, proibidos por lei ou pelas normas institucionais, nem para atividades que possam causar danos aos direitos e interesses do IPREM ISA ou de terceiros, ou que comprometam o funcionamento dos recursos tecnológicos e informacionais; Nem tampouco o envio ou armazenamento de conteúdos que promovam ou incentivem ameaças, difamação, assédio, discriminação de qualquer natureza, bem como a divulgação de material obsceno, ofensivo ou que viole direitos autorais;
- O uso do correio eletrônico institucional para fins comerciais, para assuntos estritamente pessoais ou privados de forma excessiva, bem como para o envio de mensagens do tipo “corrente” ou “spam”, é expressamente vedado;

- É proibido o envio intencional de mensagens que contenham vírus, códigos maliciosos ou quaisquer rotinas de programação capazes de causar danos aos sistemas, equipamentos ou dados institucionais;
- Recomenda-se evitar o uso do correio eletrônico institucional para assuntos de natureza pessoal, bem como a abertura ou execução de arquivos anexos provenientes de remetentes desconhecidos ou suspeitos, especialmente aqueles com extensões potencialmente perigosas, conforme orientações da área de Tecnologia da Informação;

O correio eletrônico deverá ser utilizado, preferencialmente, para comunicações internas e externas oficiais que não exijam obrigatoriamente o uso de meio físico, contribuindo para a redução de custos operacionais e o aumento da eficiência administrativa. Todas as mensagens geradas ou transmitidas por meio dos recursos de comunicação institucional são de propriedade do IPREM ISA, podendo seu uso ser monitorado, verificado ou auditado, em conformidade com a legislação aplicável e com as normas internas de segurança da informação.

8. PLANO DE CONTINGÊNCIA

O Plano de Contingência fundamenta-se no princípio da redundância em Tecnologia da Informação, compreendida como a duplicação de componentes críticos, visando aumentar a confiabilidade, a segurança e a disponibilidade dos sistemas e dos dados institucionais. Durante a ativação do Plano de Contingência, poderá ocorrer redução temporária de desempenho dos sistemas, sendo priorizados os serviços essenciais, tais como concessão de benefícios, folha de pagamento, contabilidade e atividades financeiras.

8.1.1 SERVIDOR

A infraestrutura tecnológica do IPREM é composta por servidores físicos e recursos configurados para alta disponibilidade, permitindo a manutenção, o remanejamento de serviços ou a redistribuição de cargas entre servidores e equipamentos compatíveis, de modo a preservar o funcionamento operacional.

8.1.2 MEMÓRIA RAM E *"BACKUP"*

O servidor do IPREM opera com capacidade de memória superior à necessária para suportar, quando requerido, a execução dos serviços de outro servidor que eventualmente apresente falha de memória. Na ocorrência de falha na memória RAM, poderão ser adotadas, conforme a necessidade e a disponibilidade, as seguintes medidas:

- substituição do módulo de memória RAM defeituoso, quando houver disponibilidade imediata;
- remoção do módulo defeituoso, com consequente redução da capacidade de memória do servidor afetado;
- remanejamento de módulo de memória de outro servidor, com a correspondente redução da capacidade de memória do servidor doador;
- transferência parcial ou total dos serviços de um servidor para outro, de modo a assegurar a continuidade do ambiente operacional.

O serviço de *backup* consiste na realização de cópias de segurança dos arquivos, com a finalidade de possibilitar sua restauração no menor tempo possível em caso de necessidade. Para garantir a segurança da informação, são executadas cópias de segurança diárias dos dados armazenados em servidores, sistemas de *softwares* e respectivos bancos de dados utilizados pelo IPREM, de modo a assegurar a integridade, a disponibilidade e a confiabilidade das informações institucionais.

8.1.3. ACESSO A INTERNET E REDE INTERNA

O acesso à internet no Instituto de Previdência Municipal de Ilha Solteira é realizado por meio de conexão cabeada nos computadores institucionais, garantindo maior estabilidade e segurança para a execução das atividades administrativas. Paralelamente, a instituição dispõe de rede sem fio (Wi-Fi), disponibilizada de forma controlada e restrita a dispositivos autorizados, permitindo a mobilidade necessária às rotinas institucionais. Ambas as modalidades de conexão contam com mecanismos de controle e monitoramento, contribuindo para a continuidade dos serviços e para a proteção das informações institucionais.

8.1.4. ALIMENTAÇÃO – ENERGIA ELÉTRICA

O servidor utilizado pelo Instituto de Previdência Municipal de Ilha Solteira conta com estabilizador de energia, o qual atua na proteção dos equipamentos contra variações e oscilações na rede elétrica. Esse recurso contribui para a preservação da integridade dos sistemas e das informações armazenadas, bem como para a redução de riscos de falhas ou danos decorrentes de interrupções ou instabilidades no fornecimento de energia elétrica.

9. VIOLAÇÕES

Constituem infrações à política, às normas e aos procedimentos de Segurança da Informação, dentre outras, as seguintes condutas ou ocorrências:

- Toda e qualquer ação ou situação que possa resultar, de forma direta ou indireta, efetiva ou potencial, em prejuízos financeiros ou danos à imagem institucional do IPREM ISA ou de seus segurados, comprometendo a confidencialidade, a integridade ou a disponibilidade de seus ativos de informação;
- O uso inadequado de dados institucionais, bem como a divulgação de informações sem a devida autorização da Superintendência, em desacordo com as diretrizes estabelecidas pela Instituição;
- A utilização de dados, informações, equipamentos, softwares, sistemas ou quaisquer outros recursos tecnológicos para finalidades ilícitas ou incompatíveis com as normas vigentes, incluindo práticas que violem a legislação aplicável, regulamentos internos ou externos, princípios éticos ou exigências impostas por órgãos reguladores relacionados à área de atuação do IPREM ISA ou de seus segurados;
- A omissão na comunicação imediata à Superintendência acerca de eventuais descumprimentos da política, das normas ou dos procedimentos de Segurança da Informação, dos quais servidores, segurados, estagiários ou prestadores de serviços tenham conhecimento ou presenciem.

10. SANÇÕES

O servidor que incorrer em infração poderá ser formalmente notificado, devendo a ocorrência ser comunicada de imediato ao seu superior hierárquico, à

respectiva Diretoria e à Presidência da Instituição, sendo tal conduta caracterizada como falta grave.

11. CONCLUSÃO

A manualização da Política de Segurança da Informação no Instituto de Previdência Municipal de Ilha Solteira é fundamental para garantir a proteção dos ativos informacionais e a conformidade com as normas e dispositivos legais vigentes. Ao estabelecer diretrizes claras e responsabilidades definidas, o documento contribui para a prevenção de incidentes, o fortalecimento da governança institucional e a promoção de uma cultura organizacional voltada à segurança da informação, assegurando a continuidade dos serviços e a confiabilidade institucional.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**:2022. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2022**. Tecnologia da informação — Técnicas de segurança — Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Diário Oficial da União: Brasília, DF, 6 fev. 2020.

BRASIL. **Lei nº 8.429, de 2 de junho de 1992.** Diário Oficial da União: Brasília, DF, 3 jun. 1992.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Diário Oficial da União: Brasília, DF, 18 nov. 2011.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a governança de TI: da estratégia à gestão dos processos e serviços.** 4. ed. Rio de Janeiro: Brasport, 2014.