INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE TERESINA

MANUAL DOS PROCEDIMENTOS DE CONTINGÊNCIA DAS INFORMAÇÕES

TERESINA, 2026.

SUMÁRIO

1. TERMOS UTILIZADOS

- **FISHING:** Termo que define a atividade de tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outras, por meio de e-mail com conteúdo duvidoso;
- **TORRENT:** É a extensão dos arquivos compatíveis com o protocolo de compartilhamento BitTorrent, uma tecnologia criada pela empresa também chamada BitTorrent, introduzida em 2001. Ela funciona criando uma rede P2P (ponto a ponto) entre todos os usuários do protocolo, com o intuito de distribuir arquivos entre todos os usuários da rede;
- **MALWARE:** É um termo amplo que é usado para classificar todo tipo de software malicioso usado para causar prejuízo, danificar sistemas, interceptar dados ou simplesmente irritar o usuário, afetando tanto computadores como celulares e até redes inteiras.

2. SIGLAS UTILIZADAS

- **IPMT:** Instituto de Previdência dos Servidores do Município de Teresina;
- **PRODATER:** Entidade Autárquica de Teresinense de Processamento de Dados;
- **P2P:** Point to point (ponto a ponto);
- **GTI:** Gerência de Tecnologia da Informação;
- **TI:** Tecnologia da Informação;
- **LGPD:** Lei Geral de Proteção de Dados Pessoais;
- **GDPR:** Regulamento Geral de Proteção de Dados;
- **SEI:** Sistema Eletrônico de Informações;
- **DOM:** Diário Oficial do Município de Teresina;
- **PSI:** Política de Segurança da Informação;
- **MAC:** Media Acess control.

3. UNIDADE RESPONSÁVEL

Gerência de Tecnologia da Informação (GTI) do Instituto de Previdência dos Servidores Municipais de Teresina-IPMT.

4. PRÁTICAS RECOMENDADAS PARA SEGURANÇA E CONTINGÊNCIA DE INFORMAÇÕES

4.1. Procedimentos básicos de prevenção de contingências:

4.1.1. Mantenha o software atualizado: Certifique-se de que seu sistema operacional, navegadores, antivírus e outros programas estejam sempre atualizados com as últimas correções de segurança;

4.1.2. Cuidado com phishing: Esteja atento a e-mails, mensagens ou links suspeitos. Os criminosos frequentemente usam táticas de phishing para enganar as pessoas e obter informações confidenciais. Não clique em links suspeitos ou forneça informações pessoais a sites não confiáveis;

4.1.3. Proteja sua identidade: Não compartilhe informações pessoais, como números de documento de identidade, números de seguro social ou detalhes bancários, em sites ou com pessoas que você não conhece pessoalmente. Além disso, informações de acesso físico e lógico (a exemplo de logins e senhas) devem manter-se restritas, sendo de responsabilidade de cada usuário zelar pela sua confidencialidade.

4.1.4. Downloads seguros: Somente baixe software, aplicativos e arquivos de fontes confiáveis. Evite sites de pirataria e torrents, pois eles podem conter malware;

4.1.5. Faça backup periodicamente: É fundamental que cada usuário também faça e mantenha cópias de segurança regularmente de seus dados importantes. Isso pode ajudar a recuperar informações em caso de ataques de malware ou perda de dados, evitando maiores perdas e retrabalho.

4.1.6. Nos termos do art. 27, § 2°, do Decreto n° 24.514/2023, a PRODATER é responsável pelo SEI, cabendo à PRODATER, entre outras atribuições, gerenciar o sistema de permissões, cadastrar e gerenciar usuários, estabelecer e gerenciar os perfis de acesso, acompanhar a segurança de acesso e de armazenamento digital dos dados e a preservação e integridade

dos dados armazenados eletronicamente. Já conforme a cláusula oitava do Contrato n° 09/2023 e o Termo de Referência vinculado à contratação, o Sistema Previdenciário (Sisprev) é de responsabilidade da empresa Agenda Assessoria, Planejamento e Informática Ltda, de forma que, quanto ao SEI e ao Sisprev, cabe à PRODATER e à Agenda, respectivamente, o controle de acesso físico e lógico e o back-up dos respectivos dados. Outrossim, e nos termos do art. 60 do Regimento Interno do IPMT, a Equipe Funcional de Tecnologia do IPMT supervisiona tais atividades e também atua para promover a confidencialidade, integridade e disponibilidade das informações (inclusive quanto aos controles de acessos físico e lógico).

4.2. Equipes Funcionais de Tecnologia

4.2.1. As equipes funcionais de tecnologia são grupos de profissionais especializados em diferentes áreas da Tecnologia da Informação, como desenvolvimento de software, infraestrutura de TI e suporte técnico, entre outras. Essas equipes trabalham juntas para garantir que a infraestrutura de tecnologia da organização funcione de maneira eficaz e que os sistemas de TI atendam às necessidades da instituição. No caso do IPMT, a equipe é formada por Técnicos de Informática, Programadores e Analistas de Sistemas.

4.3. Estratégia de Tecnologia e Gestão de Projetos e Processos

4.3.1. É o planejamento de longo prazo do Instituto em relação ao uso da tecnologia para alcançar seus objetivos de negócios. A gestão de projetos e processos envolve a coordenação e o controle das iniciativas de tecnologia, desde o desenvolvimento de novos sistemas até a melhoria dos processos existentes.

4.4. Segurança da Informação e Conformidade

4.4.1. É a proteção dos dados e sistemas do Instituto contra ameaças internas e externas, como hackers e vazamentos de dados;

4.4.2. A conformidade refere-se ao cumprimento das regulamentações e padrões de segurança, como o Regulamento Geral de Proteção de Dados (GDPR), a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Política de Segurança da Informação (PSI) do IPMT.

4.5. Gestão de Recursos e Orçamento

4.5.1. A gestão de recursos envolve a alocação eficiente de recursos, como pessoal, hardware e software, para atender às necessidades de tecnologia da empresa. A gestão de orçamento está relacionada ao planejamento e controle dos gastos com tecnologia, garantindo que os investimentos sejam feitos de forma adequada e que os recursos estejam disponíveis quando necessários.

4.6. Inovação e Pesquisa

4.6.1. A inovação é o processo de desenvolvimento e implementação de novas ideias, tecnologias ou métodos para melhorar os produtos, serviços ou processos da empresa. A pesquisa envolve a busca por novas tecnologias e tendências que possam beneficiar a organização a longo prazo.

4.7. Comunicação e Colaboração

4.7.1. A comunicação eficaz e a colaboração são fundamentais para o sucesso das iniciativas de tecnologia. Isso envolve a criação de canais de comunicação claros e a facilitação da colaboração entre as equipes de tecnologia e outros departamentos da empresa.

4.8. Avaliação de Riscos e Contingências

4.8.1. A avaliação de riscos é o processo de identificação e avaliação das ameaças à segurança e ao funcionamento dos sistemas de TI. As contingências são planos de ação para lidar com esses riscos, garantindo que a organização esteja preparada para enfrentar interrupções e desafios inesperados.

4.9. Aprendizado Contínuo e Desenvolvimento Tecnológico

4.9.1. A tecnologia está sempre evoluindo, e as equipes de tecnologia devem se manter atualizadas. O aprendizado contínuo envolve o desenvolvimento de habilidades e conhecimentos para acompanhar as mudanças tecnológicas e as melhores práticas correntes. O desenvolvimento tecnológico refere-se à pesquisa e implementação de novas tecnologias para manter a organização atualizada.

5. FUNDAMENTAÇÃO LEGISLATIVA

- Lei nº 2.969, de 11 de janeiro de 2001 (DOM nº 805, de 12.01.2001) - Dispõe sobre a Organização do Regime Próprio de Previdência Social dos Servidores Municipais de Teresina, e dá outras providências;
- Lei nº 5.684, de 16 de dezembro de 2021 (DOM nº 3171, de 17.12.2021) - Altera dispositivos da Lei nº 2.969, de 11 de janeiro de 2001, que "Dispõe sobre a Organização Regime Próprio de Previdência Social dos Servidores Municipais de Teresina", com modificações posteriores;
- Decreto n° 24.514, de 09 de julho de 2023 - Institui o Sistema Eletrônico de Informações (SEI);
- Portaria nº 30/2026, de 22 de janeiro de 2026, (DOM nº 4.183, de 23.01.2026) - Designa profissional para exercer as atividades de unidade orgânica da estrutura administrativa do IPMT;
- Regimento Interno do IPMT.

6. OBJETIVO

Este manual é o documento que estabelece as diretrizes e procedimentos a serem seguidos em situações de emergência, interrupções ou falhas nos sistemas de informações. Ele é projetado para ajudar a lidar com eventos inesperados que possam comprometer a integridade, disponibilidade ou confidencialidade das informações e processos.

7. ENVOLVIDOS

As partes envolvidas e diretamente responsáveis pela execução do procedimento são a Gerência de Tecnologia da Informação e todos os usuários da rede corporativa do IPMT.

8. CONTROLE DE ACESSO FÍSICO E LÓGICO

8.1 Procedimentos de controle de acesso físico

8.1.1 O acesso físico de colaboradores externos às dependências do IPMT é realizado com autorização e/ou fornecimento de crachás na recepção (portaria) e pode ser monitorado por meio de Circuito Fechado de Televisão (CFTV) e seguranças patrimoniais;

8.1.2 A sala do Data Center, que fica trancada, possui acesso restrito a pessoas autorizadas (que guardam a chave), podendo o acesso ser controlado também

por meio de câmera (CFTV). Além disso, as demais salas em geral do Instituto possuem chaves e normalmente são trancadas após o horário de expediente, com cópias armazenadas junto às equipes administrativas, de limpeza e de segurança.

8.1.3 O acesso às redes corporativas de wi-fi se dá mediante senha, que é inserida manualmente nos dispositivos (computadores) diretamente pela equipe da GTI, mediante solicitação.

8.1.4 Para garantir a segurança do acesso de celulares à rede Wi-Fi do IPMT, foi implementado o registro do MAC do equipamento, juntamente com a exigência de senha, em uma rede de convidados.

8.2 Procedimentos de controle de acesso lógico

8.2.1 Usuário faz a solicitação de acesso à informação e/ou ingresso nas redes corporativas;

8.2.2 Após análise técnica da solicitação, o acesso é autorizado ou negado;

8.2.3 Há previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

8.2.4 É possível a obtenção de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do usuário ou do responsável pelo acesso designado pelo setor e o arquivo acessado;

8.2.5 O uso de soluções de gestão dos registros emprega técnicas que promovem a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes;

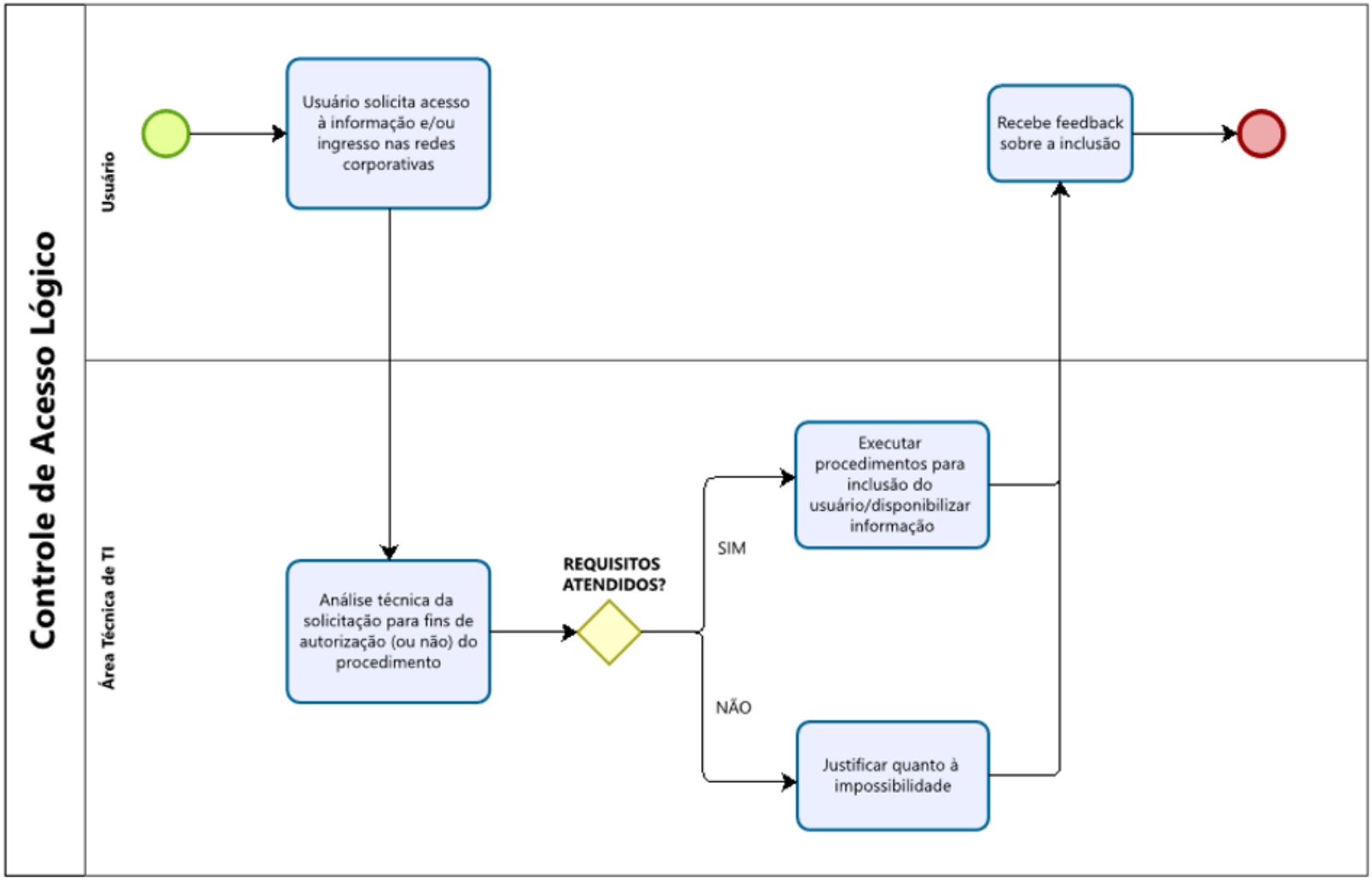
8.2.6 Eventuais problemas relacionados à Tecnologia da Informação dispõem de sistema de Ordem de Serviço para gerenciamento das chamadas, com controle de criticidade (prioridade) e de tempo de resposta, armazenamento de histórico de chamadas e direcionamento à equipe capacitada e responsável;

8.2.7 Em caso de processos no Sistema Eletrônico de Informações (SEI), a inclusão de usuário no sistema ocorre mediante solicitação da chefia imediata,

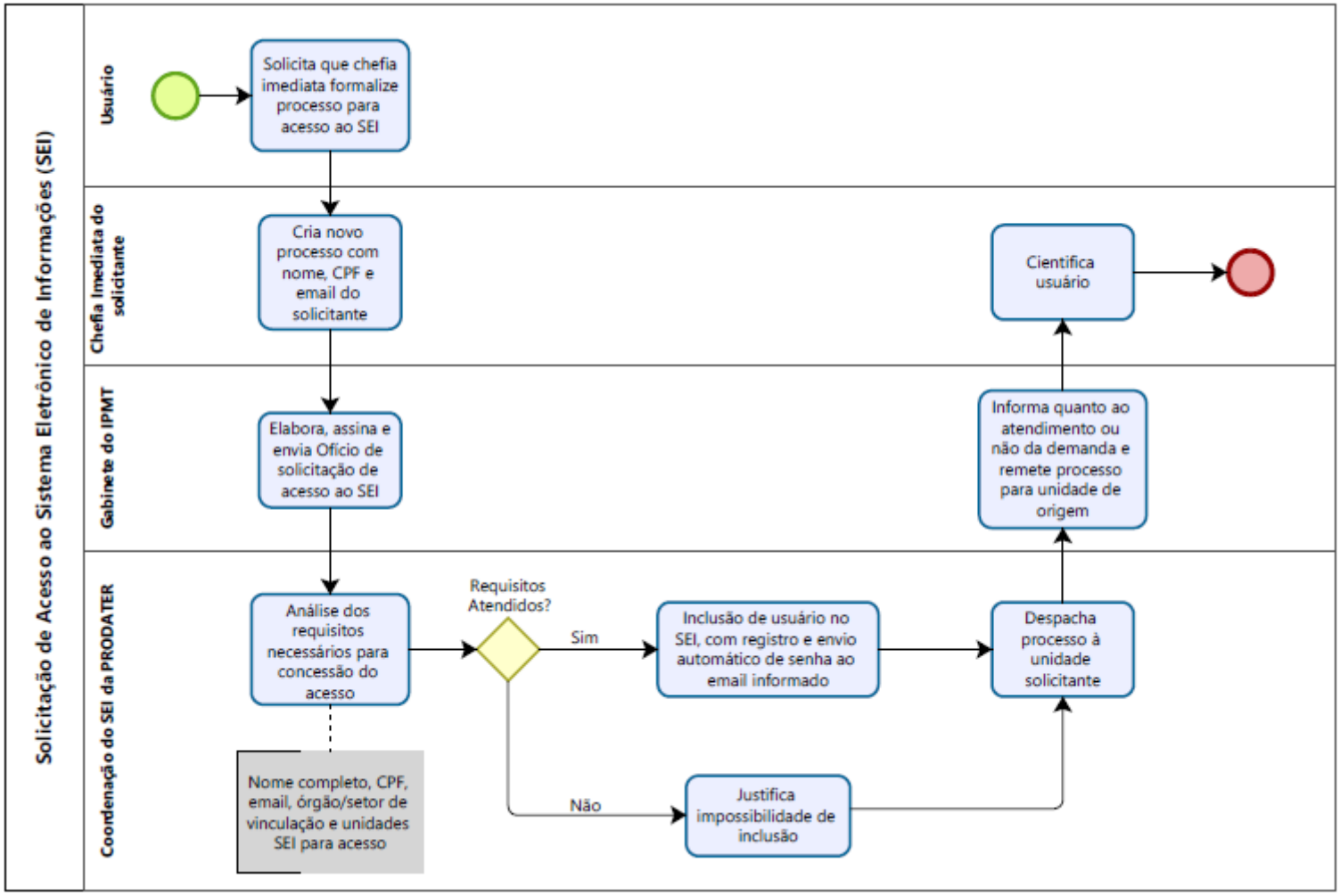
por meio de processo administrativo endereçado ao Gabinete do IPMT, que, em caso de anuência, expede Ofício à PRODATER, a qual, após conceder o acesso, informa no processo quanto ao atendimento da demanda, ou justifica o motivo da impossibilidade. Para a concessão do acesso, é preciso indicar no processo as unidades no SEI a que o acesso será concedido, bem como nome completo, CPF e email para o qual deve ser enviada a senha ao requerente, para fins de controle, registro e arquivamento pela PRODATER. Ainda, o SEI apenas permite que os usuários acessem processos e documentos cadastrados como públicos, ou que tramitaram em em unidades cujo interessado possua acesso.

9. MAPEAMENTOS

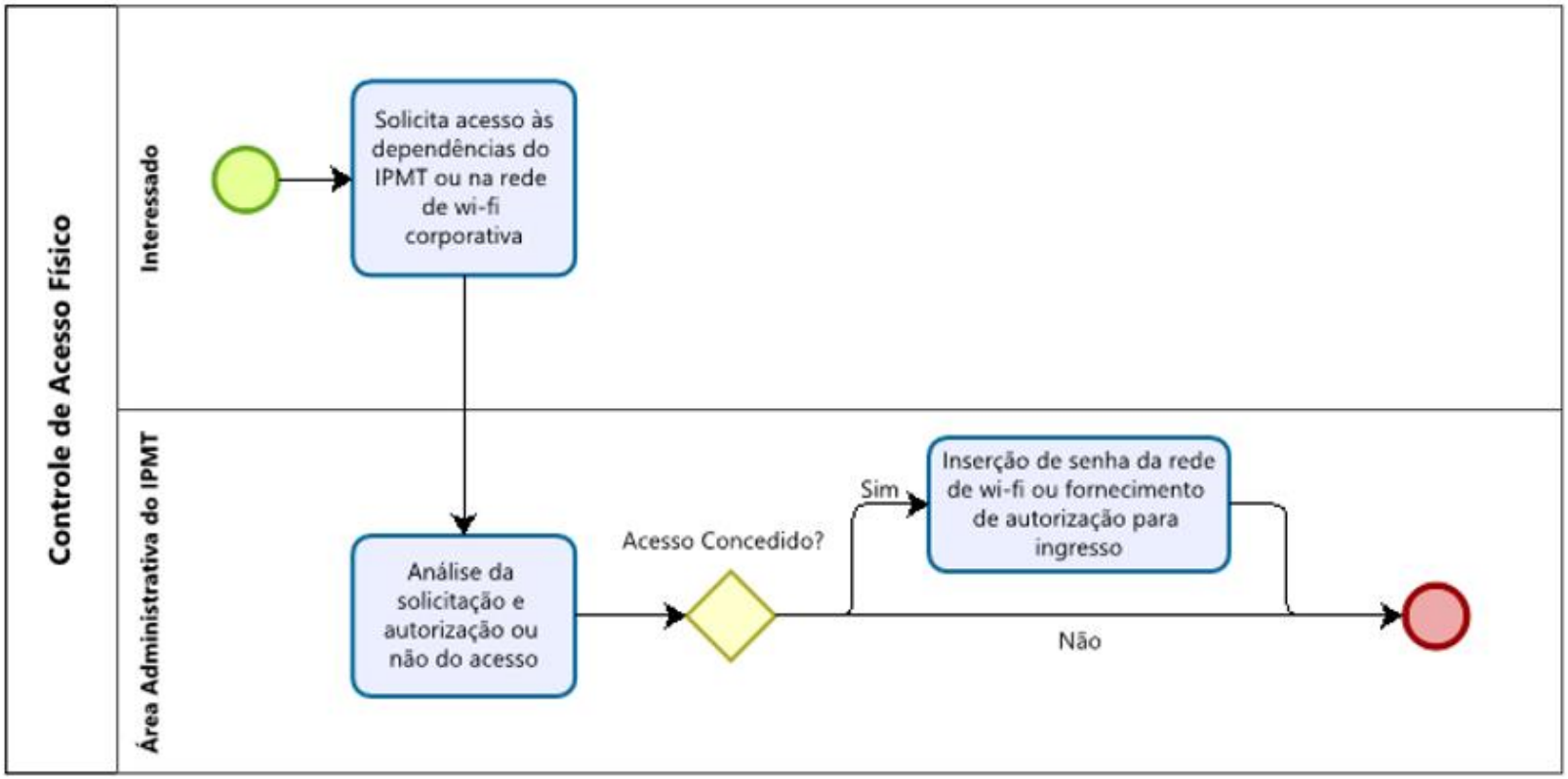
9.1 Controle de Acesso Lógico



9.2 Solicitação de Acesso ao Sistema Eletrônico de Informações (SEI)



9.3 Controle de Acesso Físico



9.4 Cópias de segurança periódicas dos arquivos e bancos de dados