INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE TERESINA

MANUAL DO PLANO DE CONTINGÊNCIA DAS INFORMAÇÕES

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

TERESINA, 2025.

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;
- **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.

3. UNIDADE RESPONSÁVEL

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

4. REGULAMENTAÇÃO BÁSICA

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;

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 regularmente: Faça cópias de segurança de seus dados importantes regularmente. Isso pode ajudar a recuperar informações em caso de ataques de malware ou perda de dados. Assim, devem ser realizadas periodicamente cópias de segurança dos sistemas informatizados e dos bancos de dados, sendo o Sistema Eletrônico de Informações (SEI) de responsabilidade da Empresa Teresinense de Processamento de Dados (PRODATER), nos termos do art. 27, § 2°, do Decreto n° 24.514/2023, e o Sistema Previdenciário (Sisprev) de responsabilidade da Agenda Assessoria, Planejamento e Informática Ltda, consoante a cláusula oitava do Contrato n° 09/2023, que também devem realizar o controle de acesso físico e lógico, com tais atividades sendo supervisionadas pela Equipe Funcional de Tecnologia do IPMT.

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 empresa funcione de maneira eficaz e que os sistemas de TI atendam às necessidades da organização. No caso do IPMT nossa 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) e a Lei Geral de Proteção de Dados Pessoais (LGPD).

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 empresa 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 da indústria. O desenvolvimento tecnológico refere-se à pesquisa e implementação de novas tecnologias para manter a empresa 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;
- PORTARIA Nº 18/2021, DE 06 DE DEZEMBRO DE 2021, (DOM nº 3164 de 7.12.2021) - 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. MAPEAMENTO DO PROCESSO

8.1. Regras de controle de acesso à Rede Corporativa do IPMT

8.1.1. Solicitação de acesso à informação e/ou ingresso na rede corporativa

8.1.2. Análise técnica da solicitação e autorização ou não do procedimento;

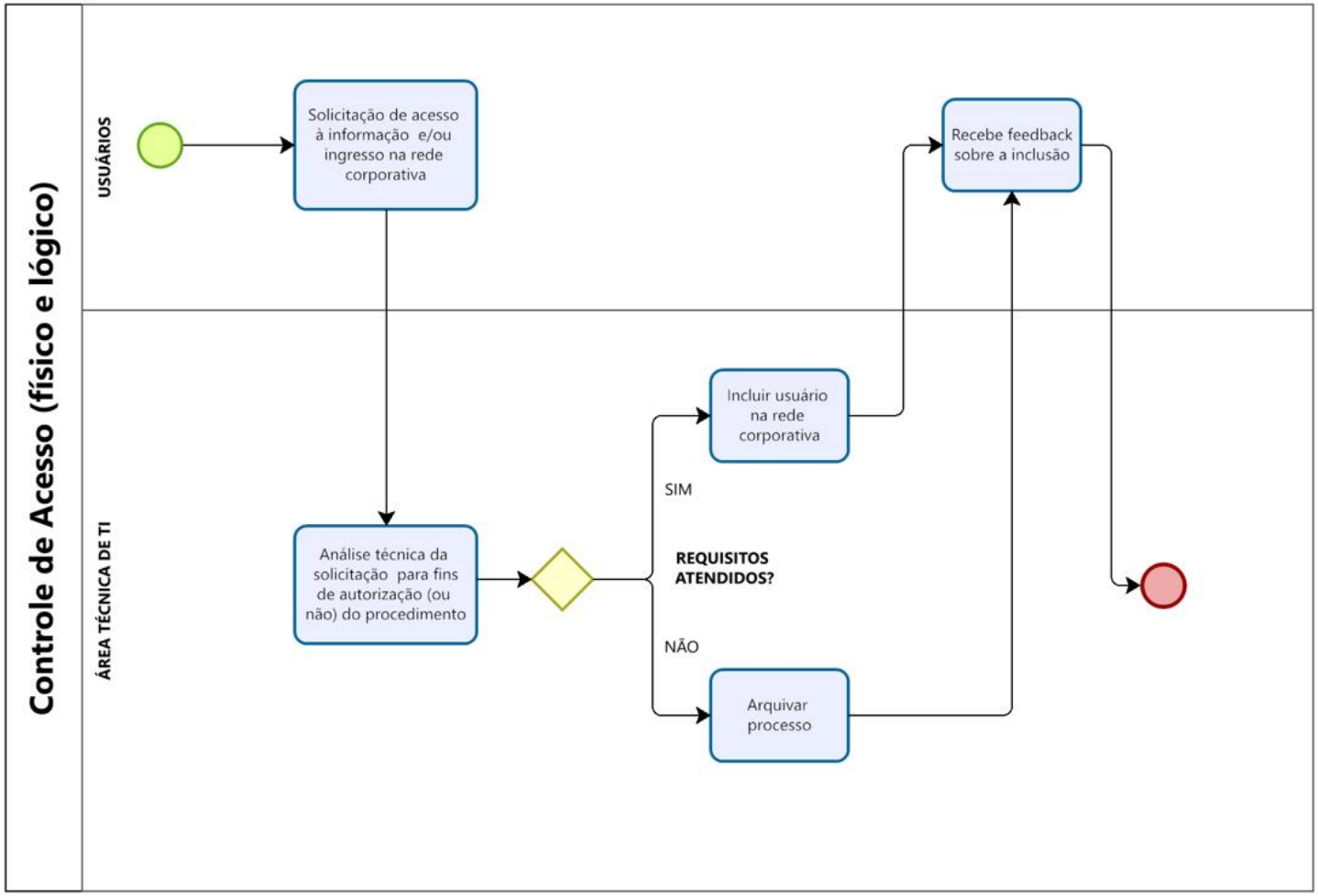
8.1.3. A previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

8.1.4. A criação 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;

8.1.5. O uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

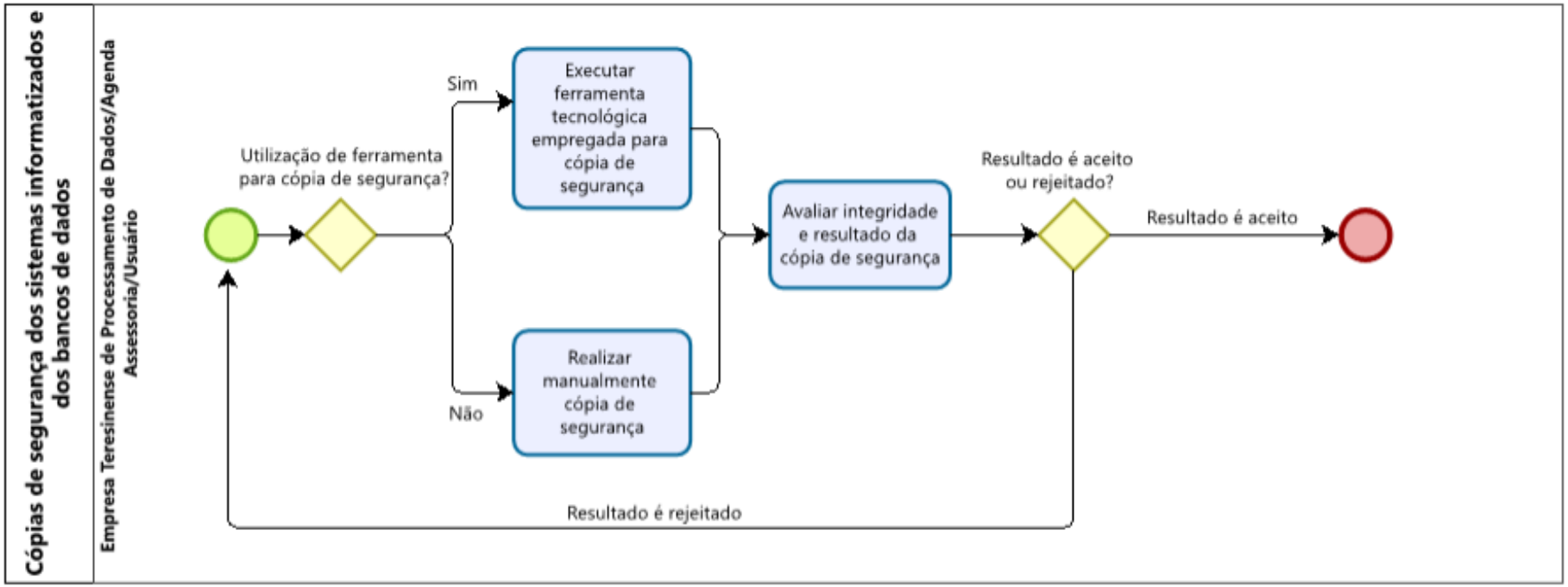
9. FLUXOGRAMAS

9.1 Controle de Acesso (físico e lógico)



Powered by bizagi Modeler

9.2 Cópias de segurança dos sistemas informatizados e dos bancos de dados



Powered by bizagi Modeler