MANUALIZAÇÃO E MAPEAMENTO NORMAS E PROCEDIMENOS TI

PROCESSO: TÉCNOLOGIA DA INFORMAÇÃO.

Unidade Gestora: Instituto Municipal de Previdência dos Servidores de São Francisco do Guaporé – IMPES.

Executora: Controle Interno.

Responsável: SISPEL - SISTEMA INTEGRADOS DE SOFTWARE (BACKUP)
TI PREFEITURA (SEGURANÇA DE REDE)

Unidade Atendida: Todas áreas e departamento do Instituto de Previdência.

1. REGULAMENTAÇÂO UTILIZADA

Portaria do MTP nº 050/2205, de 23 de maio de 2025;
Lei n° 13.709/2018, de 14 de agosto de 2018; e
Lei n° 12.965/2014, de 23 de abril de 2014.

2. OBJETIVO

Dispor sobre as regras gerais para uso da rede de computadores, de dispositivos portáteis e de demais recursos de TI do IMPES, alinhando a mesma com os princípios e as diretrizes da Política de Segurança da Informação do Instituto.

3. TERMOS E SIGLAS UTILIZADAS

3.1 Backup - Cópia de segurança de informações armazenada em meio magnético

3.2 Caixa Postal / Correio Eletrônico - Espaço em disco, onde são armazenadas as mensagens de correio eletrônico.

3.3 Chave de Acesso/Conta/Login - Código de acesso atribuído a cada Usuário. A cada Chave de Acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos disponíveis.

3.4 Correio Eletrônico - Meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores.

3.5 Download - Baixar um arquivo ou documento de outro computador, através da Internet.

3.6 Internet - Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.

3.7 Internet - Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.

3.8 Intranet - Rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os funcionários possam acessar as informações internas.

3.9 Órgão Público - Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

3.10 Servidores de Rede – Computadores com hardware e software para atender demandas no ambiente computacional específico.

3.11 Site - Páginas contendo informações, imagens, fotos, vídeos, sons, etc., que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte à rede.

3.12 Software - Programa de Computador.

3.13 RPPS – Regime Próprio de Previdência Social.

3.14 Usuários – Pessoas que utilizam recursos computacionais.

3.15 Data center - Centro de processamento de dados. Trata-se de um local onde estão concentrados os sistemas computacionais.

3.16 Nobreak - Equipamento responsável por regular a voltagem e a pureza da energia que alcança os eletrônicos conectados a esse dispositivo. Ele também alimenta os aparelhos por meio de uma bateria, quando há queda ou variações bruscas de energia.

3.17 Vírus - É um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.

3.18 LINK - É uma palavra em inglês que significa elo, vínculo ou ligação. No âmbito da informática, a palavra link pode significar hiperligação, ou seja, uma

palavra, texto ou imagem que quando é clicada pelo usuário, o encaminha para outra página na internet, que pode conter outros textos ou imagens

3.19 FIREWALL - Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança.

3.20 Help desk - Serviço de apoio a usuários para suporte e resolução de problemas técnicos.

3.21 TI – Tecnologia da informação.

3.22 Malwares - Um código malicioso, programa malicioso, software nocivo, software mal-intencionado ou software malicioso, é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações.

3.23 VPN - Virtual Private Network. Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.

3.24 USB - É uma interface de entrada e saída que permite a conexão de periféricos sem a necessidade de desligar o computador.

4 DISPOSIÇÕES GERAIS

4.1 A execução do Processo da Área de Informática deve seguir os métodos descritos neste Manual Normativo.

4.2 A competência para a proposição de alterações no Manual de Normas e

Procedimentos da Área de informática é da Superintendente.

4.3 As etapas do Processo da Área de Informática serão executadas, necessariamente, respeitando a ordem de sua descrição neste Manual Normativo.

4.4 As informações de propriedade ou controladas pelo IMPES devem ser utilizadas apenas para os propósitos determinados pela superintendência do órgão. Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações.

4.5 A identificação do usuário/senha é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela.

4.6 Todos os usuários ao tomarem conhecimento de qualquer incidente de segurança da informação devem notificar o fato, imediatamente, a seu superior

4.7 A segurança da informação é aqui caracterizada pela preservação da:

a) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

b) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) Disponibilidade, a Política de Segurança da Informação deve ser divulgada a todos os funcionários e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

4.8 Cabe a todos os funcionários usuários cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados

apenas para as finalidades aprovadas pelo IMPES; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente ao Instituto quando do descumprimento ou violação desta política.

4.9 Cabe ao superintendente do IMPES cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação.

4.10 Os sistemas possuem controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

4.11 Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

4.12 Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

4.13 Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo ao IMPES, só devem ser utilizadas em equipamentos com controles adequados.

4.14 Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser verificado pelo sistema antivírus e instalado com autorização de senha de administrador.

4.15 A superintendente do IMPES poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso.

4.16 Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

4.17 Somente os servidores que estão devidamente autorizados a falar em nome do IMPES, para os meios de comunicação, podem escrever em nome do Instituto em sites de Bate Papo (Chat Room), Redes Sociais (Facebook/ Instagram) ou Grupos de Discussão (fóruns, newsgroups).

4.18 Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc...) nos drives de rede, pois ocupam espaço comum limitado do departamento.

4.19 A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas ao Instituto.

4.20 A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas ao Instituto.

4.21 Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

4.22 Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-

mails do tipo corrente, aviso de vírus, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

4.23. O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

4.24. É vetado aos usuários do ambiente computacional compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

4.25. Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis

5 PROCEDIMENTOS DE CONTIGÊNCIA QUE DETERMINEM CÓPIAS DE SEGURANÇAS NO SISTEMAS INFORMATIZADOS E BANCO DE DADOS

5.1. O IMPES utiliza o Data Center da Prefeitura de São Francisco do Guaporé.

5.2. O Data Center supramencionado fica lotado na sede da Prefeitura de São Francisco do Guaporé.

5.3. A sala onde está o Data Center fica é refrigerada.

5.4. O sistema CECAM da empresa SISPEL, que é de utilização do corpo técnico do IMPES, está hospedado em uma das duas máquinas que compões o Data Center da Prefeitura de São Francisco do Guaporé.

5.5. Utiliza-se backups totais e são realizados todos os dias.

5.6. O backup supramencionado é realizado em mídia externa (HD externo).

5.7. Os HD`s externos ficam armazenados em uma espécie de cofre.

5.8. O cofre supramencionado está localizado no mesmo lugar físico do Data Center

6. CONTROLE DE ACESSO FISICO E LÓGICO

CONTROLE DE ACESSO FISICO

6.1 Foi instalado sistema de alarme com senha pessoal.

6.2. O sistema supramencionado é gerido por uma empresa terceirizada.

6.3. Poucos colaboradores possuem acesso ao sistema supramencionado.

CONTROLE DE ACESSO LÓGICO

6.4 As máquinas possuem login de rede para impossibilitar acessos indevidos.

6.5. Há um proxy instalado para realizar o controle de acesso da internet.

6.6. Possui usuário de proxy.

6.7. Não é permitido o download de arquivos suspeitos.

6.8. As máquinas possuem uma solução de antivírus que bloqueia pendrive e mídias externas

7 COMPOSIÇÃO DO RACK

Bastidores de fibra óticas;

- Suits gerenciáveis;

- Terminal do servidor de internet;

- Servidores de Rack.

.

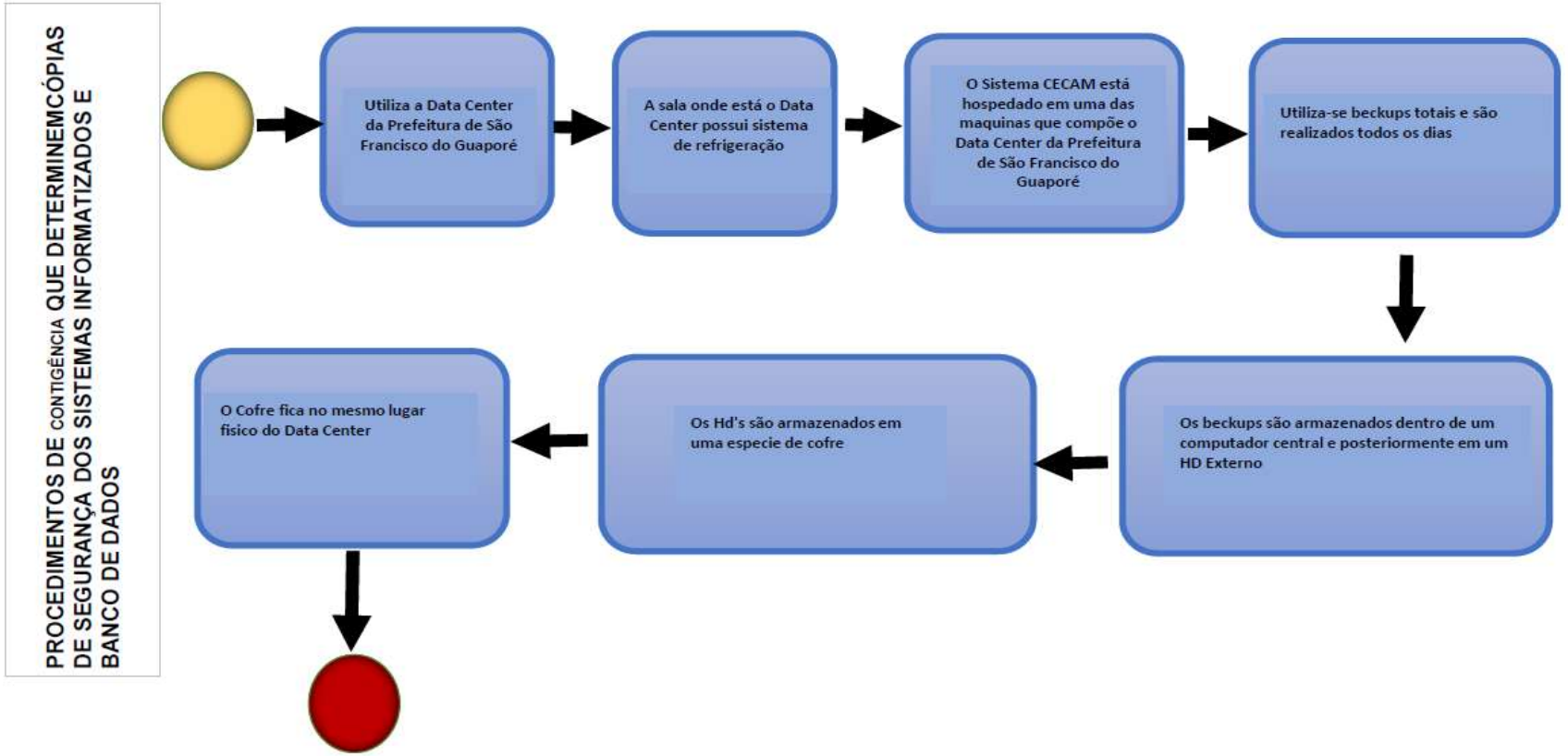
.

FLAVIA ALVES DE ALMEIDA

Superintendente/IMPES

Port. 170/2023

MAPEAMENTO PROCEDIMENTOS DE CONTIGÊNCIA QUE DETERMINEM CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS E BANCO DE DADOS



IMPES
INSTITUTO MUNICIPAL DE PREVIDÊNCIA SOCIAL DOS SERVIDORES

MAPEAMENTO DO CONTROLE DE ACESSO FÍSICO E LÓGICO