POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

IPRESF

EDIÇÃO REVISADA N.º 02
Fevereiro/2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA
FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL
Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social
Aprovado pela Resolução/CADM/IPRESF N.º 006, de 20 de fevereiro de 2020.

Expediente

PRODUÇÃO

FERNANDO GOMES DE FÁVERI
Procurador Previdenciário

REVISÃO

BEATRIS DIRCELHA DOS SANTOS
Diretora Presidente

FERNANDO GOMES DE FÁVERI
Procurador Previdenciário

FLÁVIA REGINA CELESTINO
Gerente Administrativa

APROVAÇÃO

CONSELHO ADMINISTRATIVO
Abelard Helbling Júnior
Beatris Dircelha dos Santos
Flávia Regina Celestino
Idelson Alves Porto
Yara de Oliveira Marcomini

IPRESF

FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL
CNPJ n.º 23.017.093/0001-62
Rua Barão do Rio Branco, n.º 377, Sala 303, 3º andar, Centro - CEP 89240-000
São Francisco do Sul/SC

APRESENTAÇÃO

A informação é um ativo essencial da organização administrativa e previdenciária e precisa ser adequadamente protegida. A Política de Segurança da Informação, da Fundação Instituto de Previdência Social dos Servidores de São Francisco do Sul – IPRESF, é o instrumento pelo qual se busca a proteção da informação sob sua guarda contra os diversos tipos de ameaças, internas e externas, garantindo a confidencialidade, a integridade e a disponibilidade dos dados àqueles que tenham autorização de acesso e a terceiros, de acordo com as autorizações legais, como princípios básicos, além de proteger a intimidade dos segurados e dos demais envolvidos nas atividades do IPRESF.

O presente instrumento traz procedimentos que garantem a segurança das informações, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição.

A Política de Segurança da Informação foi revisada e aprovada pelo Conselho Administrativo do IPRESF, através da Resolução CADM/IPRESF n.º 006, de 20 de fevereiro de 2020.

SUMÁRIO

1 RESOLUÇÃO CADM/IPRESF N.º 006/2020

DISPÕE SOBRE A REVISÃO E APROVAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL – IPRESF.

CONSIDERANDO os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e eficiência, aplicáveis à administração pública, conforme disposto no art. 37, caput, da Constituição Federal de 1988;

CONSIDERANDO o Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios, ao qual o Município de São Francisco do Sul formalizou adesão;

CONSIDERANDO as sugestões de alterações advindas dos servidores e segurados do IPRESF;

CONSIDERANDO que a primeira versão da Política de Segurança da Informação do IPRESF foi aprovada através da Resolução CADM/IPRESF n.º 018, de 03 de outubro de 2019, e publicada na Edição n.º 2964, de 25 de outubro de 2019, no Diário Oficial do Município de São Francisco do Sul;

O CONSELHO ADMINISTRATIVO DA FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL - IPRESF, no uso de suas atribuições legais, estabelecidas no art. 80, da Lei Complementar Municipal n.º 72, de 10 de julho de 2015, considerando a deliberação da 1ª Reunião Ordinária de 2020, ;

RESOLVE:

Art. 1º REVISAR a primeira versão da Política de Segurança da Informação da Fundação Instituto de Previdência Social dos Servidores de São Francisco do Sul – IPRESF, para fins de APROVAR e INSTITUIR sua segunda versão, nos termos do Anexo Único desta Resolução.

Art. 2º Caberá à Gerência Administrativa do IPRESF disponibilizar, de maneira formal, no prazo de até cinco dias úteis após a data de publicação desta Resolução, a segunda versão

da Política de Segurança da Informação aos agentes públicos do IPRESF, a fim de que se ateste sua ciência, compreensão e aceitação, aderindo às práticas nele disciplinadas.

Art. 3º Revogam-se as disposições em contrário, especialmente as contidas na Resolução CADM/IPRESF n.º 018, de 03 de outubro de 2019.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

São Francisco do Sul/SC, 20 de fevereiro de 2020.

FLAVIA REGINA CELESTINO
Presidente do Conselho Administrativo

ABELARD HELBLING JÚNIOR
Membro do Conselho Administrativo

BEATRIS DIRCELHA DOS SANTOS
Membro do Conselho Administrativo

IDELSON ALVES PORTO
Membro do Conselho Administrativo

YARA DE OLIVEIRA MARCOMINI
Membro do Conselho Administrativo

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO I
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituído, no âmbito da Fundação Instituto de Previdência Social dos Servidores de São Francisco do Sul – IPRESF, a 'Política de Segurança da Informação', destinado aos agentes públicos do IPRESF, com a finalidade de estabelecer orientações e procedimentos a serem adotados para o manuseio, controle e proteção das informações sob a guarda da entidade fundacional, em qualquer meio ou suporte, contra destruição, modificação e/ou divulgação indevidas e acessos não autorizados

Art. 2º Toda informação produzida ou recebida, derivada da atividade profissional pelos usuários, pertence ao IPRESF, salvo as exceções explícitas e formalizadas previamente em documento entre as partes envolvidas.

CAPÍTULO II
DOS AGENTES PÚBLICOS

Art. 3º Para os fins desta Política de Segurança da Informação, considera-se agente público todo aquele que exerce, ainda que transitoriamente, com ou sem remuneração, por eleição, nomeação, designação, contratação, cedência ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no IPRESF, incluindo servidores efetivos, cedidos, comissionados, temporários, estagiários, conselheiros, segurados, beneficiários, dependentes e pessoas jurídicas ou físicas contratadas.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 4º São princípios basilares da Política de Segurança da Informação, no âmbito do IPRESF:

I. Confidencialidade: Proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas;
II. Integridade: Garantia da exatidão das informações e dos métodos de processamento;
III. Disponibilidade: Garantia de que os usuários autorizados e os interessados tenham acesso às informações.

CAPÍTULO IV
DOS OBJETIVOS

Art. 5º São objetivos norteadores da Política de Segurança da Informação, no âmbito do IPRESF:

I. Proteger a informação sob a guarda da Fundação Instituto de Previdência Social dos Servidores de São Francisco do Sul, em qualquer meio ou suporte, de vários tipos de ameaças, para garantir a continuidade das atividades no âmbito do IPRESF, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;
II. Adotar condutas que observem os preceitos legais, de acordo com aspectos de legitimidade, legalidade e justiça;
III. Garantir a segurança dos ativos computacionais, instalações prediais e documentos em meio físico abrangendo, também, o controle de acesso de pessoas às instalações do IPRESF;
IV. Garantir a segurança de toda e qualquer informação contida em meio digital, seja em equipamentos, tráfego de informações pela rede, por correio eletrônico ou armazenada em estações de trabalho dos usuários;
V. Promover a educação e conscientização de cada usuário sobre a responsabilidade para com a segurança da informação, por meio de sugestões e ações educativas;
VI. Promover ampla divulgação da Política de Segurança da Informação a todos os servidores efetivos, cedidos, comissionados, temporários, estagiários, conselheiros, segurados, beneficiários, dependentes e pessoas jurídicas ou físicas contratadas pelo IPRESF.

CAPÍTULO V
DA AUTENTICAÇÃO DE ACESSO AOS SISTEMAS DE GESTÃO DO IPRESF

Art. 6º A autenticação de acesso dos usuários aos sistemas informatizados de gestão do IPRESF ocorrerá por meio de login e senha individuais e intransferíveis, sendo esta composta por, no mínimo 08 (oito) caracteres alfanuméricos (letras e números), com letras maiúsculas e minúsculas.

§1º As senhas deverão ser alteradas periodicamente pelos usuários ou sempre que necessário.

§2º Todas as ações executadas por meio do login individual serão de inteira responsabilidade do usuário correspondente.

CAPÍTULO VI
DO USO DO CORREIO ELETRÔNICO E DO ACESSO À INTERNET

Art. 7º A ferramenta de correio eletrônico corporativo constitui meio de comunicação corporativa do IPRESF, a ser utilizado com nome do órgão/setor seguido do domínio <@ipresf.sc.gov.br>, devendo ser utilizado de acordo com os princípios estabelecimentos na Política de Segurança da Informação.

§1º É vedado o uso de contas particulares de correio eletrônico para fins institucionais.

§2º Os e-mails encaminhados pelo correio eletrônico corporativo deverão adotar assinatura padrão com as seguintes informações:

I. Nome completo do servidor;
II. Cargo, acompanhado do registro no órgão fiscalizador da profissão, se for o caso;
III. Logomarca ou nome do IPRESF;
IV. Telefone de contato;
V. Endereço do site do IPRESF.

§3º A autenticação de acesso do usuário ao seu respectivo correio eletrônico corporativo do IPRESF ocorrerá por meio de login e senha individual e intransferível, sendo esta composta por, no mínimo 08 (oito) caracteres alfanuméricos (letras e números), com letras maiúsculas e minúsculas.

Art. 8º Os recursos de internet, correio eletrônico corporativo ou qualquer outro existente ou que venha a ser adotado, deverão ser utilizados em consonância com os interesses do IPRESF.

Art. 9º É vedada a moderação no uso do correio eletrônico corporativo, considerando-se abuso a utilização que comprometa o desempenho do servidor em horário de trabalho, a boa imagem e a segurança dos dados do IPRESF, bem como qualquer outra forma de utilização que fuja à legalidade, à moralidade ou a qualquer outro princípio administrativo.

Art. 10 É permitida a comunicação instantânea via aplicativos de celular, a exemplo de 'Whatsapp', 'Telegram', etc., e de redes sociais, no aparelho celular do IPRESF, desde que utilizado para fins corporativos, sendo vedado seu uso para fins particulares.

Art. 11 O acesso recreativo à internet deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:

I. Proibição do acesso a sites não confiáveis, impróprios, incluindo aqueles com conteúdo sexual ou preconceituoso, jogos, salas de bate-papo, apostas e assemelhados;
II. Proibição do uso de ferramentas Peer-to-Peer (P2P), para o compartilhamento de serviços e dados;
III. Proibição do uso e instalação de jogos ou do download de arquivos que comprometam o tráfego da rede (vídeos, imagens, músicas, etc.), para fins particulares;
IV. Proibição de uso excessivo ou abusivo.

CAPÍTULO VII
DO USO DA INTERNET PELA REDE WI-FI

Art. 12 O uso da Internet pela rede Wi-fi (Wireless Fidelity), no âmbito do IPRESF, é permitido aos servidores efetivos, cedidos, comissionados, temporários, estagiários e conselheiros, desde que para o uso profissional, condizente com as tarefas do cargo ou função.

§1º Os usuários deverão conhecer as regras de acesso à referida rede, contidas na Política de Uso e estar cientes das penalidades que poderão ocorrer caso haja violação das mesmas.

§2º Para visitantes ou outros usuários não mencionados no *caput*, será permitido o uso, mediante justificativa, podendo ser acatada ou não pela Gerência Administrativa do IPRESF, mediante preenchimento e assinatura de formulário com as informações necessárias, onde o usuário declarará ciência e acordo com as normas existentes na Política de Uso.

Art. 13 A Política de Uso da rede Wi-fi (Wireless Fidelity), no âmbito do IPRESF, é constituída pela seguites regras:

I. Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;
II. Responsabilizar-se pela sua identidade eletrônica, senha ou outro dispositivo de segurança, negando revelá-la a terceiros;
III. Manter seus dispositivos pessoais (notebooks, smartphones, etc.) com softwares e antivírus atualizados;
IV. Não usar a rede para trafegar informações confidenciais e/ou sigilosas, salvo quando utilizado algum meio seguro de transmissão (vpn, conexões cifradas, etc.);
V. Responder pelo mau uso dos recursos computacionais em qualquer circunstância;

VI. Responder por atos que violem as regras de uso dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na política de uso desses recursos.

Art. 14 Considerar-se-á violação das regras de Política de Uso da rede Wi-fi (Wireless Fidelity), no âmbito do IPRESF:

I. Infringir qualquer lei ou regulamento local, estadual, nacional ou internacional aplicável;
II. Acessar, mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;
III. Utilizar os recursos computacionais do IPRESF para constranger, assediar, ameaçar ou perseguir qualquer pessoa;
IV. Efetuar ou tentar efetuar qualquer tipo de acesso não autorizado aos recursos computacionais do IPRESF;
V. Utilizar os recursos computacionais do IPRESF para invadir, alterar ou destruir recursos computacionais de outras instituições;
VI. Violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a identidade eletrônica de outro usuário, senhas ou outros dispositivos de segurança;
VII. Interceptar ou tentar interceptar a transmissão de dados através de monitoração;
VIII. Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando o congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais do IPRESF;
IX. Utilizar os recursos computacionais do IPRESF para fins comerciais ou políticos, tais como mala direta, spams ou propaganda política;
X. Não fazer uso ou divulgar conteúdos impróprios como: pornografia, erotismo, racista, sexista, difamatório, falsos perfis em sites pessoais ou quaisquer outros tipos de ataques dessa categoria;
XI. Consumir inutilmente os recursos computacionais do IPRESF de forma intencional.

CAPÍTULO VIII
DAS ESTAÇÕES DE TRABALHO

Art. 15 Cada servidor do IPRESF deverá utilizar uma estação de trabalho determinada, que deverá ser protegida por senha individual e intransferível, sendo esta composta por, no mínimo 08 (oito) caracteres alfanuméricos (letras e números), com letras maiúsculas e minúsculas.

Art. 16 O uso das estações de trabalho do IPRESF deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:

I. Proibição do uso de dispositivos móveis de armazenamento sem aplicação de antivírus;
II. Proibição do armazenamento, edição ou distribuição de qualquer material de cunho sexual, preconceituoso, ou ilegal, incluindo piratarias;
III. Proibição do consumo de alimentos e bebidas nas mesas de trabalho, próximo aos equipamentos eletrônicos e em locais que armazenem informações de forma física;
IV. Proibição do uso indevido de impressoras para fins particulares;
V. Proibição da retirada de equipamentos eletrônicos da sede do IPRESF, salvo autorização da Gerência Administrativa;
VI. Proibição da retirada de arquivos físicos ou digitais da sede do IPRESF, salvo autorização da Gerência Administrativa;
VII. Proibição de instalação de softwares ou hardwares não licenciados sem autorização da Gerência Administrativa, ou qualquer outro tipo de pirataria.

Art. 17 O antivírus deverá estar sempre atualizado, cabendo ao usuário da estação de trabalho informar à Gerência Administrativa do IPRESF quaisquer atitudes suspeitas em sua estação de trabalho ou notificações que venha a receber, incluindo notificações relacionadas ao funcionamento do programa.

Art. 18 Todo e qualquer equipamento que componha o parque computacional do IPRESF, só poderá ser retirado mediante o preenchimento de formulário específico, contendo justificativa, assinatura da Gerência Administrativa do IPRESF e do responsável pela retirada.

CAPÍTULO IX
DOS PROCEDIMENTOS BÁSICOS DE SEGURANÇA

Art. 19 O IPRESF adotará providências no sentido de garantir:

I. Que os equipamentos estejam em bom estado de conservação para atender as demandas do IPRESF e não comprometam a segurança das informações produzidas;
II. Cada usuário deverá realizar o backup semanal das informações armazenadas em sua estação de trabalho, na forma estabelecida no plano de contingência, que não deverá ser disponibilizado a terceiros, salvo em caso de reestabelecimento do backup na estação de trabalho que tenha apresentado falhas que comprometam a integridade das informações, à pessoa ou empresa previamente autorizada pela Gerência Administrativa;

III. Caso não seja utilizado sistema de 'webmail' ou qualquer outro sistema de armazenamento virtual das informações do correio eletrônico corporativo, cada usuário deverá realizar o backup semanal das mesmas, seguindo os procedimentos do plano de contingência, que não deverá ser disponibilizado a terceiros, salvo em caso de reestabelecimento do backup na estação de trabalho que tenha apresentado falhas que comprometam a integridade das informações, à pessoa ou empresa previamente autorizada pela Gerência Administrativa;

IV. Os sistemas informatizados de gestão, utilizados pelo IPRESF, deverão atender os seguintes requisitos mínimos:

a. Oferecer serviços de cópias de dados, preferencialmente backup virtual, realizados diariamente;
b. Possibilitar a administração gerenciar os níveis de acesso a cada funcionalidade;
c. Possibilitar a administração gerenciar os perfis e usuários para acesso ao sistema;
d. Possibilitar a auditoria nos módulos;
e. Possibilitar o registro de login de alterações, com informação do usuário que efetuou a alteração;
f. Possibilitar o registro de tentativas de acesso sem sucesso, armazenando o endereço IP de origem.

Art. 20 Os usuários de sistemas e serviços de informação do IPRESF deverão registrar e relatar à Gerência Administrativa qualquer observação ou suspeita de fragilidade de segurança das informações armazenadas.

Art. 21 As evidências dos incidentes de segurança deverão ser coletadas e armazenadas pela Gerência Administrativa, a fim de que sejam tomadas as providências devidas.

Art. 22 A acesso aos documentos armazendos nos arquivos físicos do IPRESF só poderão ocorrer por servidor público efetivo ou cedido ao IPRESF ou pela Gerência Administrativa, autorizado e designado previamente por esta, madiante o preenchimento dos controles de retirada e devolução dos documentos, nos quais deverão constar o arquivo retirado/devolvido, nome do servidor que acessou o documento, data e horário.

§1º O armazenamento de documentos em arquivos físicos do IPRESF e o acesso aos mesmos deverão observar regras e princípios básicos de arquivologia e biblioteconomia, e da legislação aplicável, a citar-se, especialmente, a Lei de Acesso à Informação (Lei Federal n.º 12.527, de 18 de novembro de 2011), Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709, de 14 de agosto de 2018), ISO 27002, observadas as garantias legais e constitucionais de sigilo de determinadas informações de cunho pessoal.

Art. 23 Além dos procedimentos básicos descritos no Capítulo VIII, desta Política de Segurança da Informação, os agentes públicos deverão observar integralmente das disposições do Plano de Contingência, descritas no Anexo II, deste instrumento.

CAPÍTULO X
DO ACESSO REMOTO

Art. 24 O acesso remoto de terceiros à rede do IPRESF será permitido somente para atender aos interesses da Fundação, mediante autorização prévia e expressa da Gerência Administrativa, através de abertura de requisição de serviço.

§1º A ferramenta de conexão remota utilizada poderá ser 'TeamViewer', 'LoMeIn', ou outra ferramenta de uso gratuito, ou da qual o terceiro possua licença de uso.

§2º Os terceiros que tenham acesso remoto à rede do IPRESF deverão observar os seguintes requisitos, sob pena de aplicação das penalidades cabíveis:

I. Manter sigilo das informações às quais tiverem acesso, sendo de sua total e exclusiva responsabilidade qualquer operação realizada sob suas credenciais de uso;
II. Comunicar imediatamente à Gerência Administrativa qualquer situação que coloque em risco o acesso ao ambiente de rede do IPRESF.

CAPÍTULO XI
DAS PENALIDADES

Art. 25 O não cumprimento dos preceitos da Política de Segurança da Informação implicará na adoção das providências necessárias, mediante provocação ou de ofício, com vistas à aplicação das sanções administrativas cabíveis, especialmente as previstas na Lei Complementar Municipal n.º 008, de 30 de outubro de 2003, observados o contraditório e a ampla defesa, sob pena de nulidade, sem prejuízo das demais sanções cíveis e penais previstas na legislação em vigor.

CAPÍTULO XII
DAS DISPOSIÇÕES FINAIS

Art. 26 As disposições contidas no presente instrumento são de aplicação subsidiária, prevalecendo, em qualquer hipótese, o disposto na Lei Orgânica do Município de São Francisco do Sul e na Lei Complementar Municipal n.º 008, de 30 de outubro de 2003, e demais deveres e proibições legais e regulamentares.

Art. 27 Todos os usuários ficam cientes de que os ambientes, sistemas, computadores e redes do IPRESF poderão ser monitorados e gravados.

Art. 28 É vedado aos usuários de sistemas e serviços de informação do IPRESF aceitar ajuda técnica de pessoas estranhas e não autorizadas, salvo do quadro de funcionários do IPRESF ou da equipe técnica especializada contratada mediante procedimento licitatório adequado.

Art. 29 Fica vedada a divulgação ou reprodução de informações produzidas ou recebidas como resultado de atividade com o IPRESF, sem a autorização da autoridade competente.

Art. 30 Os usuários deverão ser cientificados da existência da Política de Segurança da Informação e sobre o uso correto dos ativos disponibilizados ao estabelecerem vínculo com o IPRESF, de forma a minimizar os possíveis riscos de segurança, bem como garantir o conhecimento de suas responsabilidades.

Art. 31 O IPRESF exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos, serviços e informações, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

Parágrafo Único. O usuário que tomar conhecimento de qualquer irregularidade sobre essa Política de Segurança da Informação deverá comunicar, imediatamente, a autoridade competente do IPRESF.

Art. 32 O IPRESF realizará, sempre que julgar necessário, ações preventivas e educativas visando garantir a aplicação da Política de Segurança da Informação .

Art. 33 A Política de Segurança da Informação do IPRESF será revista sempre que necessário, de ofício ou por provocação do Diretor Presidente, mediate aprovação prévia pelo Conselho Administrativo.

Art. 34 O IPRESF terá o prazo de 60 (sessenta) dias para a adequação dos procedimentos, de acordo com o estabelecido neste instrumento, a partir da sua entrada em vigor.

Art. 35 Este instrumento entra em vigor na mesma data da publicação da Resolução do Conselho Administrativo que o aprovar.

ANEXO II

PROCEDIMENTOS DE CONTINGÊNCIA

Sumário

1. Conceito de Procedimentos de Contingência

Os procedimentos de contingência em Tecnologia da Informação, no âmbito da Fundação Instituto de Previdência Social dos Servidores de São Francisco do Sul, correspondem às ações previamente planejadas deverão ser adotadas para reduzir as consequências negativas que podem ser causadas por uma situação inesperada, a fim de reduzir o tempo de indisponibilidade dos serviços e, consequentemente, evitar que mais danos e prejuízos sejam causados por razão do incidente.

2. Objetivos

Determinar as ações previamente planejadas para o enfrentamento de ações inesperadas que possam causar prejuízos ou vulnerabilidade das informações, a fim de reestabelecer os serviços prestados pelo IPRESF. O presente instrumento estabelece um conjunto de

procedimentos pré-estabelecidos para que os serviços de informática permaneçam em funcionamento total ou parcial, quando houver algum impedimento externo.

3. Aplicação e Área Responsável

Este instrumento tem abrangência no âmbito da Fundação Instituto de Previdência Social dos Servidores de São Francisco do Sul – IPRESF, a ser executado pela Gerência Administrativa.

4. Pontos Frágeis

A relação dos pontos frágeis aponta os possíveis focos de crise das tecnologias utilizadas pelo IPRESF, destacando-se:

a. Servidor de arquivos;
b. Servidor de e-mail;
c. Servidor de hospedagem;
d. Serviço de acesso à Internet;
e. Serviço de telefonia.

5. Setores Prejudicados

Os setores potencialmente prejudicados abrangem:

a. Atendimento aos aposentados e pensionistas;
b. Compras, contratos e licitações;
c. Concessão de benefícios;
d. Diretoria;
e. Contabilidade;
f. Financeiro;
g. Tesouraria;
h. Perícia médica;
i. Recursos humanos;
j. Procuradoria Previdenciária
k. Atendimento às demais entidades – Câmara de Vereadores, FUCISF, SAMAE e Prefeitura.

6. Procedimentos para Restauração dos Servidores

Os servidores são equipamentos de alta performance capazes de executar aplicações para vários usuários conectados a uma rede de computadores. Eles apresentam diversas

funcionalidades para atender às demandas desses usuários e são indispensáveis À execução das atividades de entidades públicas ou privadas, a exemplo da Fundação Instituto de Previdência Social de São Francisco do Sul – IPRESF. Essas funcionalidades podem ser o armazenamento de arquivos e bancos de dados, contas de e-mail, compartilhamento de recursos como impressoras, etc. Algumas de suas vantagens são a facilidade para gerenciar os dados de forma centralizada e permitir o acesso remoto aos usuários das aplicações da empresa.

Diversos fatores podem fazer computadores, impressoras, Internet e a própria rede, ficar fora do ar. Os principais motivos normalmente são: defeitos nos equipamentos, ataques cibernéticos, erros provocados por colaboradores, problemas na rede de computadores, rede elétrica e configurações erradas.

Para identificá-los, é preciso verificar os alertas emitidos pelo sistema operacional, softwares aplicativos, utilitários e de gestão, avisos sonoros emitidos pelos nobreaks entre outros, além de realizar testes nos dispositivos.

6.1. Servidor de arquivos

Um servidor de arquivos é um computador conectado a uma rede que tem como objetivo principal proporcionar um local para o armazenamento compartilhado de arquivos de computadores (como documentos, arquivos de som, fotografias, filmes, imagens, bases de dados, etc) que podem ser acessados pelos dispositivos que estão ligados à rede de computadores.

O Servidor seria a 'máquina principal' enquanto os dispositivos ligados ao servidor são chamados de 'clientes'. É projetado principalmente para permitir o armazenamento, compartilhamento e recuperação rápida de dados onde a computação pesada é fornecida pelas estações de trabalho.

Em caso de problemas no servidor de arquivos deve-se adotar o seguinte procedimento:

a. Avisar aos setores os serviços afetados e o prazo para restabelecimento;
b. Providenciar um novo equipamento para instalação;
c. Instalar os drivers e serviços necessários;
d. Restaurar o backup dos arquivos;
e. Configurar o acesso dos usuários e os serviços;
f. Testar a autenticação via rede e integridade dos arquivos.

6.2. Servidor de e-mails

Um servidor de e-mails é um computador que envia, recebe e armazena e-mails para usuários.

Em caso de problemas no servidor de e-mails deve-se adotar o seguinte procedimento:

a. Avisar aos setores os serviços afetados e o prazo para restabelecimento;
b. Abrir um chamado no sistema de atendimento da empresa contratada para prestação deste serviço;
c. Acompanhar através do painel do cliente o andamento do chamado;
d. Testar as principais funções do servidor de e-mails.
e. Alterar as senhas, caso necessário.

6.3. Servidor de hospedagem

Um servidor de hospedagem possui o armazenamento de um site e disponibiliza o mesmo na internet, ou seja, o serviço de hospedagem possibilita que o site seja visualizado 24h por dia em todo o mundo. Em caso de problemas no servidor de hospedagem deve-se adotar o seguinte procedimento:

a. Avisar aos setores os serviços afetados e o prazo para restabelecimento;
b. Abrir um chamado no sistema de atendimento da empresa contratada para prestação deste serviço;
c. Acompanhar através de e-mail ou telefonema, o andamento do chamado;
d. Alterar as senhas dos administradores do painel do cliente;
e. Testar as principais funções do servidor de hospedagem.

7. Serviço de Acesso à Internet

O serviço de acesso à internet disponibiliza os meios pelos quais os usuários podem conectar-se à rede mundial de computadores. Em caso de problemas no acesso à internet deve-se adotar o seguinte procedimento:

a. Avisar aos setores os serviços afetados;
b. Checar o cabeamento de rede;
c. Checar a alimentação de energia elétrica dos equipamentos de rede (modem, roteadores e switches);
d. Analisar se o problema é local ou no provedor de acesso;
e. Contactar o provedor deste serviço para solicitação de reparo;
f. Avisar aos setores o prazo para restabelecimento.

8. Serviço de Telefonia

Para a disponibilização do serviço de telefonia aos usuários, o IPRESF utiliza uma linha telefônica fixa e uma linha de telefonia móvel. Em caso de problemas no serviço de telefonia deve-se adotar o seguinte procedimento:

a. Checar a alimentação de energia elétrica dos aparelhos (telefonia fixa);
b. Analisar se o problema é local ou na operadora;
c. Contactar a operadora para solicitação de reparo;
d. Avisar aos setores os serviços afetados e o prazo para restabelecimento.

9. Notificações

As notificações devem ocorrer a todos os usuários afetados quando acontecer qualquer um dos problemas acima citados. Deverá ser notificado o problema ocorrido, causa (quando houver) e informado o prazo estimado para a resolução do mesmo e ações que os usuários devem adotar (quando for o caso).

A notificação deverá ocorrer da seguinte forma:

a. Notificação Interna:
    i. E-mail;
    ii. Whatsapp;
    iii. Telefone.
b. Notificação Externa:
    i. E-mail;
    ii. Whatsapp
    iii. Telefone;
    iv. Website;
    v. Facebook.

10. Backup

Backup é uma cópia de segurança. O objetivo da ação é o usuário se resguardar de uma ocasional perda de arquivos originais, seja por ações despropositadas do usuário, ou ainda mal funcionamento dos sistemas. Ter uma cópia de segurança permite restaurar os dados perdidos. As formas de backup atualmente disponíveis são:

a. Meios físicos: HD externo e pen-drive;
b. Meios virtuais: armazenamento nas nuvens e e-mails.

2 DENÚNCIAS

Aqueles que tiverem conhecimento de violação à Política de Segurança da Informação do IPRESF, poderão apresentar denúncia através dos seguintes instrumentos:

2.1 Por Correspondência ou Presencialmente

Endereço: FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL - IPRESF
Rua Barão do Rio Branco, n.º 377, Sala 303, 3º andar, Centro
São Francisco do Sul/SC
CEP 89240-000

Expediente: Segunda a sexta, das 8h00 às 14h00.

2.2 Comissão de Ética do IPRESF

Correspondência: A/C DO PRESIDENTE DA COMISSÃO DE ÉTICA
FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL - IPRESF
Rua Barão do Rio Branco, n.º 377, Sala 303, 3º andar, Centro
São Francisco do Sul/SC
CEP 89240-000

E-mail: <etica@ipresf.sc.gov.br>

2.3 Ouvidoria do IPRESF

Endereço: FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL - IPRESF
Rua Barão do Rio Branco, n.º 377, Sala 303, 3º andar, Centro
São Francisco do Sul/SC
CEP 89240-000

Site: <https://sistema.ouvidorias.gov.br/publico/sc/SaoFranciscodoSul/Manifestacao/RegistrarManifestacao>

3 INFORMAÇÕES, CRÍTICAS OU SUGESTÕES

Para obter maiores informações, realizar críticas ou sugestões ao conteúdo deste publicação, entre em contato com o IPRESF:

FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL - IPRESF
Rua Barão do Rio Branco, n.º 377, Sala 303, 3º andar, Centro
São Francisco do Sul/SC
CEP 89240-000

Atendimento de segunda a sexta-feira, das 8h00 às 14h00.

CANAIS DE ATENDIMENTO
E-mail: <ipresf@ipresf.sc.gov.br>
Telefone: (47) 3449-0384
Whatsapp: (47) 9 8491-7382
Site: <www.ipresf.sc.gov.br>
Facebook: <www.facebook.com/ipresf>

FUNDAÇÃO INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE SÃO FRANCISCO DO SUL
Rua Barão do Rio Branco, n.º 377, Sala 303, 3º andar
Centro, São Francisco do Sul/SC – CEP 89.240-000
CNPJ n.º 23.017.093/0001-62