MANUAL DE BOAS PRÁTICAS PARA O USO DE RECURSOS DE TECNOLOGIA

RIO DO SUL/SC

1. INTRODUÇÃO

A tecnologia faz parte da vida das pessoas, empresas privadas e setor público. Do aluno da rede pública de ensino aos grandes centros de pesquisa, da dona de casa ao executivo, todos interagem de alguma forma com recursos de TI.

Para que toda a informação que circula possa servir somente ao seu propósito, que é o de informar, sem prejudicar quaisquer pessoas ou instituições, é necessário à gestão segura dos recursos disponíveis em tecnologia da informação.

No Instituto de Previdência Social dos Servidores Públicos de Rio do Sul – Rio do Sul PREV não é diferente. Aliás, deve-se sempre adotar os procedimentos padrões, de modo a contribuir de forma positiva com a disponibilidade, integridade, confidencialidade e autenticidade da informação.

O desafio de fomentar a Segurança da Informação e Comunicações é grande, afinal, são muitos computadores, servidores e usuários distribuídos em vários pontos e instâncias. Mas está longe de ser impossível, pois depende principalmente da atenção e da atitude das pessoas sobre as boas práticas de TI.

O presente manual é destinado a todos os servidores e prestadores de serviço que acessem informações do RPPS, como os servidores da própria unidade gestora, empresas de softwares que se relacionam com a Unidade Gestora, como sistemas informatizados de cadastros, financeiro, controle, contabilidade empenho e operacional e também prestadores de serviço de hospedagem e manutenção dos servidores.

Para obter o acesso à rede e recursos de informática do Rio do Sul PREV, o servidor público, estagiário ou prestador de serviços deverá preencher e assinar a ficha cadastral com o termo de compromisso em que manifesta conhecimento, concordância e comprometimento de acatar este manual e demais normas referentes ao uso da informática.

A partir de agora você tem acesso a informações fundamentais para relacionadas à gestão de recursos de funcionários do serviço público eficiente para o seu dia a dia e adaptado aos novos tempos, assegurando que seus benefícios estejam assegurados.

2. POLÍTICAS DE USO DOS COMPUTADORES

2.1 Para que serve uma política de uso?

Para estabelecer padrões e procedimentos que busquem a segurança, estabilidade e disponibilidade dos serviços computacionais.

2.2 Quais recursos computacionais devem seguir a política de uso?

Quaisquer equipamentos, programas, meios físicos de tráfego e sistemas de armazenamento digital inseridos no ambiente computacional do Instituto de Previdência Social dos Servidores Públicos de Rio do Sul – Rio do Sul PREV incluindo notebooks, *tablets*, *smartfone*, pen drives, HD externos, impressoras, além das estações de trabalho.

2.3 O que posso instalar no computador?

Os computadores são adquiridos pelo Instituto de Previdência Social dos Servidores Públicos de rio do Sul – Rio do Sul PREV sendo distribui por estações de trabalho.

E por razões de padronização e segurança, o usuário não pode instalar aplicativos e programas por conta própria. Em caso de necessidade específica de algum programa ou sistema, deve-se solicitar autorização previa ao diretor executivo, para contactar empresa especializada em sistema de informação terceirizada pelo Instituto de Previdência Social dos Servidores Públicos de Rio do Sul – Rio do Sul PREV.

2.4 Cuidados para utilização dos equipamentos de informática no Instituto de Previdência Social dos Servidores Públicos de Rio do Sul – Rio do Sul PREV*:*

- Não ligar o computador, impressora, fax, escâner, bebedouro, etc, na mesma tomada, seja usando extensões, no breaks, estabilizadores ou adaptadores elétricos. Caso isso ocorra será gerada uma sobrecarga elétrica podendo queimar um ou mais equipamentos e ocasionar princípio de incêndio;
- Quando se perceber alterações na rede elétrica, deve-se salvar os documentos e por medida de segurança desligar os equipamentos por um período, até que a rede elétrica volte ao normal. As principais características de alterações na rede elétrica são: lâmpadas piscando ou com luminosidade fraca, constantes bips de no breaks ou estabilizador, várias interrupções no fornecimento de energia por um curto período de tempo;
- Quando não for mais utilizar os equipamentos desligar normalmente e após isso retirar o plugue da tomada;
- O abastecimento da impressora com excesso de papel, pode causar o problema na tração dos roletes uma vez que podem se puxados

mais de uma folha ao mesmo tempo, este mesmo problema pode ocorrer em caso de folhas úmidas, sempre que for abastecer com folhas verifique se as mesmas estão soltas;

- Quando a impressora estiver por muito tempo sem uso, antes da impressão solte as folhas com a mão deixando-as separadas;
- Quando ocorrer de uma folha ficar presa dentro da impressora, primeiro cancele o processo de impressão e desligue-a da rede elétrica antes de tentar remover a folha. Caso a remoção esteja exigindo muita força solicite a presença do técnico, remover uma folha pode causar desalinhamento em peças internas;
- Não retirar e colocar de maneira brusca o tôner/cartucho da impressora, pode haver derramamento do pó/tinta de impressão ocasionando acumulo de sujeira dentro do equipamento;
- Toda impressora possui um tempo de espera para que o documento seja totalmente carregado em sua memória, somente após esse procedimento é que será impresso. Então o usuário deve enviar o arquivo para impressão e aguarda ele ser impresso, não adianta mandar duas ou três vezes o mesmo documento que ele não será impresso mais rápido, e sim consumir mais papel e tôner da impressora, caso o tempo de espera ultrapasse 2 minutos ai sim poderá ser considerado um problema e deve-se verificar: papel na impressora, tôner e papel preso, caso nenhum desses seja o problema procurar o setor de tecnologia para averiguação;
- Não deixar os cabos que conectam a impressora, escâner ou o computador muito esticados ou mal encaixados;
- Deixe o computador limpo, livre de poeira e umidade;
- Em casos de relâmpagos, desligue o equipamento da tomada;
- Evite fazer refeições na frente do computador;
- Não conecte ou desconecte nenhum cabo com o computador ligado, exceto os cabos de rede e USB;
- Não bata, empurre ou mude de lugar o computador com ele ligado, isso pode prejudicar o hardware do computador;
- Não deixar materiais pesados em cima dos gabinetes e monitores;
- Não ligue e desligue o computador diversas vezes consecutivas, você pode danificar algum componente.

2.6 Como utilizar de forma segura o sistema operacional e aplicativos

- Quando utilizar um pendrive, câmeras digitais, celulares ou outros dispositivos conectados ao computador, a primeira coisa a fazer é uma varredura com o antivírus para eliminar programas maliciosos. Uma simples abertura do dispositivo sem os cuidados necessários é suficiente para infectar o computador com programas maliciosos,

corromper arquivos e pastas do sistema deixando o computador inutilizável até os devidos reparos;

- Não deixar que usuários não autorizados, até última ordem, utilizem os computadores e impressoras, pois se eles não possuírem conhecimentos para prevenir contaminação por vírus de computador ou manuseio de impressoras, poderão danificar os equipamentos ou o sistema operacional e acessar sites de conteúdo nocivos ao computador como: jogos, pornografia, *software* piratas, download de filmes e músicas. Prejudicando a utilização da rede de computadores para tarefas administrativas e acadêmicas;
- Sempre fazer o backup de seus arquivos pessoais ou de trabalho pelo ao menos uma vez por semana;
- Nunca desligar o computador diretamente na tomada elétrica ou no botão de desligar, sempre utilizar o método tradicional do sistema operacional;
- Não Clique em Links desconhecidos que você recebe por E-mail, Talk, *Messenger*;
- Em suas senhas combine letras, números e caracteres especiais;
- Nunca forneça suas senhas a ninguém;
- Não clique em link recebido através de redes sociais, pois estes podem apontar para *malwares* e sites de *phishing*. Principalmente se este link vier de alguém desconhecido;
- Nunca utilize senhas baseadas em informações pessoais;
- Jamais clique em programas recebidos por e-mail cuja origem você desconhece;
- Verifique com antivírus atualizado os arquivos recebidos por e-mail antes de executá-los;
- A menos que você solicite, bancos nunca entram em contato com clientes através de e-mail, muito menos operadoras de cartões de crédito;
- Desconfie de todas as mensagens recebidas por e-mail cujo conteúdo solicite informações ou atualizações de dados pessoais;
- Não clique em URL de bancos recebidas por e-mail. Elas normalmente direcionam usuários para sites fraudulentos;

- Em acessos a páginas da Internet que peçam *login* e senha, sempre verifique a presença do cadeado fechado no canto superior esquerdo da barra de endereço do seu navegador.

3. SEGURANÇA DA INFORMAÇÃO

3.1 O que pode ocorrer com um computador vulnerável?

Entre outras coisas, pode ocorrer:

- Roubo de informação;
- Perda de dados;
- Redução de desempenho;
- Uso do computador para atacar servidores e outros computadores.

Por isso, os cuidados com a segurança são importantes.

3.2 Como utilizar minha senha com segurança?

- Jamais compartilhe senhas com outras pessoas. Lembre-se que, a princípio, você é o responsável por tudo que ocorre com o uso de sua senha.
- Se você não consegue memorizar suas senhas e precisa anotar em algum lugar, dificulte o acesso das pessoas aos seus lembretes. Não deixe suas senhas anotadas em locais visíveis, de fácil acesso, expostas em cadernos, pastas ou marcadores em sua mesa de trabalho.
- Utilize senhas também em celulares e notebooks, protegendo suas informações em caso de extravio, furto ou roubo do equipamento.
- Sempre que possível diversifique as senhas que possui, evitando que a descoberta de uma delas dê acesso a outras informações protegidas.

3.3 Quais os riscos ao navegar na internet?

Alguns sites exploram vulnerabilidades dos navegadores e acabam instalando programas maliciosos no computador do usuário. Por isso, é importante manter os aplicativos atualizados e não fazer download de arquivos em sites desconhecidos.

3.4 Programas Maliciosos

São programas criados para executar ações maliciosas no computador, como captura de senhas e danificação de arquivos e programas. Os mais comuns são:

- *Vírus* – programa que infecta o computador utilizando-se de diversos meios. É replicado pela ação do computador infectado.
- *Cavalo de troia* – programa invasor que pode ler, copiar, apagar e lterar dados do sistema sem o conhecimento do usuário.
- *Backdoors* – programa que tenta obter controle de uma máquina aproveitando-se uma falha de segurança em um programa de computador

ou sistema operacional, abrindo uma porta para seu invasor controlar o computador remotamente.

• *Keylogger* – programa capaz de capturar e armazenar as teclas digitadas pelo usuário.

3.5 O antivírus protege contra programas maliciosos?

Em geral, o antivírus detecta programas maliciosos oriundos de e-mails, cartões de memória, pen drives etc. Contudo, é sempre bom tomar cuidado com todas as mídias que recebe. Verifique sempre se o antivírus está funcionando e atualizado.

Evite também executar programas ou abrir arquivos de origem duvidosa. Lembre-se que, por exemplo, joguinhos de computador aparentemente inofensivos, ao serem executados, poderão conter e instalar programas maliciosos, que poderão ocasionar danos irreversíveis aos seus arquivos, mau funcionamento do seu equipamento ou até mesmo furtar suas senhas. Muitas vezes, esses arquivos podem vir de amigos ou colegas de trabalho que desconhecem que seus arquivos possuem essa ameaça.

3.6 Recebi um e-mail solicitando minha senha, devo responder?

NÃO! Nunca se deve informar senhas e dados pessoais por e-mail. Há uma prática maliciosa conhecida como "*phishing*", que consiste em solicitar informações ou ações do usuário. Cuidado, como essas mensagens se assemelham a e-mails verdadeiros, é possível o recebimento de algum e, por isso, deve-se estar sempre atento.

3.7 Recebi um e-mail solicitando divulgação de um fato, o que faço?

É comum algumas mensagens do tipo "*Ajude essa criança com câncer*" ou "*Previna-se do novo vírus*" solicitando divulgação ("envie para todos da sua lista"). A maioria dessas mensagens é boato e não deve ser passada adiante. Vários vírus são disseminados por meio de links em textos ou em fotos. Não se deve, portanto, abrir anexos ou links recebidos de remetentes desconhecidos.

3.8 Como verifico se um arquivo está com vírus?

Sempre que um arquivo é acessado, a ferramenta de antivírus instalada nos computadores do Instituto de Previdência Social dos Servidores Públicos de Rio do Sul – Rio do Sul PREV verifica automaticamente se há vírus ou não, desde que esteja devidamente instalado e atualizado.

4. OS MANDAMENDOS DA SEGURANÇA DA INFORMAÇÃO

✓ Utilize senhas difíceis de serem descobertas;

- ✓ Altere sua senha periodicamente;
- ✓ Tome cuidado com *downloads*;
- ✓ Tome cuidado com e-mails de remetentes desconhecidos;
- ✓ Evite sites com conteúdos duvidosos;
- ✓ Não abra anexos de e-mails desconhecidos;
- ✓ Tome cuidado com compras na internet;
- ✓ Tome cuidado ao acessar sites de bancos;
- ✓ Não revele informações sobre você na internet;
- ✓ Ao informar dados em sites, verifique se a página é segura (com prefixo “https”).

5. CONSIDERAÇÕES FINAIS

As empresas de softwares que se relacionam com a Unidade Gestora, como sistemas informatizados de cadastros, e também prestadores de serviço de hospedagem e manutenção dos servidores deverão aceitar as determinações contidas neste Manual de Boas Práticas para o uso de recursos de tecnologia do Rio do Sul PREV, preenchendo o já mencionado cadastro de usuário, Anexo I, deste Manual.

Rio Do Sul, 22 de Novembro de 2022.

VALDENIR BORGES RIBEIRO:69231125915

Assinado de forma digital por VALDENIR BORGES RIBEIRO:69231125915
Dados: 2022.11.23 09:28:01 -03'00'

VALDENIR BORGES RIBEIRO

Diretor Executivo do Rio do Sul PREV

ANEXO I

CADASTRO DE USUÁRIO

[ ] Login [ ] Internet [ ] E-mail Pessoal [ ] E-mail institucional [ ] Sistemas _____
Nome/Razão Social:
Telefone: ( ) | CPF / CNPJ:
Setor:
Data de Admissão / Início do contrato:
Vencimento do Contrato:
Justificativa para uso/acesso dos dados e/ou sistemas: _____ _____ _____ _____
Autorização do Diretor Executivo Nome: Data: _____ Assinatura
Termo de Responsabilidade do Usuário Declaro que li, entendi e aceito as determinações contidas no Manual de Boas Práticas para o uso de recursos de tecnologia do Rio do Sul PREV, comprometendo-me ao cumprimento integral deste manual e demais relativas ao assunto. Por isso, assumo quaisquer consequências advindas do descumprimento e desrespeito às normas, sendo responsável pela(s) conta(s) solicitada(s) neste documento, fazendo uso cuidadoso das senhas de acesso e mantendo-as em sigilo. _____ Assinatura
Rio do Sul, _____/_____/_____.