



MANUAL DE USO DOS RECURSOS DE INFORMÁTICA

Diretoria Administrativa-Financeira

**REGRAS E RECOMENDAÇÕES SOBRE O USO DOS RECURSOS DE
INFORMÁTICA DA INSTITUIÇÃO E AS BOAS PRÁTICAS DE SEGURANÇA**

ELABORAÇÃO

Otto Frederico Pereira de Carvalho Filho – Técnico em Tecnologia da Informação

REVISÃO

Douglas Henrique Municelli – Diretor Administrativo-Financeiro
Amadeu Carminati Neto – Controlador Interno

APROVAÇÃO

Marcos André Breda – Diretor-Presidente

Pauliprev, 17/04/2024

É livre a reprodução exclusivamente para fins não comerciais, desde que a fonte seja citada.

1. OBJETIVO

Este documento visa enumerar situações vividas no dia a dia dos colaboradores do PAULIPREV e estabelecer regras que garantam a segurança das informações e o uso racional dos recursos de informática disponibilizados pela instituição.

2. JUSTIFICATIVA

Durante a criação da rotina de Backup da instituição foi observada pelo setor de TI a existência de diversas situações de uso dos recursos que sugerem a necessidade da elaboração deste documento como um guia aos usuários.

3. DO USO RACIONAL DOS RECURSOS DE INFORMÁTICA

O uso racional dos recursos disponibilizados pela instituição permite a completa realização do backup e a diminuição do espaço ocupado nos diversos ambientes onde é armazenado, resultando em menor tempo de execução e menor custo de manutenção.

3.1. REGRAS PARA NOMES DE ARQUIVO

a) Manter o nome dos arquivos salvos com o menor tamanho possível, desde que sua identidade e propósito possam ser reconhecidos em um acesso posterior. Evitar nomes do tipo “O que disse Fulano de Tal durante a palestra realizada em 22 de abril no Museu de Artes e Ofícios.docx”. Também deve ser evitada a profusão de subpastas sempre que possível. O setor de TI tem encontrado e corrigido muitos desses arquivos, com nomes tão grandes que não conseguem ser copiados durante o backup.

Motivo: Tanto o sistema operacional Windows (utilizado nos computadores e servidores) quanto o Linux (utilizado nos equipamentos de apoio e de backup) permitem um máximo de 255 caracteres para um nome de arquivo, mas esse total inclui o caminho completo desde a raiz do servidor, por exemplo \\Servidor\Pasta\Subpasta1\Subpasta2\ ... \arquivo.

Por questões de praticidade as pastas de uso de cada setor são conectadas durante o login ao ambiente do usuário através de uma letra de unidade (“X:”, “Z:” etc.), o que pode causar problemas com nomes grandes. Por exemplo a pasta \\VW2022-DC\DADOS\ARQUIVO_MORTO\, cujo caminho possui 32 caracteres, acaba abreviada para “X:”, escondendo 30 caracteres do nome completo na hora de salvar o arquivo. É preciso ter em mente esse fato para não exceder o total de 255 caracteres.

b) Não incluir no nome do arquivo caracteres especiais, figurinhas e emoticons. O setor de TI encontrou nomes que impediam que o arquivo fosse copiado para o ambiente de nuvem.

Motivo: Os ambientes onde esses arquivos são guardados (servidor de dados local / servidor de armazenamento / espaço remoto em nuvem) possuem sistemas operacionais distintos e regras próprias do que pode ou não pode fazer parte do nome de um arquivo. O Windows, voltado ao usuário comum, é bem mais permissivo quanto a isso do que o Unix que roda no provedor de nuvem Dropbox, por exemplo, mas todos permitem caracteres básicos e acentuados.

3.2. ARQUIVOS E PASTAS DUPLICADOS

O setor de TI encontrou diversas pastas com o mesmo conteúdo em locais diferentes do diretório de dados. Como exemplo fictício, a mesma subpasta existe em “\Manuais\José\2021\” e “\Anteriores\2021\José\Manuais\”. Para promover o uso correto do diretório de dados o setor de TI recomenda:

a) Cada setor deve, individualmente, estabelecer um critério de nomenclatura e armazenamento para pastas e arquivos, devendo os colaboradores do setor seguir esse critério de forma a manter a uniformidade das informações. Dados antigos e/ou pouco utilizados, armazenados segundo outros critérios, devem ser separados para não interferir visualmente nos atuais. O setor de TI se coloca à disposição para sugestões e/ou dúvidas.

b) Não devem ser baixados para o diretório de dados da instituição conteúdos de sites ou redes sociais sem que haja por escrito, no próprio site ou no contrato de uso de seus serviços, uma autorização para tal.

Motivo: Muitos desses sites possuem direitos de copyright sobre os conteúdos apresentados e violar esses direitos pode colocar a instituição em perigo judicial.

c) Caso seja necessária a disponibilização de arquivo ou conteúdo para outros colaboradores da instituição, deve-se armazená-lo em uma pasta à qual os usuários-alvo tenham acesso, seja a do setor (no caso de assunto pertinente somente ao próprio) ou na pasta do setor contida na pasta “Pública” (para o caso de assunto de interesse geral). Os usuários-alvo devem então ser avisados por e-mail, grupo de WhatsApp ou LAN Messenger da existência do arquivo/conteúdo com o link para o acesso. Evita-se dessa maneira o envio múltiplo, que consome espaço.

d) Os usuários que receberem o aviso de conteúdo disponível devem evitar a importação para a pasta própria do seu setor ou pasta individual, visto que tal conteúdo já existe no diretório de dados da instituição e que será feito um backup diário para o caso de exclusão acidental (desde que não tenha acontecido no mesmo dia da criação).

3.3. USO DAS IMPRESSORAS

O setor de TI tem observado trabalhos de impressão monocromáticos sendo enviados para as impressoras coloridas da instituição. É bom lembrar que as impressoras a laser monocromáticas imprimem os trabalhos com uma melhor qualidade e durabilidade. Como exemplo, trabalhos impressos em impressoras a jato de tinta podem borrar caso um líquido caia no papel depois de impresso, o que não acontece com trabalhos feitos em impressoras a laser.

Os consumíveis de jato de tinta (garrafinhas) têm custo maior e durabilidade menor do que o toner da impressora a laser, de modo que os custos por cópia (que regem a maioria dos contratos de locação) são maiores para jato de tinta.

Todos os usuários são conectados durante o login a uma impressora monocromática a laser e a uma colorida a jato de tinta, portanto apenas trabalhos que contenham informações em cores devem ser enviados à segunda.

4. DAS BOAS PRÁTICAS DE SEGURANÇA

Esse item trata de pequenos cuidados que se deve ter ao lidar com conteúdo, e-mails ou arquivos recebidos de terceiros, haja vista a grande quantidade de golpes cibernéticos com as quais um usuário normal se depara no dia-a-dia. Essas práticas devem ser tratadas com seriedade e tomadas como hábito pelo usuário da instituição. O setor de TI modificará periodicamente este documento, à medida que novos tipos de golpe forem descobertos e avisará à comunidade de usuários sobre essas mudanças.

a) Mensagens via SMS

Mensagens recebidas via SMS de números desconhecidos devem ser imediatamente descartadas, principalmente as que contêm links que induzam ao usuário acioná-los, como “Clique Aqui”, “Veja”, etc.

Bancos e instituições financeiras costumam reiterar que não se comunicam com seus clientes via SMS, então mensagens do tipo “Seu pagamento não foi aprovado” e semelhantes são certeza de golpe.

b) E-mails

- Não se deve acreditar em nomes de remetente, principalmente em mensagens inesperadas ou que tentem induzir à tomada de atitude.

Motivo: O protocolo de mensagens de correio eletrônico foi criado nos primórdios da Internet e o cabeçalho da mensagem (que contém o remetente, o destinatário e outros dados da mensagem) é composto de uma série de palavras-chave em texto simples, editável por qualquer pessoa mal-intencionada com conhecimento de como construir um cabeçalho falso. Os aplicativos de correio, sendo voltados para o usuário final, ocultam a maior parte desse cabeçalho e mostram apenas as informações mais “amigáveis”, como por exemplo o nome de fantasia do remetente; daí que um cabeçalho malicioso pode conter um nome de fantasia de uma empresa conhecida ou amigo pessoal do destinatário, enquanto as sequências que indicam quem realmente está mandando e para quem a resposta deve ser enviada são completamente diferentes. A boa notícia é que, na maioria dos aplicativos de e-mail atuais, é possível saber o

verdadeiro remetente posicionando o ponteiro do mouse (computador) ou mantendo o dedo (celular) em cima do nome de fantasia; em alguns segundos o verdadeiro remetente deve aparecer. É necessário verificar sempre se o domínio do remetente (a parte do endereço de e-mail após o símbolo de “@”) pertence mesmo a quem o nome de fantasia diz pertencer. Por exemplo, um e-mail com anúncios de promoção do supermercado “XPTZ” deve conter obrigatoriamente o domínio “xptz.com.br” ou similar.

- Assim como nas mensagens via SMS, os campos em destaque (geralmente coloridos) do tipo “Veja!”, “Clique Aqui”, etc. não devem jamais ser acionados antes da verificação do remetente e da certeza de veracidade da mensagem.

- Não se deve deixar enganar por aspectos visuais. Os elementos visuais de uma mensagem podem passar noção de autenticidade, como se a mensagem tivesse realmente sido enviada pelo pretense remetente, contendo logomarcas e traços de design conhecidos, mas esses elementos podem ser facilmente retirados de páginas da Internet ou de mensagens verdadeiras.

- Anexos devem ser, sempre que possível, salvos em uma pasta local no computador e imediatamente verificados para a presença de vírus e/ou malwares, antes de serem abertos ou executados. O setor de TI está providenciando a compra de um programa antivírus corporativo para ser instalado nas máquinas e viabilizar essa prática.

c) Redes Sociais

As redes sociais são hoje responsáveis pela maior parte dos acessos à Internet feitos por usuários leigos. Tornam-se, portanto, um “prato cheio” para golpistas e malfeitores cibernéticos, que realizam todo tipo de engenharia social para o convencimento do incauto na outra ponta da comunicação. A Inteligência Artificial está cada vez mais sendo usada nesses golpes, direta e/ou indiretamente. O setor de TI, portanto, recomenda:

- Evitar se expor demasiadamente nessas redes. É preciso entender que cada texto escrito, cada foto publicada, cada hábito descrito nessas redes pode ser (e é) armazenado para a montagem de um perfil pessoal único, com características de

consumo, renda e diversas outras informações que deveriam ser de interesse apenas privado. Essas informações são vendidas a quem quer que esteja procurando por um potencial cliente e podem ser utilizadas por criminosos cibernéticos para aplicar golpes direcionados à pessoa ou seus entes queridos.

Não se deve deixar enganar, nenhum serviço útil disponibilizado por essas redes é realmente gratuito; ele é pago com a venda de informações preciosas de quem os utiliza.

- Não confiar em mensagens em aplicativos de rede social teoricamente oriundas de pessoa(s) conhecida(s) mas que denotam um comportamento não habitual dessa(s) pessoa(s), principalmente se pedirem dinheiro, dados pessoais e/ou fornecerem número telefone ou conta bancária diferentes dos já conhecidos sob a alegação “mudei, o anterior estragou”.

Motivo: As empresas que hospedam as redes sociais realizam pouca ou nenhuma verificação da veracidade dos dados fornecidos no momento da criação de um novo perfil, de modo que é fácil criar uma conta falsa para aplicar golpes. A foto que aparece no perfil também pode ser facilmente retirada de sites e perfis de outras redes, além de poder ser mudada a qualquer momento.

- Evitar conversas interativas (chats) nas quais é muito difícil para alguém não treinado distinguir se está falando com um humano ou com uma máquina. Caso não seja possível outro tipo de comunicação, não forneça dados a pedido; se necessário, confirme apenas os dados fornecidos pela outra parte.

Motivo: Os chats falsos visam obter a maior quantidade possível de dados pessoais e financeiros da pessoa, que serão utilizados posteriormente em golpes na praça.

- Desconfiar de vídeos onde alguém famoso tenta convencer o espectador a realizar transações ou entrar em sites com promoções “imperdíveis” que “acabarão logo” ou afirmando coisas que desafiam o senso comum, como ganhar dinheiro fácil ou aplicar em fundos com rentabilidades absurdas.

Motivo: A Inteligência Artificial (IA) é hoje capaz de analisar matematicamente a voz de uma pessoa conhecida e de boa reputação e criar, através de técnicas de sintetização de fala, áudios falsos dessa pessoa. A voz recriada dessa forma é praticamente idêntica à voz original.

O tipo mais básico desse golpe reproduz um vídeo verdadeiro da “celebridade” em questão com a trilha de áudio original substituída pela fala sintetizada (qualquer editor de vídeo gratuito faz isso) e algum texto fixo em letras grandes ocultando em parte a boca da pessoa para que não seja notado o descompasso entre seus movimentos labiais e o que está sendo dito.

Em um nível mais elevado, utilizando algoritmos mais sofisticados e caros com modelos de anatomia facial, a IA é capaz de recriar a figura da pessoa conhecida e confiável em situações diversas, falando normalmente com movimentos faciais e labiais quase perfeitos. O “quase” aqui é a chave para não cair no golpe; observando-se atentamente, pelo menos nos dias de hoje, ainda é possível identificar algo de não-humano no clip de vídeo.

5. CONCLUSÃO

Manter-se a par dos tipos de ameaça que rondam o usuário de Internet e dos hábitos que tornam a navegação mais segura e fluida deve ser mister para qualquer colaborador de uma empresa. O setor de TI do Pauliprev se esforça, através desse documento, em manter a comunidade ciente dos perigos atuais e futuros e o manterá atualizado e ampliado quando for necessário.