Prefeitura Municipal de Rio Bonito do Estado do Rio de Janeiro

RIO BONITO-RJ

Assistente Administrativo

JL007-N9

NOVA CONCURSOS

OBRA

Prefeitura Municipal de Rio Bonito do Estado do Rio de Janeiro

Assistente Administrativo

Edital de Concurso Público Nº 01/2019

AUTORES

Língua Portuguesa - Profª Zenaide Auxiliadora Pachegas Branco
Legislação - Adaptação Interna
Matemática - Profº Bruno Chieregatti e João de Sá Brasil
Conhecimentos Especificos - Profº Ovidio Lopes da Cruz Netto

PRODUÇÃO EDITORIAL/REVISÃO

Elaine Cristina
Leandro Filho

DIAGRAMAÇÃO

Danna Silva
Renato Vilela

CAPA

Joel Ferreira dos Santos

NOVA CONCURSOS
www.novaconcursos.com.br
sac@novaconcursos.com.br

APRESENTAÇÃO

PARABÉNS! ESTE É O PASSAPORTE PARA SUA APROVAÇÃO.

A Nova Concursos tem um único propósito: mudar a vida das pessoas.

Vamos ajudar você a alcançar o tão desejado cargo público.

Nossos livros são elaborados por professores que atuam na área de Concursos Públicos. Assim a matéria é organizada de forma que otimize o tempo do candidato. Afinal corremos contra o tempo, por isso a preparação é muito importante.

Aproveitando, convidamos você para conhecer nossa linha de produtos "Cursos online", conteúdos preparatórios e por edital, ministrados pelos melhores professores do mercado.

Estar à frente é nosso objetivo, sempre.

Contamos com índice de aprovação de 87%*.

O que nos motiva é a busca da excelência. Aumentar este índice é nossa meta.

Acesse **www.novaconcursos.com.br** e conheça todos os nossos produtos.

Oferecemos uma solução completa com foco na sua aprovação, como: apostilas, livros, cursos online, questões comentadas e treinamentos com simulados online.

Desejamos-lhe muito sucesso nesta nova etapa da sua vida!

Obrigado e bons estudos!

*Índice de aprovação baseado em ferramentas internas de medição.

CURSO ONLINE

PASSO 1
Acesse:
www.novaconcursos.com.br/passaporte

PASSO 2
Digite o código do produto no campo indicado no site.
O código encontra-se no verso da capa da apostila.
*Utilize sempre os 8 primeiros dígitos.
Ex: JN001-19

PASSO 3
Pronto!
Você já pode acessar os conteúdos online.

SUMÁRIO

LÍNGUA PORTUGUESA

LEGISLAÇÃO

MATEMÁTICA

SUMÁRIO

CONHECIMENTOS ESPECÍFICOS

ÍNDICE

CONHECIMENTOS ESPECÍFICOS

CONHECIMENTOS SOBRE PRINCÍPIOS BÁSICOS DE INFORMÁTICA, INCLUINDO HARDWARE, IMPRESSORAS, SCANNERS E MULTIFUNCIONAIS.

A Informática é um meio para diversos fins, com isso acaba atuando em todas as áreas do conhecimento. A sua utilização passou a ser um diferencial para pessoas e empresas, visto que, o controle da informação passou a ser algo fundamental para se obter maior flexibilidade no mercado de trabalho. Logo, o profissional, que melhor integrar sua área de atuação com a informática, atingirá, com mais rapidez, os seus objetivos e, consequentemente, o seu sucesso, por isso em quase todos editais de concursos públicos temos Informática.

#FicaDica

Informática pode ser considerada como significando "informação automática", ou seja, a utilização de métodos e técnicas no tratamento automático da informação. Para tal, é preciso uma ferramenta adequada: O computador.
A palavra informática originou-se da junção de duas outras palavras: informação e automática. Esse princípio básico descreve o propósito essencial da informática: trabalhar informações para atender as necessidades dos usuários de maneira rápida e eficiente, ou seja, de forma automática e muitas vezes instantânea.

O que é um computador?

O computador é uma máquina que processa dados, orientado por um conjunto de instruções e destinado a produzir resultados completos, com um mínimo de intervenção humana. Entre vários benefícios, podemos citar:

: grande velocidade no processamento e disponibilização de informações;
: precisão no fornecimento das informações;
: propicia a redução de custos em várias atividades
: próprio para execução de tarefas repetitivas;

Como ele funciona?

Em informática, e mais especialmente em computadores, a organização básica de um sistema será na forma de:

Figura 1: Etapas de um processamento de dados.

Vamos observar agora, alguns pontos fundamentais para o entendimento de informática em concursos públicos.

Hardware, são os componentes físicos do computador, ou seja, tudo que for tangível, ele é composto pelos periféricos, que podem ser de entrada, saída, entrada-saída ou apenas saída, além da CPU (Unidade Central de Processamento)

Software, são os programas que permitem o funcionamento e utilização da máquina (hardware), é a parte lógica do computador, e pode ser dividido em Sistemas Operacionais, Aplicativos, Utilitários ou Linguagens de Programação.

O primeiro software necessário para o funcionamento de um computador é o Sistema Operacional (Sistema Operacional). Os diferentes programas que você utiliza em um computador (como o Word, Excel, PowerPoint etc) são os aplicativos. Já os utilitários são os programas que auxiliam na manutenção do computador, o antivírus é o principal exemplo, e para finalizar temos as Linguagens de Programação que são programas que fazem outros programas, como o JAVA por exemplo.

Importante mencionar que os softwares podem ser livres ou pagos, no caso do livre, ele possui as seguintes características:

- O usuário pode executar o software, para qualquer uso.
- Existe a liberdade de estudar o funcionamento do programa e de adaptá-lo às suas necessidades.
- É permitido redistribuir cópias.
- O usuário tem a liberdade de melhorar o programa e de tornar as modificações públicas de modo que a comunidade inteira beneficie da melhoria.

Entre os principais sistemas operacionais pode-se destacar o Windows (Microsoft), em suas diferentes versões, o Macintosh (Apple) e o Linux (software livre criado pelo finlandês Linus Torvalds), que apresenta entre suas versões o Ubuntu, o Linux Educacional, entre outras.

É o principal software do computador, pois possibilita que todos os demais programas operem.

#FicaDica

Android é um Sistema Operacional desenvolvido pelo Google para funcionar em dispositivos móveis, como Smartphones e Tablets. Sua distribuição é livre, e qualquer pessoa pode ter acesso ao seu código-fonte e desenvolver aplicativos (apps) para funcionar neste Sistema Operacional.
iOS, é o sistema operacional utilizado pelos aparelhos fabricados pela Apple, como o iPho-

Conceitos básicos de Hardware (Placa mãe, memórias, processadores (CPU) e disco de armazenamento HDs, CDs e DVDs)

Os gabinetes são dotados de fontes de alimentação de energia elétrica, botão de ligar e desligar, botão de reset, baias para encaixe de drives de DVD, CD, HD, saídas de ventilação e painel traseiro com recortes para encaixe de placas como placa mãe, placa de som, vídeo, rede, cada vez mais com saídas USBs e outras.

No fundo do gabinete existe uma placa de metal onde será fixada a placa mãe. Pelos furos nessa placa é possível verificar se será possível ou não fixar determinada placa mãe em um gabinete, pois eles têm que ser proporcionais aos furos encontrados na placa mãe para parafusá-la ou encaixá-la no gabinete.

#FicaDica

Placa-mãe, é a placa principal, formada por um conjunto de circuitos integrados ("chip set") que reconhece e gerencia o funcionamento dos demais componentes do computador.

Se o processador pode ser considerado o "cérebro" do computador, a placa-mãe (do inglês motherboard) representa a espinha dorsal, interligando os demais periféricos ao processador.

O disco rígido, do inglês *hard disk*, também conhecido como HD, serve como unidade de armazenamento permanente, guardando dados e programas.

Ele armazena os dados em discos magnéticos que mantêm a gravação por vários anos, se necessário.

Esses discos giram a uma alta velocidade e tem seus dados gravados ou acessados por um braço móvel composto por um conjunto de cabeças de leitura capazes de gravar ou acessar os dados em qualquer posição nos discos.

Dessa forma, os computadores digitais (que trabalham com valores discretos) são totalmente binários. Toda informação introduzida em um computador é convertida para a forma binária, através do emprego de um código qualquer de armazenamento, como veremos mais adiante.

A menor unidade de informação armazenável em um computador é o algarismo binário ou dígito binário, conhecido como bit (contração das palavras inglesas binarydigit). O bit pode ter, então, somente dois valores: 0 e 1.

Evidentemente, com possibilidades tão limitadas, o bit pouco pode representar isoladamente; por essa razão, as informações manipuladas por um computador são codificadas em grupos ordenados de bits, de modo a terem um significado útil.

O menor grupo ordenado de bits representando uma informação útil e inteligível para o ser humano é o byte (leia-se "baite").

Como os principais códigos de representação de caracteres utilizam grupos de oito bits por caracter, os conceitos de byte e caracter tornam-se semelhantes e as palavras, quase sinônimas.

É costume, no mercado, construírem memórias cujo acesso, armazenamento e recuperação de informações são efetuados byte a byte. Por essa razão, em anúncios de computadores, menciona-se que ele possui "512 mega bytes de memória"; por exemplo, na realidade, em face desse costume, quase sempre o termo byte é omitido por já subentender esse valor.

Para entender melhor essas unidades de memórias, veja a imagem abaixo:

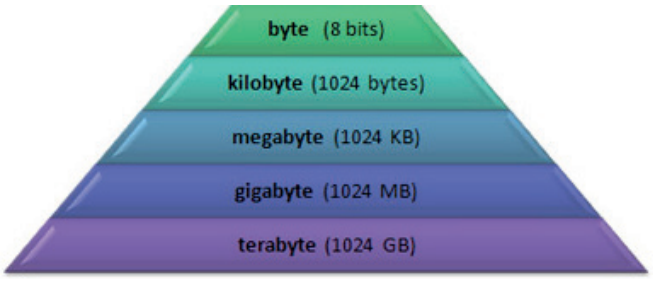


Figura 2: Unidade de medida de memórias

Em resumo, a cada degrau que você desce na Figura 3 é só você dividir por 1024 e a cada degrau que você sobe basta multiplicar por 1024. Vejamos dois exemplos abaixo:

Destacar essa tabela

Transformar 4 gigabytes em kilobytes: 4 * 1024 = 4096 megabytes 4096 * 1024 = 4194304 kilobytes.	Transformar 16422282522 kilobytes em terabytes: 16422282522 / 1024 = 16037385,28 megabytes 16037385,28 / 1024 = 15661,51 gigabytes 15661,51 / 1024 = 15,29 terabytes.

USB é abreviação de "Universal Serial Bus". É a porta de entrada mais usada atualmente.

Além de ser usado para a conexão de todo o tipo de dispositivos, ele fornece uma pequena quantidade de energia. Por isso permite que os conectores USB sejam usados por carregadores, luzes, ventiladores e outros equipamentos.

A fonte de energia do computador ou, em inglês é responsável por converter a voltagem da energia elétrica, que chega pelas tomadas, em voltagens menores, capazes de ser suportadas pelos componentes do computador.

Monitor de vídeo

Normalmente um dispositivo que apresenta informações na tela de LCD, como um televisor atual.

Outros monitores são sensíveis ao toque (chamados de touchscreen), onde podemos escolher opções tocando em botões virtuais, apresentados na tela.

Impressora

Muito popular e conhecida por produzir informações impressas em papel.

Atualmente existem equipamentos chamados impressoras multifuncionais, que comportam impressora, scanner e fotocopiadoras num só equipamento.

Pen drive é a mídia portátil mais utilizada pelos usuários de computadores atualmente.

Ele não precisar recarregar energia para manter os dados armazenados. Isso o torna seguro e estável, ao contrário dos antigos disquetes. É utilizado através de uma porta USB (Universal Serial Bus).

Cartões de memória, são baseados na tecnologia flash, semelhante ao que ocorre com a memória RAM do computador, existe uma grande variedade de formato desses cartões.

São muito utilizados principalmente em câmeras fotográficas e telefones celulares. Podem ser utilizados também em microcomputadores.

#FicaDica

BIOS é o Basic Input/Output System, ou Sistema Básico de Entrada e Saída, trata-se de um mecanismo responsável por algumas atividades consideradas corriqueiras em um computador, mas que são de suma importância para o correto funcionamento de uma máquina.

Se a BIOS para de funcionar, o PC também para! Ao iniciar o PC, a BIOS faz uma varredura para detectar e identificar todos os componentes de hardware conectados à máquina.

Só depois de todo esse processo de identificação é que a BIOS passa o controle para o sistema operacional e o boot acontece de verdade.

Diferentemente da memória RAM, as memórias ROM (Read Only Memory – Memória Somente de Leitura) não são voláteis, mantendo os dados gravados após o desligamento do computador.

As primeiras ROM não permitiam a regravação de seu conteúdo. Atualmente, existem variações que possibilitam a regravação dos dados por meio de equipamentos especiais. Essas memórias são utilizadas para o armazenamento do BIOS.

O processador que é uma peça de computador que contém instruções para realizar tarefas lógicas e matemáticas. O processador é encaixado na placa mãe através do socket, ele que processa todas as informações do computador, sua velocidade é medida em Hertz e os fabricantes mais famosos são Intel e AMD.

O processador do computador (ou CPU – Unidade Central de Processamento) é uma das partes principais do hardware do computador e é responsável pelos cálculos, execução de tarefas e processamento de dados.

Contém um conjunto de restritos de células de memória chamados registradores que podem ser lidos e escritos muito mais rapidamente que em outros dispositivos de memória. Os registradores são unidades de memória que representam o meio mais caro e rápido de armazenamento de dados. Por isso são usados em pequenas quantidades nos processadores.

Em relação a sua arquitetura, se destacam os modelos RISC (Reduced Instruction Set Computer) e CISC (Complex Instruction Set Computer). Segundo Carter [s.d.]:

... RISC são arquiteturas de carga-armazenamento, enquanto que a maior parte das arquiteturas CISC permite que outras operações também façam referência à memória.

Possuem um clock interno de sincronização que define a velocidade com que o processamento ocorre. Essa velocidade é medida em Hertz. Segundo Amigo (2008):

Em um computador, a velocidade do clock se refere ao número de pulsos por segundo gerados por um oscilador (dispositivo eletrônico que gera sinais), que determina o tempo necessário para o processador executar uma instrução. Assim para avaliar a performance de um processador, medimos a quantidade de pulsos gerados em 1 segundo e, para tanto, utilizamos uma unidade de medida de frequência, o Hertz.

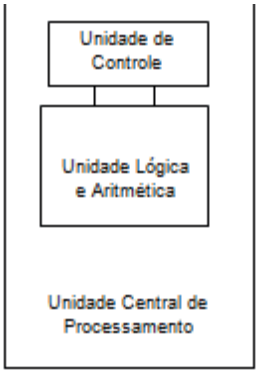


Figura 3: Esquema Processador

Na placa mãe são conectados outros tipos de placas, com seus circuitos que recebem e transmite dados para desempenhar tarefas como emissão de áudio, conexão à Internet e a outros computadores e, como não poderia faltar, possibilitar a saída de imagens no monitor.

Essas placas, muitas vezes, podem ter todo seu hardware reduzido a chips, conectados diretamente na placa mãe, utilizando todos os outros recursos necessários, que não estão implementados nesses chips, da própria motherboard. Geralmente esse fato implica na redução da

velocidade, mas hoje essa redução é pouco considerada, uma vez que é aceitável para a maioria dos usuários.

No entanto, quando se pretende ter maior potência de som, melhor qualidade e até aceleração gráfica de imagens e uma rede mais veloz, a opção escolhida são as placas off board. Vamos conhecer mais sobre esse termo e sobre as placas de vídeo, som e rede:

Placas de vídeo são hardwares específicos para trabalhar e projetar a imagem exibida no monitor. Essas placas podem ser onboard, ou seja, com chipset embutido na placa mãe, ou off board, conectadas em slots presentes na placa mãe. São considerados dispositivos de saída de dados, pois mostram ao usuário, na forma de imagens, o resultado do processamento de vários outros dados.

Você já deve ter visto placas de vídeo com especificações 1x, 2x, 8x e assim por diante. Quanto maior o número, maior será a quantidade de dados que passarão por segundo por essa placa, o que oferece imagens de vídeo, por exemplo, com velocidade cada vez mais próxima da realidade. Além dessa velocidade, existem outros itens importantes de serem observados em uma placa de vídeo: aceleração gráfica 3D, resolução, quantidade de cores e, como não poderíamos esquecer, qual o padrão de encaixe na placa mãe que ela deverá usar (atualmente seguem opções de PCI ou AGP). Vamos ver esses itens um a um:

Placas de som são hardwares específicos para trabalhar e projetar a sons, seja em caixas de som, fones de ouvido ou microfone. Essas placas podem ser onboard, ou seja, com chipset embutido na placa mãe, ou offboard, conectadas em slots presentes na placa mãe. São dispositivos de entrada e saída de dados, pois tanto permitem a inclusão de dados (com a entrada da voz pelo microfone, por exemplo) como a saída de som (através das caixas de som, por exemplo).

Placas de rede são hardwares específicos para integrar um computador a uma rede, de forma que ele possa enviar e receber informações. Essas placas podem ser onboard, ou seja, com chipset embutido na placa mãe, ou offboard, conectadas em slots presentes na placa mãe.

#FicaDica

Alguns dados importantes a serem observados em uma placa de rede são: a arquitetura de rede que atende os tipos de cabos de rede suportados e a taxa de transmissão.

Periféricos de computadores

Para entender o suficiente sobre periféricos para concurso público é importante entender que os periféricos são os componentes (hardwares) que estão sempre ligados ao centro dos computadores.

Os periféricos são classificados como:

Dispositivo de Entrada: É responsável em transmitir a informação ao computador. Exemplos: mouse, scanner, microfone, teclado, Web Cam, Trackball, Identificador Biométrico, Touchpad e outros.

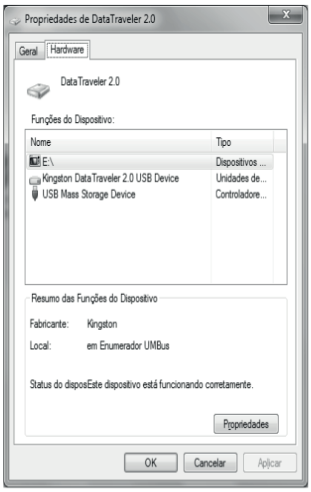
Dispositivos de Saída: É responsável em receber a informação do computador. Exemplos: Monitor, Impressoras, Caixa de Som, Ploter, Projector de Vídeo e outros.

Dispositivo de Entrada e Saída: É responsável em transmitir e receber informação ao computador. Exemplos: Drive de Disquete, HD, CD-R/RW, DVD, Blu-ray, modem, Pen-Drive, Placa de Rede, Monitor Táctil, Dispositivo de Som e outros.

#FicaDica

Periféricos sempre podem ser classificados em três tipos: entrada, saída e entrada e saída.

EXERCÍCIOS COMENTADOS



Considerando a figura acima, que ilustra as propriedades de um dispositivo USB conectado a um computador com sistema operacional Windows 7, julgue os itens a seguir

1) Escrivão de Polícia CESPE 2013

As informações na figura mostrada permitem inferir que o dispositivo USB em questão usa o sistema de arquivo NTFS, porque o fabricante é Kingston.

( ) CERTO ( ) ERRADO

Resposta: Errado - *Por padrão os pendrives (de baixa capacidade) são formatados no sistema de arquivos FAT, mas a marca do dispositivo ou mesmo a janela ilustrada não apresenta informações para afirmar sobre qual sistema de arquivos está sendo utilizado.*

2) Escrivão de Polícia CESPE 2013

Ao se clicar o ícone USB Mass Storage Device, será mostrado, no Resumo das Funções do Dispositivo, em que porta USB o dispositivo está conectado.

( ) CERTO ( ) ERRADO

Resposta: Certo - *Ao se clicar no ícone citado será de-*

monstrada uma janela com informações/propriedades do dispositivo em questão, uma das informações que aparecem na janela é a porta em que o dispositivo USB foi/está conectado.

3) Escrivão de Polícia CESPE 2013
Um clique duplo em Kingston DataTraveler 2.0 USB Device fará que seja disponibilizada uma janela contendo funcionalidades para a formatação do dispositivo USB.

( ) CERTO ( ) ERRADO

Resposta: Errado - *O Clique duplo para o caso da ilustração fará abrir a janela de propriedades do dispositivo.*

A respeito de tipos de computadores e sua arquitetura de processador, julgue os itens subsequentes

4) Escrivão de Polícia CESPE 2013
Diferentemente de um processador de 32 bits, que não suporta programas feitos para 64 bits, um processador de 64 bits é capaz de executar programas de 32 bits e de 64 bits.

( ) CERTO ( ) ERRADO

Resposta: Certo - *Se o programa for especialmente projetado para a versão de 64 bits do Windows, ele não funcionará na versão de 32 bits do Windows. (Entretanto, a maioria dos programas feitos para a versão de 32 bits do Windows funciona com uma versão de 64 bits do Windows.)*

5) Escrivão de Polícia CESPE 2013
Um processador moderno de 32 bits pode ter mais de um núcleo por processador.

( ) CERTO ( ) ERRADO

Resposta: Certo - *O processador pode ter mais de um núcleo (CORE), o que gera uma divisão de tarefas, economizando energia e gerando menos calor. EX. dual core (2 núcleos). Os tipos de processador podem ser de 32bits e 64 bits*

6) Escrivão de Polícia CESPE 2013
Se uma solução de armazenamento embasada em hard drive externo de estado sólido usando USB 2.0 for substituída por uma solução embasada em cloud storage, ocorrerá melhoria na tolerância a falhas, na redundância e na acessibilidade, além de conferir independência frente aos provedores de serviços contratados.

( ) CERTO ( ) ERRADO

Resposta: Errado - *Não há "maior independência frente aos provedores de serviço contratados", pois o acesso aos dados dependerá do provedor de serviços de nuvem no qual seus dados ficarão armazenados, qualquer que seja a nuvem. Independência para mudar de fornecedor, quando existente, não implica em dizer que o usuário fica independente do fornecedor que esteja usando no momento.*

Acerca de conceitos de hardware, julgue o item seguinte.

7) Papiloscopista CESPE 2012
Diferentemente dos computadores pessoais ou PCs tradicionais, que são operados por meio de teclado e mouse, os tablets, computadores pessoais portáteis, dispõem de recurso touchscreen. Outra diferença entre esses dois tipos de computadores diz respeito ao fato de o tablet possuir firmwares, em vez de processadores, como o PC.

( ) CERTO ( ) ERRADO

Resposta: Errado - *O uso dos processadores era algo que até um tempo atrás ficava restrito a desktops, notebooks e, em uma maior escala, a servidores, mas com a popularização de smartphones e tablets esse cenário mudou. Grandes players como Samsung, Apple e NVIDIA passaram a fabricar seus próprios modelos, conhecidos como SoCs (System on Chip), que além da CPU incluem memória RAM, placa de vídeo e muitos outros componentes.*

8) Delegado de Polícia CESPE 2004
Ao se clicar a opção WinZip, será executado um programa que permitirá a realização de operações de criptografia no arquivo para protegê-lo contra leitura indevida.

( ) CERTO ( ) ERRADO

Resposta: Errado - *WinZip é um dos principais programas para compactar e descompactar arquivos de seu computador. Perfeito para organizar e economizar espaço em seu disco rígido.*

9) Delegado de Polícia CESPE 2004
A comunicação entre a CPU e o monitor de vídeo é feita, na grande maioria dos casos, pela porta serial.

( ) CERTO ( ) ERRADO

Resposta: Errado - *As portas de vídeo mais comuns são: VGA, DVI, HDMI*

10) Delegado de Polícia CESPE 2004
Alguns tipos de mouse se comunicam com o computador por meio de porta serial.

( ) CERTO ( ) ERRADO

Resposta: Certo - *A interface serial ou porta serial, também conhecida como RS-232 é uma porta de comunicação utilizada para conectar pendrives, modems, mouses, algumas impressoras, scanners e outros equipamentos de hardware. Na interface serial, os bits são transferidos em fila, ou seja, um bit de dados de cada vez.*

CONHECIMENTO BÁSICO SOBRE SEGURANÇA DA INFORMAÇÃO.

1. Segurança da informação: procedimentos de segurança

A Segurança da Informação refere-se às proteções existentes em relação às informações de uma determinada empresa, instituição governamental ou pessoa. Ou seja, aplica-se tanto às informações corporativas quanto às pessoais.

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma corporação ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

#FicaDica

Antes de proteger, devemos saber:
- O que proteger;
- De quem proteger;
- Pontos frágeis;
- Normas a serem seguidas.

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto aos pessoais. Entende-se por informação todo conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exibida ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para definir o nível de segurança que há e, com isto, estabelecer as bases para análise de melhorias ou pioras de situações reais de segurança. A segurança de certa informação pode ser influenciada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) — Confidencialidade, Integridade e Disponibilidade — representa as principais características que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um certo grupo de informações que se almeja proteger. Outros fatores importantes são a irrevogabilidade e a autenticidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

Portanto as características básicas, de acordo com os padrões internacionais (ISO/IEC 17799:2005) são as seguintes:

- Confidencialidade – especificidade que limita o acesso a informação somente às entidades autênticas, ou seja, àquelas autorizadas pelo proprietário da informação.
- Integridade – especificidade que assegura que a informação manipulada mantenha todas as características autênticas estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
- Disponibilidade – especificidade que assegura que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários que têm autorização pelo proprietário da informação.
- Autenticidade – especificidade que assegura que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
- Irretratabilidade ou não repúdio – especificidade que assegura a incapacidade de negar a autoria em relação a uma transação feita anteriormente.

2. Mecanismos de segurança

O suporte para as orientações de segurança pode ser encontrado em:

Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que assegura a existência da informação) que a suporta.

Controles lógicos: são bloqueios que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exibida a alteração não autorizada por elemento mal-intencionado.

Existem mecanismos de segurança que sustentam os controles lógicos:

- Mecanismos de cifração ou encriptação: Permitem a modificação da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para isso, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação contrária é a decifração.
- Assinatura digital: Um conjunto de dados criptografados, agregados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não ao resguardo das informações.
- Mecanismos de garantia da integridade da informação: Usando funções de "*Hashing*" ou de checagem, é garantida a integridade através de comparação do resultado do teste local com o divulgado pelo autor.
- Mecanismos de controle de acesso: Palavras-chave, sistemas biométricos, *firewalls*, cartões inteligentes.
- Mecanismos de certificação: Atesta a validade de um documento.
- Integridade: Medida em que um serviço/informação é autêntico, ou seja, está protegido contra a entrada por intrusos.
- *Honeypot*: É uma ferramenta que tem a função proposital de simular falhas de segurança de um sistema e obter informações sobre o invasor enganando-o, e fazendo-o pensar que esteja de fato explorando uma fraqueza daquele sistema. É uma espécie de armadilha para invasores. O *HoneyPot* não oferece forma alguma de proteção.
- Protocolos seguros: Uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos citados.

3. Mecanismos de encriptação

#FicaDica

A criptografia vem, originalmente, da fusão entre duas palavras gregas:
• CRIPTO = ocultar, esconder.
• GRAFIA= escrever

Criptografia é a ciência de escrever em cifra ou em códigos. Ou seja, é um conjunto de técnicas que tornam uma mensagem ininteligível, e permite apenas que o destinatário que saiba a chave de encriptação possa decriptar e ler a mensagem com clareza.

Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para isso, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não encriptados, produzir uma continuação de dados encriptados. A operação inversa é a desencriptação.

Existem dois tipos de chave: a chave pública e a chave privada.

A chave pública é usada para codificar as informações, e a chave privada é usada para decodificar.

Dessa forma, na pública, todos têm acesso, mas para 'abrir' os dados da informação, que aparentemente não tem sentido, é preciso da chave privada, que apenas o emissor e receptor original possui.

Hoje, a criptografia pode ser considerada um método 100% seguro, pois, quem a utiliza para enviar e-mails e proteger seus arquivos, estará protegido contra fraudes e tentativas de invasão.

Os termos 'chave de 64 bits' e 'chave de 128 bits' são usados para expressar o tamanho da chave, ou seja, quanto mais bits forem utilizados, mais segura será essa criptografia.

Um exemplo disso é se um algoritmo usa uma chave de 8 bits, apenas 256 chaves poderão ser usadas para decodificar essa informação, pois 2 elevado a 8 é igual a 256. Assim, um terceiro pode tentar gerar 256 tentativas de combinações e decodificar a mensagem, que mesmo sendo uma tarefa difícil, não é impossível. Portanto, quanto maior o número de bits, maior segurança terá a criptografia.

Existem dois tipos de chaves criptográficas, as chaves simétricas e as chaves assimétricas

Chave Simétrica é um tipo de chave simples, que é usada para a codificação e decodificação. Entre os algoritmos que usam essa chave, estão:

- DES (*Data Encryption Standard*): Faz uso de chaves de 56 bits, que corresponde à aproximadamente 72 quatrilhões de combinações. Mesmo sendo um número extremamente elevado, em 1997, quebraram esse algoritmo através do método de 'tentativa e erro', em um desafio na internet.
- RC (*Ron's Code ou RivestCipher*): É um algoritmo muito utilizado em e-mails e usa chaves de 8 a 1024 bits. Além disso, ele tem várias versões que diferenciam uma das outras pelo tamanho das chaves.
- EAS (*Advanced Encryption Standard*): Atualmente é um dos melhores e mais populares algoritmos de criptografia. É possível definir o tamanho da chave como sendo de 128 bits, 192 bits ou 256 bits.
- IDEA (*International Data Encryption Algorithm*): É um algoritmo que usa chaves de 128 bits, parecido com o DES. Seu ponto forte é a fácil execução de software.

As chaves simétricas não são absolutamente seguras quando referem-se às informações extremamente valiosas, principalmente pelo emissor e o receptor precisarem ter o conhecimento da mesma chave. Dessa forma, a transmissão pode não ser segura e o conteúdo pode chegar a terceiros.

Chave Assimétrica utiliza duas chaves: a privada e a pública. Elas se sintetizam da seguinte forma: a chave pública para codificar e a chave privada para decodificar, considerando-se que a chave privada é secreta. Entre os algoritmos utilizados, estão:

- RSA (*Rivest, Shmirand Adleman*): É um dos algoritmos de chave assimétrica mais usados, em que dois números primos (aqueles que só podem ser divididos por 1 e por eles mesmos) são multiplicados para obter um terceiro valor. Assim, é preciso fazer fatoração, que significa descobrir os dois primeiros números a partir do terceiro, sendo um cálculo difícil. Assim, se números grandes forem utilizados, será praticamente impossível descobrir o código. A chave privada do RSA são os números que são multiplicados e a chave pública é o valor que será obtido.
- *El Gamal*: Utiliza-se do 'logaritmo discreto', que é um problema matemático que o torna mais seguro. É muito usado em assinaturas digitais.

Vírus

Firewall é uma solução de segurança fundamentada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser realizadas. "Parede de fogo", a tradução literal do nome, já deixa claro que o *firewall* se enquadra em uma espécie de barreira de defesa. A sua missão, consiste basicamente em bloquear tráfego de dados indesejados e liberar acessos desejados.

Para melhor compreensão, imagine um firewall como sendo a portaria de um condomínio: para entrar, é necessário obedecer a determinadas regras, como se identificar, ser esperado por um morador e não portar qualquer objeto que possa trazer riscos à segurança; para sair, não se pode levar nada que pertença aos condôminos sem a devida autorização.

Neste sentido, um firewall pode impedir uma série de ações maliciosas: um malware que utiliza determinada porta para se instalar em um computador sem o usuário saber, um programa que envia dados sigilosos para a internet, uma tentativa de acesso à rede a partir de computadores externos não autorizados, entre outros.

Você já sabe que um firewall atua como uma espécie de barreira que verifica quais dados podem passar ou

não. Esta tarefa só pode ser feita mediante o estabelecimento de políticas, isto é, de regras estabelecidas pelo usuário.

Em um modo mais restritivo, um firewall pode ser configurado para bloquear todo e qualquer tráfego no computador ou na rede. O problema é que esta condição isola este computador ou esta rede, então pode-se criar uma regra para que, por exemplo, todo aplicativo aguarde autorização do usuário ou administrador para ter seu acesso liberado. Esta autorização poderá inclusive ser permanente: uma vez dada, os acessos seguintes serão automaticamente permitidos.

Em um modo mais versátil, um firewall pode ser configurado para permitir automaticamente o tráfego de determinados tipos de dados, como requisições HTTP (veja mais sobre esse protocolo no ítem 7), e bloquear outras, como conexões a serviços de e-mail.

Perceba, como estes exemplos, tem políticas de um firewall que são baseadas, inicialmente, em dois princípios: todo tráfego é bloqueado, exceto o que está explicitamente autorizado; todo tráfego é permitido, exceto o que está explicitamente bloqueado.

Firewalls mais avançados podem ir além, direcionando determinado tipo de tráfego para sistemas de segurança internos mais específicos ou oferecendo um reforço extraem procedimentos de autenticação de usuários, por exemplo.

O trabalho de um firewall pode ser realizado de várias formas. O que define uma metodologia ou outra são fatores como critérios do desenvolvedor, necessidades específicas do que será protegido, características do sistema operacional que o mantém, estrutura da rede e assim por diante. É por isso que podemos encontrar mais de um tipo de firewall. A seguir, os mais conhecidos.

Filtragem de pacotes (packetfiltering): As primeiras soluções de firewall surgiram na década de 1980 baseando-se em filtragem de pacotes de dados (*packetfiltering*), uma metodologia mais simples e, por isso, mais limitada, embora ofereça um nível de segurança significativo.

Para compreender, é importante saber que cada pacote possui um cabeçalho com diversas informações a seu respeito, como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, entre outros. O Firewall então analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote (seja para sair ou para entrar na máquina/rede), podendo também executar alguma tarefa relacionada, como registrar o acesso (ou tentativa de) em um arquivo de log.

O firewall de aplicação, também conhecido como proxy de serviços (*proxy services*) ou apenas *proxy* é uma solução de segurança que atua como intermediário entre um computador ou uma rede interna e outra rede, externa normalmente, a internet. Geralmente instalados em servidores potentes por precisarem lidar com um grande número de solicitações, firewalls deste tipo são opções interessantes de segurança porque não permitem a comunicação direta entre origem e destino.

A imagem a seguir ajuda na compreensão do conceito. Perceba que em vez de a rede interna se comunicar diretamente com a internet, há um equipamento entre ambos que cria duas conexões: entre a rede e o proxy; e entre o proxy e a internet. Observe:

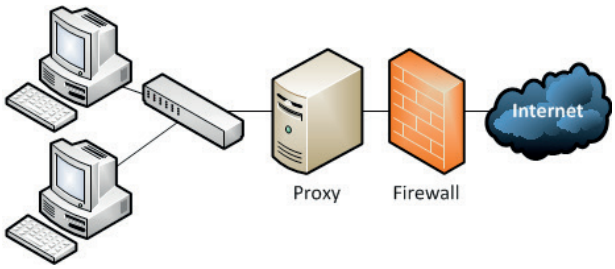


Figura 91: Proxy

Perceba que todo o fluxo de dados necessita passar pelo proxy. Desta forma, é possível, por exemplo, estabelecer regras que impeçam o acesso de determinados endereços externos, assim como que proíbam a comunicação entre computadores internos e determinados serviços remotos.

Este controle amplo também possibilita o uso do proxy para tarefas complementares: o equipamento pode registrar o tráfego de dados em um arquivo de log; conteúdo muito utilizado pode ser guardado em uma espécie de cache (uma página Web muito acessada fica guardada temporariamente no proxy, fazendo com que não seja necessário requisitá-la no endereço original a todo instante, por exemplo); determinados recursos podem ser liberados apenas mediante autenticação do usuário; entre outros.

A implementação de um proxy não é tarefa fácil, haja visto a enorme quantidade de serviços e protocolos existentes na internet, fazendo com que, dependendo das circunstâncias, este tipo de firewall não consiga ou exija muito trabalho de configuração para bloquear ou autorizar determinados acessos.

Proxy transparente: No que diz respeito a limitações, é conveniente mencionar uma solução chamada de **proxy transparente**. O proxy "tradicional", não raramente, exige que determinadas configurações sejam feitas nas ferramentas que utilizam a rede (por exemplo, um navegador de internet) para que a comunicação aconteça sem erros. O problema é, dependendo da aplicação, este trabalho de ajuste pode ser inviável ou custoso.

O proxy transparente surge como uma alternativa para estes casos porque as máquinas que fazem parte da rede não precisam saber de sua existência, dispensando qualquer configuração específica. Todo acesso é feito normalmente do cliente para a rede externa e vice-versa, mas o proxy transparente consegue interceptá-lo e responder adequadamente, como se a comunicação, de fato, fosse direta.

É válido ressaltar que o proxy transparente também tem lá suas desvantagens, por exemplo: um proxy «normal» é capaz de barrar uma atividade maliciosa, como um malware enviando dados de uma máquina para a internet; o proxy transparente, por sua vez, pode não bloquear este tráfego. Não é difícil entender: para conseguir se comunicar externamente, o malware teria que

ser configurado para usar o proxy «normal» e isso geralmente não acontece; no proxy transparente não há esta limitação, portanto, o acesso aconteceria normalmente.

1. Limitações dos firewalls

#FicaDica

Firewalls têm lá suas limitações, sendo que estas variam conforme o tipo de solução e a arquitetura utilizada. De fato, firewalls são recursos de segurança bastante importantes, mas não são perfeitos em todos os sentidos.

Seguem abaixo algumas dessas limitações:

- Um firewall pode oferecer a segurança desejada, mas comprometer o desempenho da rede (ou mesmo de um computador). Esta situação pode gerar mais gastos para uma ampliação de infraestrutura capaz de superar o problema;
- A verificação de políticas tem que ser revista periodicamente para não prejudicar o funcionamento de novos serviços;
- Novos serviços ou protocolos podem não ser devidamente tratados por proxies já implementados;
- Um firewall pode não ser capaz de impedir uma atividade maliciosa que se origina e se destina à rede interna;
- Um firewall pode não ser capaz de identificar uma atividade maliciosa que acontece por descuido do usuário - quando este acessa um site falso de um banco ao clicar em um link de uma mensagem de e-mail, por exemplo;
- Firewalls precisam ser "vigiados". Malwares ou atacantes experientes podem tentar descobrir ou explorar brechas de segurança em soluções do tipo;
- Um firewall não pode interceptar uma conexão que não passa por ele. Se, por exemplo, um usuário acessar a internet em seu computador a partir de uma conexão 3G (justamente para burlar as restrições da rede, talvez), o firewall não conseguirá interferir.

2. Sistema antivírus

Qualquer usuário já foi, ou ainda é vítima dos vírus, spywares, trojans, entre muitos outros. Quem que nunca precisou formatar seu computador?

Os vírus representam um dos maiores problemas para usuários de computador. Para poder resolver esses problemas, as principais desenvolvedoras de softwares criaram o principal utilitário para o computador, os antivírus, que são programas com o propósito de detectar e eliminar vírus e outros programas prejudiciais antes ou depois de ingressar no sistema.

Os vírus, worms, Trojans, spyware são tipos de programas de software que são implementados sem o consentimento (e inclusive conhecimento) do usuário ou proprietário de um computador e que cumprem diversas funções nocivas para o sistema. Entre elas, o roubo e perda de dados, alteração de funcionamento, interrupção do sistema e propagação para outros computadores.

Os antivírus são aplicações de software projetadas como medida de proteção e segurança para resguardar os dados e o funcionamento de sistemas informáticos caseiros e empresariais de outras aplicações conhecidas comumente como vírus ou malware que tem a função de alterar, perturbar ou destruir o correto desempenho dos computadores.

Um programa de proteção de vírus tem um funcionamento comum que com frequência compara o código de cada arquivo que revisa com uma base de dados de códigos de vírus já conhecidos e, desta maneira, pode determinar se trata de um elemento prejudicial para o sistema. Também pode reconhecer um comportamento ou padrão de conduta típica de um vírus. Os antivírus podem registrar tanto os arquivos encontrados dentro do sistema como aqueles que procuram ingressar ou interagir com o mesmo.

Como novos vírus são criados de maneira quase constante, sempre é preciso manter atualizado o programa antivírus de maneira de que possa reconhecer as novas versões maliciosas. Assim, o antivírus pode permanecer em execução durante todo tempo que o sistema informático permaneça ligado, ou registrar um arquivo ou série de arquivos cada vez que o usuário exija. Normalmente, o antivírus também pode verificar e-mails e sites de entrada e saída visitados.

Um antivírus pode ser complementado por outros aplicativos de segurança, como firewalls ou anti-spywares que cumprem funções auxiliares para evitar a entrada de vírus.

Então, antivírus são os programas criados para manter seu computador seguro, protegendo-o de programas maliciosos, com o intuito de estragar, deletar ou roubar dados de seu computador.

Ao pesquisar sobre antivírus para baixar, sempre escolha os mais famosos, ou conhecidos, pois hackers estão usando este mercado para enganar pessoas com falsos softwares, assim, você instala um "antivírus" e deixa seu computador vulnerável aos ataques.

E esses falsos softwares estão por toda parte, cuidado ao baixar programas de segurança em sites desconhecidos, e divulgue, para que ninguém seja vítima por falta de informação.

Os vírus que se anexam a arquivos infectam também todos os arquivos que estão sendo ou e serão executados. Alguns às vezes recontaminam o mesmo arquivo tantas vezes e ele fica tão grande que passa a ocupar um espaço considerável (que é sempre muito precioso) em seu disco. Outros, mais inteligentes, se escondem entre os espaços do programa original, para não dar a menor pista de sua existência.

Cada vírus possui um critério para começar o ataque propriamente dito, onde os arquivos começam a ser apagados, o micro começa a travar, documentos que não são salvos e várias outras tragédias. Alguns apenas mostram mensagens chatas, outros mais elaborados fazem estragos muito grandes.

Existe uma variedade enorme de softwares antivírus no mercado. Independente de qual você usa, mantenha-o sempre atualizado. Isso porque surgem vírus novos

todos os dias e seu antivírus precisa saber da existência deles para proteger seu sistema operacional.

A maioria dos softwares antivírus possuem serviços de atualização automática. Abaixo há uma lista com os antivírus mais conhecidos:

Norton AntiVirus - Symantec - www.symantec.com.br - Possui versão de teste.

McAfee - McAfee - http://www.mcafee.com.br - Possui versão de teste.

AVG - Grisoft - www.grisoft.com - Possui versão paga e outra gratuita para uso não comercial (com menos funcionalidades).

Panda Antivírus - Panda Software - www.pandasoftware.com.br - Possui versão de teste.

É importante frisar que a maioria destes desenvolvedores possuem ferramentas gratuitas destinadas a remover vírus específicos. Geralmente, tais softwares são criados para combater vírus perigosos ou com alto grau de propagação.

Figura 92: Principais antivírus do mercado atual

2. Tipos de Vírus

Cavalo-de-Tróia: A denominação "Cavalo de Tróia" (Trojan Horse) foi atribuída aos programas que permitem a invasão de um computador alheio com espantosa facilidade. Nesse caso, o termo é análogo ao famoso artefato militar fabricado pelos gregos espartanos. Um "amigo" virtual presenteia o outro com um "presente de grego", que seria um aplicativo qualquer. Quando o leigo o executa, o programa atua de forma diferente do que era esperado.

Ao contrário do que é erroneamente informado na mídia, que classifica o Cavalo de Tróia como um vírus, ele não se reproduz e não tem nenhuma comparação com vírus de computador, sendo que seu objetivo é totalmente diverso. Deve-se levar em consideração, também, que a maioria dos antivírus faz a sua detecção e os classificam como tal. A expressão "Trojan" deve ser usada, exclusivamente, como definição para programas que capturam dados sem o conhecimento do usuário. O Cavalo de Tróia é um programa que se aloca como um arquivo no computador da vítima. Ele tem o intuito de roubar informações como passwords, logins e quaisquer dados, sigilosos ou não, mantidos no micro da vítima. Quando a máquina contaminada por um Trojan conectar-se à Internet, poderá ter todas as informações contidas no HD visualizadas e capturadas por um intruso qualquer. Estas visitas são feitas imperceptivelmente. Só quem já esteve dentro de um computador alheio sabe as possibilidades oferecidas.

Worms (vermes) podem ser interpretados como um tipo de vírus mais inteligente que os demais. A principal diferença entre eles está na forma de propagação: os worms podem se propagar rapidamente para outros computadores, seja pela Internet, seja por meio de uma rede local. Geralmente, a contaminação ocorre de maneira discreta e o usuário só nota o problema quando o computador apresenta alguma anormalidade. O que faz destes vírus inteligentes é a gama de possibilidades de propagação. O worm pode capturar endereços de e-mail em arquivos do usuário, usar serviços de SMTP (sistema de envio de e-mails) próprios ou qualquer outro meio que permita a contaminação de computadores (normalmente milhares) em pouco tempo.

Spywares, keyloggers e hijackers: Apesar de não serem necessariamente vírus, estes três nomes também representam perigo. Spywares são programas que ficam «espionando» as atividades dos internautas ou capturam informações sobre eles. Para contaminar um computador, os spywares podem vir embutidos em softwares desconhecidos ou serem baixados automaticamente quando o internauta visita sites de conteúdo duvidoso.

Os keyloggers são pequenos aplicativos que podem vir embutidos em vírus, spywares ou softwares suspeitos, destinados a capturar tudo o que é digitado no teclado. O objetivo principal, nestes casos, é capturar senhas.

Hijackers são programas ou scripts que «sequestram» navegadores de Internet, principalmente o Internet Explorer. Quando isso ocorre, o hijacker altera a página inicial do browser e impede o usuário de mudá-la, exibe propagandas em pop-ups ou janelas novas, instala barras de ferramentas no navegador e podem impedir acesso a determinados sites (como sites de software antivírus, por exemplo).

Os spywares e os keyloggers podem ser identificados por programas anti-spywares. Porém, algumas destas pragas são tão perigosas que alguns antivírus podem ser preparados para identificá-las, como se fossem vírus. No caso de hijackers, muitas vezes é necessário usar uma ferramenta desenvolvida especialmente para combater aquela praga. Isso porque os hijackers podem se infiltrar no sistema operacional de uma forma que nem antivírus nem anti-spywares conseguem "pegar".

Hoaxes: São boatos espalhados por mensagens de correio eletrônico, que servem para assustar o usuário de computador. Uma mensagem no e-mail alerta para um novo vírus totalmente destrutivo que está circulando na rede e que infectará o micro do destinatário enquanto a mensagem estiver sendo lida ou quando o usuário clicar em determinada tecla ou link. Quem cria a mensagem hoax normalmente costuma dizer que a informação partiu de uma empresa confiável, como IBM e Microsoft, e que tal vírus poderá danificar a máquina do usuário. Desconsidere a mensagem.