

Prefeitura de Vila Velha do Estado do Espírito Santo

VILA VELHA-ES

PA – Professor Séries Iniciais

DZ071-N9

Todos os direitos autorais desta obra são protegidos pela Lei nº 9.610, de 19/12/1998.
Proibida a reprodução, total ou parcialmente, sem autorização prévia expressa por escrito da editora e do autor. Se você conhece algum caso de "pirataria" de nossos materiais, denuncie pelo sac@novaconcursos.com.br.

OBRA

Prefeitura de Vila Velha do Estado do Espírito Santo

PA - Professor Séries Iniciais

EDITAL DE CONCURSO PÚBLICO Nº002/2019, PMVV/ES DE 13 DE DEZEMBRO DE 2019

AUTORES

Língua Portuguesa - Profª Zenaide Auxiliadora Pachegas Branco
Raciocínio Lógico Quantitativo - Profº Bruno Chierigatti e João de Sá Brasil
Legislação Educacional - Profº Fernando Zantedeschi
Tecnologias Educacionais - Profª Ana Maria B. Quiqueto
Conhecimentos Pedagógicos - Profª Ana Maria B. Quiqueto
Fundamentação - Profª Ana Maria B. Quiqueto
Tópicos Língua Portuguesa - Profª Ana Maria B. Quiqueto e Profª Zenaide Auxiliadora Pachegas Branco
Matemática - Profº Bruno Chierigatti e João de Sá Brasil
Ciências - Profª Janaina Lopes de Oliviera
História e Geografia - Profª Leticia Veloso e Silvana Guimarães

PRODUÇÃO EDITORIAL/REVISÃO

Leandro Filho

Robson Silva

DIAGRAMAÇÃO

Thais Regis

Renato Vilela

CAPA

Joel Ferreira dos Santos



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

Compreensão de texto. Condições de leitura e produção textual: a enunciação. Coesão e coerência textuais.....	01
Intertextualidade.....	16
Tipologia textual.....	18
Semântica: sinonímia, antonímia, homonímia, paronímia, polissemia.....	19
Linguagem figurada.....	22
Sistema fonológico do português.....	26
Sistema ortográfico vigente.....	28
Morfossintaxe: classes de palavras e seu emprego. Formação de palavras. Morfologia nominal. Morfologia verbal. Morfologia pronominal.....	37
Processos sintáticos: subordinação e coordenação. Constituintes da oração e orações no período. Frase e discurso...	79
Valores semântico-sintáticos dos conectivos.....	88
Concordância nominal e verbal.....	88
Regência nominal e verbal.....	95
Classes de palavras.....	100
Verbos: conjugação, emprego dos tempos, modos e vozes verbais.....	100
Estrutura do período simples e do período composto. Funções sintáticas.....	100

RACIOCÍNIO LÓGICO QUANTITATIVO

Programa: Entendimento da estrutura lógica de relações arbitrárias entre as pessoas, lugares, objetos ou eventos fictícios; dedução de novas relações em função de relações fornecidas e avaliação das condições usadas para estabelecer a estrutura daquelas relações. Compreensão e análise da lógica de uma situação, utilizando as funções intelectuais; raciocínio verbal, raciocínio matemático, raciocínio sequencial, orientação espacial e temporal, formação de conceitos e discriminação de elementos.....	01
Porcentagem.....	42
Razões e Proporções.....	45
Regra de três (simples e composta).....	48
Princípio fundamental da contagem, combinatória, permutações.....	50
Problemas utilizando as operações fundamentais.....	54
Probabilidade.....	62
Conjuntos.....	64
Progressões aritméticas, geométricas e matemática financeira.....	68

LEGISLAÇÃO EDUCACIONAL

Lei Municipal nº 5.629/2015 - Plano Municipal de Educação.....	01
Lei Municipal nº 5.938/2017 - Gestão Democrática da Educação no Sistema Municipal de Ensino de Vila Velha.....	01
Lei Municipal nº 4.100/2003 - Sistema Municipal de Ensino do Município de Vila Velha e disciplina o seu funcionamento.....	03

SUMÁRIO

Lei Municipal nº 4.670/2008 – Plano de Cargos e Salários do Magistério.....	06
Lei complementar Municipal nº 019/2011- Estatuto do Magistério.....	07
Base Nacional Comum Curricular - BNCC.....	11

TECNOLOGIAS EDUCACIONAIS

Computação e armazenamento em nuvem.....	01
Sistemas operacionais - Windows e Linux.....	15
Fundamentos da Tecnologia Educacional.....	27
Dispositivos móveis e Apps.....	30
Mídias digitais.....	32
O uso da internet na educação.....	36
Uso de tecnologias no processo de ensino aprendizagem.....	42
Redes sociais em educação.....	47
Éticas nas redes.....	48
A questão da resistência às novas tecnologias.....	51
O uso da tecnologia no planejamento e gestão de projetos educacionais.....	54

CONHECIMENTOS PEDAGÓGICOS

Os quatro pilares da educação para a educação do século XXI.....	01
Teoria Sócio- interacionista de Vygotsky. Tendência Pedagógica Progressista Crítico-social dos conteúdos.....	01
Competências e Habilidades na educação.....	11
Currículo: concepções, elaboração, prática, interdisciplinaridade, transdisciplinaridade, transversalidade.....	23
Contribuições de Mikail Backthin na linguagem.....	33
As dez competências gerais da Base Nacional Comum Curricular.....	34
Metodologias Ativas.....	34
Contribuição da Neurociência para educação.....	42
Inteligências Múltiplas.....	43
Avaliação da aprendizagem: conceitos, concepções e práticas.....	51
Projeto Político Pedagógico.....	59
Mediação de Conflitos e Comunicação Não Violenta.....	66
Educação Inclusiva e legislações que fundamentam o assunto e as modalidades de ensino na educação básica.....	67
O Conselho Escolar como instrumento de Gestão Democrática.....	78
Aluno público alvo da Educação Especial.....	81
Nota Técnica MEC nº 004/2014.....	81

SUMÁRIO

FUNDAMENTAÇÃO

Base Nacional Comum Curricular – BNCC: da etapa do Ensino Fundamental (competências específicas das Áreas de Conhecimento do 1º ao 5º ano, currículo, protagonismos na Educação Básica, práticas de avaliação, inclusão. Alfabetização e letramento. Apropriação da linguagem oral e escrita nos anos do Ensino Fundamental numa perspectiva histórico-cultural. A importância da leitura dialógica na sala de aula. Ensino com base no princípio de resolução de problemas.....	01 32
--	----------

TÓPICOS LÍNGUA PORTUGUESA

Texto: leitura e compreensão de textos literários e não literários; intertextualidade; gêneros textuais.....	01
Mecanismo de coesão.....	01
Varição linguística.....	01
Princípios de fonologia, acentuação tônica e gráfica.....	01
Princípios de morfossintaxe: estrutura e formação de palavras, classes gramaticais e funções sintáticas.....	01
Alfabetização e Letramento: apropriação da linguagem oral e escrita nos anos iniciais numa perspectiva histórico-cultural.....	02

MATEMÁTICA

Números Naturais. Números Racionais. Operações com números naturais.....	01
Números racionais.....	05
Figuras geométricas. Área e perímetro.....	12
Sistemas de medidas: comprimento, área, volume, capacidade, massa, temperatura e tempo.....	21
Sistema monetário.....	26
Tratamento da informação.....	29

CIÊNCIAS

Ar: importância, composição e propriedades. Água: importância, composição, propriedades, estados físicos e ciclo da água. Composição e erosão do solo.....	01
Caracterização e classificação dos seres vivos e sua relação com o ambiente.....	19
Noções básicas de anatomia e fisiologia humana e princípios básicos de saúde.....	24

SUMÁRIO

HISTÓRIA E GEOGRAFIA

Localização espacial: pontos cardeais e colaterais. Mapas, escalas, plantas e convenções cartográficas.....	01
Transformações naturais e humanas no relevo, solo, hidrografia, clima e vegetação Brasil: população, urbanização, divisões do espaço, questão ambiental.....	07
Fontes históricas e periodização.....	19
Formação da sociedade brasileira.....	20
História e Geografia do Espírito Santo e Vila Velha.....	36

ÍNDICE

TECNOLOGIAS EDUCACIONAIS

Computação e armazenamento em nuvem.....	01
Sistemas operacionais - Windows e Linux.....	15
Fundamentos da Tecnologia Educacional.....	27
Dispositivos móveis e Apps.....	30
Mídias digitais.....	32
O uso da internet na educação.....	36
Uso de tecnologias no processo de ensino aprendizagem.....	42
Redes sociais em educação.....	47
Éticas nas redes.....	48
A questão da resistência às novas tecnologias.....	51
O uso da tecnologia no planejamento e gestão de projetos educacionais.....	54

COMPUTAÇÃO E ARMAZENAMENTO EM NUVEM

CONCEITOS E FUNDAMENTOS BÁSICOS DE INFORMÁTICA

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, conseqüentemente, 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 iPhone e o iPad.

Identificação e manipulação de arquivos

Pastas – são estruturas digitais criadas para organizar arquivos, ícones ou outras pastas.

Arquivos – são registros digitais criados e salvos através de programas aplicativos. Por exemplo, quando abrimos a Microsoft Word, digitamos uma carta e a salvamos no computador, estamos criando um arquivo.

Ícones – são imagens representativas associadas a programas, arquivos, pastas ou atalhos. As duas figuras mostradas nos itens anteriores são ícones. O primeiro representa uma pasta e o segundo, um arquivo criado no programa Excel.

Atalhos – são ícones que indicam um caminho mais curto para abrir um programa ou até mesmo um arquivo.

Clicando com o botão direito do mouse sobre um espaço vazio da área de trabalho, temos as seguintes opções, de organização:

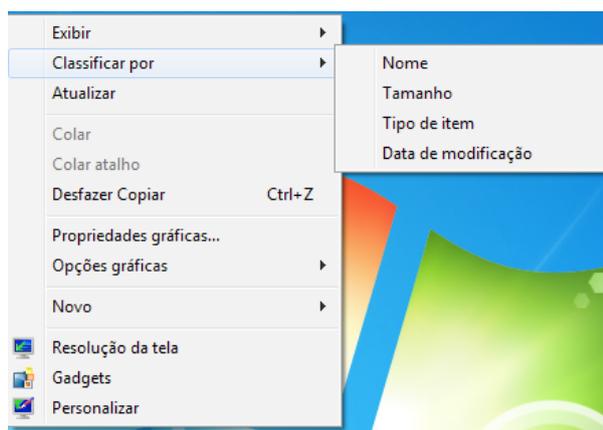


Figura 3: Organizar ícones

- Nome: Organiza os ícones por ordem alfabética de nomes, permanecendo inalterados os ícones padrão da área de trabalho.
- Tamanho: Organiza os ícones pelo seu tamanho em bytes, permanecendo inalterados os ícones padrão da área de trabalho.
- Tipo: Organiza os ícones em grupos de tipos, por exemplo, todas as pastas ficarão ordenadas em sequência, depois todos os arquivos, e assim por diante, permanecendo inalterados os ícones padrão da área de trabalho.
- Modificado em: Organiza os ícones pela data da última alteração, permanecendo inalterados os ícones padrão da área de trabalho.
- Organizar automaticamente: Não permite que os ícones sejam colocados em qualquer lugar na área de trabalho. Quando arrastados pelo usuário, ao soltar o botão esquerdo, o ícone voltará ao seu lugar padrão.
- Alinhar à grade: estabelece uma grade invisível para alinhamento dos ícones.
- Mostrar ícones da área de trabalho: Oculta ou mostra os ícones colocados na área de trabalho, inclusive os ícones padrão, como Lixeira, Meu Computador e Meus Documentos.
- Bloquear itens da Web na área de trabalho: Bloqueia recursos da Internet ou baixados em temas da web e usados na área de trabalho.
- Executar assistente para limpeza da área de trabalho:

Inicia um assistente para eliminar da área de trabalho ícones que não estão sendo utilizados.

Para acessar o Windows Explorer, basta clicar no botão Windows, Todos os Programas, Acessórios, Windows Explorer, ou usar a tecla do Windows+E. O Windows Explorer é um ambiente do Windows onde podemos realizar o gerenciamento de arquivos e pastas. Nele, temos duas divisões principais: o lado esquerdo, que exibe as pastas e diretórios em esquema de hierarquia e o lado direito que exibe o conteúdo das pastas e diretórios selecionados do lado esquerdo.

Quando clicamos, por exemplo, sobre uma pasta com o botão direito do mouse, é exibido um menu suspenso com diversas opções de ações que podem ser realizadas. Em ambos os lados (esquerdo e direito) esse procedimento ocorre, mas do lado esquerdo, não é possível visualizar a opção "Criar atalho", como é possível observar nas figuras a seguir:

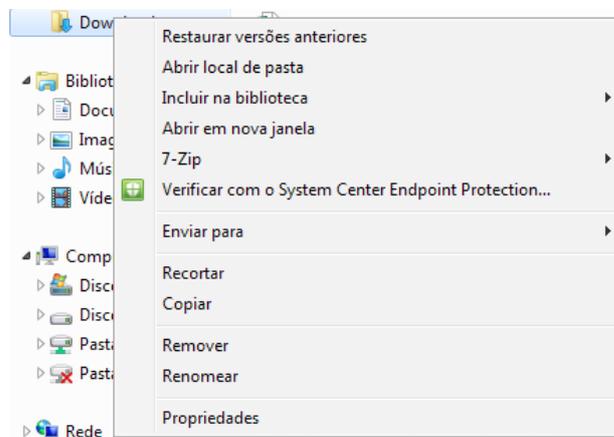


Figura 4: Windows Explorer – botão direito

A figura a cima mostra as opções exibidas no menu suspenso quando clicamos na pasta DOWNLOADS com o botão direito do mouse, do lado esquerdo do Windows Explorer.

No Windows Explorer podemos realizar facilmente opções de gerenciamento como copiar, recortar, colar e mover, pastas e arquivos.

-Copiar e Colar: consiste em criar uma cópia idêntica da pasta, arquivo ou atalho selecionado. Para essa tarefa, podemos adotar os seguintes procedimentos:

- 1º) Selecione o item desejado;
- 2º) Clique com o botão direito do mouse e depois com o esquerdo em "copiar". Se preferir, pode usar as teclas de atalho CTRL+C. Esses passos criarão uma cópia do arquivo ou pasta na memória RAM do computador, mas a cópia ainda não estará em nenhum lugar visível do sistema operacional.
- 3º) Clique com o botão direito do mouse no local onde deseja deixar a cópia e depois, com o esquerdo, clique em "colar". Também podem ser usadas as teclas CTRL + V, para efetivar o processo de colagem.

Dessa forma, teremos o mesmo arquivo ou pasta em mais de um lugar no computador.

-Recortar e Colar: Esse procedimento retira um arquivo ou pasta de um determinado lugar e o coloca em outro. É como se recortássemos uma figura de uma revista e a colássemos em um caderno. O que recortarmos ficará apenas em um lugar do computador.

Os passos necessários para recortar e colar, são:

- 1º) Selecione o item desejado;
- 2º) Clique com o botão direito do mouse e depois com o esquerdo em "recortar". Se preferir, pode usar as teclas de atalho CTRL+X. Esses passos criarão uma cópia do arquivo ou pasta na memória RAM do computador, mas a cópia ainda não estará em nenhum lugar visível do sistema operacional.
- 3º) Clique com o botão direito do mouse no local onde deseja deixar a cópia e depois, com o esquerdo, clique em "colar". Também podem ser usadas as teclas CTRL + V, para efetivar o processo de colagem.

Lixeira: Contém os arquivos e pastas excluídos pelo usuário. Para excluímos arquivos, atalhos e pastas, podemos clicar com o botão direito do mouse sobre eles e depois usar a opção "Excluir". Outra forma é clicar uma vez sobre o objeto desejado e depois pressionar o botão delete, no teclado. Esses dois procedimentos enviarão para lixeira o que foi excluído, sendo possível a restauração, caso haja necessidade. Para restaurar, por exemplo, um arquivo enviado para a lixeira, podemos, após abri-la, restaurar o que desejarmos.

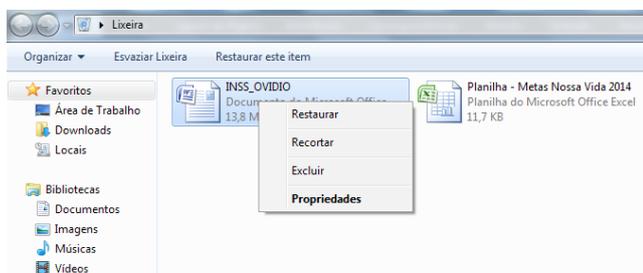


Figura 5: Restauração de arquivos enviados para a lixeira



#FicaDica

A restauração de objetos enviados para a lixeira pode ser feita com um clique com o botão direito do mouse sobre o item desejado e depois, outro clique com o esquerdo em "Restaurar". Isso devolverá, automaticamente o arquivo para seu local de origem. Outra forma de restaurar é usar a opção "Restaurar este item", após selecionar o objeto.

Alguns arquivos e pastas, por terem um tamanho muito grande, são excluídos sem irem antes para a Lixeira. Sempre que algo for ser excluído, aparecerá uma mensagem, ou perguntando se realmente deseja enviar aquele item para a Lixeira, ou avisando que o que foi selecionado será permanentemente excluído. Outra forma de excluir documentos ou pastas sem que eles fiquem armazenados na Lixeira é usar as teclas de atalho Shift+Delete.

No Linux a forma mais tradicional para se manipular arquivos é com o comando `chmod` que altera as permissões de arquivos ou diretórios. É um comando para manipulação de arquivos e diretórios que muda as permissões para acesso àqueles, por exemplo, um diretório que poderia ser de escrita e leitura, pode passar a ser apenas leitura, impedindo que seu conteúdo seja alterado.

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:

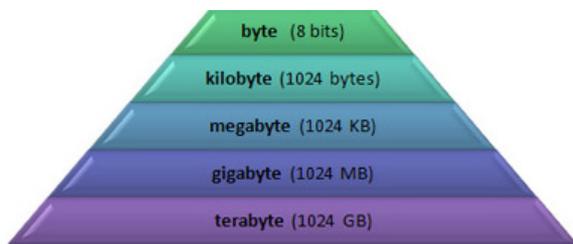


Figura 6: Unidade de medida de memórias

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:

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

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 precisa 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.

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.



#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.

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.

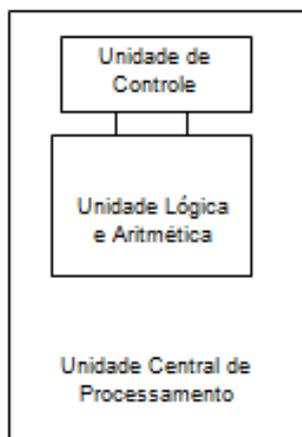


Figura 7: Esquema Processador

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.

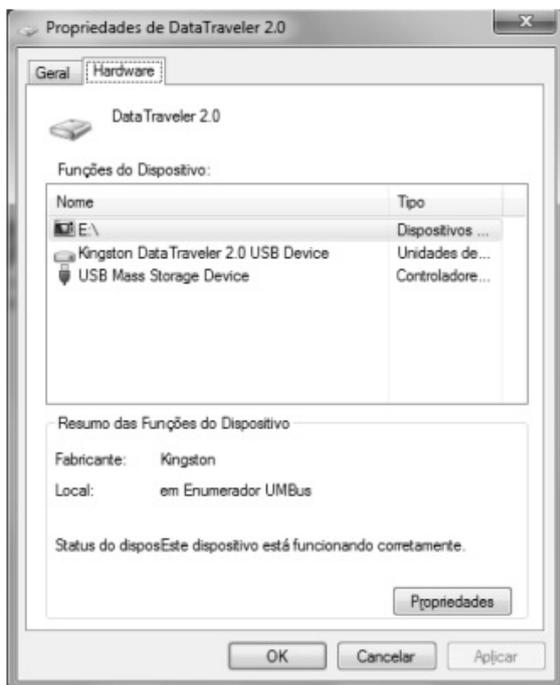


#FicaDica

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 arquivos 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 , 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 demonstrada 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  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 , 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.

REDES DE COMPUTADORES

Redes de Computadores refere-se à interligação por meio de um sistema de comunicação baseado em transmissões e protocolos de vários computadores com o objetivo de trocar informações, entre outros recursos. Essa ligação é chamada de estações de trabalho (nós, pontos ou dispositivos de rede).

Atualmente, existe uma interligação entre computadores espalhados pelo mundo que permite a comunicação entre os indivíduos, quer seja quando eles navegam pela internet ou assiste televisão. Diariamente, é necessário utilizar recursos como impressoras para imprimir documentos, reuniões através de videoconferência, trocar e-mails, acessar às redes sociais ou se entreter por meio de jogos, etc.

Hoje, não é preciso estar em casa para enviar e-mails, basta ter um tablet ou smartphone com acesso à internet nos dispositivos móveis. Apesar de tantas vantagens, o crescimento das redes de computadores também tem seu lado negativo. A cada dia surgem problemas que prejudicam as relações entre os indivíduos, como pirataria, espionagem, *phishing* - roubos de identidade, assuntos polêmicos como racismo, sexo, pornografia, sendo destacados com mais exaltação, entre outros problemas.

Há muito tempo, o ser humano sentiu a necessidade de compartilhar conhecimento e estabelecer relações com pessoas a distância. Na década de 1960, durante a Guerra Fria, as redes de computadores surgiram com objetivos militares: interconectar os centros de comando dos EUA para com objetivo de proteger e enviar dados.

Alguns tipos de Redes de Computadores

Antigamente, os computadores eram conectados em distâncias curtas, sendo conhecidas como redes locais. Mas, com a evolução das redes de computadores, foi necessário aumentar a distância da troca de informações entre as pessoas. As redes podem ser classificadas de acordo com sua arquitetura (Arcnet, Ethernet, DSL, Token ring, etc.), a extensão geográfica (LAN, PAN, MAN, WLAN, etc.), a topologia (anel, barramento, estrela, ponto-a-ponto, etc.) e o meio de transmissão (redes por cabo de fibra óptica, trançado, via rádio, etc.).

Veja alguns tipos de redes:

Redes Pessoais (*Personal Area Networks* – PAN) – se comunicam a 1 metro de distância. Ex.: Redes Bluetooth;

Redes Locais (*Local Area Networks* – LAN) – redes em que a distância varia de 10m a 1km. Pode ser uma sala, um prédio ou um campus de universidade;

Redes Metropolitanas (*Metropolitan Area Network* – MAN) – quando a distância dos equipamentos conectados à uma rede atinge áreas metropolitanas, cerca de 10km. Ex.: TV à cabo;

Redes a Longas Distâncias (*Wide Area Network – WAN*) – rede que faz a cobertura de uma grande área geográfica, geralmente, um país, cerca de 100 km;

Redes Interligadas (Interconexão de WANs) – são redes espalhadas pelo mundo podendo ser interconectadas a outras redes, capazes de atingirem distâncias bem maiores, como um continente ou o planeta. Ex.: Internet;

Rede sem Fio ou Internet sem Fio (*Wireless Local Area Network – WLAN*) – rede capaz de conectar dispositivos eletrônicos próximos, sem a utilização de cabeamento. Além dessa, existe também a WMAN, uma rede sem fio para área metropolitana e WWAN, rede sem fio para grandes distâncias.

Topologia de Redes

Astologias das redes de computadores são as estruturas físicas dos cabos, computadores e componentes. Existem as topologias físicas, que são mapas que mostram a localização de cada componente da rede que serão tratadas a seguir. e as lógicas, representada pelo modo que os dados trafegam na rede:

Topologia Ponto-a-ponto – quando as máquinas estão interconectadas por pares através de um roteamento de dados;

Topologia de Estrela – modelo em que existe um ponto central (concentrador) para a conexão, geralmente um *hub* ou *switch*;

Topologia de Anel – modelo atualmente utilizado em automação industrial e na década de 1980 pelas redes Token Ring da IBM. Nesse caso, todos os computadores são entreligados formando um anel e os dados são propagados de computador a computador até a máquina de origem;

Topologia de Barramento – modelo utilizado nas primeiras conexões feitas pelas redes Ethernet. Refere-se a computadores conectados em formato linear, cujo cabeamento é feito sequencialmente;

Redes de Difusão (Broadcast) – quando as máquinas estão interligadas por um mesmo canal através de pacotes endereçados (unicast, broadcast e multicast).

Cabos

Os cabos ou cabeamentos fazem parte da estrutura física utilizada para conectar computadores em rede, estando relacionados a largura de banda, a taxa de transmissão, padrões internacionais, etc. Há vantagens e desvantagens para a conexão feita por meio de cabeamento. Os mais utilizados são:

Cabos de Par Trançado – cabos caracterizados por sua velocidade, pode ser feito sob medida, comprados em lojas de informática ou produzidos pelo usuário;

Cabos Coaxiais – cabos que permitem uma distância maior na transmissão de dados, apesar de serem flexíveis, são caros e frágeis. Eles necessitam de barramento ISA, suporte não encontrado em computadores mais novos;

Cabos de Fibra Óptica – cabos complexos, caros e de difícil instalação. São velozes e imunes a interferências eletromagnéticas.



#FicaDica

Após montar o cabeamento de rede é necessário realizar um teste através dos testadores de cabos, adquirido em lojas especializadas. Apesar de testar o funcionamento, ele não detecta se existem ligações incorretas. É preciso que um técnico veja se os fios dos cabos estão na posição certa.

Sistema de Cabeamento Estruturado

Para que essa conexão não prejudique o ambiente de trabalho, em uma grande empresa, são necessárias várias conexões e muitos cabos, sendo necessário o cabeamento estruturado.

Por meio dele, um técnico irá poupar trabalho e tempo, tanto para fazer a instalação, quanto para a remoção da rede. Ele é feito através das tomadas RJ-45 que possibilitam que vários conectores possam ser inseridos em um único local, sem a necessidade de serem conectados diretamente no hub.

Além disso, o sistema de cabeamento estruturado possui um painel de conexões, o *Patch Panel*, onde os cabos das tomadas RJ-45 são conectados, sendo um concentrador de tomadas, favorecendo a manutenção das redes. Eles são adaptados e construídos para serem inseridos em um rack.

Todo esse planejamento deve fazer parte do projeto do cabeamento de rede, em que a conexão da rede é pensada de forma a realizar a sua expansão.

Repetidores: Dispositivo capaz de expandir o cabeamento de rede. Ele poderá transformar os sinais recebidos e enviá-los para outros pontos da rede. Apesar de serem transmissores de informações para outros pontos, eles também diminuem o desempenho da rede, podendo haver colisões entre os dados à medida que são anexas outras máquinas. Esse equipamento, normalmente, encontra-se dentro do hub.

Hubs: Dispositivos capazes de receber e concentrar todos os dados da rede e compartilhá-los entre as outras estações (máquinas). Nesse momento nenhuma outra máquina consegue enviar um determinado sinal até que os dados sejam distribuídos completamente. Eles são utilizados em redes domésticas e podem ter 8, 16, 24 e 32 portas, variando de acordo com o fabricante. Existem os Hubs Passivos, Ativos, Inteligentes e Empilháveis.

Bridges: É um repetidor inteligente que funciona como uma ponte. Ele lê e analisa os dados da rede, além de relacionar diferentes arquiteturas.

Switches: Tipo de aparelho semelhante a um hub, mas que funciona como uma ponte: ele envia os dados apenas para a máquina que o solicitou. Ele possui muitas portas de entrada e melhor performance, podendo ser utilizado para redes maiores.

Roteadores: Dispositivo utilizado para conectar redes e arquiteturas diferentes e de grande porte. Ele funciona como um tipo de ponte na camada de rede do modelo OSI (*Open Systems Interconnection* - protocolo de inter-

conexão de sistemas abertos para conectar máquinas de diferentes fabricantes), identificando e determinando um IP para cada computador que se conecta com a rede.

Sua principal atribuição é ordenar o tráfego de dados na rede e selecionar o melhor caminho. Existem os roteadores estáticos, capaz de encontrar o menor caminho para tráfego de dados, mesmo se a rede estiver congestionada; e os roteadores dinâmicos que encontram caminhos mais rápidos e menos congestionados para o tráfego.

Modem: Dispositivo responsável por transformar a onda analógica que será transmitida por meio da linha telefônica, transformando-a em sinal digital original.

Servidor: Sistema que oferece serviço para as redes de computadores, como por exemplo, envio de arquivos ou e-mail. Os computadores que acessam determinado servidor são conhecidos como clientes.

Placa de Rede: Dispositivo que garante a comunicação entre os computadores da rede. Cada arquitetura de rede depende de um tipo de placa específica. As mais utilizadas são as do tipo Ethernet e Token Ring (rede em anel).

Computação na nuvem (cloud computing)

Ao utilizar e acessar arquivos e executar tarefas pela internet, o usuário está utilizando o conceito de computação em nuvens, não há a necessidade de instalar aplicativos no seu computador para tudo, pois pode acessar diferentes serviços online para fazer o que precisa, já que os dados não se encontram em um computador específico, mas sim em uma rede, um grande exemplo disso é o Google com o Google Docs, Planilhas, e até mesmo porta arquivos como o Google Drive, ou de outras empresas como o One Drive.

Uma vez devidamente conectado ao serviço online, é possível desfrutar suas ferramentas e salvar todo o trabalho que for feito para acessá-lo depois de qualquer lugar — é justamente por isso que o seu computador estará nas nuvens, pois você poderá acessar os aplicativos a partir de qualquer computador que tenha acesso à internet.



#FicaDica

Basta pensar que, a partir de uma conexão com a internet, você pode acessar um servidor capaz de executar o aplicativo desejado, que pode ser desde um processador de textos até mesmo um jogo ou um pesado editor de vídeos. Enquanto os servidores executam um programa ou acessam uma determinada informação, o seu computador precisa apenas do monitor e dos periféricos para que você interaja.

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 às 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 piores 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 furto, 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.
- Irretratibilidade ou não repúdio – especificidade que assegura a incapacidade de negar a autoria em relação a uma transação feita anteriormente.

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.

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 decifrar 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 quadrilhões 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 Rivest Cipher*): 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.