

MATHEUS SANTOS

INFORMÁTICA PARA CONCURSOS

SEM COMPLICAÇÃO:



Sobre o autor



MATHEUS SANTOS é servidor público federal (Analista Judiciário TI – TRE/AM) e professor de informática/TI para concursos públicos. Formado em Análise e Desenvolvimento de sistemas e pós-graduado em MBA em Gestão de Projetos de TI, ele combina expertise técnica com experiência em educação. **Aprovado em mais de sete concursos**, Matheus conquistou resultados impressionantes: 1º lugar em Técnico Judiciário TI do TRT/11 (2017), Agente de Polícia Rodoviária Federal (2019), Analista Judiciário do TRT/14 (2022) e 4º lugar em Analista Judiciário TSE Unificado do TRE-AM (2024). É criador do canal no *YouTube* ‘Projeto Eu concursado’ e cofundador do ‘Ser Aprovado Concursos Públicos’, plataformas onde compartilha conhecimento e inspira candidatos a alcançar seus objetivos.

Instagram: @bymatheussantos

Apresentação da obra

Se você sente que estuda informática e mesmo assim erra questões na prova, **o problema pode não ser você** — pode ser o jeito que você está estudando. Pense bem: quantos materiais você já estudou que pareciam complicados demais, técnicos demais, distantes da realidade das bancas?

A maioria dos materiais ensina informática de forma complexa, técnica e distante do que realmente cai em concursos públicos.

Este livro faz o oposto.

Aqui, você vai aprender informática de forma simples, objetiva e com foco total no que realmente importa. Sem enrolação. Sem excesso de teoria. Sem perder tempo com conteúdo que não cai.

Você vai direto ao essencial: entender os assuntos mais cobrados, fixar o conteúdo na memória e aumentar seu desempenho nas provas.

Porque, no final, não importa saber tudo — importa acertar questões. E este livro foi feito exatamente para isso.

Bons estudos!

O autor.

Sumário

Sobre o Autor.....	V
Apresentação da obra	VII
CAPÍTULO 1 – CONCEITOS RELACIONADOS À INTERNET	1
1.1 INTERNET	1
1.1.1 Como surgiu?.....	1
1.1.2 Outros conceitos relacionados à internet	4
1.1.3 Protocolo de comunicação	4
1.1.4 Endereçamento IP	4
1.1.5 Serviços e ferramentas da internet.....	4
1.1.6 Segurança na internet.....	5
1.1.7 Conectividade e tecnologias.....	5
1.2 INTRANET.....	5
1.2.1 Quais são as características da INTRANET?.....	5
1.2.1.1 Acesso restrito.....	5
1.2.1.2 Ambiente corporativo.....	6
1.2.1.3 Protocolos e serviços da internet.....	6
1.3 EXTRANET	6
1.3.1 Quadro comparativo	7
1.4 VPN – VIRTUAL PRIVATE NETWORK	8
1.4.1 Finalidade	8
1.4.2 Funcionamento.....	8
1.4.3 Protocolos de VPN	8
1.4.4 Tipos de VPN.....	9
1.4.5 Vantagens do uso de VPN	9
1.4.6 Desvantagens e limitações.....	9
1.4.7 Segurança e criptografia.....	9
1.5 CONCEITOS E MODOS DE UTILIZAÇÃO DE TECNOLOGIAS, FERRAMENTAS, APLICATIVOS E PROCEDIMENTOS ASSOCIADOS A INTERNET/INTRANET	10
1.5.1 Conceitos de internet e intranet.....	10
1.5.1.1 Diferenças principais	10
1.5.2 Tecnologias relacionadas à internet/intranet.....	10
1.5.3 Ferramentas e aplicativos associados à internet/intranet	10
1.5.4 Modos de utilização.....	11
1.5.5 Procedimentos de segurança na internet/intranet	11
1.5.6 Tendências tecnológicas associadas	11
1.6 NAVEGADORES DE INTERNET.....	11
1.6.1 Principais navegadores.....	11
1.6.2 Principais funcionalidades	12
1.6.3 Segurança em navegadores.....	12

1.6.4	Cookies e dados armazenados.....	12
1.6.5	Configurações de privacidade.....	13
1.6.6	Padrões WEB e compatibilidade.....	13
1.6.7	Questões de provas recentes.....	13
1.6.8	Funcionalidades comuns.....	13
1.6.9	Diferenciais do Internet Explorer.....	14
1.6.10	Diferenciais do Mozilla Firefox.....	14
1.6.11	Diferenciais do Google Chrome.....	15
1.6.12	Mecanismo de busca.....	15
1.7	FERRAMENTAS DE PESQUISA E NAVEGAÇÃO.....	15
1.8	CORREIO ELETRÔNICO.....	17
1.8.1	Assinatura de <i>e-mail</i>	17
1.8.2	Protocolos de <i>E-mail</i>	18
1.8.3	Pastas de <i>e-mail</i>	18
1.8.4	Envio de <i>e-mail</i>	18
1.8.5	Recebimento de <i>e-mail</i>	19
CAPÍTULO 2 – REDES DE COMPUTADORES.....		21
2.1	INTRODUÇÃO A REDES.....	21
2.1.1	Funcionamento.....	22
2.2	CLASSIFICAÇÃO DE REDES.....	23
2.2.1	Quanto ao tamanho (área geográfica).....	23
2.2.2	Classificação quanto à arquitetura.....	26
2.2.2.1	Arquitetura ponto a ponto.....	26
2.2.2.2	Arquitetura cliente-servidor.....	26
2.2.3	Classificação quanto à topologia.....	27
2.2.3.1	Ponto a ponto.....	27
2.2.3.2	Barramento.....	28
2.2.3.3	Anel.....	28
2.2.3.4	Estrela.....	29
2.2.3.5	Malha.....	29
2.2.3.6	Árvore.....	30
2.2.3.7	Híbrida.....	31
2.3	DIREÇÃO DE COMUNICAÇÃO/MODO DE TRANSMISSÃO DE DADOS.....	31
2.3.1	Modos de transmissão de dados.....	31
2.3.1.1	Simplex.....	31
2.3.1.1.1	Características.....	32
2.3.1.2	Half-duplex.....	32
2.3.1.2.1	Características.....	32
2.3.1.3	Full-duplex.....	32
2.3.1.3.1	Características.....	33
2.4	UNICAST × MULTICAST × BROADCAST.....	33

2.4.1	Unicast	33
2.4.2	Multicast	33
2.4.3	Broadcast	34
2.5	MEIOS DE TRANSMISSÃO	34
2.5.1	Meios guiados	34
2.5.1.1	Par trançado	34
2.5.1.1.1	Tipos de cabo de par trançado	34
2.5.2	Cabo coaxial	36
2.5.3	Fibra óptica	36
2.5.4	Características dos meios guiados	37
2.6	MEIOS NÃO GUIADOS	37
2.7	PARADIGMA DE COMUNICAÇÃO	38
2.7.1	Comutação de circuitos e comutação de pacotes	38
2.7.2	Comutação de circuitos	38
2.7.2.1	Definição	38
2.7.2.2	Funcionamento	39
2.7.3	Comutação de Pacotes	39
2.7.3.1	Definição	39
2.7.3.1.1	Funcionamento	40
2.8	ARQUITETURA DE REDES (OSI TCP/IP)	40
2.8.1	Modelo OSI (<i>Open Systems Interconnection</i>)	41
2.8.2	Modelo TCP/IP	44
2.8.3	Quadro comparativo: OSI X TCP/IP	45
2.9	DISPOSITIVOS DE INTERCONEXÃO (EQUIPAMENTOS DE REDE)	45
2.9.1	Placa de rede	45
2.9.2	Repetidores	46
2.9.3	Bridges (pontes)	46
2.9.4	Roteadores	47
2.9.5	Hub	47
2.9.6	Switch	48
2.9.7	Camada 2 ou 3?	48
2.9.8	Modem	49
2.9.1	Gateway	49
2.9.1.1	Principais características	50
2.9.2	Access point	50
2.9.3	Download x Upload	50
2.10	PROTOCOLOS	51
2.10.1	HTTP/HTTPS (<i>Hypertext Transfer Protocol/Secure</i>): transferência de páginas web	51
2.10.2	Características do HTTP	51
2.10.3	Códigos de status HTTP	52
2.10.4	FTP (<i>File Transfer Protocol</i>): transferência de arquivos	52
2.10.4.1	Principais características	52
2.10.4.2	Portas utilizadas:	52

2.10.5	SMTP (<i>Simple Mail Transfer Protocol</i>): envio de e-mails.....	52
2.10.5.1	Principais características	52
2.10.5.2	Portas utilizadas	53
2.10.6	POP3/IMAP: recebimento de e-mails.....	53
2.10.6.1	Principais características	53
2.10.6.2	Portas utilizadas	53
2.10.7	DNS (<i>Domain Name System</i>): tradução de nomes de domínio para endereços IP...53	
2.10.7.1	Principais características	54
2.10.7.2	Porta utilizada.....	54
2.10.8	DHCP (<i>Dynamic Host Configuration Protocol</i>): atribuição de endereços IP dinâmicos.....	54
2.10.8.1	Principais características	54
2.10.8.2	Portas utilizadas	54
2.10.9	SNMP (<i>Simple Network Management Protocol</i>): gerenciamento de redes.....	54
2.10.9.1	Principais características	54
2.10.9.2	Portas utilizadas	54
2.10.10	Telnet/SSH (<i>Secure Shell</i>): acesso remoto a dispositivos	55
2.10.10.1	Principais características	55
2.10.10.2	Portas utilizadas	55
2.10.11	TLS/SSL: segurança na comunicação de dados.....	55
2.10.11.1	Principais características	55
2.10.11.2	Portas utilizadas	55
2.10.11.3	TLS × SSL: diferenças	56
2.10.12	TCP e UDP – Protocolos de transporte.....	56
2.10.12.1	TCP (<i>Transmission Control Protocol</i>): confiabilidade na transmissão	56
2.10.12.1.1	Principais características	56
2.10.12.1.3	Portas comuns:	56
2.10.12.2	UDP (<i>User Datagram Protocol</i>): velocidade e eficiência	56
2.10.12.2.1	Principais características	57
2.10.12.2.2	Exemplos de uso	57
2.10.12.2.3	Portas comuns	57
2.10.13	Protocolo IP (<i>Internet Protocol</i>): endereçamento e roteamento de dados.....	57
2.10.13.1	Versões DO IP.....	57
2.10.13.2	Portas utilizadas	58
2.10.13.2	Características	58
2.10.13.2	Camada de enlace	58
2.10.13.2	Camada física	58
2.10.14	Outros protocolos importantes.....	58
2.11	TABELA DE PROTOCOLOS E PORTAS.....	59
CAPÍTULO 3 – COMPUTAÇÃO EM NUVEM.....		61
3.1	INTRODUÇÃO À COMPUTAÇÃO EM NUVEM	61
3.1.1	Vantagens	62
3.1.2	Características.....	63
3.2	MODELOS DE SERVIÇO.....	65

3.2.1	SAAS (Software As A Service).....	65
3.2.2	PAAS (Plataform As A Service).....	66
3.2.3	IAAS (Infrastructure As A Service).....	66
3.3	TIPOS DE NUVEM.....	67
3.3.1	Nuvens públicas.....	67
3.3.2	Nuvens privadas.....	67
3.3.3	Nuvens híbridas.....	68
3.3.4	Nuvens comunitárias.....	68
	CAPÍTULO 4 - SEGURANÇA DA INFORMAÇÃO.....	69
4.1	INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO.....	69
4.1.1	Ameaça.....	70
4.1.2	Vulnerabilidade.....	70
4.1.3	Risco.....	70
4.1.4	Impacto.....	70
4.1.5	SEGURANÇA COMO UM ATIVO.....	71
4.1.5.1	Controle físico.....	71
4.1.5.2	Controle lógico.....	71
4.1.5.3	Controles administrativos.....	72
4.2	PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO.....	72
4.2.1	Confidencialidade.....	73
4.2.2	Integridade.....	73
4.2.3	Disponibilidade.....	74
4.2.4	Autenticidade.....	74
4.2.5	Não repúdio / Irretratabilidade.....	75
4.2.5.1	Mecanismos para garantir o não repúdio.....	75
4.3	MALWARES.....	76
4.4	VÍRUS.....	76
4.4.1	Características.....	77
4.4.2	Características principais.....	78
4.5	WORM.....	79
4.5.1	Características.....	79
4.6	CAVALO DE TROIA.....	79
4.7	BOT.....	80
4.8	BOTNET.....	81
4.9	SPYWARE.....	81
4.9.1	Tipos de spyware.....	81
4.10	BACKDOOR.....	82
4.11	ROOTKIT.....	82

4.12	RANSOMWARE	82
4.13	SCAREWARE	83
4.14	ATAQUES E AMEAÇAS	83
4.14.1	Engenharia social	83
4.14.2	Phishing	83
4.14.2.1	Como evitar?	84
4.14.3	Vishing (Voice Phishing)	84
4.14.3.1	Como evitar?	84
4.14.3	Baiting (isca)	84
4.14.4	Pretexting (falsa identidade)	85
4.14.4	Tailgating (acesso físico)	85
4.14.4	Pharming	85
4.14.4.1	Pharming x Phishing: qual a diferença?	86
4.15	Ataques à Rede	86
4.15.1	Ataque Man-in-the-Middle (MitM)	86
4.15.2	Packet Sniffing	86
4.15.2.1	Sniffing passivo	86
4.15.2.2	Sniffing ativo	86
4.15.3	Spoofing	87
4.15.3.1	Principais tipos de spoofing	87
4.15.3.1.1	IP Spoofing	87
4.15.3.1.2	ARP Spoofing	87
4.15.3.1.3	DNS Spoofing	87
4.15.3.1.4	E-mail Spoofing	87
4.15.3.1.5	Caller ID Spoofing	87
4.16	Ataques de Negação de Serviço (DoS e DDoS)	88
4.16.1	Ataque DoS (Denial of Service)	88
4.16.2	Ataque DDoS (Distributed Denial of Service)	88
4.16.3	Principais tipos de ataques DOS e DDOS	88
4.16.3.1	Ataque de volume (flooding)	88
4.16.3.1.1	Tipos comuns	89
4.16.3.2	Ataque de protocolo	89
4.16.3.2.1	Tipos comuns	89
4.16.3.3	Ataque de aplicação (layer 7 DDoS)	89
4.16.3.3.1	Tipo comum	89
4.16.3.4	Ataque de força bruta (brute force)	89
4.17	ATAQUES A APLICAÇÕES WEB	90
4.17.1	Defacement	90
4.17.1.1	Como funciona o Defacement?	90
4.17.2	SQL Injection (Injeção de SQL)	90
4.17.2.1	Como funciona	90
4.17.2.2	Como se proteger	91
4.17.3	Cross-Site Scripting (XSS)	91
4.17.3.1	Como funciona	91

4.17.3.2	Tipos de XSS.....	91
4.17.3.3	Como se proteger	91
4.17.4	Cross-Site Request Forgery (CSRF)	92
4.17.4.1	Como funciona.....	92
4.17.4.2	Como se proteger	92
4.17.5	Hoax.....	92
4.17.6	Spam	93
4.18	MECANISMOS DE SEGURANÇA.....	93
4.18.1	VPN.....	94
4.19	POLÍTICA DE SEGURANÇA	94
4.19.1	Senhas	95
4.20	FERRAMENTAS ANTIMALWARES	95
4.20.1	Métodos de detecção.....	96
4.21	ANTIVÍRUS.....	96
4.21.1	Escaneamento de vírus conhecidos.....	96
4.21.2	Sensoreamento heurístico.....	96
4.21.3	Busca algorítmica.....	97
4.21.4	Checagem de integridade.....	97
4.21.5	Principais antivírus do mercado	97
4.22	Gerações dos antivírus.....	97
4.23	FIREWALL.....	98
4.23.1	Firewall pessoal.....	99
4.24	IDS, IPS, HONEYPOT.....	102
4.24.1	IDS (<i>Intrusion Detection System</i> – Sistema de Detecção de Intrusão).....	102
4.24.1.1	Funcionamento do IDS	102
4.24.1.2	Tipos de IDS	102
4.24.1.3	Vantagens e desvantagens do IDS	103
4.24.2	IPS (<i>Intrusion Prevention System</i> – Sistema de Prevenção de Intrusão).....	103
4.24.2.1	Funcionamento do IPS.....	104
4.24.2.2	Tipos de IPS.....	104
4.24.2.3	IDS × IPS	105
4.25	HONEYPOT (Pote de mel – Sistema de engano).....	105
4.25.1	Funcionamento do honeypot.....	106
4.25.2	Tipos de honeypots.....	106
4.25.3	Outros tipos de honeypots.....	106
4.26	Backup e seus Tipos	107
4.26.1	Tipos de backup.....	107
4.26.1.1	Backup completo (<i>full backup</i>)	107
4.26.1.2	Backup incremental.....	107
4.26.1.3	Backup diferencial	108
4.26.1.4	Backup espelhado (<i>mirror backup</i>)	108
4.26.1.5	Backup de imagem (<i>image backup</i>)	108

4.26.1.6	Backup na nuvem (cloud backup).....	108
4.26.2	Tabela comparativa (tipos de backup).....	109
4.26.3	Tabela comparativa (restauração).....	109
4.27	Criptografia.....	110
4.27.1	Criptografia simétrica.....	110
4.27.2	Criptografia assimétrica.....	111
4.28	Funções de Hash.....	113
4.29	Assinatura Digital.....	114
4.30	Certificação Digital.....	114
CAPÍTULO 5 - SISTEMAS OPERACIONAIS		117
5.1	CONCEITO DE SISTEMAS OPERACIONAIS.....	117
5.1.1	Hardware x Software.....	118
5.2	SISTEMA OPERACIONAL WINDOWS.....	120
5.2.1	Versões do Windows 10.....	120
5.3	SISTEMA DE ARQUIVOS.....	121
5.4	CONEXÃO ENTRE VÁRIOS DISPOSITIVOS.....	122
5.4.1	Menu Iniciar.....	122
5.4.2	Central de ações.....	123
5.4.3	Cortana.....	123
5.4.4	Microsoft Edge.....	124
5.4.5	Microsoft Hello.....	124
5.4.6	Botão Visão de Tarefas.....	124
5.4.7	Tela de configurações Windows.....	125
5.4.8	Lixeira.....	126
5.4.9	Gerenciador de Tarefas.....	126
5.4.10	Limites para nomes de arquivos.....	126
5.4.11	Caracteres inválidos.....	127
5.4.12	Manipulação de arquivos.....	127
5.4.12.1	Comandos do Prompt do Windows.....	128
5.4.13	Seleção de arquivos.....	129
5.5	WINDOWS 11 - PRINCIPAIS FUNCIONALIDADES.....	130
5.5.1	Interface gráfica e menu Iniciar.....	130
5.5.2	Explorador de arquivos.....	131
5.5.3	Recursos de multitarefa.....	131
5.5.4	Segurança.....	131
5.5.5	Integração com nuvem.....	132
5.5.6	Widgets.....	132
5.5.7	Configurações do sistema.....	132
5.5.8	Atalhos importantes.....	132

CAPÍTULO 1

CONCEITOS RELACIONADOS À INTERNET

1.1 INTERNET

Vamos iniciar os estudos sobre a internet e nada melhor do que trazermos alguns conceitos que podem estar na sua prova.

Internet é uma rede de comunicação de milhões de computadores conectados, que oferece inúmeros serviços.

São bilhões de páginas publicadas sobre os mais variados temas, organizadas em *websites*.

Websites:



1.1.1 Como surgiu?

A internet pessoal surgiu num **contexto militar**, nos anos 1960, na época da Guerra Fria, nos Estados Unidos. O Departamento de Defesa americano pretendia criar uma rede de comunicação de computadores em pontos estratégicos. A intenção era descentralizar informações

valiosas de forma que não fossem destruídas por bombardeios se estivessem localizadas em um único servidor.

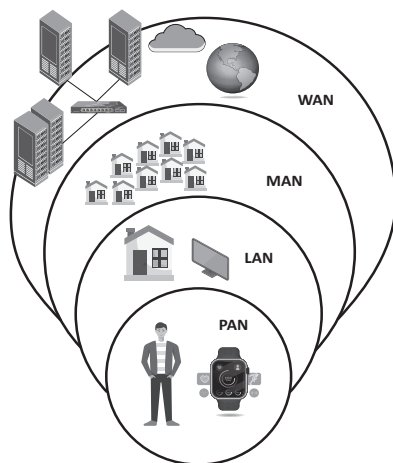
Assim, a **ARPA** (Advanced Research Projects Agency), uma das subdivisões do Departamento, criou uma rede conhecida por ARPANET, ligada por um *backbone* (“espinha dorsal”, isto é, estruturas de rede capazes de manipular grandes volumes de informações), que passava por debaixo da terra, o que dificultava sua destruição. O acesso à ARPANET era **restrito a militares e pesquisadores** e demorou a chegar ao público em geral, pois temiam o mau uso da tecnologia por civis e países não aliados.

INTER: ENTRE

NET: REDE

Como ela trata da comunicação entre redes, pode ser considerada – na verdade – **um conglomerado de redes menores**.

Para entender melhor sobre isso, vamos falar mais sobre a classificação das redes e detalhá-la um pouco mais em um capítulo específico à frente.



Conforme vimos acima, a internet nada mais é do que um conglomerado de redes. Nesse aspecto podemos conceituar redes como uma conexão entre dispositivos que se conectam.

Vamos exemplificar por intermédio da classificação abaixo:

- **PAN** (*Personal Area Network* – Rede de área **PESSOAL**): essa classificação é para redes em que os **dispositivos são pessoais**, ou seja, quando você conecta, por exemplo, dispositivos pessoais sem que uma pessoa externa acesse.

Ex.: Imagine que você conecte seu celular a uma pequena caixa de som para escutar uma banda de pagode no churrasco da sua sogra, ou ainda conecte seu *smartphone* a um relógio digital que faça a medição da sua pressão e também funções do seu celular.

- **LAN** (*Local Area Network* – Rede de área **LOCAL**): quando falamos de LAN basta você imaginar o contexto da sua **residência, seu escritório ou uma empresa**. Nesse caso,

você precisa conectar dispositivos, como computadores, impressoras, e esse acesso é dentro desse ambiente físico e das pessoas que estão conectadas nessa rede.

Repare que na LAN saímos de um contexto pessoal e partimos para um contexto local.

- **MAN** (*Metropolitan Area Network* – Rede Local): são projetadas justamente para interconectar sistemas de cidades próximas ou de uma região metropolitana.

Este tipo de rede é caracterizado por ter alcance maior do que as do tipo LANs. Além disso, apresentam uma boa relação custo/benefício, pois oferecem uma relação melhor do que as redes WANs, por um custo semelhante ao das redes LANs.

Então, a MAN é uma rede que conecta bairros e regiões metropolitanas.

- **WAN** (*Wide Area Network* – Rede de Longa Distância): vai um pouco além da MAN e consegue abranger área maior, como um país ou até mesmo um continente.

Quando falamos da WAN, estamos diante da própria internet que conecta outras diversas redes menores.



CAIU NA PROVA - EXATUS 2016 - Analista Judiciário (TRE SC)/Apoio Especializado/Arquitetura

É um conglomerado de redes locais, interconectadas e espalhadas pelo mundo inteiro, através do protocolo de internet facilitando o fluxo de informações espalhadas por todo o globo terrestre.

- Intranet.
- LAN.
- Internet.
- Extranet.

Comentário: lembre-se que, falou de conglomerado de redes interconectas e espalhadas pelo mundo, estamos falando de INTERNET.

Gabarito: letra **c**.

Além dessas quatro classificações, existem outras que podem vir a ser cobradas em sua prova:

- **CAN** (*Campus Area Network*): rede que interliga diversas LANs em um campus universitário, complexo industrial ou base militar.

Ex.: rede de internet em um *campus* universitário.

- **SAN** (*Storage Area Network*): Rede de alta velocidade dedicada ao armazenamento e transferência de dados entre servidores e dispositivos de armazenamento.

Ex.: *datacenters* que utilizam redes SAN para gerenciar grandes volumes de dados.

- **HAN** (*Home Area Network*): rede doméstica que conecta dispositivos como computadores, *smart* TVs, câmeras e dispositivos IoT.

Ex.: Uma casa com dispositivos inteligentes conectados.

CAPÍTULO 2

REDES DE COMPUTADORES

2.1 INTRODUÇÃO A REDES

Vamos começar o estudo de um assunto que muitos concurseiros têm dificuldade, mas que certamente após essa aula vão gabaritar as questões desse tópico do edital.

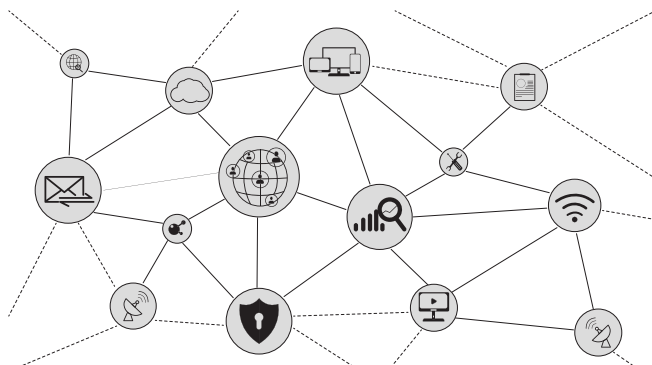
Primeiro, vamos para o **conceito de redes de computadores**.

Uma rede de computadores é um conjunto de **dois ou mais dispositivos (também chamados de nós)** que usam um conjunto de regras (protocolo) em comum para compartilhar recursos (*hardware*, troca de mensagens) entre si, através de uma determinada conexão, podendo ser: por fio de cobre, fibra ótica, ondas de rádio e, também, via satélite.

Computadores, servidores, celulares e modems são exemplos de **nós conectados** a uma rede. Esses equipamentos estão por toda parte, como em nossas casas, nas empresas e em órgãos públicos.

E você pode perguntar: “Mas, professor, para que serve uma rede de computadores?”

Vamos lá, a rede de computadores quebra barreiras geográficas e possibilita que **informações sejam compartilhadas entre pessoas e empresas** do mundo inteiro, disponibilizando informação local ou globalmente, e são úteis para a prestação de diversos serviços essenciais.



Pense num *streaming* que você acessa por meio da sua *smart tv* conectada à internet, ou, ainda, aplicações como enviar e receber *e-mails*, ou receber áudio pelo celular e outros serviços que envolvam a transmissão de dados: eles só são possíveis através de uma rede.

Outros exemplos de aplicações para a rede:

- a) **Compartilhamento de arquivos:** permite compartilhar arquivos de dados por meio de uma rede;
- b) **Acesso e utilização de aplicativos:** permite acessar e utilizar aplicações através da rede;
- c) **Compartilhar *hardware*:** possibilita aos usuários de uma rede compartilhar dispositivos de *hardware*, como impressoras e discos rígidos.
- d) **Modelo cliente-servidor:** permite que os dados sejam armazenados em servidores, no qual os dispositivos do usuário final (clientes) possam acessar essas informações.
- e) **Voz sobre IP (VoIP):** permite aos usuários enviar dados de voz por meio de protocolos de Internet;
- f) **Comunicação:** pode incluir vídeo, imagens, texto e voz;
- g) **E-commerce:** permite aos usuários vender e comprar produtos e serviços pela internet;
- h) **Jogos:** permite que usuários joguem simultaneamente, mesmo estando em locais diferentes.



CAIU NA PROVA – Assistente Legislativo (ALEGO) 2006/Assistente Administrativo

Uma rede de computadores é um conjunto de unidades processadoras interconectadas que permite, inclusive, o compartilhamento de recursos, como impressoras, discos entre outros.

Comentário: exatamente, uma rede de computadores permite o compartilhamento de recursos entre os computadores que nela estejam conectados.

Gabarito: **certo**.

2.1.1 Funcionamento

Conforme vimos, os dispositivos de rede usam uma variedade de *hardware* e *software* para especificar e **padronizar a forma como os dados são enviados ou recebidos**.

Portanto, qualquer rede de computadores precisa de **equipamentos, conexões e regras** para que essa comunicação possa ser feita.

Em redes, chamamos de **nós** esses pontos de comunicação, e entre os meios para que essas transmissões de dados possam ocorrer estão, por exemplo, os **modems, cabos, roteadores, placas, portas de comunicação, entre outras estruturas**.

Além disso, alguns **protocolos (regras)** regem a comunicação entre esses sistemas e garantem que a transmissão de dados ocorrerá sem problemas, por meio de normas para a transmissão, verificação e envio de dados.

Os protocolos são uma forma com que equipamentos diferentes com arquiteturas diferentes conseguem comunicar-se entre si.

No caso de serviços na nuvem, grandes empresas possuem diversos servidores com mecanismos de *backup* que permitem que você não corra riscos de perder suas informações.

- **Consumo de energia:** uma grande vantagem sem dúvidas é quanto ao consumo de energia. O que você acha mais econômico? Manter um servidor em sua empresa rodando 24h na sala de TI para que os seus serviços não parem ou manter um serviço na nuvem que consome a energia do ambiente físico da empresa que te fornece?

Logo podemos dizer que o consumo de energia é muito menor quando se tem serviços alocados na nuvem, pois o seu servidor é que possui a responsabilidade de manter esses recursos funcionando por 24h.



CAIU NA PROVA - CEBRASPE (CESPE) - 2023 - Analista Fazendário Municipal (Pref Fortaleza)/Administração

Certo analista fazendário recebeu arquivo em formato PDF e deverá aproveitar parte das informações e dos dados constantes do arquivo para elaborar parecer técnico. Considerando essa situação hipotética, julgue o item seguinte.

O analista poderá salvar o arquivo recebido na nuvem, pois este serviço permite ao usuário armazenar e acessar arquivos e dados remotamente.

Comentário: como vimos no estudo teórico, quando armazenamos um arquivo na nuvem, podemos acessá-los remotamente a partir de qualquer dispositivo conectado à internet.

Gabarito: **certo**.



3.1.2 Características

- **Serviços mensuráveis:** corresponde à capacidade de você mensurar os serviços. Ex.: quanto de recurso você está consumindo na nuvem. Imagine que você contrate um armazenamento para 100 GB, em *cloud computing* você tem acesso a relatórios que

4.26 Backup e seus Tipos

O *backup* é um processo essencial para garantir a integridade e disponibilidade dos dados em caso de falhas, exclusão acidental, corrupção ou ataques cibernéticos. Ele consiste na **cópia e armazenamento de informações em locais seguros**, permitindo a recuperação em situações adversas. No contexto de concursos públicos, especialmente aqueles organizados pelo CEBRASPE, é comum a cobrança dos diferentes tipos de *backup* e suas características.

4.26.1 Tipos de backup

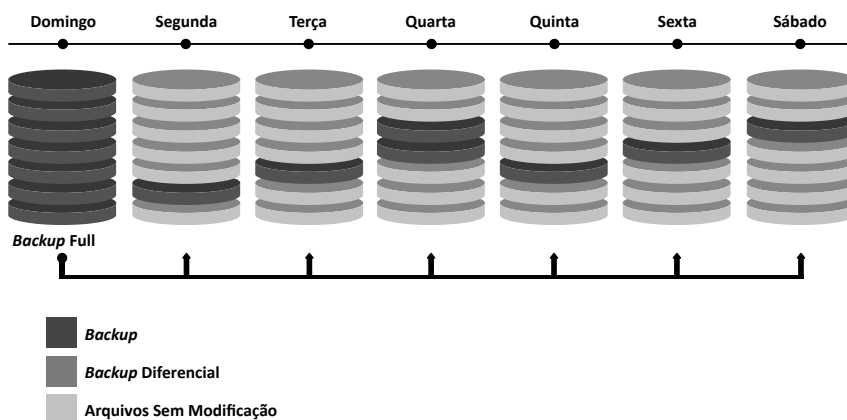
4.26.1.1 Backup completo (full backup)

O *backup* completo consiste na **cópia integral de todos os dados selecionados**. Ele é o mais confiável, pois permite a restauração imediata sem necessidade de combinações com outros *backups*. No entanto, tem como desvantagens o alto consumo de espaço de armazenamento e o tempo necessário para sua realização. Esse tipo de *backup* é geralmente realizado periodicamente, servindo como base para outros métodos, como o incremental e o diferencial.



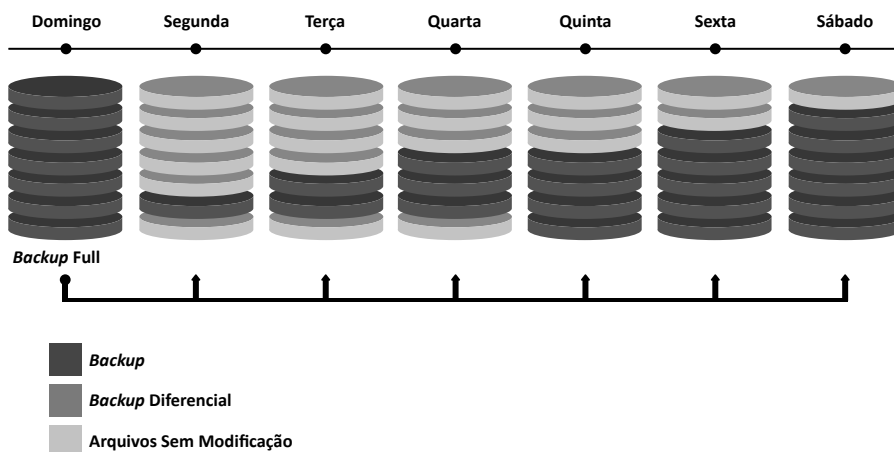
4.26.1.2 Backup incremental

O *backup* incremental copia **apenas os arquivos que foram modificados ou criados desde o último backup, seja ele completo ou incremental**. Esse método reduz significativamente o espaço de armazenamento e o tempo necessário para a cópia dos dados. Entretanto, sua principal desvantagem está na restauração, pois exige que o *backup* completo e todos os incrementais subsequentes sejam recuperados na ordem correta. Isso pode tornar o processo mais demorado e complexo.



4.26.1.3 Backup diferencial

O *backup* diferencial também copia os arquivos modificados desde o último *backup* completo, mas, **diferentemente do incremental, ele não zera a flag de arquivamento dos arquivos**. Com isso, a cada novo *backup* diferencial, o volume de dados armazenados aumenta, pois ele sempre copia todas as alterações desde o último *backup* completo. A principal vantagem desse método é que a restauração é mais simples do que no incremental, pois requer apenas o último *backup* completo e o mais recente *backup* diferencial.



4.26.1.4 Backup espelhado (mirror backup)

O *backup* espelhado é **semelhante ao backup completo, mas sem a retenção de versões antigas dos arquivos**. Ele mantém uma cópia exata dos dados no momento da realização do *backup*, removendo arquivos que forem excluídos do ambiente original. Sua vantagem está na atualização constante dos dados, mas, por outro lado, não permite a recuperação de arquivos excluídos, pois eles são automaticamente removidos do *backup*.

4.26.1.5 Backup de imagem (image backup)

O *backup* de imagem realiza a cópia completa de um sistema, incluindo o sistema operacional, aplicativos e configurações. Ele é muito utilizado para recuperação completa em caso de falhas graves, pois permite restaurar um ambiente inteiro rapidamente. Apesar de sua eficiência, esse tipo de *backup* ocupa grande espaço de armazenamento e geralmente requer *softwares* especializados para sua criação e recuperação.

4.26.1.6 Backup na nuvem (cloud backup)

O *backup* na nuvem armazena os dados em servidores remotos acessíveis pela internet. Ele pode ser configurado para ocorrer automaticamente, garantindo a segurança das informações mesmo em casos de desastres físicos. Entre suas vantagens estão a acessibilidade remota e a proteção contra falhas locais. No entanto, sua dependência de uma conexão com a internet e os possíveis custos associados podem ser desvantagens a serem consideradas.

- **CTRL** – Permite selecionar arquivo por arquivo de acordo com o clique do *mouse*, ou seja, pode-se selecionar vários arquivos, mas tem de ir determinando o arquivo específico.

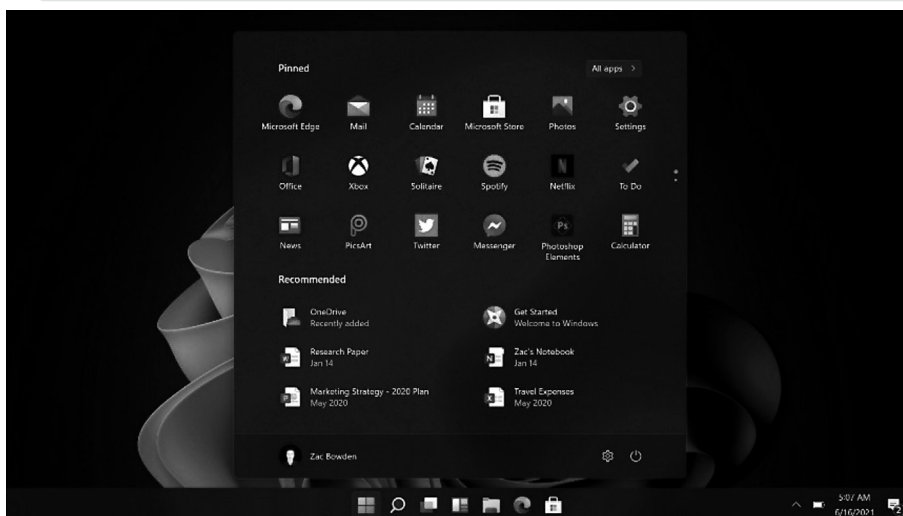


- **SHIFT** – Com essa tecla, pode-se clicar em um primeiro arquivo e depois pressionar a tecla SHIFT e clicar em um arquivo posterior serão selecionados todos os arquivos daquele intervalo.

5.5 WINDOWS 11 - PRINCIPAIS FUNCIONALIDADES

O Windows 11 é o sistema operacional desenvolvido pela Microsoft como sucessor do Windows 10, apresentando mudanças significativas na interface, requisitos de segurança, recursos de produtividade e integração com serviços em nuvem. Seu foco está na modernização visual, no aumento da segurança e na melhoria da experiência do usuário.

5.5.1 Interface gráfica e menu Iniciar



O Windows 11 apresenta uma interface redesenhada, com elementos centralizados por padrão na barra de tarefas. O menu Iniciar deixou de utilizar os blocos dinâmicos (*Live Tiles*),

presentes no Windows 10, passando a exibir uma lista de aplicativos fixados na parte superior e recomendações de arquivos e programas utilizados recentemente na parte inferior.

A barra de tarefas também foi reformulada, com ícones centralizados, novo botão de *Widgets* e integração com funcionalidades modernas do sistema. Apesar da centralização padrão, o usuário pode configurar o alinhamento dos ícones para a esquerda.

A pesquisa do sistema continua integrada ao menu Iniciar e permite localizar aplicativos, arquivos, configurações e resultados na *web*.

5.5.2 Explorador de arquivos

O Explorador de arquivos recebeu um novo *layout* visual, com substituição da Faixa de Opções (*Ribbon*) por uma barra de comandos simplificada. As funções mais utilizadas, como copiar, colar, renomear e excluir, permanecem disponíveis de forma mais objetiva.

Uma das principais inovações é a implementação de abas no Explorador, permitindo a navegação por múltiplas pastas dentro de uma única janela, recurso semelhante ao funcionamento de navegadores de internet.

O menu de contexto (acessado pelo botão direito do *mouse*) foi simplificado. Para acessar o modelo clássico completo, o usuário deve selecionar a opção *Mostrar mais opções*.

5.5.3 Recursos de multitarefa

O Windows 11 aprimorou os recursos de organização de janelas por meio do *Snap Layouts*. Ao posicionar o cursor sobre o botão de maximização da janela, são exibidas opções de organização automática da tela em diferentes formatos, como divisão em duas, três ou quatro partes.

O recurso *Snap Groups* permite que conjuntos de janelas organizadas sejam mantidos agrupados, facilitando a alternância entre tarefas.

Além disso, o sistema mantém o recurso de Áreas de Trabalho Virtuais, permitindo ao usuário criar múltiplos *desktops* independentes para diferentes atividades, como trabalho, estudo ou lazer.

5.5.4 Segurança

O Windows 11 estabelece novos padrões mínimos de segurança. Entre eles, destaca-se a exigência do módulo TPM 2.0 (*Trusted Platform Module*), responsável por armazenar chaves criptográficas e reforçar a proteção contra ataques.

O sistema também exige suporte ao *Secure Boot*, recurso que impede a inicialização de *softwares* não confiáveis durante o processo de *boot*.

O Windows Hello permite autenticação biométrica por meio de reconhecimento facial, impressão digital ou PIN. O sistema também inclui o Microsoft Defender, antivírus nativo que oferece proteção contra vírus, *malwares* e outras ameaças digitais.

Esses requisitos tornam o Windows 11 mais seguro em comparação às versões anteriores.