Estratégia Concursos

Aula 03

PRF (Policial) Bizu Estratégico - 2023

(Pré-Edital)

Autor:

Heloísa Tondinelli, Elizabeth Menezes de Pinho Alves, Marcela Neves Suonski, Willian Henrique Daronch, Arthur Fontes da Silva Jr, Leonardo Mathias

21 de Fevereiro de 2023

BIZU ESTRATÉGICO DE INFORMÁTICA – PRF

Olá, prezado aluno. Tudo certo?

Neste material, traremos uma seleção de *bizus* da disciplina de **Informática** para o concurso da **PRF**.

O objetivo é proporcionar uma revisão rápida e de alta qualidade aos alunos por meio de tópicos que possuem as maiores chances de incidência em prova.

Todos os *bizus* destinam-se a alunos que já estejam na fase bem final de revisão (que já estudaram bastante o conteúdo teórico da disciplina e, nos últimos dias, precisam revisar por algum material bem curto e objetivo).

Elizabeth Menezes

@elizabethmpalves

Leonardo Mathias

@profleomathias

ANÁLISE ESTATÍSTICA

Pessoal, segue abaixo uma análise estatística dos assuntos mais exigidos pela Banca Cebraspe no âmbito da disciplina de Informática.

Assunto	% de cobrança
Conceitos e modos de utilização de tecnologias, ferramentas, aplicativos e procedimentos associados a internet.	24,86%
Windows	14,12%
Computação na nuvem (cloud computing).	11,86%
Ferramentas e aplicativos comerciais de navegação.	9,04%
Noções de vírus, worms, phishing e pragas virtuais.	9,04%
Conceitos de proteção e segurança.	7,91%
Aplicativos para segurança (antivírus, firewall, anti-spyware, etc).	6,21%

Com essa análise, podemos verificar quais são os temas mais exigidos pela banca Cebraspe e, através disso, focaremos nos principais pontos em nossa revisão!

Informática – PRF		
Assunto	**Bizus**	**Caderno de Questões**
Conceitos e modos de utilização de tecnologias, ferramentas, aplicativos e procedimentos associados a internet.	1 a 2	http://questo.es/3za5bi
Computação na nuvem (cloud computing)	3 a 4	http://questo.es/35xajf
Ferramentas e aplicativos comerciais de navegação	5	http://questo.es/53h3y4
Conceitos de proteção e segurança	6	http://questo.es/c7ru0z
Noções de vírus, worms, phishing e pragas virtuais	7	http://questo.es/tbpj55
Windows	8	http://questo.es/9myc4w

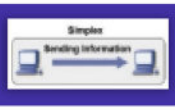
Conceitos e modos de utilização de tecnologias, ferramentas, aplicativos e procedimentos associados a internet.

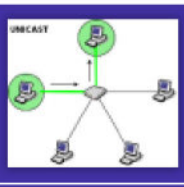
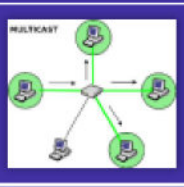
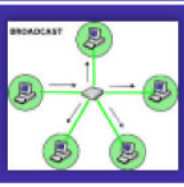
1. Definição de Redes de Computadores

- Uma rede é um conjunto de terminais, equipamentos, meios de transmissão e comutação que interligados possibilitam a prestação de serviços.

2. Pontos importantes

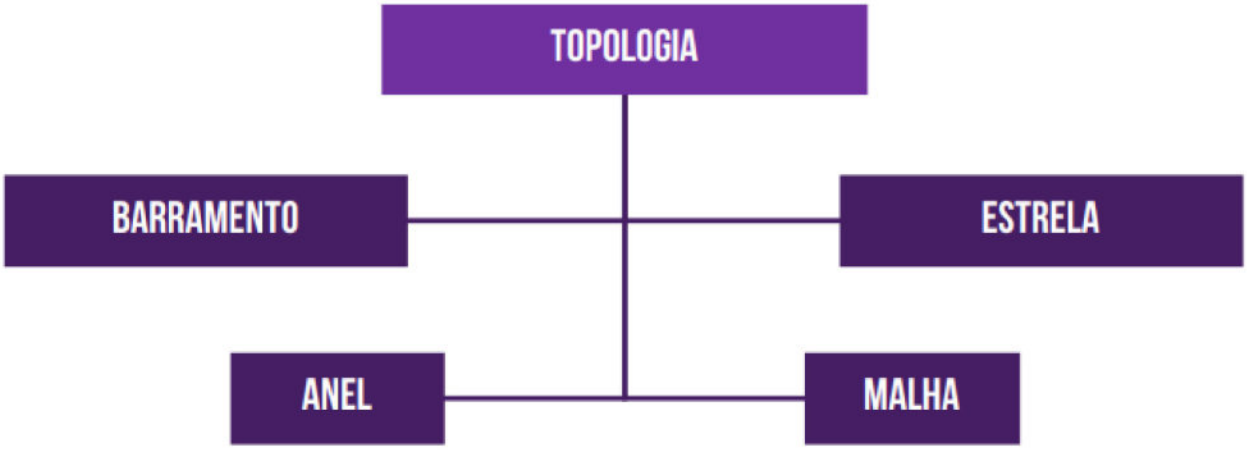
TIPO DE CONEXÃO	DESCRIÇÃO
PONTO-A-PONTO	Conexão que fornece um link dedicado entre dois dispositivos.
PONTO-MULTIPONTO	Conexão que fornece um link compartilhado entre mais de dois dispositivos.

TIPO	REPRESENTAÇÃO	DESCRIÇÃO
SIMPLEX		Uma comunicação é dita simplex quando há um transmissor de mensagem, um receptor de mensagem e esses papéis nunca se invertem no período de transmissão.
HALF-DUPLEX		Uma comunicação é dita half-duplex quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados, porém nunca simultaneamente.
FULL-DUPLEX		Uma comunicação é dita full-duplex quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados simultaneamente.

TIPO	REPRESENTAÇÃO	DESCRIÇÃO
UNICAST		Uma mensagem só pode ser enviada para um destino. Grosso modo, quando você envia uma mensagem no Whatsapp para uma pessoa específica, você está enviando uma mensagem unicast.
MULTICAST		Uma mensagem é enviada para um grupo de destino. Grosso modo, quando você cria uma lista de transmissão no Whatsapp com um grupo de pessoas e os envia uma mensagem, você está enviando uma mensagem multicast.
BROADCAST		Uma mensagem é enviada para todos os destinos. Grosso modo, quando você cria uma lista de transmissão no Whatsapp com todos os seus contatos e os envia uma mensagem, você está enviando uma mensagem broadcast.

TIPO	SIGLA	DESCRIÇÃO	DISTÂNCIA
PERSONAL AREA NETWORK	PAN	Rede de computadores pessoal (celular, tablet, notebook, entre outros).	De alguns centímetros a alguns poucos metros.
LOCAL AREA NETWORK	LAN	Rede de computadores de lares, escritórios, prédios, entre outros.	De algumas centenas de metros a alguns quilômetros.
METROPOLITAN AREA NETWORK	MAN	Rede de computadores entre uma matriz e filiais em uma cidade.	Cerca de algumas dezenas de quilômetros.
WIDE AREA NETWORK	WAN	Rede de computadores entre cidades, países ou até continentes.	De algumas dezenas a milhares de quilômetros.

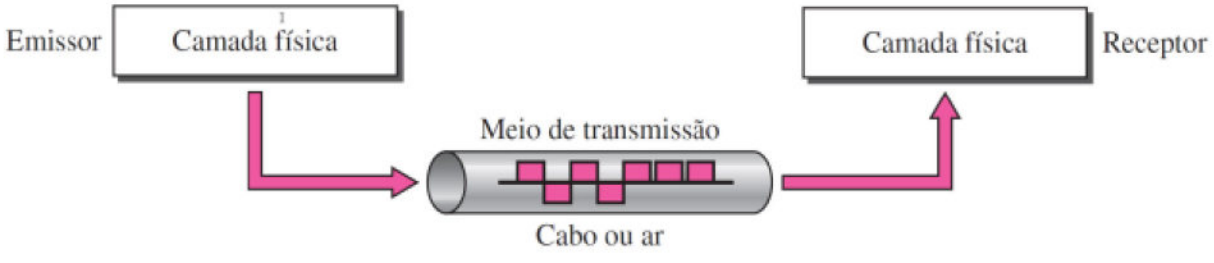
TIPO DE REDE	DESCRIÇÃO
PONTO A PONTO	Também chamada de Rede Par-a-Par, é o modelo de rede mais simples de ser montado. Nesse modelo, todas as máquinas podem compartilhar dados e periféricos umas com as outras. Essas redes são comuns em residências e entre filiais de empresas, porque demandam um baixo custo, são facilmente configuráveis e possibilitam altas taxas de velocidade de conexão.
CLIENTE/ SERVIDOR	É um modelo de redes mais complexo, porém mais robusto e confiável. Nesse modelo, existe uma máquina especializada, dedicada e geralmente remota, respondendo rapidamente aos pedidos vindos dos demais computadores da rede – o que aumenta bastante o desempenho de algumas tarefas. É a escolha natural para redes grandes, como a Internet – que funciona tipicamente a partir do Modelo Cliente/Servidor.



TIPO DE TOPOLOGIA	DESCRIÇÃO
FÍSICA	Exibe o layout (disposição) dos links e nós de rede.
LÓGICA	Exibe o fluxo ou percurso dos dados na rede.

TIPO	REPRESENTAÇÃO	DESCRIÇÃO
BARRAMENTO (BUS)		Todas as estações ficam ligadas ao mesmo meio de transmissão, isto é, um único cabo (chamado backbone) em que os nós se ligam através de conectores. Há maior facilidade na instalação e economia de cabeamento, mas não há isolamento de falhas – uma ruptura no cabo implica a interrupção da comunicação.
ANEL (RING)		Cada dispositivo possui uma conexão ponto-a-ponto com outros dois dispositivos conectados lado a lado, e fazendo uso de uma comunicação com transmissão unidirecional (simplex). Nesse caso, a mensagem circula o anel, sendo regenerada e retransmitida a cada nó, passando pelo dispositivo de destino que copia a informação enviada, até retornar ao emissor original. Nesse momento, o link é liberado para que possa ser utilizado pelo nó seguinte.
ESTRELA (STAR)		As estações estão ligadas a um nó central controlador, pelo qual passam todas as mensagens, não havendo tráfego direto entre os dispositivos. O enlace entre estações e o nó central é Ponto-a-Ponto. É a topologia mais usada atualmente por facilitar a adição de novas estações e a identificação ou isolamento de falhas, em que – se uma conexão se romper – não afetará a comunicação de outras estações.
MALHA (MESH)		Cada estação possui um link ponto a ponto dedicado geralmente com transmissão bidirecional (full duplex) entre cada uma das demais estações. Em outras palavras, todos os computadores estão interligados entre si, de modo que caso haja uma ruptura em algum cabo, não cai a rede inteira, somente o nó conectado a esse cabo.

TIPO DE MEIO	DESCRIÇÃO
GUIADO	Trata-se da transmissão por cabos ou fios de cobre, onde os dados transmitidos são convertidos em sinais elétricos que propagam pelo material condutor. Exemplo: cabos coaxiais, cabos de par traçado, fibra óptica, entre outros.
NÃO-GUIADO	Trata-se da transmissão por irradiação eletromagnética, onde os dados transmitidos são irradiados através de antenas para o ambiente. Exemplo: ondas de rádio, microondas, infravermelho, bluetooth e wireless.



TIPO	REPRESENTAÇÃO	DESCRIÇÃO
CABO COAXIAL		Consiste em um fio central de cobre, envolvido por uma blindagem metálica. Isolantes de plástico flexível separam os condutores internos e externos e outras camadas do revestimento que cobrem a malha externa. Esse meio de transmissão é mais barato, relativamente flexível e muito resistente à interferência eletromagnéticas graças à malha de proteção que possui. Esse cabo cobre distâncias maiores que o cabo de par trançado e utiliza um conector chamado BNC.
CABO DE PAR TRANÇADO		Consiste de quatro pares de fios trançados blindados ou não, e envolto de um revestimento externo flexível. Eles são trançados para diminuir a interferência eletromagnética externa e interna – quanto mais giros, maior a atenuação. Este é o cabo mais utilizado atualmente por ser o mais barato de todos e ser bastante flexível. Esse cabo cobre distâncias menores que o cabo coaxial e utiliza um conector chamado RJ-45 (Memorizem!).
CABO DE FIBRA ÓPTICA		Consiste em uma Casca e um Núcleo (de vidro) para transmissão de luz. Possui capacidade de transmissão virtualmente infinita, é imune a interferências eletromagnéticas e consegue ligar distâncias maiores sem a necessidade de repetidores. Como desvantagens, podemos dizer que é incapaz de fazer curvas acentuadas, além de ter um custo de instalação e manutenção muito alto em relação ao par trançado. Há dois tipos de fibra: Monomodo e Multimodo.

PLACA DE REDE	HUB (CONCENTRADOR)	BRIDGE (PONTE)
		
Equipamento de rede de comunicação bidirecional (entrada e saída de dados) conectado à placa-mãe do computador. Toda placa de rede possui um número identificador chamado Endereço MAC (48 Bits).	Dispositivo de rede capaz de aumentar o alcance de uma rede local por meio da reqeneração de sinais. É capaz de trabalhar apenas com broadcast, isto é, ao receber um pacote de dados, distribui para todas as máquinas da rede.	Equipamento capaz de separar uma rede em seqmentos menores, reduzindo as chances de colisões quando várias máquinas desejam transmitir dados ao mesmo tempo. São dispositivos capazes de enviar dados para máquinas específicas.
SWITCH (COMUTADOR)	**ROUTER (ROTEADOR)**	**MODEM**
		
Equipamento semelhante às Bridqes, no entanto possuem mais portas. Em contraste com hubs, são capazes de enviar transmitir dados para máquinas específicas (unicast ou multicast). Por segmentarem a rede, reduzem as colisões e diminuem o fluxo de informações.	Equipamento que permite interligar redes distintas e são capazes de escolher as melhores rotas para transmissão de pacotes de dados. É responsável por interligar dispositivos de uma rede local (Ex: Computador, Notebook, Smartphone, Impressora, etc) à internet.	Equipamento capaz de converter sinais digitais em sinais analógicos e vice-versa, em geral por meio de uma linha telefônica. Os três modelos principais são: Acesso Discado; Modem ADSL; e Cable Modem.

PADRÕES DE REDES OU ARQUITETURA DE INTERCONEXÃO

Trata-se de um conjunto de padrões de interconexão de redes de computadores.

PADRÃO	NOME
IEEE 802.3	Ethernet (LAN)
IEEE 802.5	Token Ring (LAN)
IEEE 802.11	Wi-Fi (WLAN)
IEEE 802.15	Bluetooth (WPAN)
IEEE 802.16	WiMAX (WMAN)
IEEE 802.20	Mobile-Fi (WWAN)

PADRÃO ETHERNET (IEEE 802.3)

Padrão de interconexão atualmente em redes locais cabeadas baseada no envio de pacotes de dados – possui diversas variantes como Fast Ethernet, Gigabit Ethernet, 10G Ethernet, etc.

EVOLUÇÃO DOS PADRÕES ETHERNET	
PADRÃO (CABO DE PAR TRANÇADO)	PADRÃO – TAXA MÁXIMA DE TRANSMISSÃO
Ethernet	10BASE-T / 10 Mbps
Fast Ethernet	100BASE-T / 100 Mbps
Gigabit Ethernet	1000BASE-T / 1000 Mbps
10G Ethernet	10GBASE-T / 10000 Mbps

PADRÃO TOKEN RING (IEEE 802.5)

Arquitetura de conexão redes locais cabeada atualmente em desuso. Possui comunicação unidirecional (simplex), arquitetura ponto-a-ponto e topologia lógica em anel.

PADRÃO WIRELESS (IEEE 802.11)

Arquitetura de conexão de redes locais sem fio que define um conjunto de padrões de transmissão e codificação para comunicações não cabeadas.

EVOLUÇÃO DO PADRÃO WIRELESS (802.11)		
PADRÃO	FREQUÊNCIA	TAXA MÁXIMA DE TRANSMISSÃO
IEEE 802.11B	2.4 Ghz	11 Mbps
IEEE 802.11A	5.0 Ghz	54 Mbps
IEEE 802.11G	2.4 Ghz	54 Mbps
IEEE 802.11N	2.4 ou 5.0 Ghz	150, 300 até 600 Mbps
IEEE 802.11AC	5.0 Ghz	500 Mbps, 1 Gbps ou +

PADRÃO WIMAX (IEEE 802.16)

O Padrão WiMAX especifica um padrão sem fio de alta velocidade para Redes Metropolitanas (WMAN), criado por um consórcio de empresas para promover interoperabilidade entre equipamentos. Seu raio de comunicação com o ponto de acesso pode alcançar até cerca de 40 km, sendo recomendável para prover acesso à internet banda larga a empresas e residências em que o acesso ADSL ou HFC se torna inviável por questões geográficas.

INTERNET

A Internet é basicamente um vasto conjunto de redes de computadores diferentes que utilizam um padrão comum de comunicação e oferece um determinado conjunto de serviços.

PRINCIPAIS SERVIÇOS	DESCRIÇÃO
WORLD WIDE WEB (WWW)	Trata-se do serviço de visualização de páginas web organizadas em sites em que milhares de pessoas possuem acesso instantâneo a uma vasta gama de informação online em hipermídia que podem ser acessadas via navegador – é o serviço mais utilizado na Internet. Em geral, esse serviço utiliza protocolos como HTTP e HTTPS.
CORREIO ELETRÔNICO	Trata-se do serviço de composição, envio e recebimento de e-mails entre partes de uma maneira análoga ao envio de cartas – é anterior à criação da Internet. Utiliza tipicamente um modo assíncrono de comunicação que permite a troca de mensagens dentro de uma organização. Em geral, esse serviço utiliza protocolos como POP_3, IMAP e SMTP.
ACESSO REMOTO	Trata-se do serviço que permite aos usuários facilmente se conectarem com outros computadores, mesmo que eles estejam em localidades distantes no mundo. Esse acesso remoto pode ser feito de forma segura, com autenticação e criptografia de dados, se necessário. Em geral, esse serviço utiliza protocolos como SSH e TELNET.
TRANSFERÊNCIA DE ARQUIVOS	Trata-se do serviço de tornar arquivos disponíveis para outros usuários por meio de downloads e uploads. Um arquivo de computador pode ser compartilhado ou transferido com diversas pessoas através da Internet, permitindo o acesso remoto aos usuários. Em geral, esse serviço utiliza protocolos como FTP e P_2P.

WORLD WIDE WEB (WWW)
A Web é uma aplicação que é executada na Internet – trata-se de uma série de páginas web que podem ser acessadas por meio de um navegador web.

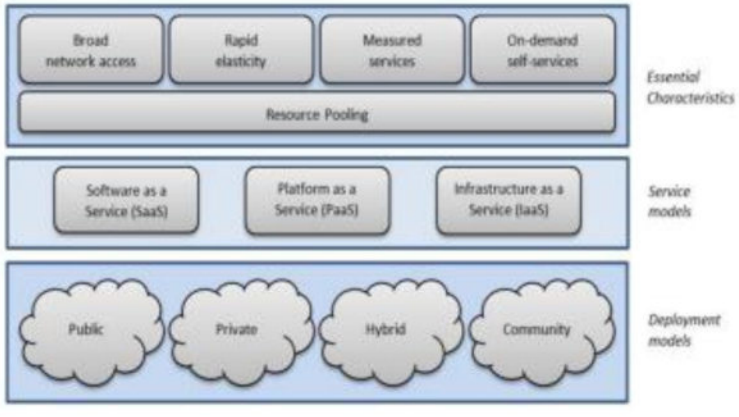
INTERNET DAS COISAS
Trata-se do conceito que se refere à interconexão digital de objetos físicos cotidianos entre si e com usuários por meio de sensores ou softwares capazes de transmitir dados pela internet.

TECNOLOGIAS DE ACESSO	DESCRIÇÃO
DIAL-UP	Trata-se de uma conexão discada através de um modem e uma linha de telefonia fixa. Era a maneira mais popular de acesso da década de 90, hoje encontra-se em desuso. Apresenta um alto custo de implementação, é bastante instável e possui baixas taxas de transmissão. *Era banda larga?* Não, era banda estreita – com taxas máximas de 56Kbps. Se hoje você reclama que a sua internet de 100 Mbps está lenta, lembre-se que uma internet discada era 2000x mais lenta!
ADSL	Trata-se da conexão de banda larga (assim como todas as outras que veremos a seguir) oferecida por empresas de telefonia fixa. ADSL é a sigla para Asymmetric Digital Subscriber Line ou Linha de Assinante Digital Assimétrica. Essa tecnologia possui uma grande vantagem: embora utilize a mesma infraestrutura da telefonia, a transmissão de dados ocorre em frequências mais altas que as de voz, permitindo – portanto – o uso da internet sem ocupar o telefone.
HFC	Trata-se da conexão híbrida de banda larga via cabos de concessionárias de TV a Cabo (NET, GVT, OI). HFC é a sigla para Hybrid Fiber-Coax e representa o hibridismo entre fibra óptica e cabo coaxial. *Por que é um hibridismo, Diego?* Porque os cabos de fibra óptica partem do backbone central, passam pelos postes até chegar mais próximo das residências e se conectar a um receptor óptico. A partir daí, cabos coaxiais saem do receptor e distribuem o sinal entre as casas.
FIBRA ÓPTICA	Trata-se da conexão direta via fibra óptica até a residência do contratante do serviço de internet. Pois é, já existe tecnologia que permite uma conexão direta até a sua casa por meio de um cabo de fibra óptica. Ainda não está disponível em diversas localizações (como a minha casa), mas essa tecnologia tende a se popularizar.
PLC	Trata-se da tecnologia que permite o acesso à internet banda larga via rede elétrica. PLC é a sigla para Power Line Communication. Como vantagem, é uma tecnologia bastante portátil, visto que basta plugar o modem em uma tomada compatível com o serviço para se obter o acesso. No Brasil, embora o serviço seja autorizado pelas agências responsáveis, os investimentos foram baixos por questões estratégicas e econômicas.
RADIODIFUSÃO	Trata-se da tecnologia que permite o acesso à internet banda larga via radiofrequência. As ondas de rádio, em sua maior parte, são omnidirecionais, isto é, quando uma antena transmite ondas de rádio, elas se propagam em todas as direções em broadcast. Elas podem percorrer grandes distâncias e podem atravessar paredes, não necessitando que antenas transmissoras estejam completamente alinhadas. No entanto, não pode haver grandes obstáculos entre o emissor e o receptor de sinal, como montanhas.
SATÉLITE	Uma rede via satélite é uma combinação de nós que fornecem comunicação de um ponto a outro na Terra. Nesse contexto, um nó pode ser um satélite, uma estação terrestre ou o terminal/telefone de um usuário final. Vocês sabiam que é possível utilizar a Lua como satélite? Não há nenhum problema, mas prefere-se o emprego de satélites artificiais que permitem a instalação de equipamentos eletrônicos para regenerar o sinal que perdeu intensidade durante seu trajeto.
TELEFONIA MÓVEL	Trata-se da tecnologia projetada para estabelecer comunicação entre duas unidades móveis, denominadas Estações Móveis; ou entre uma unidade móvel e outra fixa, normalmente chamada Unidade Terrestre. Um provedor de serviços tem de ser capaz de localizar e rastrear uma unidade que faz chamada, alocar um canal à chamada e transferir o canal de uma estação rádio base a outra à medida que o usuário que faz a chamada deixa a área de cobertura.

Computação na nuvem (cloud computing)

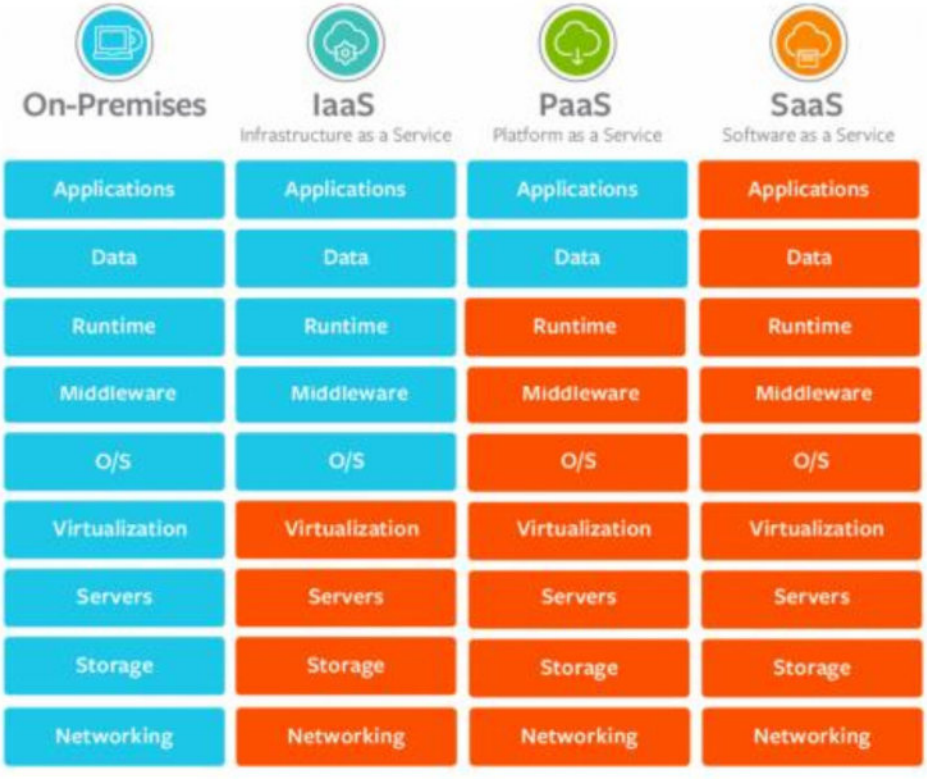
3. Definição

- A Computação em Nuvem pode ser definida como um conjunto de recursos virtuais facilmente utilizáveis e acessíveis, tais como hardware, plataforma de desenvolvimento, serviços, data centers e servidores distribuídos em diferentes posições geográficas pelo mundo.

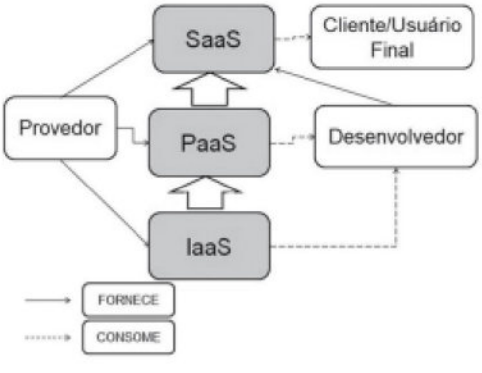


4. Pontos Importantes

CARACTERÍSTICA	DESCRIÇÃO
SERVIÇOS MENSURÁVEIS	Os serviços de nuvem monitoram todos os recursos de tecnologia de modo a otimizá-los da melhor maneira possível e de forma transparente tanto para o fornecedor quanto para o consumidor dos serviços.
ELASTICIDADE RÁPIDA	A elasticidade rápida é a capacidade de um sistema de se adaptar a uma variação na carga de trabalho quase instantaneamente – de forma automática e transparente.
AMPLO ACESSO À REDE	Todas as funcionalidades estão disponíveis através da rede e são acessíveis por meio de mecanismos que promovem o uso de plataformas heterogêneas (smartphones, laptops, tablets, etc).
AGRUPAMENTO DE RECURSOS	Recursos computacionais devem ser agrupados para servir a múltiplos consumidores, com recursos físicos e virtuais sendo arranjados e rearranjados dinamicamente conforme a demanda desses consumidores.
AUTOSSERVIÇO SOB DEMANDA	O autosserviço sob Demanda trata da capacidade de fornecer funcionalidades computacionais de maneira automática, sem que haja a necessidade de o usuário interagir com provedor de serviço.



MODELO DE NUVEM	DESCRIÇÃO
IAAS INFRASTRUCTURE AS A SERVICE	Trata-se da capacidade que o provedor tem de oferecer uma infraestrutura de processamento e armazenamento de forma transparente.
PAAS PLATFORM AS A SERVICE	Trata-se da capacidade oferecida pelo provedor para o desenvolvimento de aplicativos que serão executados e disponibilizados na nuvem.
SAAS SOFTWARE AS A SERVICE	Trata-se de aplicativos de internet, armazenados em nuvem, que fornecem uma série de serviços sob demanda com potencial de escala global via navegador web.



MODELOS DE IMPLANTAÇÃO	DESCRIÇÃO
NUVEM PÚBLICA	Trata-se de uma infraestrutura de nuvem aberta para o público em geral via Internet – os serviços são disponibilizados a qualquer pessoa que queira utilizá-los ou comprá-los (gratuitamente ou não).
NUVEM PRIVADA	Trata-se de uma infraestrutura de nuvem que pode ser acessada por um grupo exclusivo e restrito de pessoas de uma organização pela internet ou por uma rede interna privada.
NUVEM HÍBRIDA	Trata-se da combinação de duas ou mais infraestruturas de nuvens distintas (privadas, comunitárias ou públicas) que permanecem como entidades únicas, mas que são unidas por tecnologias padronizadas ou proprietárias – e devem permitir a portabilidade de dados e aplicações.
NUVEM COMUNITÁRIA	Trata-se de uma nuvem exclusiva e restrita para grupos que possuam interesses em comum. Pode ser de propriedade, administração e operação por uma ou mais organizações na comunidade, um terceiro, ou alguma combinação deles – e pode existir dentro ou fora das instalações.

DEFINIÇÃO ARMAZENAMENTO EM NUVEM
Armazenamento em Nuvem significa armazenamento virtualizado ou – colocado de maneira mais simples – trata-se de backup online. Esse termo define recursos que permitem a um usuário de Internet, em qualquer lugar, com qualquer sistema operacional e qualquer dispositivo de hardware possa acessar arquivos na Internet em sites que permitem o armazenamento de cópias de segurança.

Ferramentas e aplicativos comerciais de navegação

5. Pontos Importantes

FUNCIONALIDADE	DESCRIÇÃO
PÁGINA INICIAL	A Página Inicial é a página aberta por padrão na inicialização de um navegador. Uma funcionalidade que poucos conhecem é que é possível configurar mais uma página como Página Inicial (Google Chrome retirou essa possibilidade em sua última versão).
DOWNLOADS	Para salvar um arquivo em seu computador, você pode realizar um download. O arquivo será salvo no seu local de downloads padrão. É permitido também pausar/cancelar downloads; visualizar a lista de arquivos transferidos; alterar local de salvamento padrão; etc.
HISTÓRICO	Essa funcionalidade é responsável por permitir que o usuário veja os sites que ele visitou anteriormente – exceto os sites visitados em uma guia ou janela de navegação privada.
NAVEGAÇÃO ANÔNIMA	Essa funcionalidade permite navegar com privacidade, sem guardar histórico de páginas visitadas, sem salvar buscas realizadas na barra de pesquisa, sem salvar cookies e dados de sites, sem salvar informações fornecidas em formulários, entre outros.
IMPRIMIR	Essa funcionalidade permite imprimir páginas web em diversas configurações diferentes.
TELA CHEIA	A maioria dos navegadores permite que você utilize o navegador em Modo Tela Cheia ou Tela Inteira. Nesse modo, você não visualiza nenhum botão, menu ou barra de ferramentas – o site ocupa todo o monitor.
BLOQUEADOR DE POP-UPS	Pop-up é uma espécie de janela que é aberta à frente de um site, geralmente como uma propaganda ou informação de destaque. O bloqueador permite que você impeça que a maioria dessas janelas apareçam, oferecendo mais controle à navegação do usuário.
PROTEÇÃO CONTRA RASTREAMENTO	Essa funcionalidade ajuda a evitar que informações sobre a sua navegação sejam enviadas a provedores de conteúdo terceirizados nos sítios que você visita. Já o Do Not Track é um mecanismo passivo que solicita ao site para não te rastrear.
COOKIES	Pequenos arquivos de texto capazes de armazenar informações básicas sobre o visitante de um site na internet, tais como nome, idioma, estado de autenticação, registros de navegação, carrinho de compra, lista de produtos, entre outros.

CACHE	Cache é um conjunto de informações armazenadas temporariamente por um navegador no seu computador com imagens e partes de sites visitados para acelerar a navegação, carregando as páginas visitadas anteriormente de forma mais rápida.
PLUGINS	Plugins são programas ou componentes externos instalados no navegador e que permitem a utilização de recursos que não estão disponíveis nativamente, tais como recursos multimídia e tipos especiais de conteúdos web.
EXTENSÕES	Pequenos programas que adicionam novos recursos ao navegador e personalizam sua experiência de navegação. No entanto, elas já são integradas a lógica de aplicação do navegador.
COMPLEMENTOS	Essa é uma particularidade do navegador web Firefox que chama de Complementos (ou Add-On) o conjunto de Extensões, Temas e Plugins desse browser.

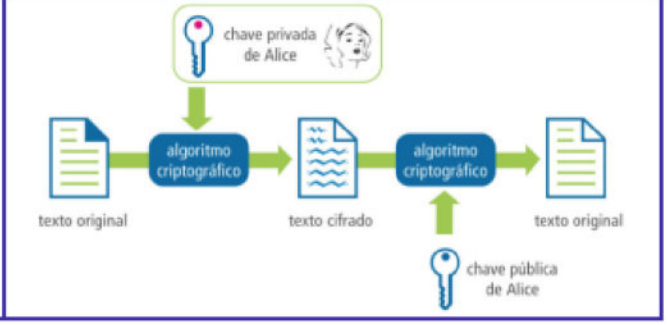
Conceitos de proteção e segurança

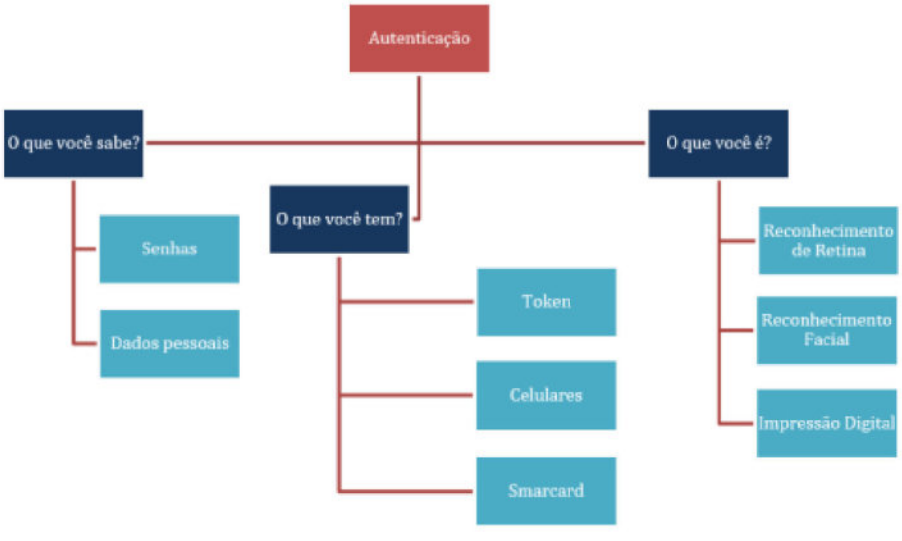
6. Pontos Importantes

PRINCÍPIOS DE SEGURANÇA	DESCRIÇÃO
CONFIDENCIALIDADE	Capacidade de um sistema de não permitir que informações estejam disponíveis ou sejam reveladas a entidades não autorizadas – incluindo usuários, máquinas, sistemas ou processos.
INTEGRIDADE	Capacidade de garantir que a informação manipulada está correta, fidedigna e que não foi corrompida – trata da salvaguarda da exatidão e completeza da informação.
DISPONIBILIDADE	Propriedade de uma informação estar acessível e utilizável sob demanda por uma entidade autorizada.

PRINCÍPIOS ADICIONAIS	DESCRIÇÃO
AUTENTICIDADE	Propriedade que trata da garantia de que um usuário é de fato quem alega ser. Em outras palavras, ela garante a identidade de quem está enviando uma determinada informação.
IRRETRATABILIDADE	Também chamada de Irrefutabilidade ou Não-repúdio, trata da capacidade de garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a sua autoria.

TIPO DE CRIPTOGRAFIA	DESCRIÇÃO
CRIPTOGRAFIA SIMÉTRICA (CHAVE SECRETA)	Utiliza um algoritmo e uma única chave secreta para cifrar/decifrar que tem que ser mantida em segredo.
CRIPTOGRAFIA ASSIMÉTRICA (CHAVE PÚBLICA)	Utiliza um algoritmo e um par de chaves para cifrar/decifrar – uma pública e a outra tem que ser mantida em segredo.
CRIPTOGRAFIA HÍBRIDA (CHAVE PÚBLICA/SECRETA)	Utiliza um algoritmo de chave pública apenas para trocar chaves simétricas – chamadas chaves de sessão – de forma segura. Após a troca, a comunicação é realizada utilizando criptografia simétrica.

CRIPTOGRAFIA ASSIMÉTRICA UTILIZADA PARA GARANTIR O PRINCÍPIO DA CONFIDENCIALIDADE	CRIPTOGRAFIA ASSIMÉTRICA UTILIZADA PARA GARANTIR O PRINCÍPIO DA AUTENTICIDADE
	
O emissor criptografa o texto original com a chave pública do receptor de forma que somente ele consiga descriptografá-lo com sua chave privada para visualizar o texto original.	O emissor criptografa o texto original com sua chave privada de forma que o receptor possa descriptografá-lo com a chave pública do emissor.



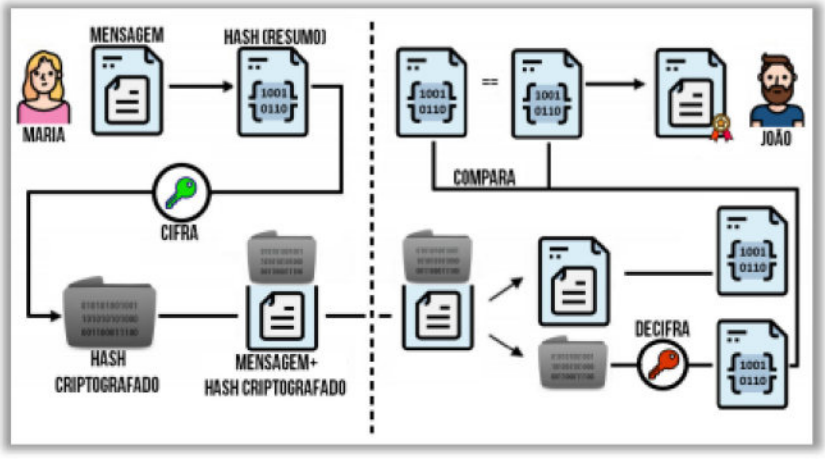
MÉTODOS DE AUTENTICAÇÃO	DESCRIÇÃO
O QUE VOCÊ SABE?	Trata-se da autenticação baseada no conhecimento de algo que somente você sabe, tais como: senhas, frases secretas, dados pessoais aleatórios, entre outros.
O QUE VOCÊ É?	Trata-se da autenticação baseada no conhecimento de algo que você é, como seus dados biométricos.
O QUE VOCÊ TEM?	Trata-se da autenticação baseada em algo que somente o verdadeiro usuário possui, tais como: celulares, crachás, Smart Cards, chaves físicas, tokens, etc.

AUTENTICAÇÃO FORTE

Trata-se de um tipo de autenticação que ocorre quando se utiliza pelo menos dois desses três métodos de autenticação. Um exemplo é a Autenticação em Dois Fatores (ou Verificação em Duas Etapas).

ASSINATURA DIGITAL

Trata-se de um método matemático de autenticação de informação digital tipicamente tratado como substituto à assinatura física, já que elimina a necessidade de ter uma versão em papel do documento que necessita ser assinado. Por meio de um Algoritmo de Hash, é possível garantir a integridade dos dados.



FUNCIONAMENTO DA ASSINATURA DIGITAL

Maria possui uma mensagem em claro (sem criptografia). Ela gera um hash dessa mensagem, depois criptografa esse hash utilizando sua chave privada. Em seguida, ela envia para João tanto a mensagem original quanto o seu hash. João gera um hash da mensagem original e obtém um resultado, depois descriptografa o hash da mensagem utilizando a chave pública de Maria e obtém outro resultado. Dessa forma, ele tem dois hashes para comparar: o que ele gerou a partir da mensagem em claro e o que ele descriptografou a partir da mensagem criptografada. Se forem iguais, significa que Maria realmente enviou a mensagem, significa que ela não pode negar que enviou a mensagem e, por fim, significa que a mensagem está íntegra.

CERTIFICADO DIGITAL

Certificado Digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável – chamada Autoridade Certificadora – e que cumpre a função de associar uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas com o intuito de tornar as comunicações mais confiáveis e auferindo maior confiabilidade na autenticidade. Ele é capaz de garantir a autenticidade, integridade e não-repúdio, e até confidencialidade.

TIPO	GERAÇÃO DO PAR DE CHAVES	TAMANHO DA CHAVE (BITS)	ARMAZENAMENTO	VALIDADE (ANOS)
CERTIFICADO A1/S1	POR SOFTWARE	RSA 1024 OU 2048	DISCO RÍGIDO (HD) E PENDRIVE	1
CERTIFICADO A2/S2	POR SOFTWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	2
CERTIFICADO A3/S3	POR HARDWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	5
CERTIFICADO A4/S4	POR HARDWARE	RSA 2048 OU 4096	SMARTCARD (COM CHIP) OU TOKEN USB	6

GARANTIAS

A criptografia sempre garante **confidencialidade**! Por meio da utilização de cifras simétricas, é possível garantir a **autenticidade** caso a chave seja conhecida apenas por dois participantes. Por meio de cifras assimétricas, é possível realizar o processo de criptografia (em que se garante a **confidencialidade** e a **integridade** por meio de uma função de hash); e realizar o processo de assinatura digital (em que se garante **integridade**, **autenticidade** e **não-repúdio**).

Noções de vírus, worms, phishing e pragas virtuais

7. Pontos Importantes

DEFINIÇÃO DE MALWARE
Códigos maliciosos (Malwares, do inglês *Malicious Softwares*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

FORMAS COMUNS DE INFECÇÃO DE MALWARES
Pela exploração de vulnerabilidades existentes nos programas instalados ou pela auto-execução de mídias removíveis infectadas, como pen-drives;
Pelo acesso a páginas maliciosas, utilizando navegadores vulneráveis ou pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas web ou de outros computadores.

DEFINIÇÃO DE VÍRUS
Programa ou parte de um programa, normalmente malicioso, que se propaga infectando, inserindo cópias de si mesmo, anexando-se ou hospedando-se em arquivos ou programas existentes na máquina.

TIPOS DE VÍRUS	DESCRIÇÃO
VÍRUS DE SCRIPT	Escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML.
VÍRUS DE MACRO	Tipo específico de vírus de script normalmente recebido ao acessar páginas web ou por e-mail e que tenta infectar arquivos manipulados por aplicativos que utilizam essas linguagens mencionadas anteriormente como os arquivos que compõe o Microsoft Office.
VÍRUS DE BOOT	Também conhecido como Vírus de Setor de Carga ou Vírus de Setor de Inicialização, ele é ativado quando o computador é ligado e é carregado na memória antes do sistema operacional.
VÍRUS DE ARQUIVO	Também conhecido como Vírus de Programa ou Parasitário, trata-se do vírus mais tradicional e comum. Ele infecta e causa danos ao se conectarem a arquivos executáveis (.exe, .com, .dll, etc), sobrescrevendo o código original e causando danos quase sempre irreparáveis.
VÍRUS POLIMÓRFICO	Também conhecido como Vírus Mutante, é capaz de assumir múltiplas formas a cada infecção com o intuito de burlar o software de antivírus.
VÍRUS METAMÓRFICO	Trata-se de um vírus que se transforma a cada infecção, mas que – diferentemente do polimórfico – se reescreve completamente a cada infecção, podendo mudar seu tamanho e comportamento, aumentando a dificuldade de detecção.
VÍRUS STEALTH	Projetados explicitamente para não serem detectados pelo antivírus e têm a capacidade de se remover da memória temporariamente para evitar que o antivírus o detecte.
VÍRUS TIMEBOMB	Conhecido como Vírus Bomba Relógio, trata-se de um vírus que – após infectar a máquina – permanece latente (oculto), apenas se replicando, e seu código malicioso é programado para ser ativado em um determinado momento específico, executando sua carga útil.

TIPOS DE MALWARES	DESCRIÇÃO
WORM	Worm (ou Verme) é um programa capaz de se replicar automaticamente, enviando cópias de si mesmo. Diferente dos vírus, ele não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos através da rede, mas – sim – pela exploração automática de vulnerabilidades existentes em programas instalados em computadores ou pela execução direta de suas cópias.
BOT	Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do Worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.
BOTNET	Rede formada por centenas ou milhares de computadores zumbis e que permitem potencializar as ações danosas executadas pelos bots.
CAVALO DE TROIA	O Trojan é um programa que age utilizando o princípio do Cavalo de Troia, em um arquivo é enviado se fazendo passar por um aplicativo útil, como um "presente de grego", mas que na verdade possui funcionalidades maliciosas escondidas. Muitas vezes, o trojan abre portas de comunicação para que através da Internet a máquina possa ser invadida ou monitorada.
RANSOMWARE	Trata-se de um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia, e que exige pagamento de um resgate (*Ransom*, em inglês) para restabelecer o acesso ao usuário – trata-se de uma espécie de extorsão virtual.
SPYWARE	Software espião, capaz de violar a privacidade das informações de usuários, coletando dados da máquina ou da rede e disponibilizando-as a terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.
KEYLOGGER	Trata-se de um spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador e enviá-las a um invasor.
SCREENLOGGER	Trata-se de um spyware – similar ao keylogger – capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.

ADWARE	Trata-se de um spyware projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos quando as propagandas são direcionadas.
SNIFFER	Um Sniffer é programa que age monitorando o tráfego na rede, através da captura de pacotes de dados, em busca de informações sensíveis como o endereço dos sites acessados, senhas de acesso, e-mails, etc.
BACKDOOR	Um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
ROOTKIT	Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
BOMBAS LÓGICAS	Trata-se de um software malicioso normalmente instalado por um usuário autorizado, como um administrador da rede, que o mantém no sistema deixando-o programado para causar danos (como excluir arquivos importantes) em um determinado evento, como por exemplo o caso de ficar mais de 30 dias sem efetuar login.
EXPLOITS	Trata-se de um software criado por hackers para permitir explorar vulnerabilidades conhecidas de sistemas e assim permitir que iniciantes (*Script Kiddies*) possam praticar ações de invasões sem conhecimentos avançados.
HIJACKER	O Hijacker (sequestro, em inglês) é um software malicioso que modifica o registro do sistema operacional, alterando o funcionamento do navegador, modificando sua página inicial, abrindo páginas automaticamente, inserindo botões inadvertidamente.

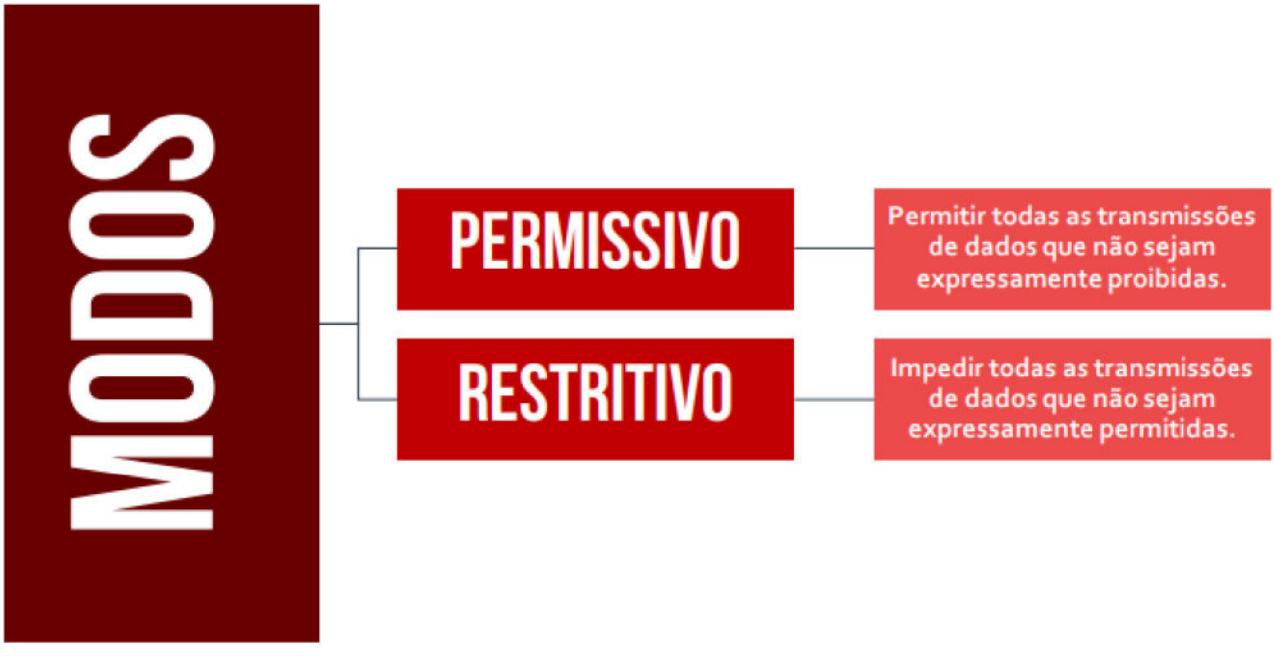
TIPOS DE ATAQUES	DESCRIÇÃO
ENGENHARIA SOCIAL	Trata-se de uma técnica muito utilizada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O termo é utilizado para os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança.
FORÇA BRUTA	Consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário. Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta.
NEGAÇÃO DE SERVIÇO	Negação de serviço (Denial of Service – DoS) é uma técnica pela qual um atacante busca retirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (Distributed Denial of Service – DDoS).
IP SPOOFING	O IP Spoofing (Falsificação/Mascaramento de IP) é uma técnica de invasão comumente empregada quando o mecanismo de autenticação de uma rede é baseado em endereços IP, isto é, quando a identificação de um usuário é realizada baseado em seu número de endereço IP.
E-MAIL SPOOFING	Técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. Essa técnica é possível devido a características do protocolo SMTP (Simple Mail Transfer Protocol) que permitem que campos do cabeçalho sejam falsificados.
PHISHING SCAM	Fraude em que o golpista tenta enganar um usuário para obtenção de dados pessoais e financeiros que permitam a aplicação de um golpe, combinando técnicas computacionais e de engenharia social. Um exemplo de phishing é um e-mail que possa induzir o usuário a clicar em um link falso levando-o para uma página clonada ou um arquivo malicioso.
PHARMING	Ataque que possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original. É um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS. Nesse caso, quando o usuário tenta acessar um site legítimo, o navegador web é redirecionado, de forma transparente, para uma página falsa.
HOAX	Trata-se de uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental.
MAN IN THE MIDDLE	Trata-se de um ataque em que os dados trocados entre duas partes são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. Durante o ataque, a comunicação é interceptada pelo atacante e retransmitida. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação.
DEFACEMENT	Trata-se de uma técnica que consiste em alterar o conteúdo da página web. Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente os atacantes alteram a página principal do site, porém páginas internas também podem ser alteradas.

Aplicativos para segurança (antivírus, firewall, anti-spyware, etc)

8. Pontos Importantes

DEFINIÇÃO DE FIREWALL

São dispositivos, em forma de software e/ou de hardware, que possuem a função de regular o tráfego de dados entre redes distintas, impedindo a transmissão e/ou a recepção de acessos nocivos ou não autorizados de uma rede para outra. Ele controla, analisa, registra, policia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização.



TÉCNICA	DESCRIÇÃO
CONTROLE DE SERVIÇOS	Determina os tipos de serviços de internet que podem ser acessados, de entrada ou saída. O firewall pode filtrar o tráfego com base no endereço IP e número de porta TCP; pode oferecer software de proxy que recebe e interpreta cada solicitação de serviço antes de passá-la adiante, ou pode hospedar o próprio software do servidor, como um serviço web ou de correio.
CONTROLE DE DIREÇÃO	Determina a direção em que determinadas solicitações de serviço podem ser iniciadas e permitidas para fluir através do firewall.
CONTROLE DE USUÁRIO	Controla o acesso a um serviço de acordo com qual usuário está tentando acessá-lo. Essa característica normalmente é aplicada aos usuários dentro do perímetro do firewall (usuários locais). Ela também pode ser aplicada ao tráfego que chega de usuários externos; esse último exige alguma forma de tecnologia de autenticação segura.
CONTROLE DE COMPORTAMENTO	Controla como determinados serviços são utilizados. Por exemplo: o firewall pode filtrar e-mail para eliminar spam ou pode permitir o acesso externo a apenas uma parte da informação em um servidor web local.

TIPOS DE FIREWALL	DESCRIÇÃO
FIREWALL PESSOAL	Software utilizado para proteger um único computador, controlando o tráfego dos dados contra acessos não autorizados provenientes da internet.
FILTRO DE PACOTES	Firewall mais antigo capaz de executar uma política de filtragem com base na combinação de regras específicas (protocolo, porta e lista negra/branca) para examinar cada pacote – sem estado.
FILTRO DE ESTADO DE SESSÃO	Firewall mais moderno que analisa informações dos cabeçalhos dos pacotes de dados e cria uma tabela de estados de conexões para realizar a filtragem baseado nas conexões – com estado.

PROXY

- Proxy é um servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores. Ele funciona como um Firewall no sentido de que é capaz de impedir que sua rede interna seja exposta à Internet – redirecionando solicitações da/para web quando necessário e podendo realizar análise de conteúdo da aplicação.

DEFINIÇÕES DE PROXY
Servidor que visa intermediar as mensagens de nível de aplicação entre clientes internos e servidores externos, para impor uma política de segurança de uma empresa.
Servidor que funciona como intermediário entre um navegador da web e a Internet.
Servidor que permite realizar um controle de acesso a endereços da internet, bloqueando páginas através de seus endereços e/ou palavras previamente definidas.
Servidor que age como intermediário nas requisições entre componentes da rede e entidades externas ou internas a ela de modo a simplificar ou controlar a sua complexidade.
Servidor (sistema de computador ou uma aplicação) que atua como um intermediário entre os computadores de uma rede e a Internet.

Windows

9. Pontos Importantes

ENTRADA DE MENU	DESCRIÇÃO
NOME DO USUÁRIO	O nome da conta de usuário aparece no canto superior direito do menu Iniciar. É possível visualizar arquivos abertos e pastas: Downloads, Meus Documentos, Favoritos, Links, Minhas Imagens, Minhas Músicas e Meus Vídeos.
DOCUMENTOS	Este comando abre rapidamente sua biblioteca de Documentos, fazendo com que seja cada vez mais importante armazenar seus trabalhos aqui.
IMAGENS	É possível visualizar fotos digitais e imagens armazenadas. O ícone de cada imagem e uma imagem em miniatura da sua foto.
CONFIGURAÇÕES	Esta área permite que você ajuste as toneladas de configurações confusas do seu computador.
DESLIGAR	Ao clicar aqui, você desliga, reiniciar ou suspende o seu computador ou dispositivo.

OPÇÕES	DESCRIÇÃO
SUSPENDER	Este estado consome pouca energia – o computador é iniciado mais rapidamente e o usuário volta de imediato ao ponto em que parou. Não é preciso se preocupar se vai perder seu trabalho por esgotamento de bateria, pois o Windows salva automaticamente todo o trabalho e desliga o computador se a bateria estiver com pouca carga.
DESLIGAR	Desliga seu computador ou dispositivo.
REINICIAR	Reinicia seu computador ou dispositivo.

10. Caracteres Inválidos - Windows

- São os caracteres que não podem ser utilizados em nomes de arquivos e pastas no sistema de arquivos do Windows:

CARACTERES INVÁLIDOS	SÍMBOLO	REPRESENTAÇÃO	BONECO
ASPAS	"	Cabelo do boneco	
DOIS-PONTOS	:	Olhos do boneco (deitado)	
ASTERISCO	*	Boca do boneco	
MENOR QUE	<	Braço esquerdo do boneco	
PIPE	|	Corpo do boneco ou barra vertical	
MAIOR QUE	>	Braço direito do boneco	
BARRA	/	Perna esquerda do boneco	
BARRA INVERTIDA	\	Perna direita do boneco	
INTERROGAÇÃO	?	Sexo indefinido do boneco	

Vamos ficando por aqui.

Esperamos que tenha gostado do nosso Bizu!

Bons estudos!

"***A única pessoa que você está destinado a se tornar é a pessoa que você decide ser.***"

(Ralph Waldo Emerson)

Elizabeth Menezes

@elizabethmpalves

Leonardo Mathias

@profleomathias

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.