SENAI

VERSÃO PARA DOWNLOAD

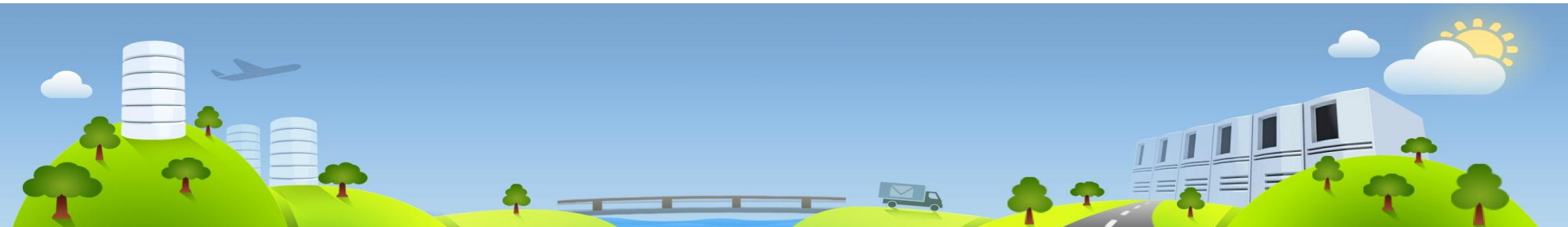
CURSO COMPETÊNCIAS TRANSVERSAIS

TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

OLÁ!
SEJA BEM-VINDO AO CURSO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Neste curso, abordaremos Sistemas Operacionais, Software e seu Licenciamento, Hardware, Ativos de Redes, Cabeamento Estruturado, Pilares de Segurança, Boas Práticas de Segurança, Mitigando Ataques e Boas Práticas de Governança.

SUMÁRIO



INTRODUÇÃO

O que vamos estudar?

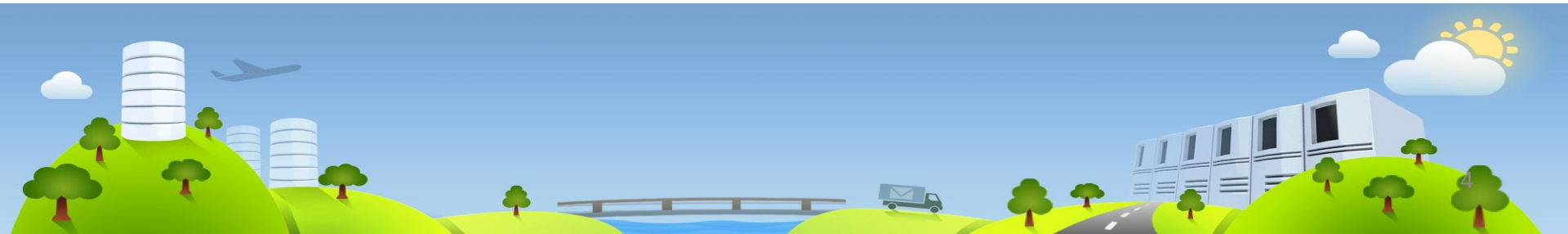
Para conseguir ter uma noção sobre a estrutura de TIC, vamos passar por diversas áreas como computação, redes de computadores, segurança e governança. Essas áreas, mesmo trabalhando de forma distinta, acabam se completando dentro de um mesmo ambiente de TIC. Os seguintes assuntos serão estudados dentro dos seus respectivos módulos:

Software e Hardware
Sistemas Operacionais
Softwares e seu licenciamento
Hardware

Segurança da Informação
Pilares da Segurança
Mitigando Ataques

Infraestrutura
Ativos de Rede
Cabeamento Estruturado

Governança de TIC
Boas Práticas de Governança

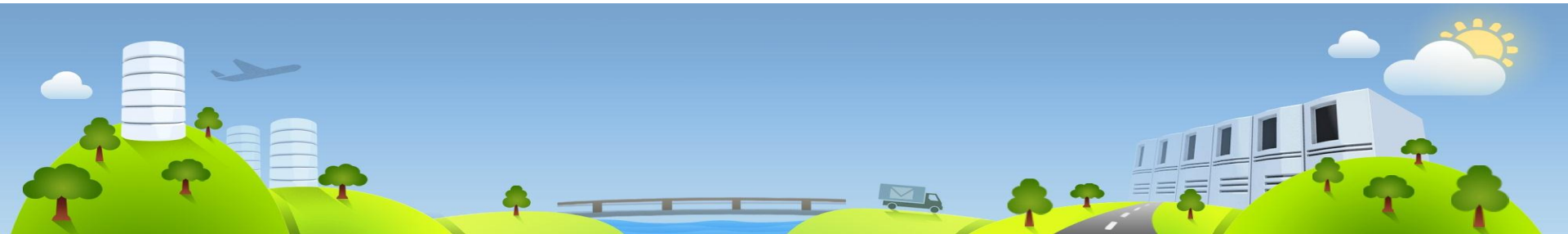


Atualmente essa sigla TIC (Tecnologia da Informação e Comunicação) vem fazendo parte da vida de diretores e gestores empresariais. O ganho de espaço da TIC dentro das empresas deve-se essencialmente a dois motivos:

- avanço da utilização de tecnologias dentro das empresas;
- gestores perceberam que a Tecnologia da Informação é algo de extrema importância para os negócios da instituição.

TIC corresponde a todas as tecnologias que são utilizadas para que um processo computacional seja realizado. TIC não é apenas uma tecnologia, ou um recurso novo que foi inventando, TIC é um conjunto de tecnologias que são utilizadas constantemente por todo mundo.

Agora mesmo você está usufruindo da TIC para acessar este curso. A TIC pode ter uma estrutura mais simplificada, geralmente encontrada em residências ou estruturas mais robustas encontradas em empresas, indústrias e universidades.

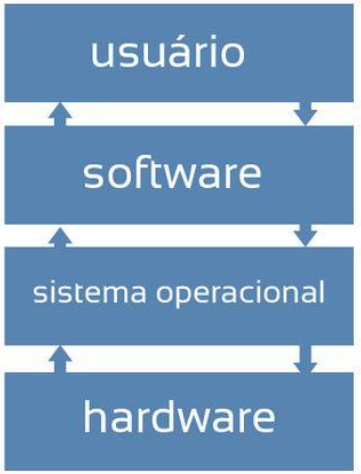


Software/ Hardware

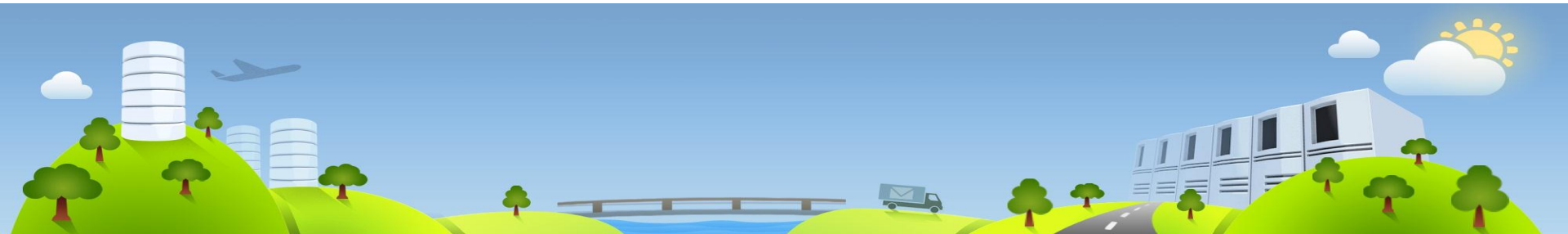
Sistemas Operacionais

O Sistema Operacional(SO) é um *software*, geralmente um conjunto de *softwares*, que gerencia todos os recursos presentes em um computador. Esse gerenciamento atua tanto no *hardware*, como em outros *softwares* também. O SO é responsável por fazer a interação com o *hardware* do computador. O SO tem algumas tarefas complexas, como:

Gerenciar processos;
Gerenciar memória;
Gerenciar recursos;
Gerenciar hardware;



Atualmente existem diversos tipos de sistemas operacionais presentes no mercado, cada um atendendo uma necessidade específica. Na seguinte tabela são apresentados os tipos de sistemas operacionais mais utilizados hoje em dia.



Tipos de Sistemas Operacionais

Portáteis

Sistemas desenvolvidos especificamente para equipamentos móveis, como: celular, *tablet*, *smartphones*.

Exemplos

IOS, Android, Windows Phone, Firefox IOS

Tipos de Sistemas Operacionais

Pessoais

Esses sistemas são os mais utilizados pelos usuários comuns e geralmente são fáceis de utilizar.

Exemplos

Windows, MacOs, Ubuntu, Fedora

Tipos de Sistemas Operacionais

Servidores

São sistemas que trabalham em rede fornecendo algum tipo de serviço para os usuários. Ex.: servidor de arquivos, impressão, antivírus etc.

Exemplos

Windows Server, Debian, Slackware, CentOS, BSD

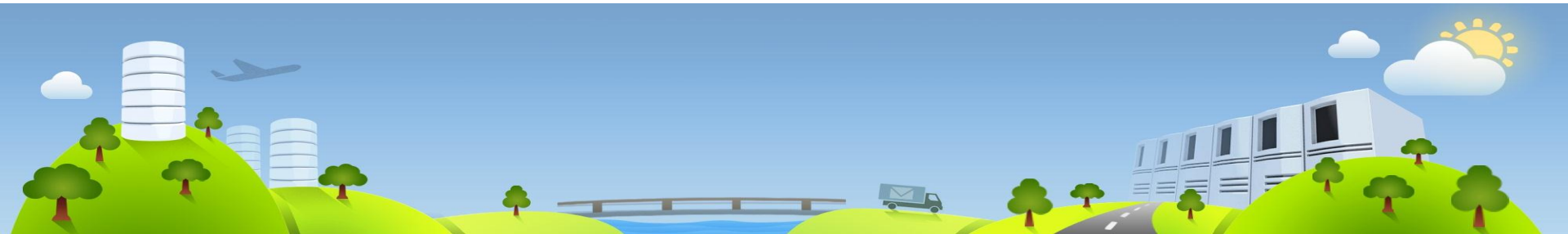
Tipos de Sistemas Operacionais

Grande Porte

São sistemas utilizados em grandes computadores, conhecidos como *mainframe*.

Exemplos

z/OS, OS/390



Tipos de Sistemas Operacionais

Embarcados

São sistemas simples desenvolvidos para atender uma necessidade bem específica. Podemos encontrar esse tipo de sistema em micro-ondas, geladeiras, relógio ponto.

Exemplos

QNX, VxWorks.

Tipos de Sistemas Operacionais

Tempo Real

Esses tipos de sistemas precisam ter um tempo de resposta muito rápido para não comprometer as tarefas que ele exerce. Geralmente esses sistemas trabalham em situações críticas, como controle de tráfego aéreo, sistema de freio ABS.

Exemplos

FreeRTOS, AIX, CMX

Tipos de Sistemas Operacionais

Smart Cards

São sistemas que rodam em pequenos cartões, como cartão de crédito, telefonia móvel, cartões de fidelidade.

Exemplos

JavaCard, MS Windows Card, ZeitControl Basic Card

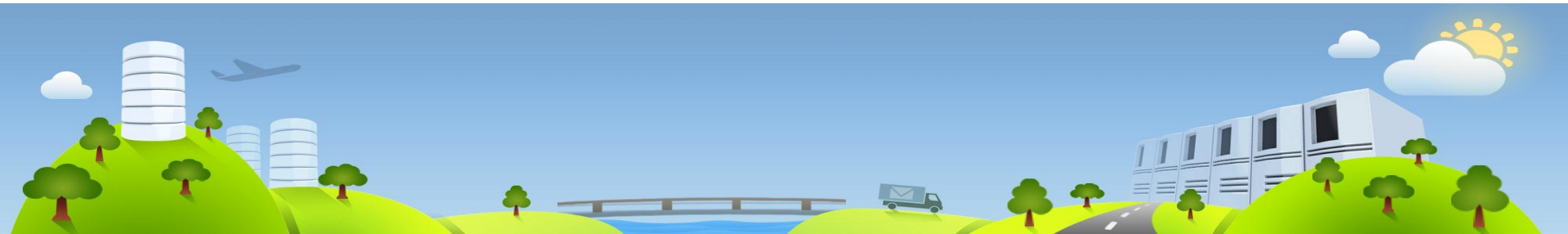
Tipos de Sistemas Operacionais

Multiprocessadores

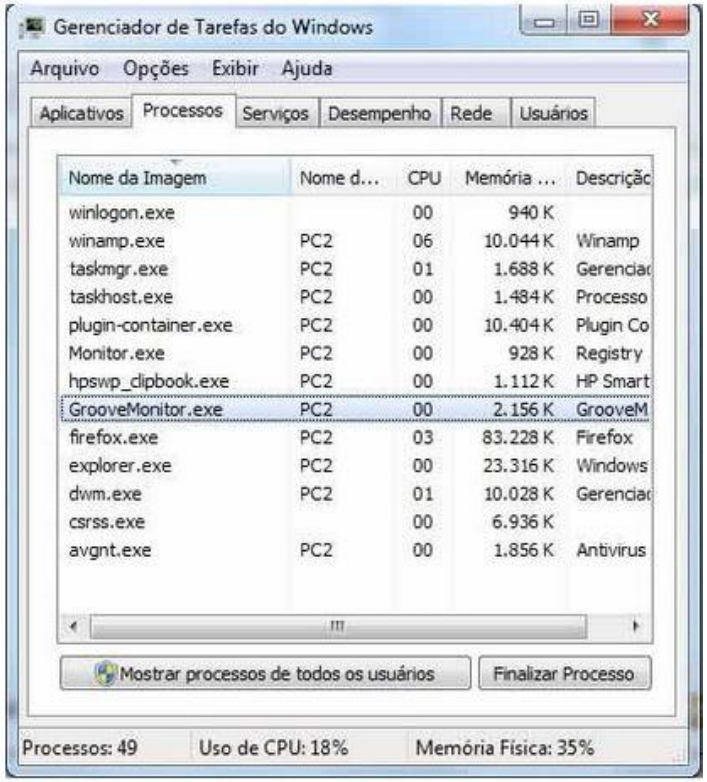
Esses sistemas têm a capacidade de trabalhar com vários processadores simultaneamente.

Exemplos

K42



O SO tem a capacidade de gerenciar diversos recursos simultaneamente; vários processos precisam ser executados para que o SO se mantenha em funcionamento. Se você estiver utilizando um SO da Microsoft, basta digitar as teclas em sequência CTRL + ALT + Delete e uma janela semelhante à figura ao lado será apresentada. Nessa janela, conhecida como Gerenciador de Tarefas, conseguimos saber a porcentagem de CPU utilizada pelos programas, memória RAM utilizada, utilização da placa de rede, espaço em disco disponível, entre outras informações.

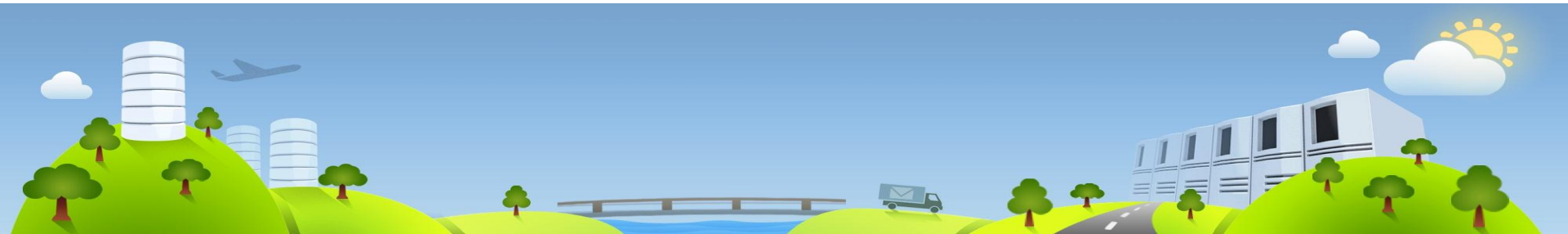


Drives

Um papel de extrema importância que o SO realiza é fazer a interação com o *hardware*. Para realizar essa interação o SO utiliza um*driver* para conseguir identificar e gerenciar os*hardwares* instalados no computador. Há situações em que o próprio SO já tem o *driver*necessário, fazendo com que o usuário não precise instalar nada extra para que o*hardware* funcione. Nesse tipo de caso falamos que o equipamento é Plug and Play, pois a partir da conexão do *hardware* na máquina o próprio sistema reconhece e deixa o dispositivo pronto para ser usado. A seguir alguns dispositivos que geralmente trabalham com essa tecnologia.

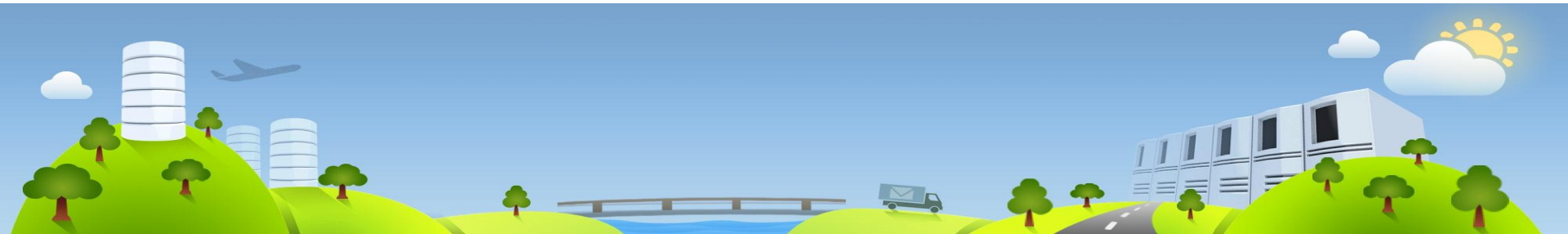
Escolha do Sistema Operacional

Um profissional de TI tem que ter o conhecimento de qual sistema operacional utilizar em determinada situação. A escolha do sistema operacional deve partir da necessidade que ele deve satisfazer. Após o levantamento das funcionalidades e compatibilidades que o SO tem, devemos realizar o levantamento de quais sistemas atendem essa demanda atualmente. É muito importante que o SO escolhido seja um sistema atualizado, pois sistemas antigos possuem uma tendência maior a falhas de segurança.



Mesmo com uma infinidade de sistemas operacionais, grande parte dos usuários utiliza os sistemas da Microsoft. A W3C, empresa de pesquisas e estatísticas WEB, gera mensalmente relatórios com as características dos computadores que acessam os mais de 72 mil *sites* que a empresa analisa. A seguinte tabela mostra a estatística de acesso realizada no mês de janeiro de 2014.

Sistema Operacional	% Utilização
Windows 7	39.34%
Windows XP	13.80%
Mac OS X	10.05%
iOS 7	7.87%
Windows 8	7.70%



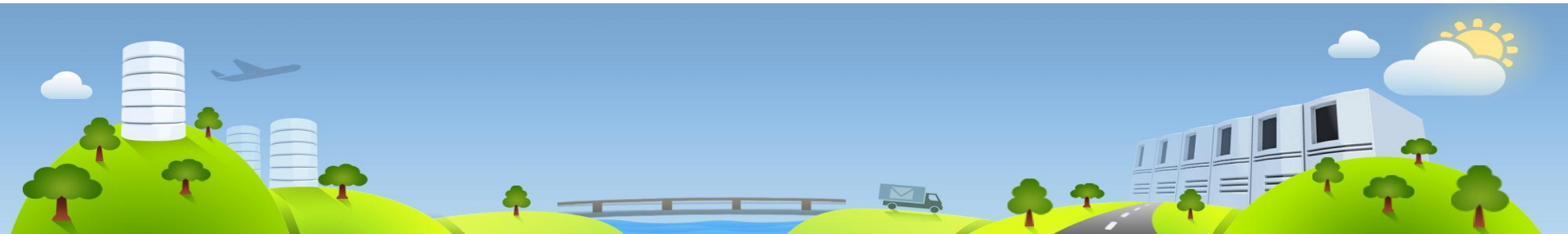
Softwares e seu licenciamento

Podemos definir como *software* toda parte lógica de um computador. Através do *software* conseguimos realizar nossas tarefas como editar um texto, escutar música, navegar na Internet etc. O *software* é desenvolvido utilizando uma linguagem de programação; atualmente existem centenas de linguagens que são utilizadas para finalidades específicas. Algumas linguagens utilizadas no mercado são Java, PHP, Visual Basic, ASP, Phyton, Perl etc. Em pesquisa realizada em 2013 a empresa Tiobe *software* levantou as linguagens de programação mais utilizadas em 2013.

Quando um *software* é desenvolvido, ele deve atender um tipo de licenciamento. O licenciamento informa os direitos e deveres que o usuário deve ter com esse programa. Grande parte dos *softwares* traz, no momento da sua instalação, um termo descrevendo a responsabilidade que o usuário deve ter com o *software*. Caso o usuário não aceite os termos, a instalação não é concluída.

As linguagens de programação mais utilizadas

Posição	Linguagem de Programação
1	C
2	Java
3	Objective-C
4	C++
5	PHP
6	C#
7	Visual Basic
8	Python
9	Perl
10	JavaScript



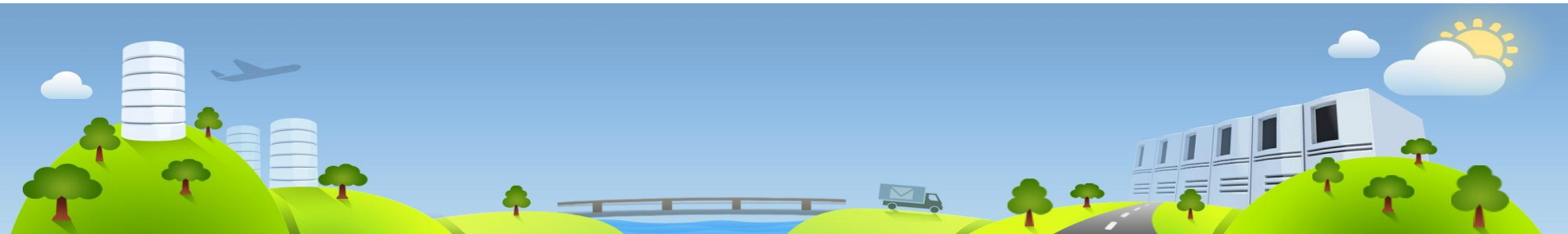
Esse tipo de licença permite que o usuário copie, modifique e redistribua o programa. A Free Software Foundation define quatro liberdades que o *software* precisa ter para ser considerado livre.

1 - Liberdade de executar o programa independente do propósito;
2 - Liberdade de acessar o código fonte e estudar como o programa funciona e adaptar para as suas necessidades;
3 - Liberdade de redistribuir cópias com a intenção de ajudar ao seu próximo;
4 - Liberdade de aperfeiçoar o programa e disponibilizá-lo para que toda a comunidade se beneficie dele.

Exemplo de *softwares* livres: Mozilla Firefox (navegador), Mozilla Thunderbird (e-mail), Filzip (compactador), LibreOffice (editor de texto, planilhas eletrônicas, apresentação de slides, desenho, entre recursos), Media player classic (reprodutor de vídeos).

Esse tipo de *software* possui direitos autorais, ou seja, cópia, redistribuição ou modificação são proibidos pelo desenvolvedor. O *software* proprietário é o inverso do *software* livre. Qualquer alteração necessária nesse tipo de*software* tem que ser solicitado e autorizada pelo distribuidor. Esse modelo de *software* pode ser adquirido de forma gratuita ou paga, dependendo de o desenvolvedor escolher a forma que irá disponibilizar o mesmo.

Exemplo de *softwares* proprietários: AVG (anti-vírus), Winzip (compactador), Windows (sistema operacional).

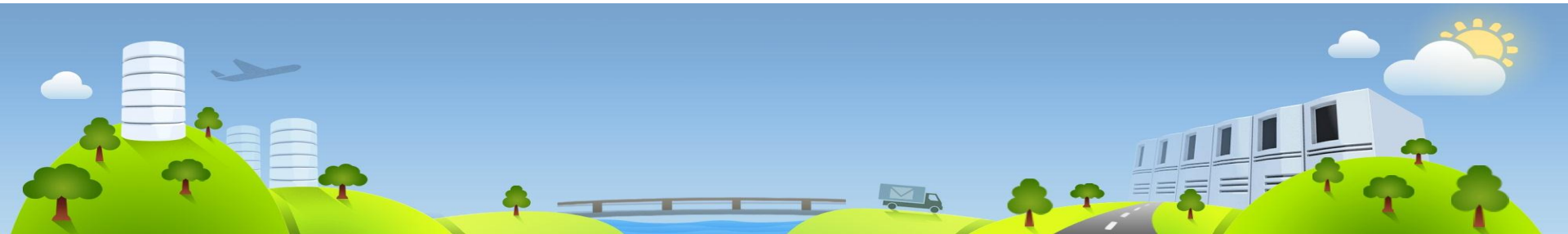


Software que precisa ser comprado para ter o direito à utilização: dependendo do termo que está vinculado ao *software* comprado, o mesmo pode ter seu código fonte alterado pelo usuário que adquiriu. A grande maioria dos *softwares* comerciais também é proprietária.

Exemplo de softwares comerciais: Microsoft Office (editor de texto, planilhas eletrônicas, apresentação de slides, Desenho, entre outros recursos), Adobe Photoshop (edição de imagens), Vegas Pro (edição de vídeos), Solidworks (desenho CAD).

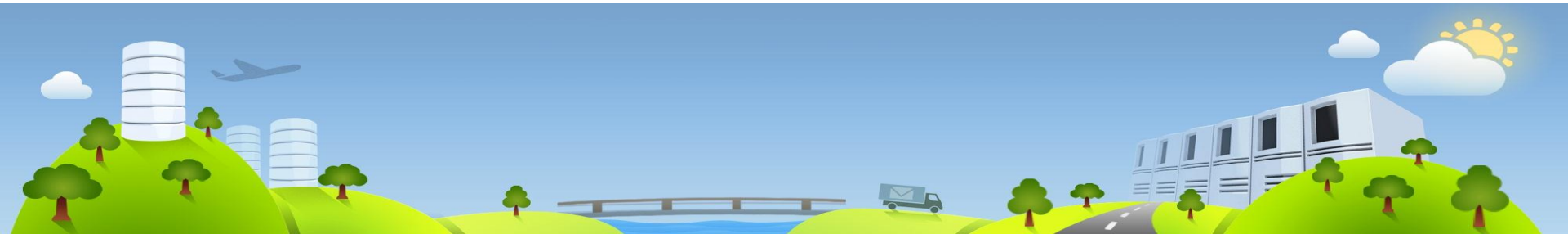
Software gratuito, ou *freeware*, são programas pelos quais o usuário não precisa pagar para utilizar. É muito importante verificar se o *software* que é preciso instalar pode ser utilizado em determinado cenário. Existem *softwares* que são gratuitos para algumas situações como somente para uso doméstico ou escolar, sendo proibida a utilização em um ambiente empresarial.

Exemplo de *softwares* gratuitos: Avast! Free Antivirus(anti-vírus), WinRAR(compactador), Skype(permite realizar ligações e mensagens de texto).



Antes de instalar um *software* é preciso saber qual licença ele utiliza. A instalação de *softwares* comerciais ou proprietários, sem a devida aquisição ou autorização da empresa desenvolvedora, encaixa-se em um crime de pirataria. Muitos *softwares* comerciais são encontrados facilmente hoje na Internet sem nenhum tipo de cobrança, esses tipos de programas são considerados piratas, pois a empresa não tem ciência da disponibilização de*software*. As Leis n. 9.609/98 e n. 9.610/98 protegem o direito de autor sobre programas de computador, essa lei prevê as seguintes penalidades em caso de infringência dessas leis.

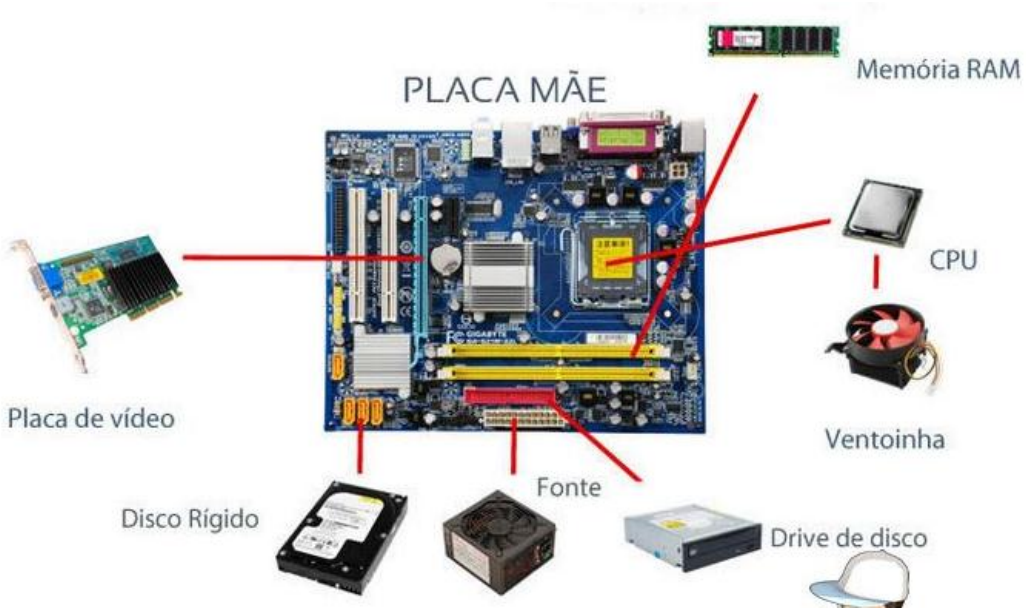
Violar direito de autor: detenção de seis meses a dois anos ou multa. Reprodução para fins de comércio: reclusão de um a quatro anos e multa. Exposição à venda, aquisição, ocultação ou armazenamento para fins de comércio, de cópia produzida com violação de direito autoral: reclusão de um a quatro anos e multa. Qualquer dos delitos acima pode gerar uma indenização que pode chegar a 3000 vezes o valor de cada *software*.



Hardware

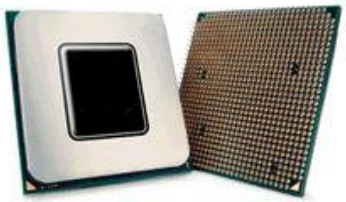
No mundo da informática *hardware* é definido como qualquer equipamento que pode exercer alguma função computacional especifica. De forma resumida *hardware* é toda parte física de um computador, *notebook*, celular, *tablet* entre outros. Com toda evolução dos computadores, centenas de tipos de *hardware*, com a mais vasta finalidade, foram desenvolvidos.

O computador é um conjunto de *hardware*, onde cada peça realiza uma função específica. No decorrer deste capítulo vamos estudar os principais componentes de um computador:



Processador

Responsável por executar todas as instruções e tarefas solicitadas ao computador, geralmente chamado de "cérebro" por exercer essa tarefa complexa. O processador é um dispositivo que esquenta muito devido a sua alta taxa de processamento, por isso encontramos geralmente um *cooler*(ventilador) na parte superior desse dispositivo.

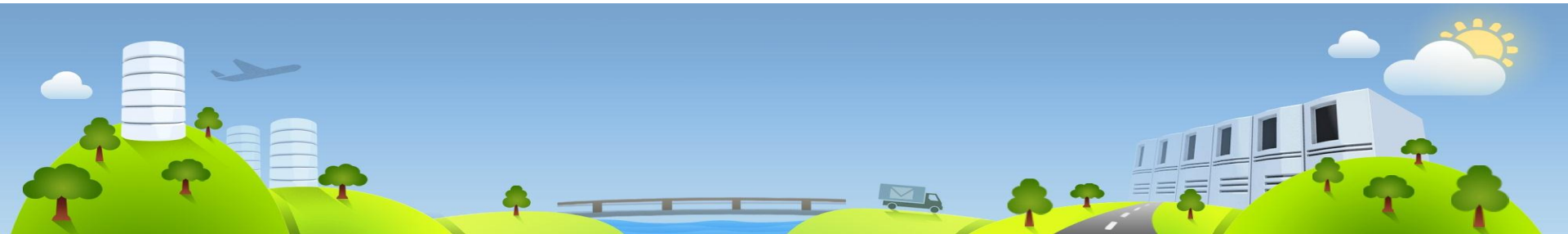


Hard disk (HD)

O hard disk (HD) é responsável por armazenar dados de forma permanente, diferentemente da memória RAM seus dados não são perdidos quando o computador é desligado. Os HD tem a capacidade de armazenar informações na casa dos Terabytes.

Memória RAM

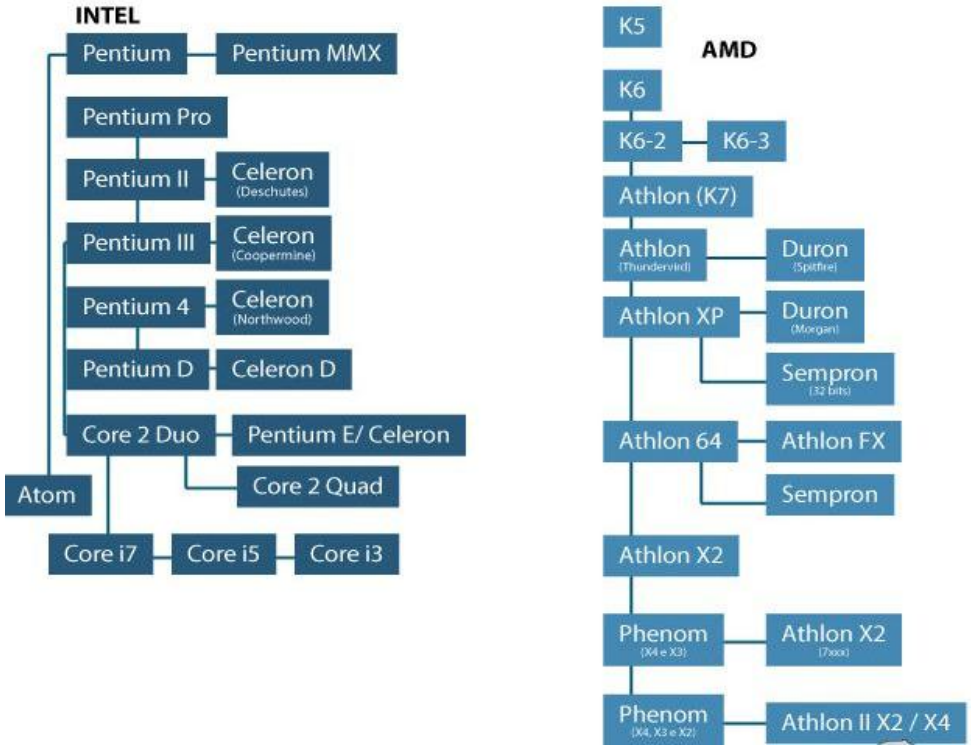
Tem a função de armazenar informações que o processador precisa para conseguir executar sua função. RAM(Random Access Memory) significa memória de acesso randômico, os dados armazenados nesse dispositivo são perdidos quando o computador é desligado. Hoje o padrão DDR 3 é o mais usado no mercado.

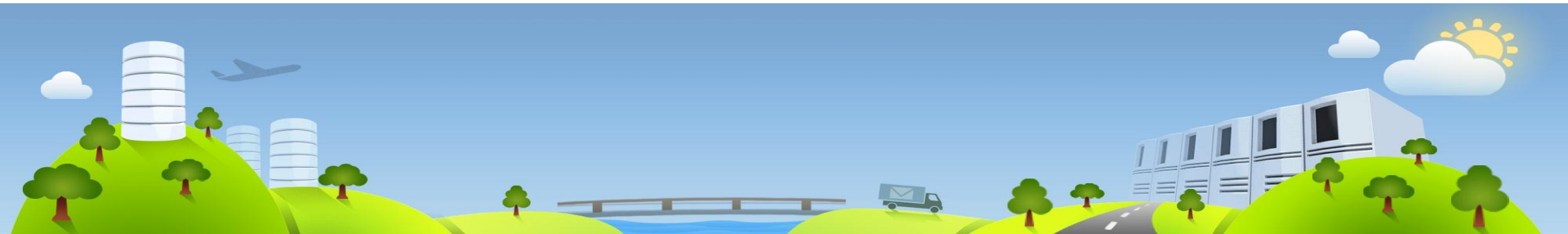


Modelos de processadores

Atualmente as empresas Intel e AMD dominam o mercado de processadores. Essas empresas já vêm a anos evoluindo de suas linhas de processadores, a seguir os modelos que já foram lançados.

Além da linha de processadores voltada para equipamentos desktop, as duas empresas contam com processadores desenvolvidos especificamente para servidores. A Intel possui a linha XEON e a AMD trabalha com o modelo Opteron.





Parte Interna – HD

1 - Pratos: são os discos onde os dados são armazenados. São feitos de alumínio (ou de um tipo de cristal) recoberto por um material magnético e por uma camada de material protetor.

2 - Motor: componente responsável por fazer o disco girar. Geralmente os HDs trabalham na velocidade de 5400rpm(rotação por minuto), 7200rpm e os mais recentes a 10000rpm.

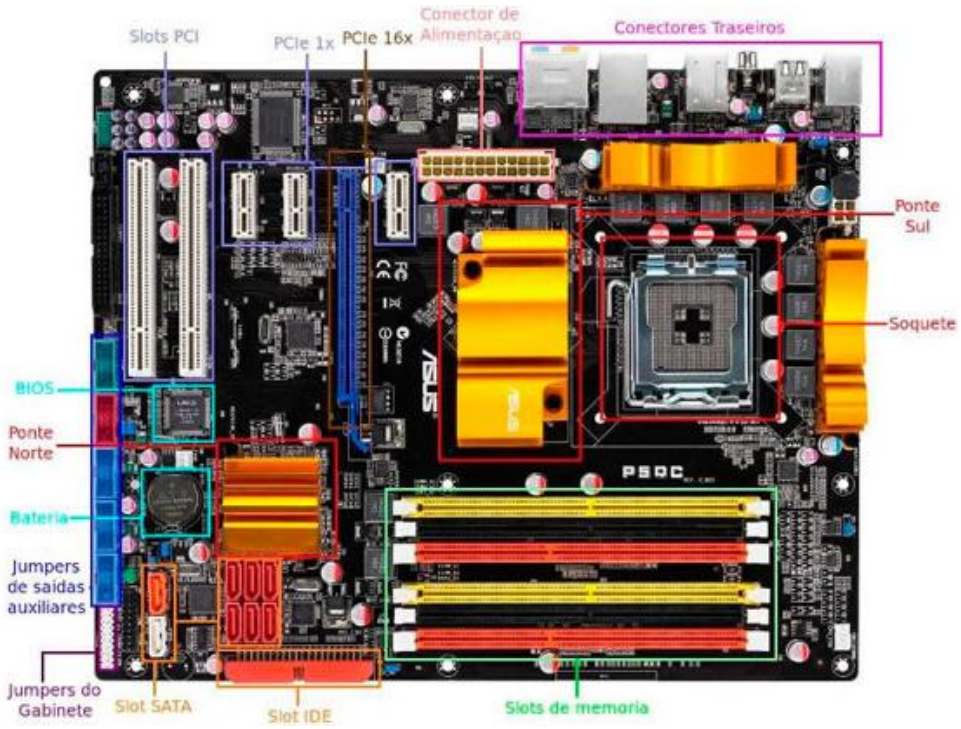
3 - Cabeça: contém uma bobina que utiliza impulsos magnéticos para manipular as moléculas da superfície do disco e, assim, gravar dados. A cabeça de leitura e gravação não toca nos discos.

4 - Braço: função de posicionar os cabeçotes sob a superfície dos pratos.

Placa mãe

Responsável por interligar todos os dispositivos encontrados no computador. Através das trilhas encontradas na placa-mãe, os componentes conseguem trocar dados entre si. Nesse *hardware* são encontrados diferentes conectores, *slots* e portas utilizados para interligar diferentes tecnologias de placas de vídeo, som, rede, processadores, memórias RAM e Hd.

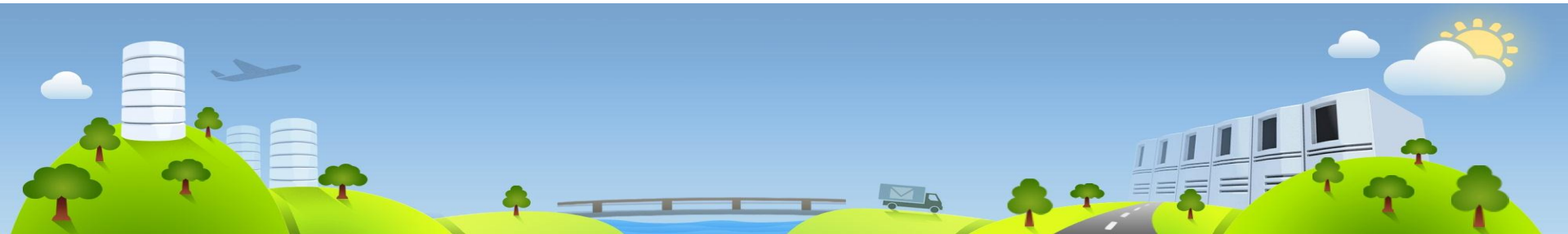
A distribuição dos componentes de uma placa-mãe pode variar de acordo com o fabricante. A seguir um exemplo de placa-mãe da marca ASUS.



Drive de CD/DVD

Servem basicamente para ler CD e DVDs. Atualmente a maioria desses *drives* realiza a gravação em CDs e DVDs. Geralmente na parte externa da bandeja é identificada a função que o leitor realiza.

Sigla	Função
CD-ROM	Apenas lê CDs
CD-RW	Lê e grava CDs
CD-RW + DVD (combo)	Lê CDs e DVDs e grava CDs
DVD-RW	Lê e grava CDs e DVDs

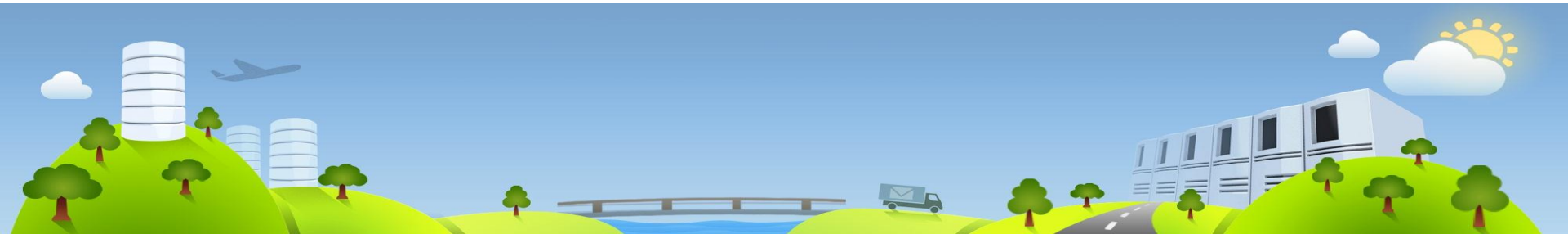


Placa de vídeo

Possui a função de gerar a imagem e enviar para um monitor. Podemos encontrar essas placas acopladas na própria placa-mãe, nesse caso chamamos de uma placa *onboard*, ou adquiri-se uma placa *offboard* e a conecta-la em algums*lot* PCI-Express. A vantagem de uma placa *offboard* é o seu desempenho superior comparado a uma placa *onboard*. A vantagem da placa *onboard* é o preço, pois se torna mais econômico comprar uma placa-mãe com uma placa de vídeo *onboard* do que comprar uma placa-mãe sem vídeo e comprar uma placa de vídeo *offboard*.

Periféricos

Chamamos de periféricos os dispositivos que são conectados na parte externa do gabinete. Geralmente essas conexões são realizadas através das portas PS/2(mouse e teclado) e USB(grande maioria dos equipamentos está utilizando essa interface para se conectar à placa-mãe). As próximas imagens exemplificam alguns periféricos.



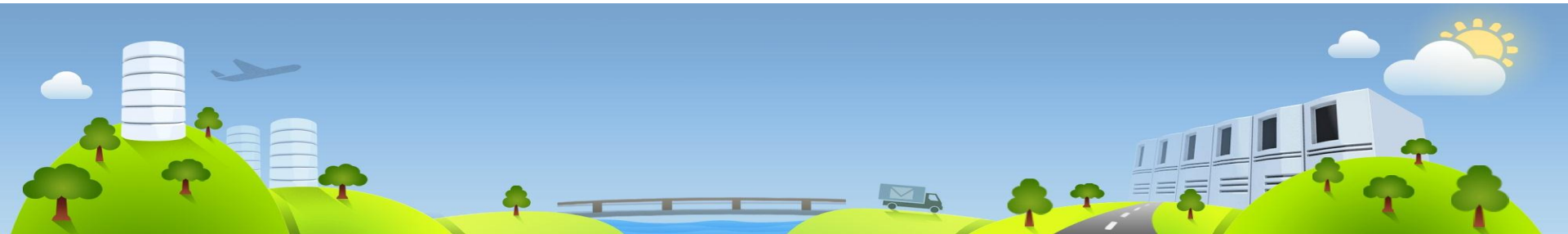
Fonte de alimentação

Dispositivo responsável por fornecer energia para todo computador. A fonte de alimentação utiliza conectores para passar energia à placa-mãe, *drives* e processador. Essas fontes são chamadas também de fontes chaveadas, pois convertem a tensão alternada(AC) para tensão contínua (DC).

Qual componente é mais importante?

Depois de estudar os principais componentes de um computador, qual *hardware* você considera mais importante?
Na verdade todos os dispositivos de um computador são importantes. Você, sem um *mouse* não consegue realizar muitas tarefas, um computador, sem um processador, memória RAM ou placa de vídeo, nem liga.

Todas as peças de um computador devem estar funcionando perfeitamente para que o mesmo consiga realizar suas atividades.



REDE

Ativos de redes

Ativos de redes são considerados os principais equipamentos dentro de uma infraestrutura de TI. Por meio desses equipamentos conseguimos ter conectividade com outros dispositivos em uma rede. Os ativos de redes também possuem as seguintes funcionalidades:

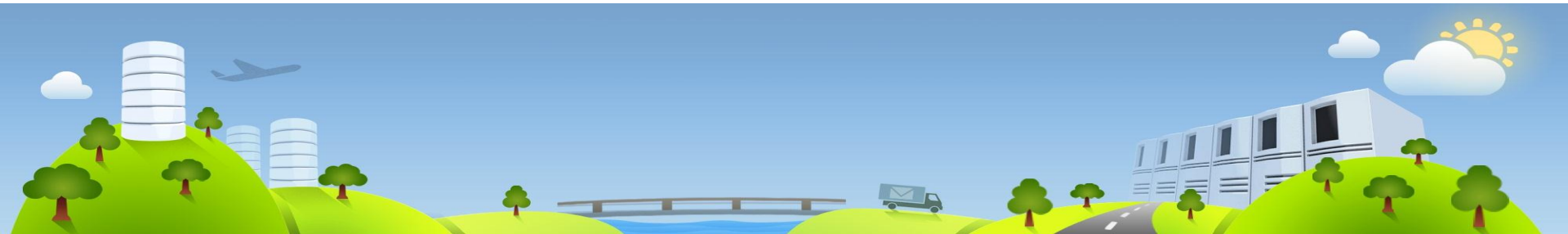
- Regenerar e retransmitir sinais de dados.
- Direcionar os pacotes para que tomem o melhor caminho até o destino.
- Proporcionar segurança para a rede.

Importância dos ativos

Os ativos são equipamentos que precisam ter a garantia de funcionamento aliada à segurança e ao desempenho. É importante que todo administrador de rede tenha conhecimento do que está acontecendo com esses equipamentos em tempo real. Para realizar essa tarefa é imprescindível a utilização de *softwares* de monitoramento em todos os ativos de uma rede.

Softwares de monitoramento consagrados no mercado:

- Nagios
- Cacti
- Zabbix
- MRTG

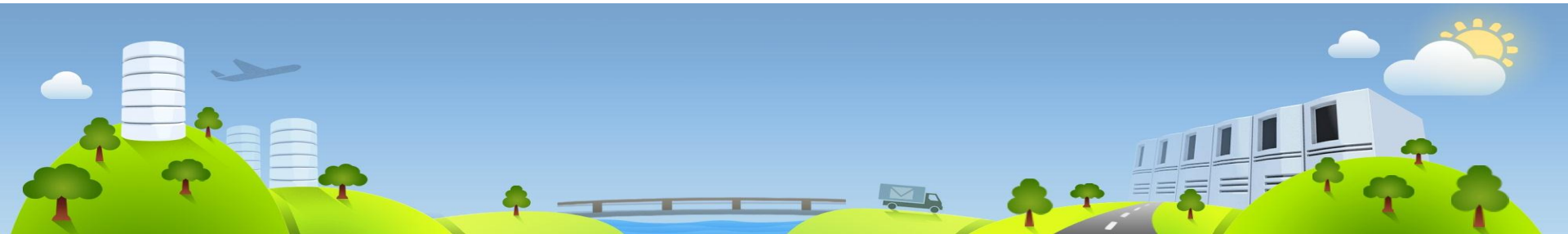


Tipos de ativos

Hoje, com ampliação significativa das redes de computadores, vários ativos de redes foram desenvolvidos para atender as diversas necessidades do mercado. Empresas especializadas em ativos de redes como Cisco, Juniper, HP, Aruba sempre investem em inovações e soluções tecnológicas na área de equipamentos de redes. Com todo esse trabalho por parte dessas empresas, a quantidade de soluções presentes no mercado é altíssima.
Nos próximos *slides* vamos estudar os principais equipamentos que uma rede possui, sendo que sem eles a comunicação entre computadores não se tornaria possível.

Switch

Switch (também chamado de comutador) é um equipamento multiportas utilizado para conectar dispositivos finais(ex.: computador, servidor) em uma rede local. Esse dispositivo trabalha na camada 2 do Modelo OSI, ou seja, ele utiliza o endereçamento MAC para realizar a entrega dos dados para o destinatário.



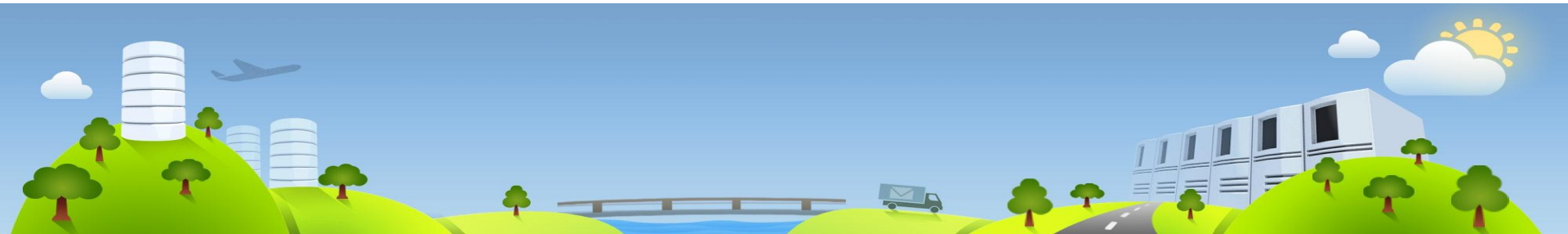
Atualmente existem dois tipos de switchs, os gerenciáveis e não gerenciáveis:

Switchs não gerenciáveis: são equipamentos que não permitem a realização de nenhuma configuração. São equipamentos mais simples indicados para o uso doméstico e em pequenas empresas.

Switch gerenciáveis: são equipamentos que permitem a realização de configurações e ativação de novos recursos. Os recursos suportados dependem do modelo adquirido; alguns recursos que os switchs suportam são: agregação de *link*, PoE (Power over Ethernet), segurança de portas, VLANs, QOS.

Roteador

O roteador é um equipamento que trabalha na camada 3 do modelo OSI e tem a função principal de conectar redes diferentes. Para conseguir alcançar a rede de destino, o roteador utiliza o endereço IP para realizar o encaminhamento desses pacotes até chegar ao seu destino. Esse equipamento suporta vários tipos de tecnologias, como: fibra óptica, ethernet, 3G, seriais e *wirelless*.



Tipos de roteadores

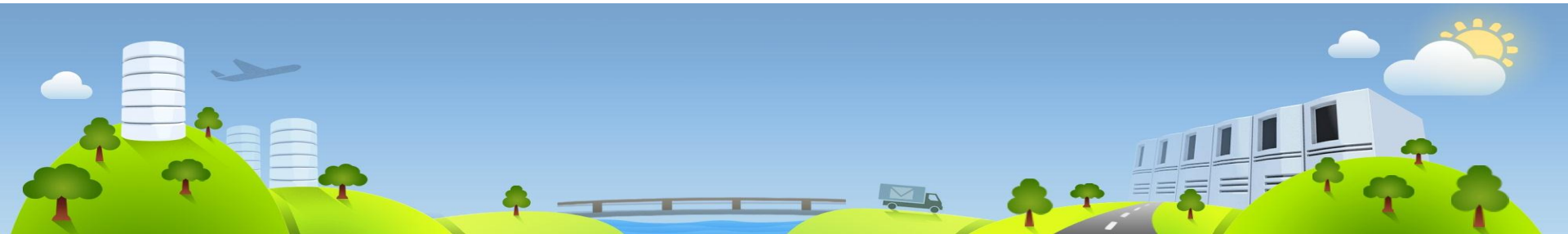
Podemos dividir os roteadores em dois tipos, um para o uso doméstico e outro utilizado em ambientes empresariais.

Roteadores domésticos: possuem uma limitação em relação a recursos suportados, quantidade de memória RAM e processador. Esses dispositivos são desenvolvidos para trabalhar com uma baixa quantidade de pacotes. São ideais para utilizar em um ambiente doméstico ou para pequenos escritórios.

Roteadores empresariais: suportam uma quantidade muito grande de recursos e funcionalidades; são desenvolvidos para trabalhar com uma alta taxa de dados e são ideais para ambientes empresariais. Os roteadores empresariais geralmente suportam: protocolo de roteamento dinâmico, voip, firewall, vpn etc.

HUB

Dispositivo multiporta utilizado para conectar dispositivos finais em uma rede local de computadores. Esse é um equipamento antecessor ao switch, seu uso vem caindo drasticamente principalmente em ambientes empresarias. O desuso do HUB se deve a dois fatores cruciais em uma rede de computadores: baixo desempenho e falta de segurança.
Ainda encontramos muitos hubs nos ambientes domésticos, pois seu preço compensa mais do que a aquisição de um switch. Devemos evitar a utilização de hubs em ambientes empresariais, pelos motivos já citados.



Um fator de extrema importância na escolha dos ativos de redes é a velocidade com que as portas operam. A velocidade é a capacidade máxima de dados que uma determinada interface pode trafegar por segundo. Atualmente as portas ethernet podem trafegar nessas velocidades:

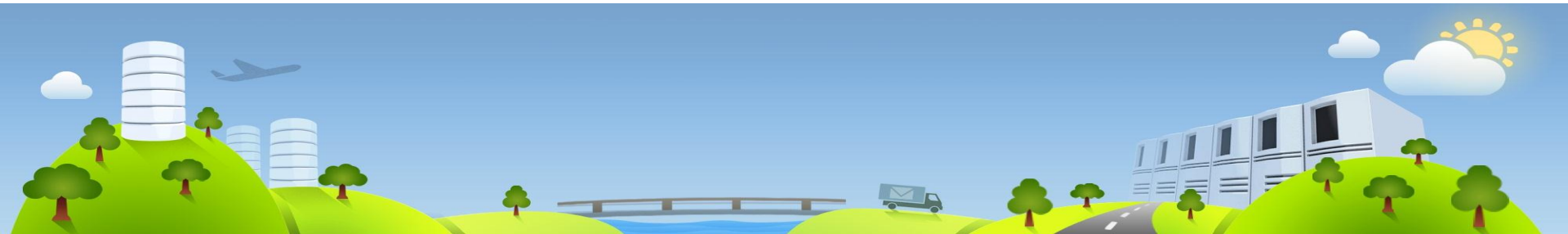
Tipo de porta	Velocidade
Ethernet	10 Mbit/s
Fast Ethernet	100 Mbit/s
Giga Ethernet	1 Gbit/s(1000 Mbit/s)
10 Giga Ethernet	10Gbit/s(10000 Mbit/s)

Um mesmo equipamento pode oferecer diferentes tipos de portas, ou seja um switch pode ter, por exemplo 24 portas Fast Ethernet e mais quatro portas Giga Ethernet.

Conformidade entre ativo e cabeamento

Para utilizar ao máximo a largura de banda disponível em cada interface, uma conformidade entre o cabeamento e interfaces deve existir. Não adianta utilizar uma interface Giga Ethernet com um cabeamento que só suporta 100Mbit/s, pois em vez dos dados estarem trafegando a uma velocidade de 1Gbit/s, eles estarão trafegando a apenas 100 Mbit/s.

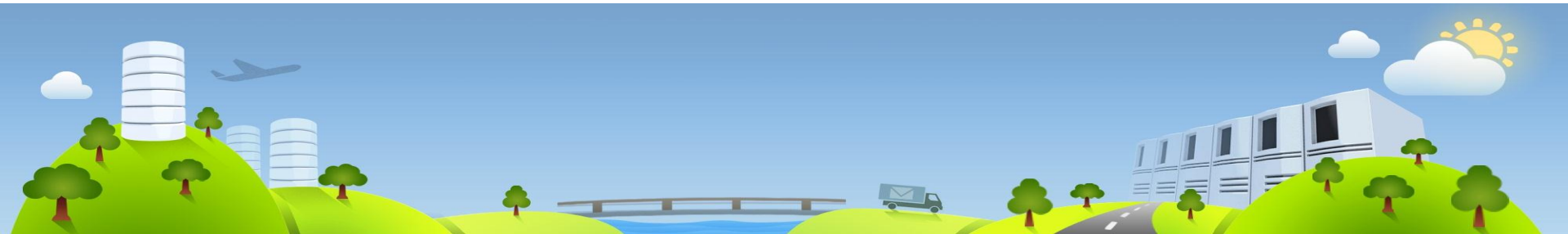
Toda essa situação deve ser analisada antes da aquisição de ativos e cabeamento a fim de evitar gastos desnecessários, pois ativos que oferecem interfaces mais rápidas possuem um custo maior.



Roteador wireless ou Access Point

Tipos de roteadores

Equipamento responsável em fornecer conexão a dispositivos finais através da rede sem-fio(*wireless*). Esse dispositivo trabalha na camada 2 do Modelo OSI, assim como o switch. Quando um dispositivo que possui placa de rede sem-fio se conecta a uma rede *wireless*, ele se associa a um Access Point (AP) e através desse AP o cliente conseguirá obter acesso aos serviços de rede.

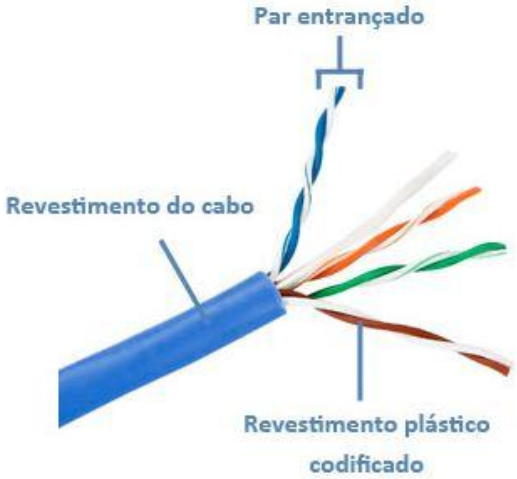


Cabeamento estruturado

Atualmente existe uma grande quantidade de tipos de cabos utilizados para interligação de equipamentos em uma rede computacional. Essa variedade de cabeamento vem para atender as diferentes necessidades, velocidades, alcance e ambiente. Para padronizar toda essa variedade de cabeamento, alguns órgãos como TIA (Telecommunications Industry Association), ISO (International Organization for Standardization), IEEE (Institute of Electrical and Electronics Engineers) e ANSI (American National Standards Institute) cuidam dessa tarefa e de toda parte de inovação, testes e padronização de cabeamentos.

Cabeamento UPT

Cabo de Par Trançado Não Blindado (UTP) consiste em quatro pares de fios coloridos codificados que são trançados juntos e envolvidos em um revestimento de plástico flexível. O trançado dos fios visa cancelar os sinais não desejados(ruídos). Esse efeito de cancelamento também ajudará a evitar interferências de fontes internas chamadas diafonia (linha cruzada).



Categorias

Categoria de cabeamento UTP

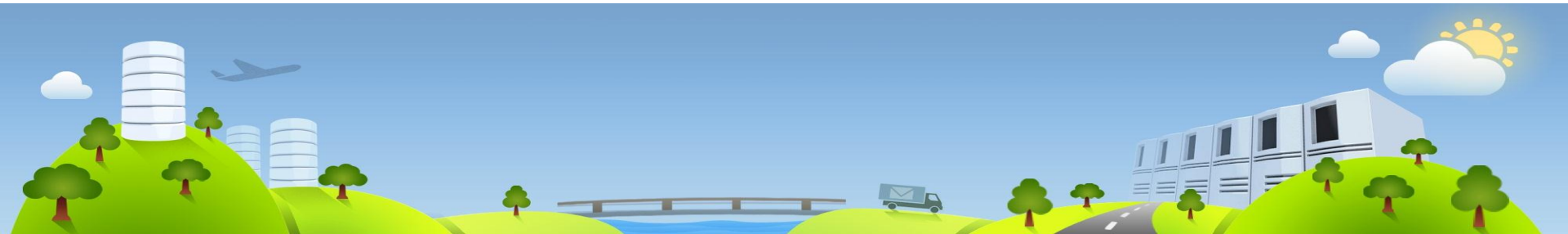
Os cabos UTP são colocados em categorias de acordo com suas características técnicas, por exemplo, a capacidade de transportar taxas mais elevadas de largura de banda.

Categoria 5: características de desempenho para cabeamento e conexões em transmissões de dados e voz na velocidade de até 100Mbps.

Categoria 5e: é uma melhora nas características dos materiais utilizados na categoria 5, que permite um melhor desempenho, sendo especificada até 100Mhz e velocidades de 1Gbps.

Categoria 6a: desempenho especificado até 250Mhz e velocidades de 1Gbps até 10Gbps.

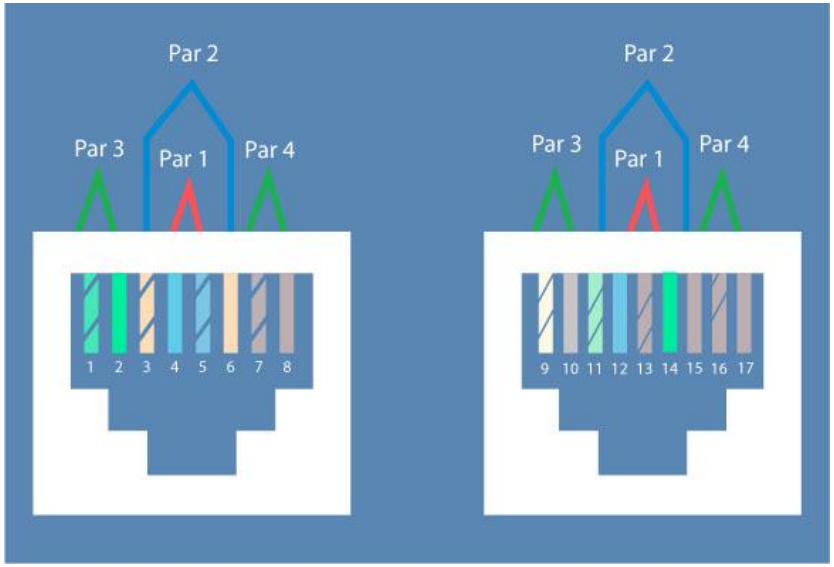
Todas essas categorias suportam uma distância máxima de 100 metros. A partir disso, a rede não opera com o mesmo desempenho, pois ocorre atenuação do sinal. Para resolver esse tipo de situação, um dispositivo intermediário(switch, hub, roteador) pode ser inserido, fazendo com que o mesmo regenere o sinal e acabe com a atenuação. Uma outra solução é a utilização de fibra óptica.

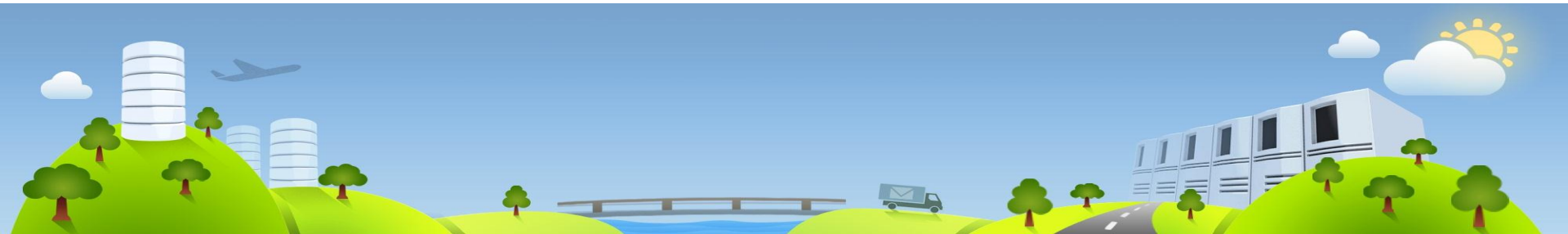


Cabeamento de par trançado blindado(STP), possui uma malha blindada global que proporciona uma maior imunidade às interferências externas eletromagnética e de radiofrequência. Sua blindagem interna que envolve cada par trançado do cabo tem objetivo de reduzir a diafonia. Se a blindagem não for aterrada em uma das extremidades do cabo STP, ela se transformará em uma antena, multiplicando os problemas de interferência.

Cabeamento direto e crossover

Para realizar a conexão entre dispositivos podemos utilizar um cabo UTP ou STP, direto ou *crossover*. Dependendo da sequência que foi utilizada nas extremidades vamos ter um cabo direto ou *crossover*. As extremidades devem estar no padrão TIA 568A ou 568B.



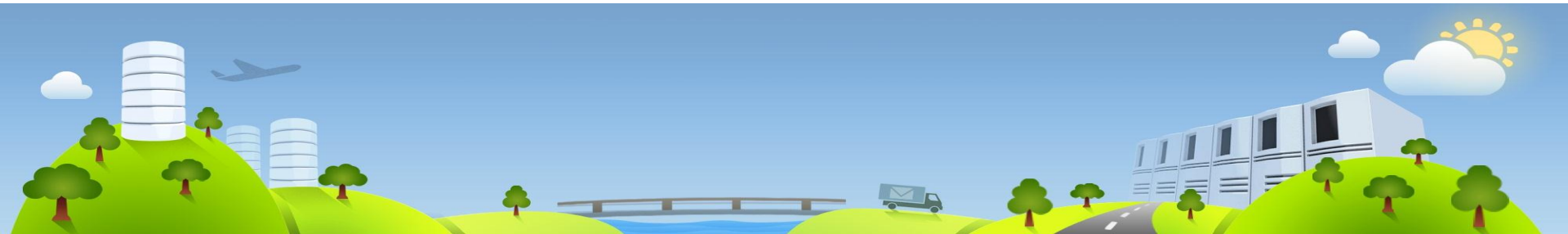


Cabeamento estruturado

Cabeamento direto e crossover

Para determinado tipo de conexão devemos utilizar o cabo correto, direto ou *crossover*. A tabela a seguir mostra em que situações devemos utilizar esses tipos de cabos.

Tipo de Cabo	Padrão	Quando usar
Cabo Direto	Ambas extremidades no padrão T568A ou T568B	Cabo UTP de cobre para conectar dispositivos de rede não semelhantes; Exceto a conexão entre o roteador e computador
Cabo Crossover	Uma extremidade no padrão T568A e a outra T568B	Cabo UTP de cobre para conectar dispositivos similares de rede



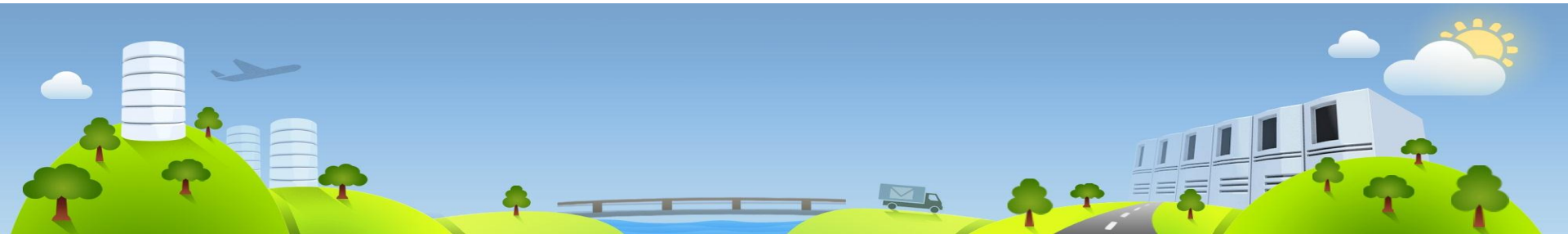
Segurança no cabeamento

O cabeamento de cobre é propenso à interferência de sinal externo e isso prejudica o desempenho do cabo. Sinais externos podem distorcer e corromper os sinais de dados transportados pelo meio físico de cobre. As ondas de rádio e os dispositivos eletromagnéticos, como luzes fluorescentes, motores elétricos e outros dispositivos são fontes de ruído em potencial.

Esse cabeamento ainda sofre riscos de fogo, em que o isolamento e o revestimento dos cabos podem ser inflamáveis ou produzir fumaça tóxica quando aquecidos ou queimados.

- TIA 568: Especificação geral sobre cabeamento estruturado em instalações comerciais.
- TIA 569: Especificações gerais para encaminhamento de cabos (infra-estrutura, canaletas, bandejas, eletrodutos, calhas).
- TIA 570: Especificação geral sobre cabeamento estruturado em instalações residenciais.
- TIA 606: Administração da documentação.
- TIA 607: Especificação de aterramento.

É de suma importância empresas adotarem essas normas, que garantem desempenho e segurança para toda rede de computadores.



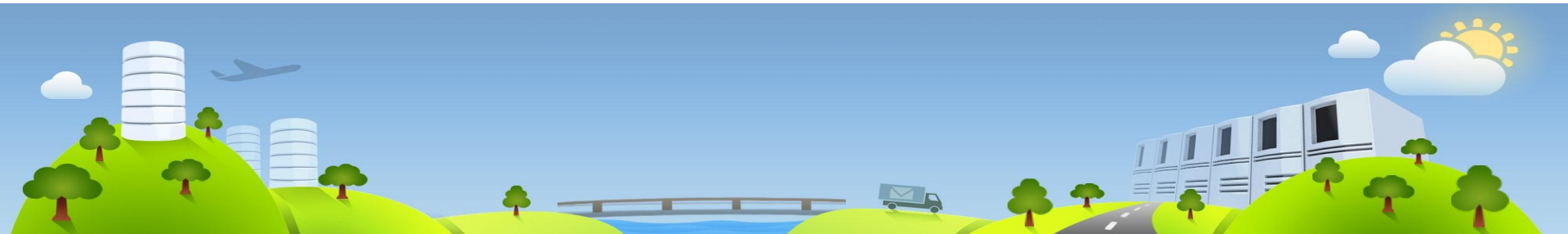
Introdução

Serviços de redes são aplicações existentes em servidores de redes. Esses serviços possuem características distintas dependendo do protocolo que foi escolhido. Por meio dos serviços de redes podemos disponibilizar algum recurso aos usuários da rede, proporcionar segurança, monitorar e automatizar tarefas. A seguir, listagem de protocolos muito utilizada em uma rede computacional.

Serviço	Função
DHCP	Dynamic Host Configuration Protocol: disponibiliza informações sobre a rede para os dispositivos finais.
LDAP	Lightweight Directory Access Protocol: pesquisa dados de usuários em diretórios.
HTTPS	HyperText Transfer Protocol Secure: mesma função do http porém mais seguro, pois criptografa as informações
IMAP	Internet Message Access Protocol, outro protocolo para recebimento de correio eletrônico.

Serviço	Função
HTTP	HyperText Transfer Protocol, usado para navegar em páginas *web*
FTP	File Transfer Protocol: para localizar e capturar arquivos.
Telnet	Terminal de acesso remoto em modo texto
SSH	Secure Shell Terminal: terminal de acesso remoto, porém com mais segurança, pois criptografa os dados.
VNC	Acesso remoto por interface gráfica

Serviço	Função
NFS	Network File System: compartilha arquivos em redes UNIX.
SMB	Server Message Block: compartilha arquivos e impressoras.
IPP	Internet Printing Protocol: serve para acessar impressoras.
SMTP	Simple Mail Transfer Protocol: para envio de correio eletrônico.
POP3	Post Office Protocol v3: para recebimento de correio eletrônico.
DNS	Domain Name System: converte nome em endereços endereços IP e vice-versa.



Serviços

HTTP e HTTPS

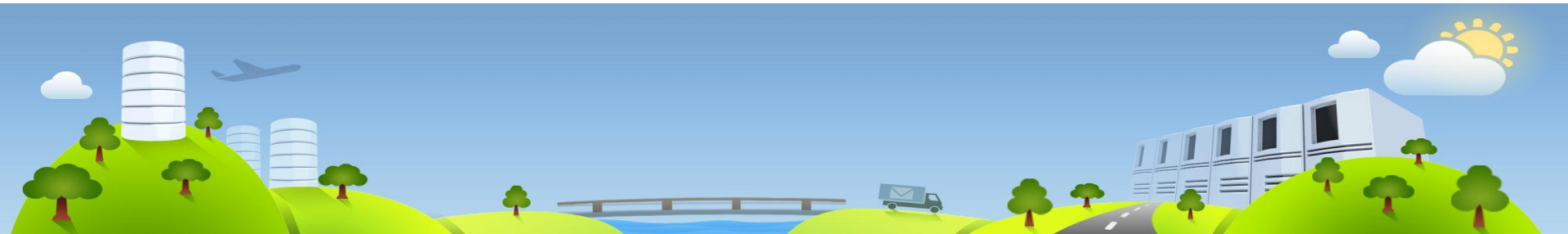
HTTP é uma sigla que está presente sempre que precisamos acessar determinado *site*. É através desse serviço que conseguimos navegar em páginas *web*. O HTTP utiliza texto claro para trafegar seus dados, isso acaba gerando um problema de segurança, pois caso algum invasor intercepte essa comunicação, todos os dados serão visíveis e compreensíveis.

HTTPS mantém a mesma funcionalidade do HTTP, porém criptografa todas as informações trocadas. A criptografia resolve o problema de segurança do HTTP, caso o invasor intercepte os dados, eles vão estar
incompreensíveis, pois estão todos embaralhados. Outra vantagem na utilização desse protocolo é a garantia de você estar acessando realmente um *site* legítimo, não um*site* falso. Essa garantia é fornecida com a utilização do certificado digital, em que a empresa certificadora garante a autenticidade do *site*.

Telnet e SSH

Telnet é um protocolo utilizado para acessar máquinas de forma remota. Através do Telnet é possível realizar manutenções em qualquer máquina da rede a partir de qualquer dispositivo que aceite esse serviço. O acesso remoto traz a vantagem de não precisar se deslocar fisicamente para realizar o
acesso a qualquer dispositivo. O telnet utiliza texto claro na transmissão de dados e isso prejudica bastante a segurança.

SSH possui a mesma finalidade que o Telnet, mas com a vantagem de criptografar todas as informações. É recomendado sempre que possível utilizar o SSH ao invés do Telnet.



FTP e SMB

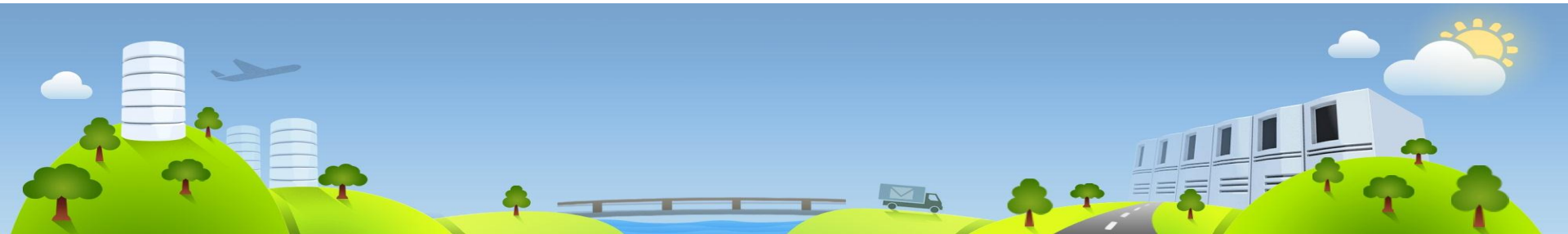
FTP é um dos protocolos mais antigos e utilizados para a transferência de arquivos. A transferência de arquivos acontece entre um dispositivo cliente (dispositivo que solicita a conexão) e um servidor (dispositivo que recebe a solicitação). Através de um cliente , o usuário consegue realizar *download* e *uploads* para o servidor. O FTP é muito utilizado em páginas WEB para disponibilizar *download* de arquivos.

O SMB, assim como o FTP, tem como função principal o compartilhamento de arquivos, com o passar dos anos esse protocolo foi evoluindo e atualmente é possível compartilhar
impressoras, definir níveis de acesso e autenticações. O SMB é uma das formas mais utilizadas quando é preciso compartilhar arquivos entre equipamentos que possuem diferentes sistemas operacionais, por exemplo compartilhar arquivos entre máquinas Linux com dispositivos Windows.

DNS e DHCP

DNS é, talvez, um dos protocolos mais importantes e utilizados na Internet. O papel principal do DNS é a tradução de nomes em endereços IP, sem esse protocolo não conseguiríamos acessar um *site* pelo nome, exemplo: www.sc.senai.br/. Sem ele teríamos que saber o endereço IP de cada *site* para conseguir acessar, um processo totalmente inviável atualmente.

DHCP é um protocolo utilizado para disponibilizar a configuração da rede para os computadores que solicitam esse tipo de informação. Se um dispositivo estiver configurado para utilizar DHCP, ele iniciará uma procura por um servidor DHCP em toda rede, esse servidor DHCP disponibilizará informações de endereço IP, mascara, *gateway*padrão, DNS entre outras configuradas para o cliente que solicitou.



SMTP e POP3

SMTP é protocolo padrão utilizado para o envio de *e-mail* por meio da Internet. Após o cliente ter montado o *e-mail* e inserido o destinatário, o protocolo SMTP entra em ação levando a mensagem até o servidor de destino. O SMTP é um protocolo antigo e considerado relativamente simples. Como o SMTP só realiza o envio de mensagem, um outro protocolo é necessário para realizar a entrega ao destinatário.

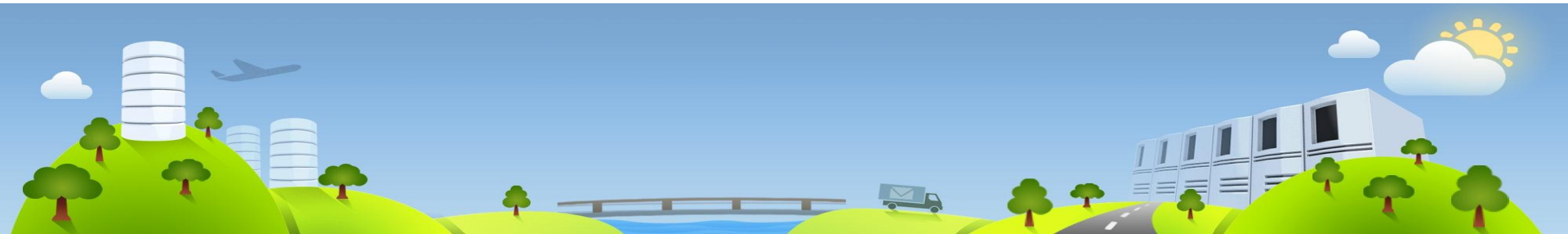
O POP que está atualmente na sua versão 3 é responsável pela entrega dos *e-mails*. Esse protocolo permite que as mensagens localizadas na caixa do correio eletrônico possam ser baixadas para a máquina local.

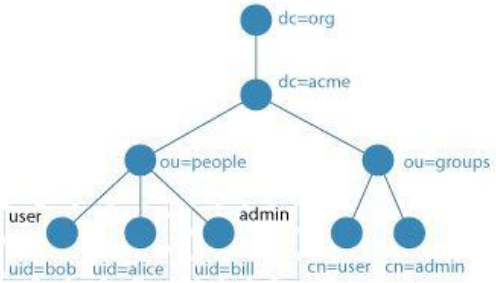
O envio efetivo do *e-mail* se dá através da utilização desses dois protocolos: SMTP e POP. O IMAP (Internet Message Access Protocol) é um protocolo com características semelhantes ao POP, porém com algumas funcionalidades extras e pode ser utilizado como substituto do POP3, desde que o servidor suporte esse protocolo.

LDAP

LDAP é um protocolo utilizado para a pesquisa em diretórios. Diretório, nesse caso, é um banco de dados utilizado para a realização de consultas, principalmente consultas de autenticação. Com a implantação do LDAP, a empresa tem o benefício de uma autenticação centralizada, em que clientes podem utilizar o mesmo *login* e senha para
acessar diferentes tipos de sistema. Isso traz uma comodidade muito interessante a todos os usuários, pois não é preciso várias credenciais para acessar diferentes sistemas.

Os diretórios do LDAP seguem uma hierarquia formando uma árvore, a imagem a seguir ilustra essa estrutura.

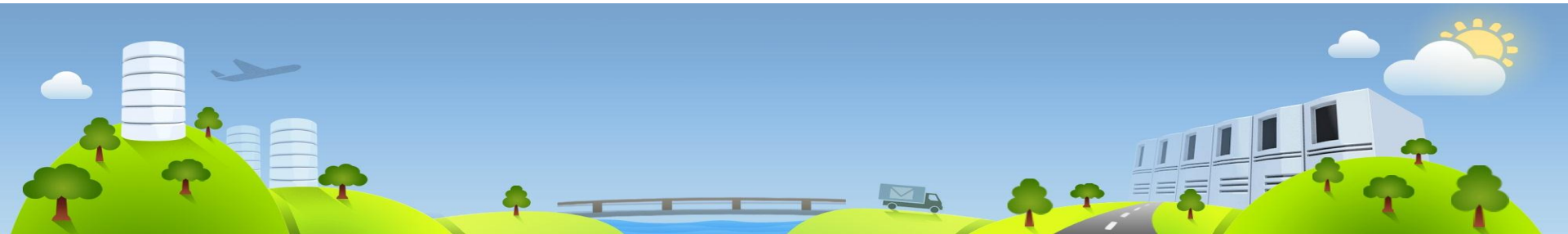




Características dos serviços

A seguir portas utilizadas na camada de transporte dos protocolos abordados neste capítulo.

Protocolo	Porta da camada de transporte
HTTP	80 TCP
HTTPS	443 TCP
Telnet	23 TCP
SSH	22 TCP
FTP	20 e 21 TCP
SMB	445 UDP
DNS	53 TCP/UDP
DHCP	67 UDP - servidor / 68 UDP - cliente
SMTP	25 TCP/UDP
POP	110 TCP
IMAP	143 TCP/UDP
LDAP	389 TCP/UDP

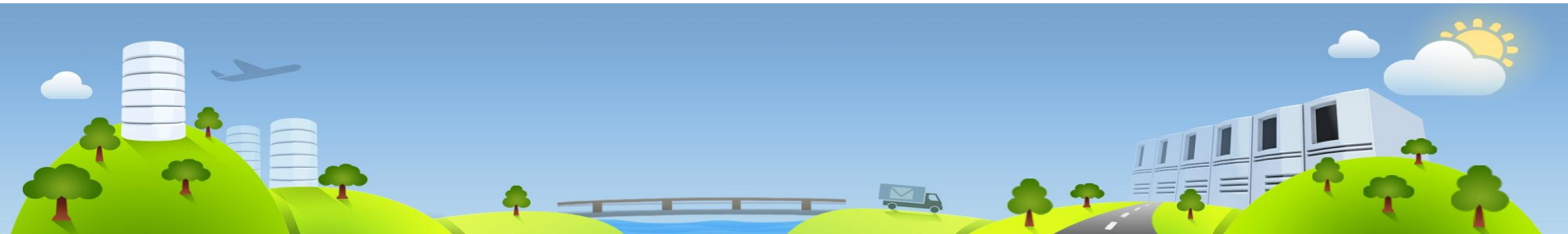


SEGURANÇA

Pilares de Segurança

Atualmente uma empresa contém muitas informações importantes, como dados sigilosos de clientes, informações particulares de colaboradores, documentos internos restritos etc. Perca, roubo ou divulgação dessas informações pode causar um impacto negativo à empresa. Com o conhecimento do valor dessas informações e o risco que elas sofrem hoje, a utilização da segurança da informação que atenda as regras de negócios da empresa é de extrema necessidade.

Em TI a garantia de segurança se dá por meio da garantia de confiabilidade, integridade e disponibilidade da informação. Esses três termos definem os pilares da segurança da informação. Hoje analistas de segurança da informação trabalham para proteger esses pilares e utilizam a união da tecnologia, boas práticas e conscientização para tentar alcançar esse objetivo.



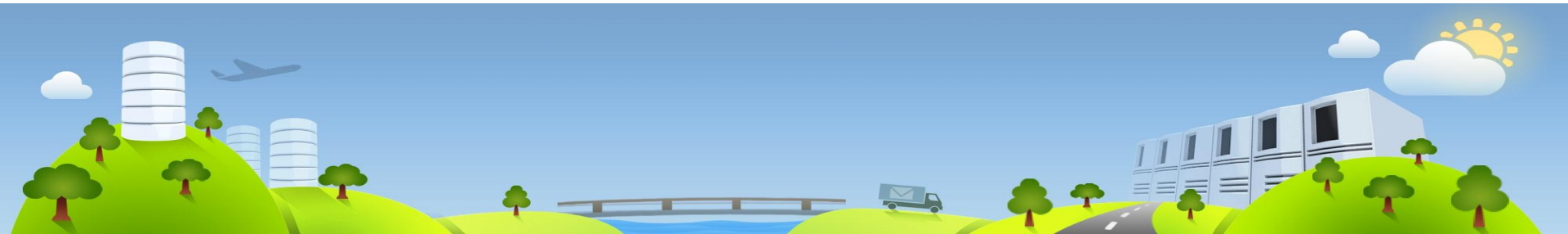
Confidencialidade é uma propriedade que visa disponibilizar uma informação somente a pessoas autorizadas. Para alcançar esse objetivo geralmente a técnica de autenticação é utilizada. Exemplo: caso o indivíduo não tenha a credencial correta(*login* e senha), o mesmo não consegue acessar determinada informação.

Integridade é uma propriedade que visa garantir que determinada informação não seja alterada por pessoas não autorizadas. Para alcançar esse objetivo geralmente a técnica de permissão é utilizada, em que somente pessoas com determinada permissão podem realizar a alteração de uma informação. Exemplo: caso um indivíduo não tenha permissão de escrita em um documento, o mesmo não consegue alterar determinada informação.

A disponibilidade visa garantir que determinada informação sempre estará disponível para que as pessoas com autorização acessem. Para alcançar esse objetivo geralmente a técnica de redundância é utilizada, em que caso algum equipamento passe por problemas o outro assume, fazendo com que o serviço não se torne indisponível. Exemplo: caso um servidor que hospeda determinado *site* tenha problemas, um outro servidor automaticamente assuma o serviço.

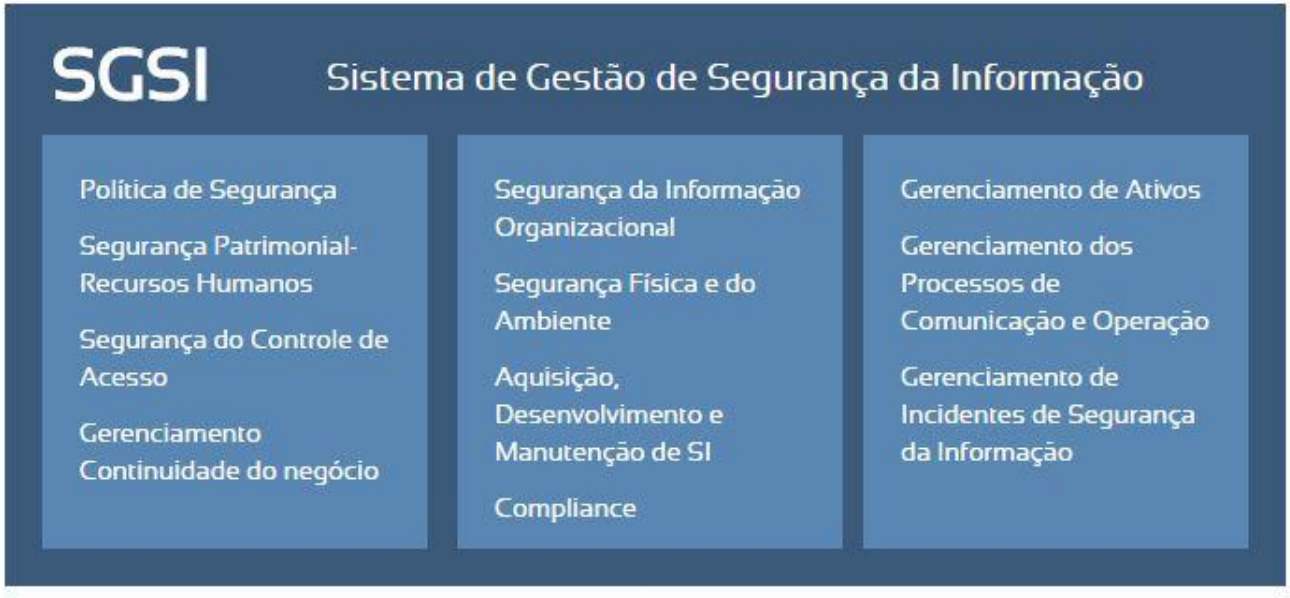
Algumas bibliografias sobre segurança da informação trazem outros pilares que devem ser protegidos afim de garantir a segurança da informação. A seguir, alguns desses pilares:

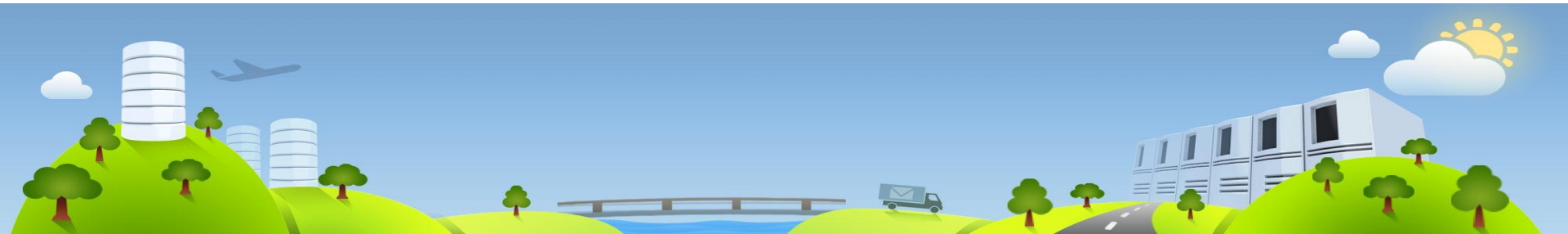
- Autenticidade - Garantia que a informação é autêntica, atesta a origem da mesma.
- Legalidade - Garante a legalidade jurídica da informação.
- Auditoria - Possibilidade de rastrear a informação. Por meio da auditoria é possível identificar participantes, locais e horários.
- Não repúdio - A impossibilidade de negar que determinada informação ou serviço foi criada ou alterada.



A implantação da segurança da informação é uma tarefa complexa em um ambiente empresarial, mas traz muitos benefícios à instituição. Para padronizar as práticas que devem ser adotadas em relação à segurança da informação a ISO 27002 foi desenvolvida. Essa norma engloba requisitos, boas práticas, organização de processos, e ferramentas que devem ser implementadas pela empresa para alcançar uma boa gestão da segurança da informação.

A ISO 27002 é um documento bastante extenso que reune vários temas; a imagem abaixo ilustra alguns assuntos principais abordados por essa norma.





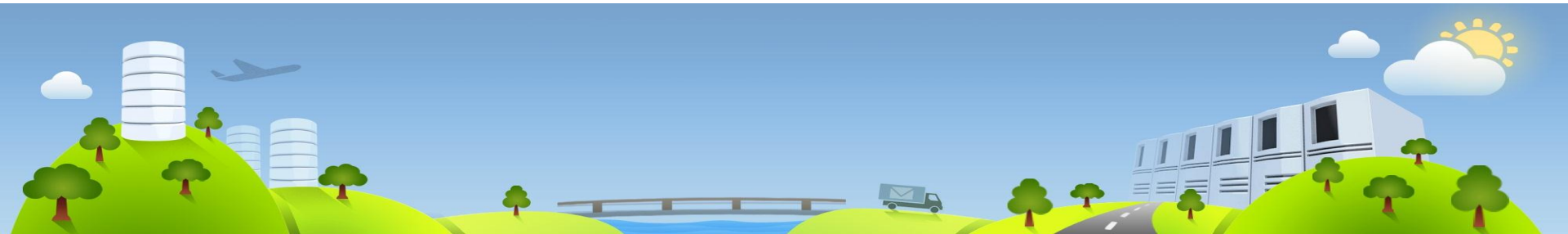
Introdução

Hoje o mercado oferece uma série de soluções voltadas para a segurança da informação. Essas soluções estão cada vez mais robustas e versáteis, conseguindo atender a necessidade de cada empresa. Com certeza as empresas devem realizar um estudo sobre as soluções presentes no mercado e aderir a que mais atenda a sua necessidade, mas confiar nessa solução como única forma de prevenir problemas de segurança é um grande erro.

Elaboração da Senha

Geralmente precisamos de senhas para acessar qualquer tipo de sistema, a elaboração da senha é um passo muito importante para tentar prevenir o acesso indevido a sistemas. A seguir são listadas algumas boas práticas para a elaboração de senhas:

- Mude sua senha frequentemente, no mínimo três vezes por ano.
- Utilize senhas com no mínimo oito caracteres e com a combinação de letras (maiúsculas e minúsculas), caracteres especiais e números.
- Memorize sua senha, não a deixe salva em um arquivo do seu computador, não envie por *e-mail* e nem deixe ela anotada em qualquer local.
- Não compartilhe suas senhas com ninguém.



- Não use senhas simples, como data de nascimento, seu nome ou de familiares, endereço, número de telefone ou qualquer outra informação pessoal.

- Não repita sequências conhecidas como 111, abc, qwert, 123 em qualquer parte da sua senha.

- Não digite sua senha em computadores públicos, pois esses computadores podem estar infectados por algum *spyware* (programa espião) ou *keyloggers* (programa que captura o que é digitado);

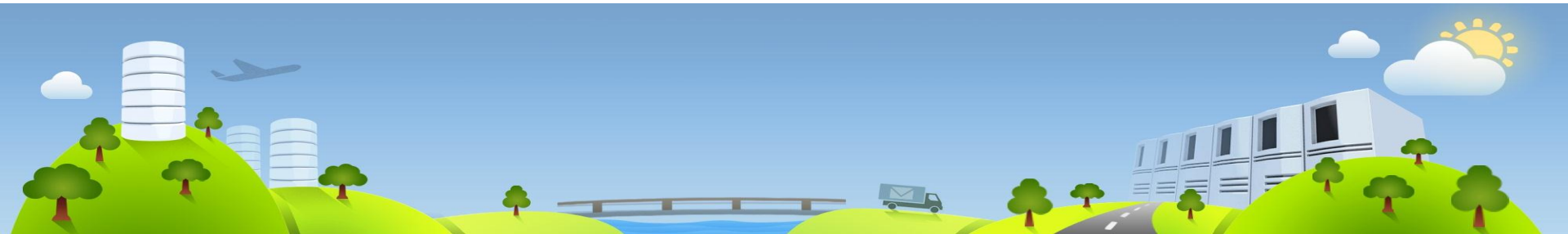
- Não utilize a mesma senha para *sites* diferentes.

Verifique o nível de segurança da sua senha nesse serviço oferecido pela MicroSoft:
https://www.microsoft.com/pt-br/security/pc-security/password-checker.aspx

Acesso a sites e Spam

Esse termo é utilizado para os *e-mails* que recebemos sem que tenhamos solicitado, geralmente esses *e-mails* são enviados para uma grande quantidade de pessoas. A utilização dessa técnica está diretamente ligada a ataques à segurança, sendo um dos métodos preferidos dos invasores para propagar códigos maliciosos, disseminação de golpes e roubo de informações. Para prevenir esse tipo de ataque, as seguintes medidas podem ser adotadas.

- Cuidado quando o campo "assunto" traz textos alarmantes, atraentes ou vagos demais, como: Você ganhou..., Parabéns! Você foi..., Conta em atraso, Comprovante de depósito etc.



- Observe sempre o remetente do *e-mail*,*hackers* costumam tentar enganar as pessoas mudando o endereço, como: @caixa.com ao invés de @caixa.gov.br.

- Não clique em *links* e nem baixe anexos de e-mails enviados por remetentes que você desconhece.

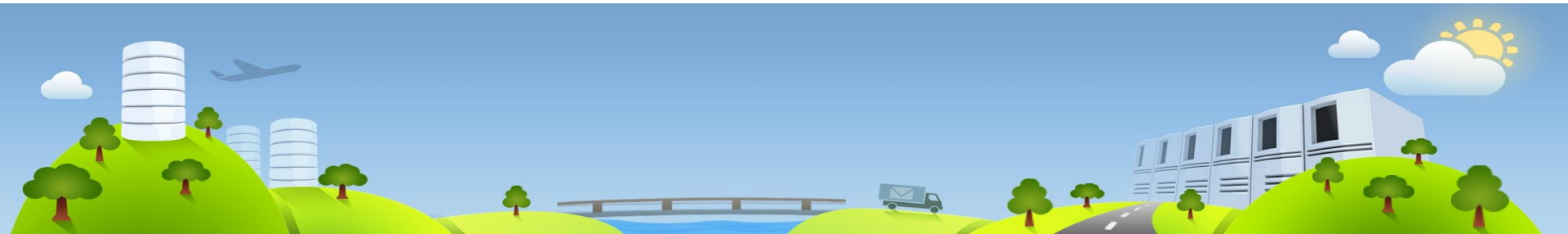
Diariamente acessamos diversos *sites* e às vezes nem percebemos se o endereço que está sendo acessado é um endereço verdadeiro. Invasores utilizam a técnica de*phishing* para realizar a falsificação de *sites*. O *phishing* de *site* é uma cópia fiel de determinado *site*, só que com um endereço inválido. A próxima imagem mostra um exemplo de *phishing*. A maneira de prevenir esse tipo de ataque é sempre observar a URL que está sendo acessada. Através do *phishing* o *site* falsificado pode capturar *login*, senha, informações pessoais e até o número do cartão de crédito.

Técnica phishing: repare que o endereço do site não é o verdadeiro.

Download de Programas

Atualmente existem centenas de *sites* que oferecem o serviço de *downloads* de programas. Alguns desses *sites* são conhecidos e possuem bastante credibilidade, outros já não possuem toda essa confiança. Temos que tomar cuidado ao baixar arquivos de *sites*, pois junto com o arquivo pode vir algum *adwares* (programa usado para capturar informações pessoais) ou até mesmo um vírus que comprometa o funcionamento da máquina. Podemos seguir essas boas práticas para evitar a contaminação do computador.

- Baixe arquivos, apenas de *sites* confiáveis. Quando possível, baixe o programa diretamente do *site* do fabricante.
- Utilize o antivírus antes de realizar a instalação. Caso o antivírus detecte algum problema de segurança, um alerta será emitido.
- Cuidado com programas de compartilhamento de arquivos, como Torrent, Ares, Emule etc. Dependendo da configuração esses programas podem compartilhar arquivos que você não queira publicar, ou até mesmo seu hd inteiro.



Mitigando Ataques

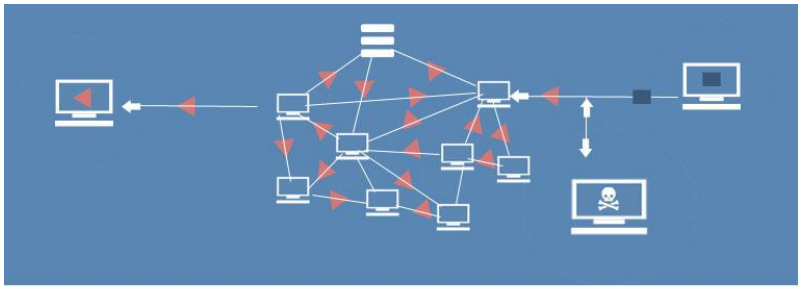
Introdução

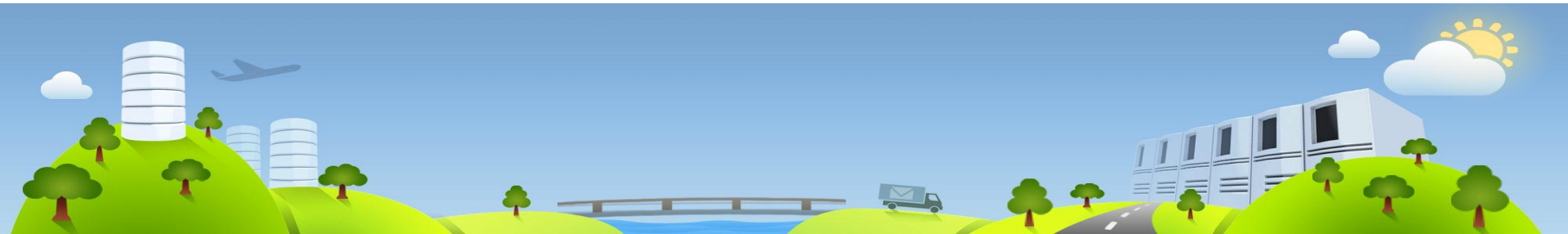
Todo gestor de TI deve ter em mente que não existe uma rede ou servidor 100% seguro, todos eles estão vulneráveis a algum tipo de ataque, mas nem por isso medidas de segurança devem ser deixadas de lado. Mitigar ataques é um conceito muito utilizado na área da segurança da informação, que trata de tentar evitar ao máximo que algum ataque seja bem sucedido.

Nos próximos *slides* vamos estudar algumas formas de prevenir alguns tipos de ataques que comprometem a segurança.

Ataques à confidencialidade e integridade

Uma forma de ter acesso às informações sem a devida permissão é interceptar tudo que passa pela rede, sem que o usuário perceba. Ataques como Man-in-the-Middle-Attack(Ataque Homem no Meio) e DNS poisoning(Envenenamento DNS) utilizam esse conceito para capturar informações sem que o usuário saiba. Dependendo do objetivo do atacante, as informações que chegam até ele podem ser alteradas, prejudicando a integridade das informações.



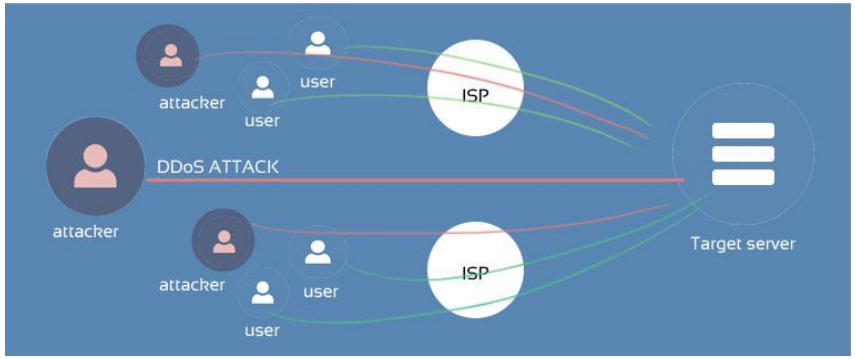


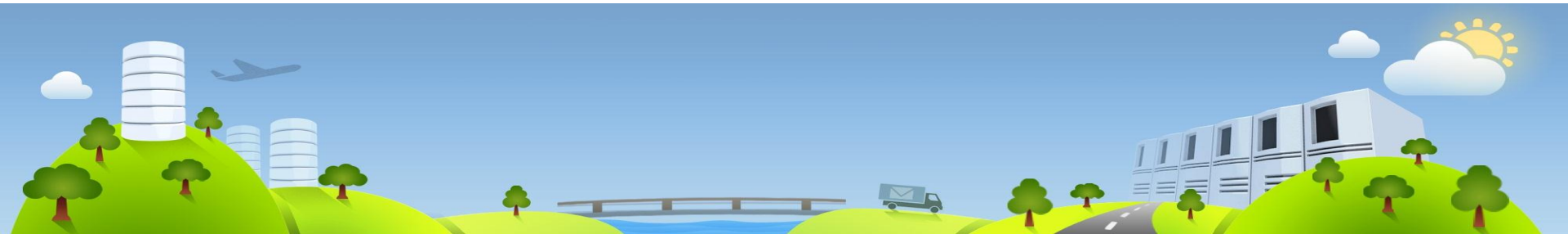
Ataques a Disponibilidade

As seguintes medidas podem ser adotadas para evitar esse tipo de ataque:

- Sempre que possível, acesse *sites* que utilizem o protocolo HTTPS, principalmente quando trat-se de transações financeiras.
- Monitore seu servidor DNS, caso a quantidade de requisições esteja baixa, pode ser um sinal de tentativa de ataque;
- Não utilize hub na sua rede, dê preferência à utilização de switchs;
- Não se conecte em rede Wireless que você não conheça.

Caso um invasor queira deixar algum servidor indisponível ele pode gerar uma sobrecarga no sistema, fazendo com que o servidor fique inoperante devido à alta taxa de requisições. O atacante, por exemplo, pode sobrecarregar a largura de banda e o processamento do servidor, deixando o servidor indisponível para o acesso. Ataques do tipo DOS (Ataque de negação de serviços) e DDOS (Ataque de negação de serviços distribuídos) afetam a disponibilidade do servidor ou de algum serviço específico.





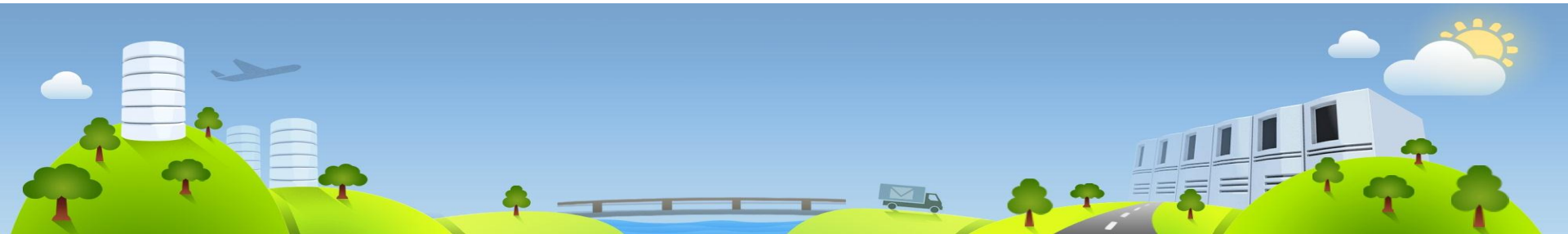
Disponibilização de Serviços

Os ataques DDOS e DOS são os mais temidos e difíceis de prevenir, mas algumas ações podem ser tomadas para dificultar esse ataque:

- Monitore os serviços e pacotes que trafegam pela rede em que o servidor está instalado.
- Quando possível, permita apenas que determinadas faixas de Ips realizem Ping no servidor.
- Utilize ferramentas IDS(Sistema de Identificação de Intrusos) e IPS (Sistemas de Prevenção de Intrusões) para analisar ações incomuns na rede e no servidor.
- Conheça o serviço que você está instalando e disponibilizando para os clientes e verifique se o mesmo não possui atualizações ou configurações extras para evitar esse tipo de ataque.

Hoje um mesmo servidor pode ser utilizado para disponibilizar vários serviços simultaneamente, como FTP, HTTP, HTTPS, DHCP etc. Uma boa forma de mitigar ataques é deixar somente ativos os serviços que realmente vão ser utilizados. Quando um serviço é instalado ele abre uma porta no sistema operacional, essa porta pode ser utilizada como fonte de entrada para o atacante. Podemos fazer uma analogia de um servidor com uma casa domiciliar, onde quanto mais portas uma casa tiver, mais chances de encontrar alguma vulnerabilidade ela terá.

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-03-24 09:25 BRT
Nmap scan report for gmail.com (173.194.118.85)
Host is up (0.0014s latency).
Other addresses for gmail.com (not scanned): 173.194.118.86
rDNS record for 173.194.118.85: gru09s09-in-f21.1e100.net
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
2222/tcp open  EtherNet/IP-1
```

GOVERNANÇA

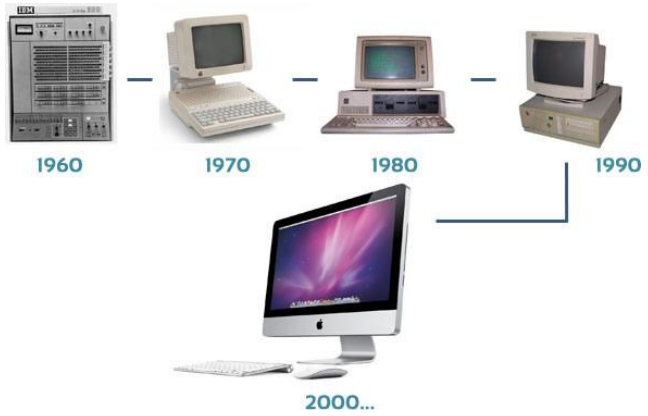
Boas Práticas de Governança

Introdução

Durante vários anos a TI foi considerada uma área responsável apenas por deixar os computadores e serviços tecnológicos funcionando. Em muitas empresas o setor de informática era considerada uma área que gerava gastos à instituição. Esse tratamento com a TI fez com que ela fosse considerada uma área sem muita influência aos negócios da empresa.

Com o passar dos anos, gestores perceberam a importância da TI para os negócios e surgiu a necessidade de dar mais atenção a esse setor. A partir dessa necessidade, metodologias foram desenvolvidas a fim de criar uma padronização na utilização da tecnologia da informação dentro da instituição.

Atualmente Cobit e ITIL são ferramentas essenciais que auxiliam os gestores no controle da tecnologia da informação dentro da empresa.



Cobit

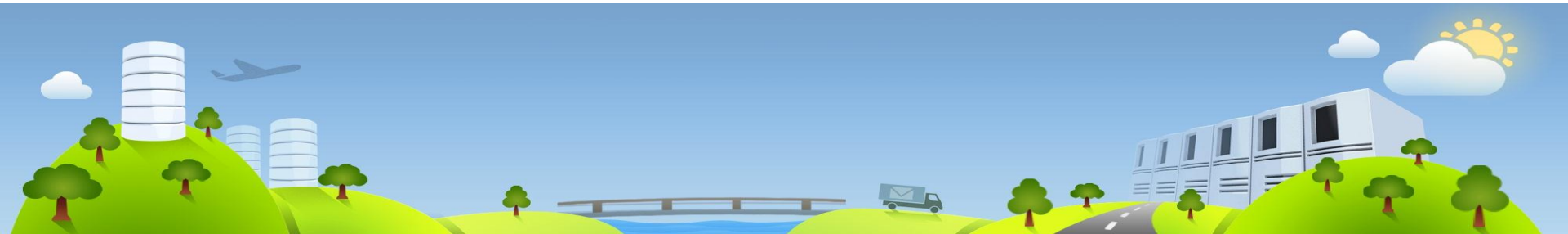
O Cobit é um *framework* de muito sucesso na área de gestão de TI e, em 2012, sofreu mais uma atualização indo agora para sua versão 5. O Cobit 5 é o *framework* da ISACA (isaca.org) que auxilia a GRC (Governança, Riscos e Compliance) e tem a proposta de alinhar a TI com as regras de negócio da Instituição.

A utilização do Cobit 5 auxilia a empresa a criar valor para TI, equilibrando o investimento em recursos e os riscos organizacionais. O Cobit 5 atende as áreas funcionais de TI, os negócios da empresa e as partes interessadas. Empresas de todos os tamanhos, privadas ou públicas, podem utilizar o Cobit como *framework* para governança de TI.

Para garantir todas essas funcionalidades, esse novo *framework* se baseia em cinco princípios.

- Reunir as necessidades dos *stakeholders* (parte interessada, ex.: gestores, gerentes, proprietários, fornecedores).
- Cobrir a empresa fim-a-fim.
- Aplicar um *framework* único e integrado.
- Aplicar uma abordagem holística.
- Separar a governança da gestão.

Através desses princípios o Cobit 5 consegue gerar vários benefícios à empresa, como:

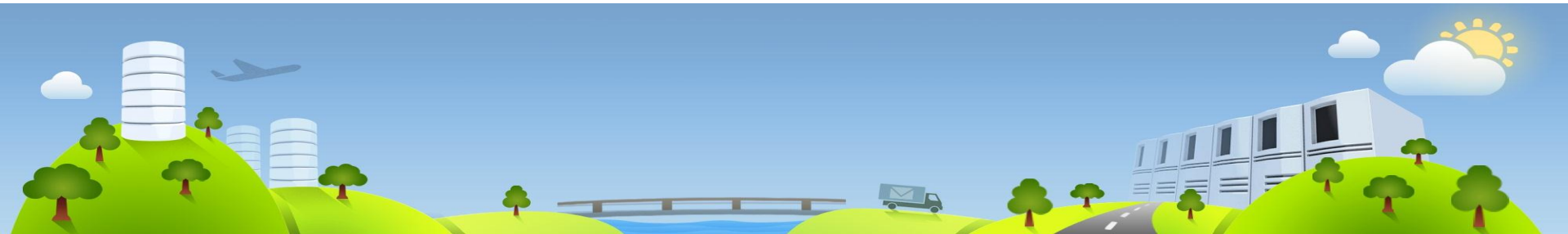


- manter informações de alta qualidade para apoiar decisões de negócios;
- alcançar objetivos estratégicos e benefícios por meio da utilização eficaz e inovadora de TI;
- alcançar a excelência operacional por meio da aplicação confiável e eficiente da tecnologia;
- manter riscos relacionados à TI a um nível aceitável;
- otimizar o custo dos serviços de TI e de tecnologia;
- suporte à conformidade com leis, regulamentos, acordos contratuais e políticas.

Por meio dessa nova abordagem, a versão 5 do Cobit busca aproximar ainda mais a TI do negócio. Com o alinhamento da TI com as áreas estratégicas da empresa, os investimentos em relação aos recursos tecnológicos se tornam mais eficientes e conseguem trazer um retorno positivo para a empresa.

ITIL

O ITIL(Information Technology Infrastructure Library, Biblioteca de Infraestrutura de TI) é um*framework* que engloba as melhores práticas para a gestão da Tecnologia da Informação. Atualmente o ITIL está na sua terceira versão e foi criado pelo governo britânico. As práticas que o ITIL une são testadas e comprovadas na prática e são resultados de anos de observações e estudos.



O ITIL sugere que a área de TI seja vista como uma prestadora de serviços e que esses serviços tenham um ciclo de vida. Utilizando esse ciclo de vida é possível mensurar e gerenciar o valor que estes serviços podem agregar ao negócio da empresa.

A utilização do ITIL dentro da empresa consegue trazer vantagens para a instituição. A própria literatura do ITIL organiza seus benefícios em quatro categorias:

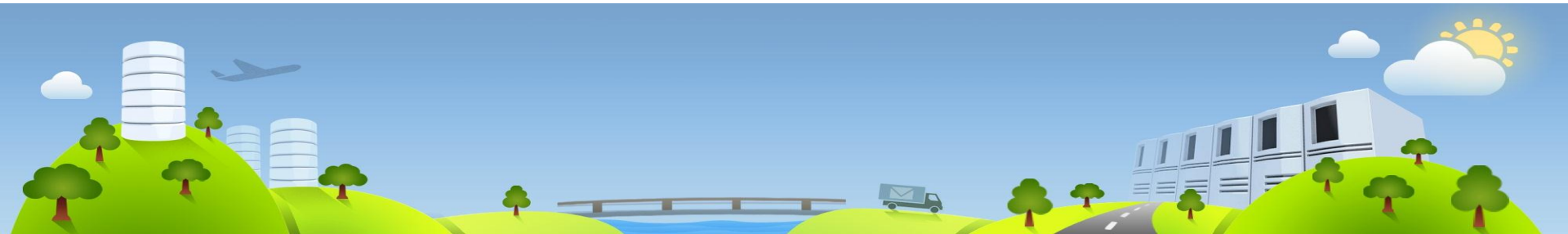
Benefício para o negócio

O negócio da empresa se torna mais estável se houver um acordo de níveis de serviço (SLA) segmentado por cliente, serviço, setor etc. Nesse contrato SLA, é estipulado tempo para resolução de problemas, atendimento ao cliente, tempo mínimo de funcionamento da estrutura de TI.

Com o monitoramento dos níveis de serviços é possível analisar se as metas foram alcançadas e se existe sustentabilidade no negócio.

Benefício para inovação

Cada serviço está em constante avaliação, o que abre a oportunidade para a realização de melhorias na estrutura implantada.
O ITIL aborda o gerenciamento de mudança em que é realizado um ciclo de atividades que pode acarretar uma revisão. O processo de revisão garante que a gestão passe por inovações a fim de melhorar cada vez mais os processos.



Benefício financeiro

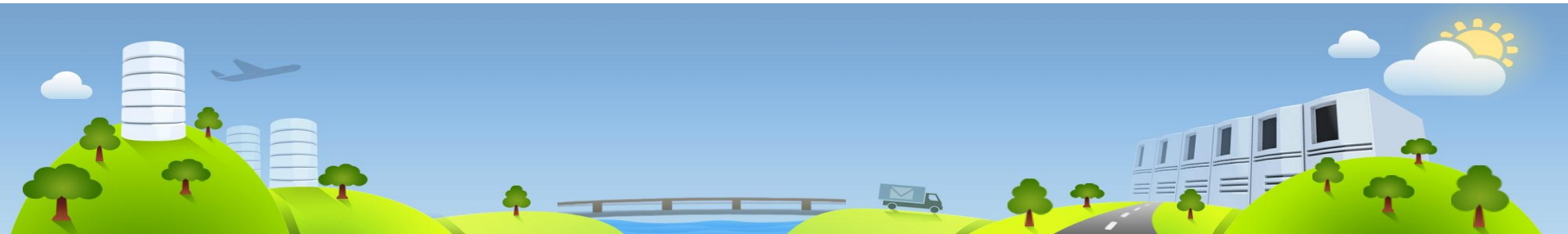
Por meio do gerenciamento de problemas, menos incidentes ocorrem e, consequentemente, o tempo de serviço parado é menor e isso reflete uma maior produtividade.

Com o gerenciamento de continuidade, a empresa planeja quanto tempo a estrutura de retorno entra em ação após uma parada, fazendo com que os serviços não fiquem indisponíveis.

Benefício para funcionários

Os funcionários ficam motivados quando percebem que a estrutura proposta funciona bem e auxilia o seu trabalho.

O ITIL tem como premissa a transparência nos processos, deixando o colaborador satisfeito, pois o mesmo compreende o método que é utilizado pela empresa.



REVISÃO

Sistema Operacional

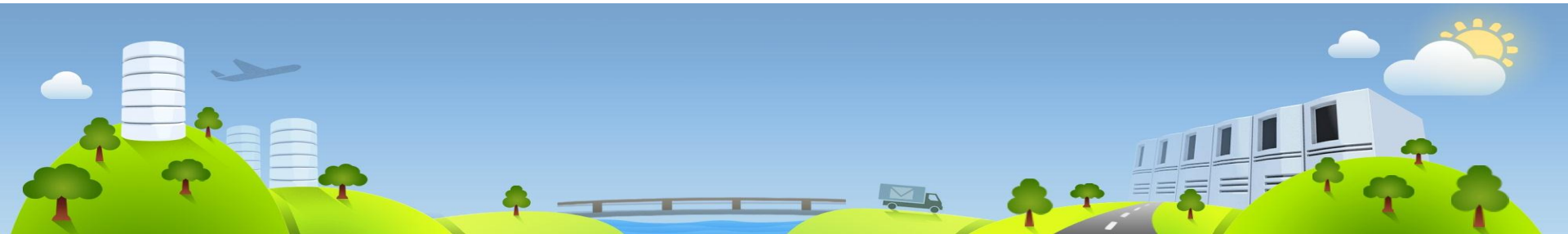
O Sistema Operacional(SO) é um *software*, geralmente um conjunto de *softwares*, que gerencia todos os recursos presentes em um computador. O SO tem algumas tarefas complexas, como:

- Gerenciar processos;
- Gerenciar memória;
- Gerenciar recursos;
- Gerenciar hardware;

Um papel de extrema importância que o SO realiza é fazer a interação com o *hardware*. Para realizar essa interação o SO utiliza um *driver* para conseguir identificar e gerenciar os *hardwares* instalados no computador. Há situações em que o próprio SO já tem o driver necessário, fazendo com que o usuário não precise instalar nada extra para que o *hardware* funcione.

Um profissional de TI tem que ter o conhecimento de qual sistema operacional utilizar em determinada situação. A escolha do sistema operacional deve partir da necessidade que ele deve satisfazer.

Após o levantamento das funcionalidades e compatibilidades que SO tem, devemos realizar o levantamento de quais sistemas atendem essa demanda atualmente.



Softwares e seu licenciamento

Podemos definir como *software* toda parte lógica de um computador. Através do *software* conseguimos realizar nossas tarefas como editar um texto, escutar música, navegar na Internet etc. O *software* é desenvolvido utilizando uma linguagem de programação, atualmente existem centenas de linguagens que são utilizadas para finalidades específicas. Algumas linguagens utilizadas no mercado são Java, PHP, Visual Basic, ASP, Phyton, Perl etc.

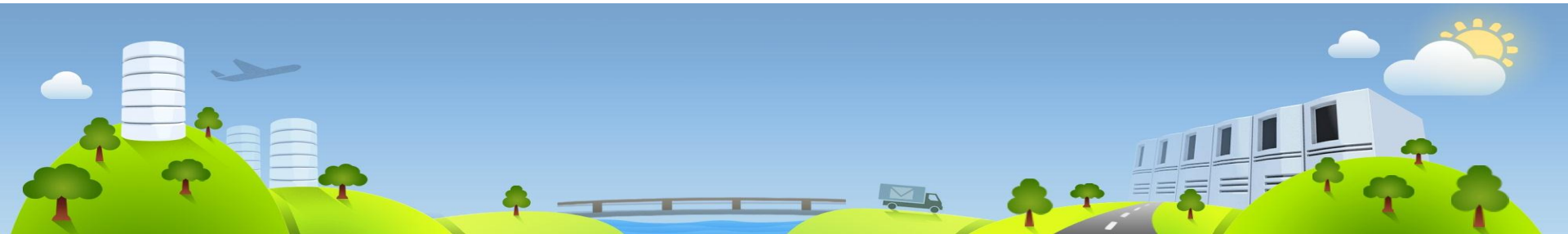
Quando um *software* é desenvolvido ele deve atender um tipo de licenciamento. Atualmente os seguintes tipos de *softwares* são os mais encontrados no mercado:

- *Software* Livre
- *Software* Proprietário
- *Software* Comercial
- *Software* Gratuito

Antes de instalar um software é preciso saber qual licença ele utiliza. A instalação de *softwares* comerciais ou proprietários, sem a devida aquisição ou autorização da empresa desenvolvedora, encaixa-se em um crime de pirataria.

Hardware

No mundo da informática *hardware* é definido como qualquer equipamento que pode exercer alguma função computacional específica. De forma resumida *hardware* é toda parte física de um computador, notebook, celular, *tablet* entre outros. O computador é um conjunto de *hardware*, em que cada peça realiza uma função específica.



Todas as peças de um computador devem estar funcionando perfeitamente para que o mesmo consiga realizar suas atividades. Mesmo determinados *hardwares* possuindo funções mais complexas que outros, eles não conseguem trabalhar sozinhos. É muito importante realizar manutenções periódicas em todos os componentes, evitando que o PC (Computador Pessoal) não venha a falhar e comprometer o serviço.

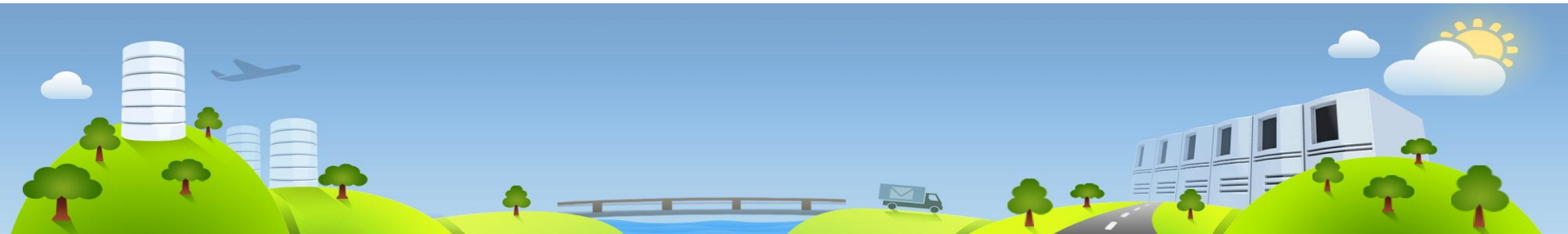
Ativos de Rede

Ativos de redes são considerados os principais equipamentos dentro de uma infraestrutura de TI. Através desses equipamentos conseguimos ter conectividade com outros dispositivos em uma rede. Os ativos de redes também possuem as seguintes funcionalidades:

- regenerar e retransmitir sinais de dados;
- direcionar os pacotes para que tomem o melhor caminho até o destino;
- proporcionar segurança para a rede.

Principais ativos de redes atualmente:

- Switch
- Roteador
- HUB
- Access Point



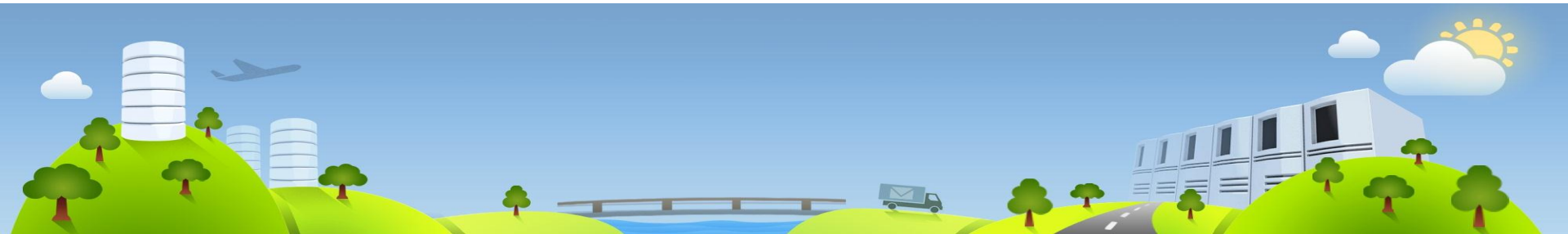
Cabeamento Estruturado

Atualmente existe uma grande quantidade de tipos de cabos utilizados para interligação de equipamentos em uma rede computacional. Essa variedade de cabeamento vem para atender as diferentes necessidades, velocidades, alcance e ambiente.
Os seguintes cabeamentos são utilizados para a realização de conexão em uma rede de dados:

- Cabeamento UTP (direto e*crossover*);
- Cabeamento STP.

O órgão TIA fornece uma série de normas que padronizam todo cabeamento estruturado de uma empresa, ambiente comercial ou doméstico. A seguir, algumas normas e o que elas especificam.

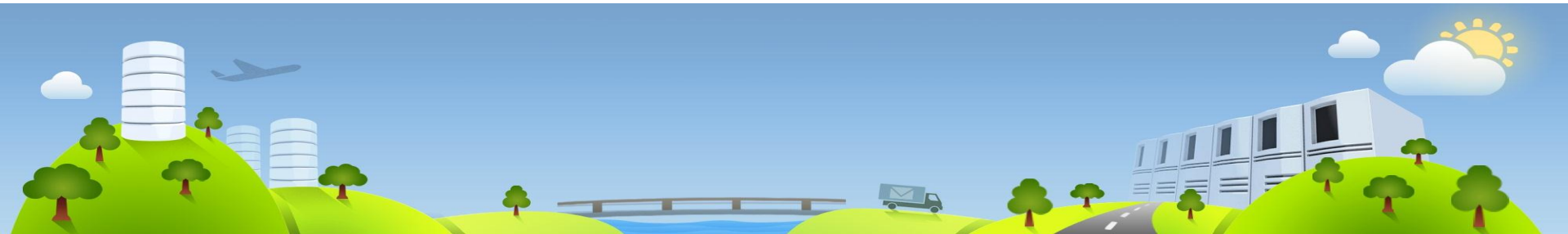
- TIA 568: Especificação geral sobre cabeamento estruturado em instalações comerciais.
- TIA 569: Especificações gerais para encaminhamento de cabos (infra-estrutura, canaletas, bandejas, eletrodutos, calhas).
- TIA 570: Especificação geral sobre cabeamento estruturado em instalações residenciais.
- TIA 606: Administração da documentação.
- TIA 607: Especificação de aterramento.



Pilares da Segurança

Atualmente uma empresa contém muitas informações importantes, como dados sigilosos de clientes, informações particulares de colaboradores, documentos internos restritos etc. Perca, roubo ou divulgação dessas informações podem causar um impacto negativo à empresa. Em TI a garantia de segurança se dá através da garantia de confiabilidade, integridade e disponibilidade da informação. Esses três termos definem os pilares da segurança da informação.

A implantação da segurança da informação é uma tarefa complexa em um ambiente empresarial, mas traz muitos benefícios à instituição. Para padronizar as práticas que devem ser adotadas em relação à segurança da informação, a ISO 27002 foi desenvolvida. Essa norma engloba requisitos, boas práticas, organização de processos e ferramentas que devem ser implementadas pela empresa para alcançar uma boa gestão da segurança da informação.



Boas Práticas em Segurança

Hoje o mercado oferece uma série de soluções voltadas para a segurança da informação. Essas soluções estão cada vez mais robustas e versáteis, conseguindo atender a necessidade de cada empresa. Com certeza as empresas devem realizar um estudo sobre as soluções presentes no mercado e aderir a que mais atenda a sua necessidade, mas confiar nessa solução como única forma de prevenir problemas de segurança é um grande erro.

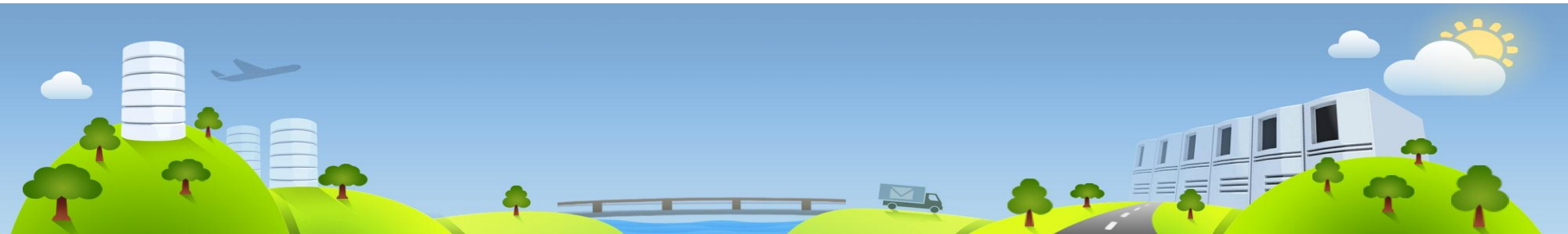
Todo gestor de TI deve ter em mente que não existe uma rede ou um servidor 100% seguro, todos eles estão vulneráveis a algum tipo de ataque, mas nem por isso medidas de segurança devem ser deixadas de lado. Mitigar ataques é um conceito muito utilizado na área da segurança da informação, que trata de tentar evitar ao máximo que algum ataque seja bem sucedido.

Boas Práticas em Governança TI

Durante vários anos a TI foi considerada uma área responsável apenas por deixar os computadores e serviços tecnológicos funcionando. Com o passar dos anos, gestores perceberam a importância da TI para os negócios e surgiu a necessidade de dar mais atenção a esse setor. A partir dessa necessidade, metodologias foram desenvolvidas a fim de criar uma padronização na utilização da tecnologia da informação dentro da instituição.

Atualmente Cobit e ITIL são ferramentas essenciais que auxiliam os gestores no controle da tecnologia da informação dentro da empresa.

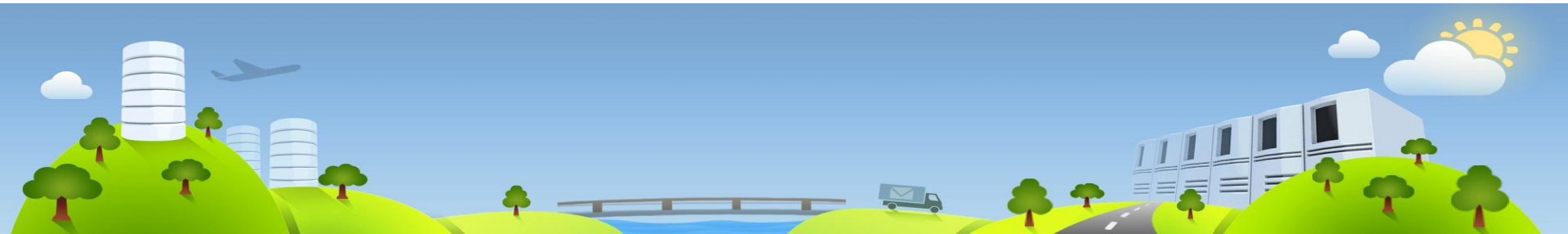
A utilização do Cobit 5 auxilia a empresa a criar valor para TI, equilibrando o investimento em recursos e os riscos organizacionais.



O Cobit 5 atende as áreas funcionais de TI, os negócios da empresa e as partes interessadas. Empresas de todos os tamanhos, privadas ou públicas, podem utilizar o Cobit como *framework* para governança de TI.

Atualmente o ITIL está na sua terceira versão e foi criado pelo governo britânico. As práticas que o ITIL une são testadas e comprovadas na prática e são resultados de anos de observações e estudos. O ITIL sugere que a área de TI seja vista como uma prestadora de serviços e que esses serviços tenham um ciclo de vida.

Utilizando esse ciclo de vida é possível mensurar e gerenciar o valor que estes serviços podem agregar ao negócio da empresa.

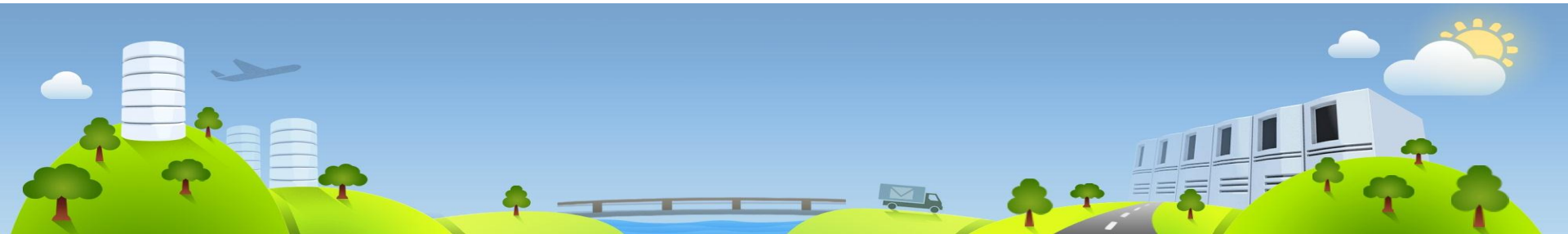


Conteúdo Extra

Modelo OSI

O modelo OSI é um modelo de referência desenvolvido pela ISO. Esse modelo foi desenvolvido com o objetivo de facilitar o entendimento e a forma como a comunicação em uma rede de computadores acontece. Esse modelo é dividido em sete camadas.

Camada Modelo OSI	Função da Camada	Protocolos da Camada
7 - Aplicação	Camada em que estão os serviços e protocolos que compõem os aplicativos.	Http, https, ssh, telnet, pop, snmp, smtp, ftp.
6 - Apresentação	Formata os dados para serem apresentados à camada de aplicação.	ASCII, jpg, tls
5 - Sessão	Responsável por iniciar e encerrar as conexões de rede.	Rpc, sql, nfs,
4 - Transporte	Proporciona comunicação fim-a-fim entre os dispositivos finais.	Tcp, udp, sctp, dccp
3 - Redes	Fornece o roteamento dos pacotes entre o dispositivo de origem e o destino.	Ipv4, arp, ipv6, icmp, arp
2 - Enlace de Dados	Responsável por controlar como os dados vão acessar o meio físico.	Ethernet, 802.11, hdlc, frame relay, ppp
1 - Física	Responsável pelos meios de conexão(interfaces) utilizados para trafegar os dados pelas redes de computadores.	Modem, 1000base-TX, hub, RS-232, Rj45



Portas TCP/UDP

Todo protocolo que trabalha na camada de aplicação possui uma porta padrão em que recebe as requisições de outros dispositivos. A IANA(Internet Assigned Numbers Authority) é o órgão responsável por esse controle de portas utilizadas pelas aplicações.

No *link* abaixo seguem as aplicações que estão regulamentas para utilizar as portas TCP/UDP.

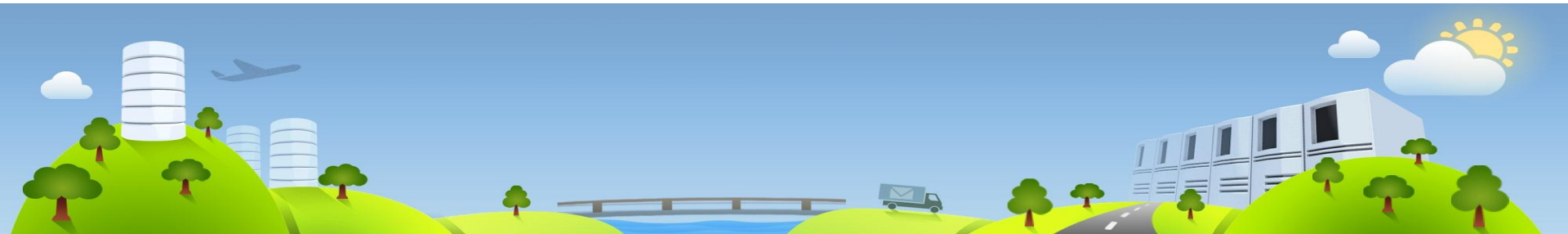
http://goo.gl/fSiOJ8

Segurança

O mundo da segurança da informação está sempre em constante evolução, novos ataques surgem a cada momento e, consequentemente, trazem uma preocupação extra para quem trabalha na área. Atualmente existem vários tipos de ataques, cada ataque se beneficia de alguma vulnerabilidade na rede ou no protocolo.

No *link a seguir são apresentados alguns tipos de ataques bastante conhecidos na área de segurança.*

http://goo.gl/XKfMh8



Após concluir seus estudos, acesse o ambiente virtual para realizar o Desafio Final!