**Administrador de sistemas:** Formar e treinar a equipa, estratégia de salvaguarda e recuperação de dados e aplicações, critérios de gestão de utilizadores, suporte técnico aos utilizadores, estratégia de atualização dos sistemas e apps. Planear, implementar, configurar e manter: o bom funcionamento da infraestrutura, as aplicações inerentes ao funcionamento da organização, **requisitos de segurança** (confidencialidade, integridade, disponibilidade). Participar nas políticas de segurança. Analisar/selecionar novas tecnologias ou tendências que possam ser úteis. Adaptar os requisitos legais que devam ser cumpridos. O administrador deve supervisionar e planear as componentes de infraestrutura, sistemas e segurança. O Administrador de Sistemas sempre é o **único e exclusivo** responsável pela adaptação do funcionamento e desempenho da infraestrutura e sistemas aos requisitos da organização

**CPD(Centro de Processamento de Dados):** local de colocação dos sistemas e equipamentos onde se desenvolve a infraestrutura; **Vantagens:** único local onde se deve assegurar os critérios ambientais (temperatura, humidade, poeiras, etc.) melhorando as condições de funcionamento da infraestrutura crítica, facilita a adoção de alternativas de alimentação elétrica SOS(UPS, geradores, etc.), instalação de pisos e tetos falsos para melhor distribuição de cabos, permite segurança para armários e equipamentos de telecomunicações adequados.

**Custos operacionais:** aumentam em função dos equipamentos ativos, ocupa espaço, upgrades tecnológicos. Aumento da quantidade de equipamentos, necessidade de refrigeração e, consumo energético pelos 2. Para reduzir custos, reduzir custos energéticos e não adotar política de mais equipamentos para mais serviços, para isso recorrer à **virtualização** dos servidores.

**Virtualização:**(só existe 1 servidor por norma), onde são criados vários servidores virtuais (convidados. Transforma hardware em software), simulando o equipamento físico com uma aplicação. **Convidado:** tem sistema operativo, reserva de características (disco, memória, placas de rede) do hospedeiro, distribuídas de forma dinâmica. Os convidados são independentes entre si (podem criar infraest. virtuais com ativos de rede para interligar). Custos administrativos existem, embora não cresçam na mesma proporção da instalação física. Aumenta taxa de utilização do hospedeiro, menos equipamentos físicos, facilita administração. Diminui custos administrativos e energéticos. | Se o hospedeiro para, os convidados param, limitações de desempenho (se mal dimensionado), convidados têm de ter licenças de OS e OS separados.

**Containers:** partilham partes do sistema operativo e bibliotecas. Não têm de ter licenças OS e OS separados(bom ou mau). Exige menos recurso físicos. Caso problemas de segurança, hospedeiro e convidado podem ser afetados.

**Armazenamento:** **DAS (Direct Attached Storage)-** Blockdevice. Sistema possui próprio armazenamento de utilização exclusiva (pode haver partilhas com custos implicados, não há economia de escala na partilha do armazenamento) que tem o OS, apps e dados. Adição e remoção de armazenamento requer intervenção física muitas das vezes com desativação temporária do sistema. Salvaguarda de dados executada pelo próprio sistema (consome recursos). **Network Attached Storage (NAS)-** File System. Forma económica de facultar grande espaço de armazenamento a vários sistemas. Rápido de instalar e configurar. Normalmente suporta **RAID (Redundant Access of Independent Disks).** Definir permissões a pastas e ficheiros. Elevada utilização de recursos(bom)|| Mau: Ocupa recursos de rede, aumento da latência e potenciais problemas de transf. de dados, afetado pela disponibilidade da rede. **Storage Area Network (SAN):** mais dispendioso e com maior capacidade. Rede própria com maior desempenho. Deve disponibilizar elevada fiabilidade e segurança. Recurso a infraestrutura Gigabit Ethernet mas ideal é Fibre channel (FC). Deve existir redundância de ligações na SAN. ||**Dois protocolos e várias implementações:** Fibre Channel Protocol (FCP), Fibre Channel over IP (FCIP), Internet Fibre Channel Protocol (iFCP), Fibre Channel over Ethernet (FCoE), Non-Volatile Memory Express over Fibre Channel (FC-NVMe) permite interconexão dos sistemas e discos SSD por ligação PCI express. OU Internet Small Computer System Interface (iSCSI).

**FC:** implica existência de equipamentos específicos para interligação com infraest. Informática, como Host Bus Adapter (HBA), Converged Network Adapter (CNA) e switch/gateway FC. Topologias físicas são variadas, desde a ligação simples via switch FC até à malha designada por Core Edge. **FCIP e IFCP-** permitem ao contrário do FCoE, interconexão de SAN remotas. FCIP é implementado ao níveo da própria SAN, IFCP é ao nível do dispositivo, logo não se pode conectar diretamente SANs FCIP, IFCP. Ambas baseiam e usam TCP/IP. FC tem constrangimentos: tipologia de discos (resolvido por substituição de HDDS) e protocolos (NVme, FC-NVMe usa protocolo e arquitetura que não se limita a disco SSD).

**iSCSI:** alternativa económica. Nativa do OS, não necessita de placas ou dispositivos específicos. Interconexão de SAN remotas. Baseia-se em TCP/IP. Tem software initiator (que tira partido do armazenamento e acede ao target como se fosse discos SCSI locais) e um software target (que disponibiliza o armazenamento). **Redundant Array of Independent Disks (RAID):** Replicar IRT um disco para outro, expandir capacidade de disco usando espaço de outro disco. Raid software (Suportado direta. por OS recente), Raid Hardware (controlador específico, não impede Raids que não necessitam dele). Raid 0:Striping(+espaço e desempenho,-segurança);1:Mirroring(+segurança e desempenho, espaço); 5:Striping with parity(min 3 discos, dados em 2 discos, 3 para paridade) (+capa,desemp,segurança), espaço max é tam disco menor x numero discos -1.; 10: strip with mirror

SAN é designado por **virtualização de storage** (não está fisicamente ligada a cada sistema). Sistema de armazenamento proporciona discos lógicos (Logical Units LUN) aos servidores na SAN, usufruindo dos protocolos apropriados. Disco lógico pode ser disco físico, parte de disco físico ou espalhados por diversos discos físicos. Cliente acede ao disco lógico da mesma forma que a um disco local, tendo acesso à capacidade atribuída a ele. Gestão e armazenamento através de apps, sem precisar de parar. Permite criação de snapshots, clonagem, e mirroring dos disco.

Normas ISO 27000 apoiadas de outras normas ISSO 22301 e 22313, definem critérios para manter a continuidade de negócio. Definem regras tendo em mente organizações, mas adaptáveis à dimensão (até para particulares). Objetivo de normalizar metodologias e possibilitar critério comuns. É uma metodologia Top-Down, não faz sentido ser uma decisão individual, sem o apoio dos decisores (numa organização, a gestão de topo). Definem o **Business Continuity Management (BCM)**

**Business Continuity Management (BCM):** O modelo usado é o Plan-Do-Check-Act (PDCA)- um modelo de contínua observação, planeamento e ação, como parte essencial para aplicação do modelo, integra um conjunto de critérios que devem ser cumpridos:

**Primeiros-Maximum Tolerable Period of Disruption (MTPD):** tempo máximo de desempenho inferior aos requisitos da infraestrutura informática. **Maximum Tolerable Downtime (MTD):** tempo máximo de inoperacionalidade da infraestrutura informática. Objetivo é num período inferior ao definido por estes critérios a atividade e requisitos de desempenho da organização (isto é, o negócio) seja retomada, estes valores podem não ser fixos, estáticos (períodos mais exigentes; serviços mais importantes), o BCM deve especificar todos os aplicáveis.

**Segundos- Mininum Business Continuity Objective (MBCO):** nível mínimo de operacionalidade a manter durante uma disrupção na infraestrutura (ex. S1 pode não estar operacional, mas o S2 tem de ser manter a funcionar aceitavelmente). MTD/MTPD será certamente mais restrito para os serviços associados a este objetivo. **Service Level Agreement (SLA):** conjunto de parâmetros qualitativos e quantitativos de segurança, integridade e disponibilidade (ou seja, em termos de tempo de resposta) de um serviço, pretendidos e aceite pela organização.

**Businness Impact Analysis (BIA):** Identifica as atividades críticas da organização e as suas dependências; permite desta forma priorizar as operações de recuperação após uma disrupção; **Risk Assessment (RA):** Constituído pelos cenários que podem afetar a continuidade de negócio, a probabilidade de ocorrerem e o seu impacto. Habitualmente representado por uma matriz de risco, cada item tem associada uma probabilidade (1 menos possivel-5 mais possivel) e um impacto (1marginal-4catastrofico) (severidade) Risco= Impacto x Probabilidade. **Business Continuity Plan (BCP):** parte integrante do BCM e documenta os procedimentos a efetuar para responder, recuperar, retomar e restaurar a um nível pré-definido de operação após a interrupção. **Disaster Recovery Plan (DRP):** parte integrante do BCM. Podem ocorrer problemas que violem o SLA, se o MBCO ou o MTD não são afetados, o BCM deve ter procedimentos necessários para recuperar SLA dos serviços em disrupção, se são afetados, o DRP assume controlo até recuperação da situação. Todas as ameaças e falhas que possam ocorrer devem ser avaliadas e, possivelmente, eliminadas – ou pelo menos mitigadas. Começa-se por analisar o SLA, medindo e validando os critérios. Um sistema que cumpre o SLA combinado **designa-se por sistema seguro.**

**Probabilidade de falha de um serviço:** serviço depende de componentes, que dependem de outros componentes. A probabilidade de falha é a soma das probabilidades de todos os fatores. Contudo é mais vulgar o uso do tempo médio entre falhas (**Mean Time Between Failures MTBF) = (Mean Time To Fail MTTF) + (Mean Time To Repair/Replace MTTR). Disponibilidade:** MTTF/MTBF. O cálculo do MTBF de serviço ou sistema que depende de subcomponentes em série pode ser calculado como o inverso da soma da **taxa de falhas por hora** (**λ**) ou **milhão de horas (FIT)** de cada subcomponente. Aumento do MTTF através de um controlo de qualidade dos produtos/serviços, o mesmo nem sempre aplica-se ao MTTR. Aumentar a disponibilidade através da redundância, necessária total independência e autonomia dos componentes (λ1 x λ2 x λ3).

**Prevenção de falhas (Fault Avoidance):** objetivo evitar ocorrer falhas que metam em causa a continuidade do negócio, uso de monitorização e alarmística (uso cpu e disco, temperaturas, humidade,etc.). **Tolerância a falhas (Fault Tolerance):** classifica sistema/serviço como- **Full Fault Tolerant**(mantém funcionamento); **Gracefull Degradation**(degradação temporária), **Fail Soft**(degradação significativa/prolongada), **Fail Safe**(indisponibilidade mas integridade). **SPOF (Single Point Of Failure):** componentes comuns (alimentação elétrica, sistemas de controlo de redundância). **CMF (Common-Mode Fault):** falhas que afetam componentes independentes (Atualização de servidores independentes) spof é um cmf mas o contrário não.

**Recovery Time Objective (RTO):** tempo médio de recuperação dos sistemas e infraestruturas; **Recovery Point Objective (RPO)** tempo máximo de perda de dados aceite; **Work Recovery Time (WRT)** tempo necessário para repor os dados e aplicações e testá-los ||Em teoria, é sempre possível arranjar uma estratégia para assegurar a continuidade de negócio, porém podem implicar custo desapropriado ao benefício obtido, logo necessário analisar e calcular o custo da mitigação do risco face ao benefício obtido: **Asset Value (AV):** valor do item em causa, **Exposure Factor (EF):** exposição ao risco do item, **Single Loss Expenditure (SLE)=** AV x EF, **Annualized Loss Expectancy (ALE)=** **Annualized Rate of Occurrence (ARO)** x SLE. Valor obtido deve ser comparado com custo da açao necessária para o mitigar. Pode n ser tao simples devido a valor de dados

**Prevenir perda de dados**(influencia RPO, WRT mas o RTO é ou pode ser independente): Mirroring ou Cópias de segurança.

**Mirroring para local Remote:** Pode ser síncrono(RPO WRT Nulos) ou assíncrono(próximo de nulo), facilita a recuperação em caso de desastre, necessidade de garantir a confidencialidade e integridade dos dados (provocando latência na rede, consequência na disponibilidade de operação, inerentemente SLA). Depende do amb de exc e possib de manter sistema.

**Cópias de segurança:** Deve ser sempre feita em duplicado, uma delas em local remoto **Integral** - Copia todos os dados, maior tempo de cópia (pior RPO), menor tempo de reposição (melhor WRT). **Incremental**- Necessita cópia integral/completa prévia, copia todos os dados que foram alterados desde a copia incremental anterior (ou integral se for a primeira). **Diferencial-** Necessita cópia integral/completa prévia, copia todos os dados que foram alterados desde a copia integral anterior.

**Network Access Control (NAC):** controlo de acesso a infraestrutura por políticas de segurança. Objetivos- mitigar/prevenir ataques zero-day, aplicar política de segurança ao longo da infraest., usar identidades para controlo de acesso. Podem ser alcançados através de vários mecanismos (políticas de segurança com definição de controlo de segurança, filtragem, prevenção, …). NAC vai atuar como um sistema de deteção e resposta automática IRT para impedir ameaças antes de danos. Implementação através de 2 critérios: **Pré-admissão-** refere-se a sistemas, serviços(sistema tem de cumprir todos requisitos de segurança, como atualizações e ter antivirius, antes que posso comunicar com a rede); **Pós-admissão-** envolve utilizadores que acedem à rede (permite/nega acesso baseado na atividade do utilizador, usa matriz de autorizações pre-definida).

**Identificação Users:** necessitam de se autenticar. **Password Authentication Protocol (PAP)-** troca de duas mensagens no início da auth (user envia identificação e senha; sistema de auth valida identificação/senha; devolve autorização ou negação de acesso). Considerado **inseguro** pq: identificação/senha enviadas em texto claro (legível); sem proteção bruteforce; identificação/senha necessitam ser previamente definidas (**segredo partilhado**). 1.auth request->2.auth Ack->3.Auth Nak.

**Challenge-Handshake Authentication Protocol (CHAP)(mais seguro)-** troca 3 mensagens, verifica periodicamente identidade do user. Ainda necessário segredo partilhado. Campo: Código indica a operação em curso; identificador é um número aleatório e serve para mapear os desafios e as respostas; Dados tem tamanho do texto de desafio ou resposta, desafio (se código = 1) ou resposta (se código = 2), nome que identifica o dispositivo que enviou o desafio.

**Policy Enforcement Point (PEP):** ponto de acesso à rede. Deverá ter a identificação e credenciais dos utilizadores para validar acess OU contactar um **Policy Decision Point (PDP)** (se encarregará de validar credenciais inseridas).

**Extensible Authentication Protocol (EAP):** não é especificamente um protocolo, mas sim uma framework para auth. Permite múltiplos sistemas na auth (biometria, cartões...). Permite PEP funcionar em pass-through (ex: AP sem fios). Possibilita PEP ser transparente e auth ser diretamente no PDP. Pode-se implementar vários mecanismos de segurança recorrendo ao EAP: **Protected Extensible Authentication Protocol (PEAP)-** encapsula o EAP num túnel Transport Layer Security (TLS). Normas Wifi Protected Access (**WPA**) incluem PEAP.

**Segredo pré-partilhado** enquadra-se na cifra simétrica, garante confidencialidade pois exige chave para decifrar a mensagem. Para ser efetivo, ser exclusivo de um par de entidades (para N entidades deverão existir combinações de N dois a dois) C(n,2).

**Identity Management:** gestão de identidades. Pode ser: **Centralizada (**controlo de acesso distribuído**),** implica várias entidades localizadas ao longo do sistema/infraestrutura que executem a verificação do acesso. Sincronização complexa, elevado esforço administrativo, users costumam usar mesma senha em todos serviços e sistemas, porém oferece vantagens no controlo de autorização de acessos; OU **Descentralizada,** exige menor esforço administrativo, oferece **Single Sign-On (SSO)-** não implica sync de senhas, entidades authent apenas uma vez, porém, obriga mais esforço de autorização de acessos. Nas organizações é mais necessário assegurar gestão centralizada dos utilizadores, logo **Serviço de diretório:** consiste numa base de dados que inclui informação sobre objetos e entidades.

Vários desses serviços são baseados no **Lightweight Directory Access Protocol (LDAP)** **RFC 3494** (ex:Active directory Domain Services): considerado uma evolução do protocolo X.500, suportando dialogo com ele e mantendo varias das sua definições (classes e atributos).Vantagem importante é suportar a exportação de ramos da árvore ou toda. **LDAP RFC 4511(atual):** base dados não relacional, pode alojar auths das entidades. Estrutura de dados muito flexível e otimizada para operações de consulta. Estrutura em árvore, cada ramo um **objeto** que possui **atributos**, topo designado **root.** Atributos indexados para otimizar pesquisa/consulta. O cliente(humano/sistema) acede diretorio global (pode ter vários servers LDAP) através de cliente ou **Directory User Agent (DUA),** este cliente por sua vez interage com um ou + servidores ou **Directory System Agents (DSA)** através do protocolo LDAP. LDAP usa **TCP,** como **mecanismo de transporte** e baseia-se na **Abstract Syntax Notation One (ASN.1):** todas as mensagens encapsuladas num formato denominado **LDAPMessage,** sequencia em formato string contendo um numero de sequencia, identificador, operação pretendida e mensagem. Caso msg em q numero de sequencia n seja reconhecido, conexão é terminada, devolve ent indicação de desconexão com **ProtocolError.** Noutro casos, conexão imediatamente terminada (pode ou n devolver msg).

**Definição dos atributos dos objetos no LDAP** têm que cumprir definição do **schema** (definidos na **RFC 4512**) não sendo ent livre. O **Schema:** contém as classes possíveis contendo cada uma os atributos que são válidos e que tipo de utilização é permitida em cada um (alguns atributos obrigatórios, outros opcionais), definição das classes implementa o conceito de herança (subclasses incorporam atributos de superclass, podem definir mais atributos). Existem classes **estruturais** e **auxiliares** (opcionais), objeto pertence uma classe estrutural mas pode pertencer a varias auxiliares. **Atributos obrigatórios:** **Domain Component (DC)** (pode pertencer à classe **dcObject**(auxiliar) normalmente com classe **Organization** (estrutural), alternativamente classe **Domain.** Frequente a nomeação baseada no nome do dominio DNS, cada uma das suas partes um dc, separados por vírgulas (DNS i.pp.tt, root: dc=i;dc=pp;dc=tt). **Distinguished Name (DN):** nome q identifica um objeto único e exclusivo na árvore. Se corresponde ao root chama-se **base DN** ou **root DN**. DN tem de ser único no LDAP identificando inequivocamente o objeto, **Relative Distinguished Names (RDN):** nomes de atributos podem repetir ao longo da estrutura, só que em ramos diferentes da arvore.

Quando entidade se autêntica numa infraestrutura há uma sequência de passos necessários: **identificação (**anunciar quem é a entidade**->**nome de user(id) e senha de acesso), **autenticação**: sistema valida o par e devolve sucesso da identificação. Estes passos terão de ser efetuados para todos os serviços que ID pretende aceder. Porém, é necessário verificar **Autorização:** verificar se o ID pode aceder ao serviço, dessa forma, usa-se **serviço centralizado de autenticação**: designado **Policy Decision Point (PDP)**. Que está intimamente ligado ao **Policy Information Point (PIP)** que serve a validação da autorização. Porém, user normalmente não acede diretamente ao PDP mas sim a um serviço que se encarrega de contactar com o PDP, o **Policy Enforcement Point (PEP)**: normalmente serviço de rede, porém, pode também ser um acesso por túnel VPN ou um Access point, nesse caso chama-se **Network Access Service OU Network Access Server (NAS).**Normalmente é necessário (para controlo interno ou cumprir obrigações legais) registo dos acessos concedidos e negados às entidades, que se chama **Accounting.** Juntamente com a **Authentication** e **Authorization** anteriores, temos os sistemas **AAA.**

Para assegurar suporte ao **AAA** foram desenvolvidos protocolos/métodos como: 1/2/3/4

**1- Remote Authentication Dial In User Service (RADIUS) (RFC 2865):** em simultâneo um serviço e um protocolo que assegura as comunicações entre o **PEP** e o **PDP;** comunicação que ocorre em UDP para evitar constrangimentos associados ao TCP; Pode ter um **PIP** e **accounting local** ou através de extensões, comunicar com outros serviços que implementes essas funções; Pedidos de accounting registados apenas para inicio e fim de sessão; Usa 8 bits para definir os pares **Atributo – Valor (AV).**

**2-** **Terminal Access Controller Access-Control System Plus (TACACS+):** Ao contrário do RADIUS usa TCP. Diferença significativa- isola as verificações (autenticação e autorização) e repete autorização sempre que execução de novo comando é requerida.

3- **Diameter (RFC 6733 na versão atual):** Evolução baseada no RADIUS mas não compatível. **Aspetos mais importantes:** Suporta o EAP, **SCTP (Stream Control Transmission Protocol),** redes cabladas, wifi, 3G, IP Multimedia Systems (IMS), e LTE/4G; permite mecanismos de failover; baseado em TCP; Usa 32 bits para definir os pares **Atributo – Valor (Attribute-Value Pair AVP**) por isso mais escalável (AVP contêm informação de autenticação, accounting, autorização, encaminhamento, segurança e configuração para o pedido e resposta).

4- **Kerberos(método):** terceira parte que assegura identificação e auth, fornecendo tickets às entidades que solicitem. Solução de **Single Sign-On (SSO),** dá proteção às credenciais de auth. Uso de criptografia de chave secreta. Cada uma das entidades a quem pode distribuir chaves designa-se por **principal (**utilizadores e recursos**)**. Divide a infraestrutura em **realms**, cada um contém obrigatoriamente o serviço de distribuição de chaves denominada **Key Distribution Center (KDC)**, todos os principals estão registados no KDC que mantém uma base de dados das chaves de todos. Servidor de autenticação executa as funções do KDC, dois serviços distintos e paralelos: **Authentication Service (AS)**- Possui uma chave partilhada com os principals, aceita ou rejeita a tentativa de acesso, fornece aos principals um ticket que lhes permite provar a sua identidade ao **TGS** E **Ticket Granting Service (TGS)-** Fornece os **Ticket-Granting tickets (TGT)** (chaves de sessão para comunicação temporárias, pois TGT tem tempo de vida), aos principals. Se não houver sincronização horária nos principals, o acesso será negado. **TGT** prova que o principal se autenticou no **KDC** e está autorizado a pedir acessos aos recursos. || **Tickets-** mensagens encriptadas que provam a autorização de acesso a um recurso. User pede ticket, se user e recurso estão autenticados e o user tem permissão para usar recurso, **TGS** fornece ticket. Possuem parâmetros de utilização específicos sem ser o tempo de vida. Ticket expira, deve solicitar renovação ou novo ticket. Estando todos os principals autenticados, assegura a toda a estrutura a identidade e autorização uns dos outros. || Nomes de principals num realm possuem reservas (ex:krbgt). Símbolos @ e / são usados para separar o nome do principal do nome do realm e componentes do nome do principal respetivamente (ex:user@realm e sftp/server@realm) **||** Kerberos pode gerir relações de confiança entre realms distintos, com esta relação de confiança é possível a um principal de um realm aceder a recursos de um realm distinto sem necessitar de possuir credenciais no AS desse outro realm. Consiste em definir cada TGS como principal no outro realm. Independentemente do realm em que se encontra, cada principal pode obter um ticket de acesso a recursos do outro realm. Considera-se que um realm pode comunicar com outro realm se ambos partilham uma chave **inter-realm** (usada para encriptar os tickets de pedido de acesso a recursos do realm remoto) **||**Kerberos suporta também **hierarquia** entre realms (ex: domínios Active Directory da Microsoft na mesma tree). Havendo hierarquia, a **relação de confiança é transitiva**, isto é, se o realm A confia no realm B e o realm B confia no realm C, então o realm A confia no realm C **||** **Desvantagem:** KDC é um SPOF; Chaves baseiam-se nas senhas dos utilizadores, pelo que uma senha “fraca” potencia a sua captura e posterior acesso à chave; Não disponibiliza mecanismos de tolerância a falhas, pelo que é razoável configurar mais do que um KDC no mesmo realm, porém, sincronização das bases de dados tem de ser feita com recurso a sistemas externos (automáticos ou manuais) e aplicações deverão estar preparadas com base em tentativa-erro (KDC principal não responder, tentar no KDC alternativos até obter sucesso ou falha após percorrer todos os KDC), já se encontra no Active Directory da Microsoft **||** Caso o KDC principal esteja inoperacional, a administração do Kerberos não pode ser efetuada até que ele seja restaurado

**Dados:** Infraest. pode ser substituída, mas dados não necessariamente. O custo de perda de dados não é quantificável, o que acarreta efeitos secundários (legais, fiscais, operacionais, de reputação...). Por vezes são secretos ou privados, pelo que acesso de terceiros acarreta perde de credibilidade e fugas de informação. Dados são essenciais à operação da organização ou pessoal, importa que sejam **credíveis**, **disponíveis** e **confidenciais.** Porém, estes princípios não se aplicam da mesma forma a todas as áreas da infraest. (rede, equipamentos, dados). **Disponibilidade**:interpretada como estar disponível na altura (e/ou espaço de tempo) apropriado. **Segurança:** conceitos necessários para que a informação esteja disponível, certa e legível apenas a quem está autorizado, este conceito pode ser (e é) estendido à própria infraestrutura com as devidas alterações ou adaptações aplicáveis. Tríade **CID** espelha a base da segurança.

**Confidencialidade:** garante que existe o nível apropriado de secretismo em cada nó de processamento e que se previnem as fugas de informação. Deve existir em todo o sistema e não apenas em algumas partes. Obtida através de encriptação de dados guardados e transmitidos e comunicações seguras. Anulada através: Sniffing de comunicações, engenharia social, roubo de credenciais de autenticação. Sem, os dados podem ser lidos por quem não tem autorização apropriada. **Integridade:** garante exatidão e fiabilidade do sistema e na prevenção da alteração não autorizada de dados. Garante que ataques e erros não comprometem a informação e o sistema. Obtida através de boa gestão das capacidades dos agentes do sistema, de mecanismos de deteção de intrusão e Controlos de acesso apropriados. Sem, um sistema pode funcionar sobre dados incorretos sem o saber. **Disponibilidade:** Garante capacidade necessária a fim de atuar de forma previsível e com desempenho aceitável. Obtida através evitar pontos únicos de falha, medidas de salvaguarda de informação, mecanismos de redundância, garantir disponibilidade a quem dela precisa. Afetada por denial of service attack.

**Arrumar**

**TP1:  
MBR (Master Boot Record)** - área especial no disco rígido que contém informações essenciais para iniciar o sistema operativo do computador, como o código de inicialização e a tabela de partição. Este está localizado no primeiro setor do disco e é fundamental para o processo de inicialização do computador.

**GPT (GUID Partition Table) -** é um padrão de tabela de partição para o layout da tabela de partição em um disco rígido físico, usando um identificador de globally unique identifier (GUID). Embora seja parte do padrão Extensible Firmware Interface (EFI), Este também é usado em alguns sistemas BIOS, porque Este resolve algumas limitações do MBR.

**NTFS (New Technology File System) -** é um sistema de arquivos proprietário desenvolvido pela Microsoft. Começou a ser usado em 1993 com o Windows NT 3.1, substituindo o FAT. O NTFS possui recursos como suporte a metadados e a recuperação de dados, que não estão presentes no FAT.

**ACL (Access Contol List) -** é uma lista de permissões associada a um objeto. Cada entrada na lista especifica um sujeito e um conjunto de operações permitidas para esse sujeito. O sistema de arquivos NTFS usa ACLs para controlar o acesso a arquivos e pastas.

**Journaling** - registo de operações de escrita antes de serem aplicadas, deste modo havendo uma falha grave não é necessário verificar a integridade de todo o disco, apenas a zona que estava a ser escrita.

**DHCP (Dynamic Host Configuration Protocol) -** é um protocolo de serviço TCP/IPque oferece configuração dinâmica de terminais, com concessão de endereços IP de host, máscara de sub-rede, default gateway (gateway padrão), número IP de um ou mais servidores DNS, sufixos de pesquisa do DNS e número IP de um ou mais servidores WINS.

**DHCP (Dynamic Host Configuration Protocol)** - é um protocolo de serviço TCP/IPque oferece configuração dinâmica de terminais, com concessão de endereços IP de host, máscara de sub-rede, default gateway (gateway padrão), número IP de um ou mais servidores DNS, sufixos de pesquisa do DNS e número IP de um ou mais servidores WINS.

------

**GSS-API-** independente de mecanismo específicos de segurança. Permite que aplicações solicitem servições de segurança sem saber os detalhes do mecanismo especifico que está a ser utilizado.

**Criptografia**

**Cifras:** Blocos de entrada iguais não devem produzir blocos cifrados iguais. Método de cifra pode ser **bloco** (o texto original é dividido em partes de igual tamanho, cada uma das partes é cifrada com a mesma chave K, é adicionado um padding ao texto ou truncado no bloco final a chave para que as dimensões das partes (texto e chaves repetidas) seja igual) ou **contínua** (stream).

**Cipher Block Chaining (CBC)-** A cifra de cada bloco (excluindo o primeiro) é aplicada ao bloco seguinte (usualmente através de uma operação XOR) e o resultado é cifrado

**Counter (CTR)-** É aplicado um vetor de inicialização à chave e o resultado dessa aplicação é que é usada como chave para o bloco, vetor inicial até pode ser zero, mas os seguintes são incrementados de um valor pré-determinado.

**Caso contínuo:** o texto original é dividido em partes de igual tamanho, cada uma das partes é cifrada com uma chave diferente K = K1K2K3…KN, **chave periódica** número de chaves K pode ser menor que o número de partes do texto P, caso em que uma chave pode ser repetida

**RTP (Real-time Transport Protocol):** um protocolo de rede usado para a entrega de dados em tempo real, como áudio e vídeo, providencia mecanismo para ordenar pacotes e verificar integridade depois da chegas (pacotes têm nºsequência).

**O cabeçalho IP contém campos que permitem diferenciar o tráfego**: IPv4 o campo de 8 bits Type of Service (TOS), No IPv6 o campo de 8 bits Traffic Class (TC). Permitem definir a prioridade do tráfego por forma a que os nós intermédios possam tratá-lo de forma diferenciada. Dispositivos mais antigos estes campos utilizavam apenas os 3 bits mais significativos representando o IP Precedence, depois todos os bits passaram a ser utilizados sob a designação **Differentiated Service (DS**) também conhecido por **DiffServ,** 6bits mais significativos são designados por **Differentiated Service Code Point (DSCP**), inclui **IP Precedence** (permite compatibilidade com nós antigos), enquanto os 2 menos significativos são designados por **Explicit Congestion Notification (ECN)**

**----**

O algoritmo **Random Early Detection (RED)** pode ser aplicado nos nós atravessados para evitar o **tail-drop,** mantém dois valores de ocupação da fila, minth a partir da qual descarta novos pacotes aleatoriamente com probabilidade p crescente até mathth, em que descartava todos os novos.

**Assinatura digital:** garantir autenticação e não repúdio.

**QOS:** **Soft QoS** e **Hard QoS**, ambos criam filas (queues)….

**/etc/passwd:** Cada linha do ficheiro corresponde a uma conta de utilizador e contém 7 atributos separados pelo símbolo de dois pontos: login-name, hash da password (x indica que hash se encontra no /etc/shadow), UID (nºunico de 16bits que identifica o user), GID primário (nºde 16bits que indica o GID do grupo primário do user), Nome longo ou desc de user, Pasta home (pasta corrente apos o login), programa inicial (tipicamente Shell exc após login, s n preenchido aplica-se Shell omissão).