Resumo 4SEG – AV2

* Com o crescimento da importância da área de TI para o sistema corporativo, surgiu o conceito de Governança de TI, que tem por **objetivo**:
* Melhorar os processos de TI;
* Alinhar a gestão da TI com estratégias da organização;
* Melhor gerir os recursos de TI (aplicativos, informações, infraestrutura e pessoas).
* A Governança de TI possibilita a organização a:
* Obter todas as vantagens de sua informação;
* Maximizar os benefícios;
* Capitalizar as oportunidades;
* Ganhar em poder competitivo.
* A Governança tem como pilares:
* Controles Robustos;
* Eficiência Organizacional;
* Controles Robustos.

Diferença entre Governança e Gestão de TI:

Governança: é responsável por definir como funcionam as coisas na TI e verificar se as normas e políticas estão sendo seguidas corretamente.

Gestão: é responsável por manter o desempenho de serviços, promover a transformação digital na empresa, manter a satisfação dos usuários e clientes dos serviços, além de fazer a gestão da equipe de TI.

Isso implica essencialmente em garantir que a TI faça certo as coisas certas, ou seja, padronizar os processos, definir como os serviços serão solicitados e atendidos, desenvolver projetos que deem um gás no desempenho da TI, mitigar os riscos possíveis e medir os resultados que a TI está entregando para o negócio.

Para auxiliar nesse acompanhamento, existem padrões e **frameworks** que permitem a medição de desempenho de soluções e a adoção de boas práticas.

Os mais adotados no mercado são:

* ISO/IEC 27001 – gestão da segurança da informação;
* ITIL (Information Technology Infrastructure Library) – conjunto de boas práticas para gerenciamento de serviços de TI;
* COBIT (Control Objectives for Information and Related Technology) – guia de boas práticas para governança e gestão de TI.

Organizações:

**ISO/IEC** – órgãos internacionais que cria normas que se baseiam em leis nacionais. Trabalham juntos para **não** evitar o OVERLAP (sobreposição) de padrões.

**ABNT** - criação das normas e sua importância se deu em três partes (BS 7799).

**ISO/IEC 17799**

Objetivos:

* Estabelecer códigos **de boas práticas** para a gestão de segurança da informação;
* Dar instrumentos para a implantação de **segurança da informação** de acordo com a características de uma empresa;
* **Confidencialidade**, **Integridade** e **Disponibilidade** (**CID**) das informações, que são fatores muito importantes para segurança e integridade das informações;

Obs.:

**Confidencialidade**: Garantia de que o acesso á informação seja obtido somente por pessoas autorizadas;

**Integridade**: Salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

**Disponibilidade**: Garantia de que os usuários autorizados obtenham acesso á informação e aos ativos correspondentes sempre que necessário.

* **Muito genérica** pois se adapta a cada empresa;
* A **ordem** **desses controles** **não significa o** **seu grau de importância** ou criticidade. Dependendo das circunstâncias todas as seções podem ser importantes e críticas.

Benefícios:

* Vantagem Competitiva;
* Melhoria no Desempenho do Negócio e Gerenciamento dos Riscos;
* Atrair novos investimentos, melhoria da reputação da marca e remoção de barreiras comerciais;
* Operações com menos burocracia, Redução de Perda e Redução de Gastos;
* Evolução da Comunicação Interna;
* Melhoria da Satisfação do Cliente.

**Seções de controle da ISO/IEC 17799:2005**

1. **Política de Segurança da Informação:**

Seu objetivo é prover uma orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

**Seus itens de controles são:**

- Documentação da política de segurança da informação;

- Análise crítica da política de segurança da informação.

1. **Organizando a Segurança da Informação:**

Seu objetivo é gerenciar a segurança da informação dentro da organização.

**Seus itens de controles interno são:**

- Comprometimento da direção com a segurança da informação;

- Coordenação da segurança da informação;

- Acordos de confidencialidade;

- Contato com autoridades;

- Análise crítica independente de segurança da informação.

**Seus itens de controles externo são:**

- Identificação dos riscos relacionados com partes externas;

- Identificando a segurança da informação, quando tratando com clientes;

-Identificando segurança da informação nos acordos com terceiros.

1. **Gestão de ativos para manter a segurança dos ativos:**

Seu objetivo é alcançar e manter a proteção adequada dos ativos da organização.

**Seus itens de controles são:**

- Responsabilidade pelos ativos;

- Classificação da informação.

1. **Segurança em Recursos Humanos:**

Seu objetivo é assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos pré, intra e pós contratação.

1. **Segurança Física e do Ambiente:**

Seu objetivo é prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

**Seus itens de controles são:**

- Áreas seguras

- Segurança de equipamentos:

1. **Gestão das Operações e Comunicações:**

Seu objetivo é garantir a operação segura e correta dos recursos de processamento da informação.

**Seus itens de controles são:**

- Procedimentos e responsabilidades operacionais;

- Gerenciamento de serviços terceirizados;

- Planejamento e aceitação dos sistemas;

- Proteção contra códigos maliciosos e códigos móveis;

- Cópias de segurança;

- Gerenciamento da segurança em redes;

- Manuseio de mídias;

- Políticas e procedimentos para a troca de informações;

- Serviços de comércio eletrônico;

- Monitoramento.

1. **Controle de Acesso:**

Seu objetivo é controlar o acesso à informação.

**Seus itens de controles são:**

- Requisitos de negócio para controle de acesso;

- Gerenciamento de acesso do usuário;

- Responsabilidade dos usuários;

- Controle de acesso à rede;

- Controle de acesso ao sistema operacional;

- Controle de acesso à aplicação e à informação;

- Computação móvel e trabalho remoto.

1. **Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação:**

Seu objetivo é garantir que a segurança é parte integrante de

sistemas de informação.

**Seus itens de controles são:**

-Requisitos de segurança de sistemas de informação;

- Processamento correto nas aplicações;

- Controles criptográficos;

- Segurança dos arquivos do sistema;

- Segurança em processos de desenvolvimento e de suporte;

- Gestão de vulnerabilidades técnicas.

1. **Gestão de Incidentes e Segurança da Informação:**

Seu objetivo é assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados permitindo a tomada de ação informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

**Seus itens de controles são:**

- Notificação de fragilidades e eventos de segurança da informação;

- Gestão de incidentes de segurança da informação e melhorias.

1. **Gestão da Continuidade do Negócio**

Seu objetivo é não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

**Seus itens de controles são:**

- Aspectos da gestão da continuidade do negócio, relativos à segurança da informação;

1. **Conformidade:**

Seu objetivo é evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

**Seus itens de controles são:**

- Conformidade com requisitos legais;

- Conformidade com normas e políticas de segurança da informação e conformidade técnica;

- Considerações quanto à auditoria de sistemas de informação.

**IPSec e VPN**

VPN – A rede virtual privada é uma conexão a garantir que os dados confidenciais sejam transmitidos com segurança. Normalmente utiliza-se IPSEC para estabelecer VPNS.

IPSEC - É um conjunto de padrões da Internet definido e mantido pelo IETF. É implementado na camada de rede e tudo acima dessa camada fica seguro por conta da encriptação.

A segurança no nível IP compreende três áreas funcionais:

Autenticação, Confidencialidade e Gerenciamento de chaves.

* O mecanismo de autenticação garante que um pacote recebido foi, realmente, transmitido pela parte identificada como origem no cabeçalho do pacote. Além disso, esse mecanismo garante que o pacote não foi alterado em trânsito.;
* A funcionalidade de confidencialidade permite que os nós se comunicando encriptem mensagens para impedir espreita por terceiros;
* A funcionalidade de gerenciamento de chaves trata da troca segura de chaves.

\* Para oferecer segurança, o IAB (Internet Architecture Board) inclui autenticação e encriptação como recursos de segurança necessários no IPV6. Mas também pode ser usados com o IPV4 atual.

\* O recurso principal do IPsec que lhe permite dar suporte a essas aplicações variadas é que ele pode encriptar e/ou autenticar todo o tráfego no nível IP.

**Documentos do IPsec:**

Arquitetura: abrange os conceitos gerais, requisitos de segurança, definições e mecanismos definindo a tecnologia IPsec.

Authentication Header (AH): AH é um cabeçalho de extensão para fornecer autenticação de mensagem. Como a autenticação de mensagem é fornecida pelo ESP, o uso de AH está desaconselhado;

Encapsulating Security Payload (ESP): consiste em um cabeçalho e término de encapsulamento, usados para fornecer encriptação ou uma combinação de encriptação e autenticação.

Internet Key Exchange (IKE): esta é uma coleção de documentos descrevendo os esquemas de gerenciamento de chaves para uso com IPsec.

Algoritmos criptográficos: esta categoria compreende um grande conjunto de documentos que definem e descrevem algoritmos criptográficos para encriptação, autenticação de mensagem, funções pseudoaleatórias (PRFs) e troca de chave criptográfica.

Tanto AH quanto ESP admitem dois modos de uso: modo transporte e túnel.

**Modo Transporte**:

* Oferece proteção principalmente para os protocolos da camada superior;
* Normalmente, é usado para a comunicação de ponta a ponta entre dois hospedeiros;
* O ESP no modo transporte encripta e opcionalmente autentica o payload IP, mas não o cabeçalho IP. AH no modo transporte autentica o payload IP e partes selecionadas do cabeçalho IP.

**Modo Túnel**:

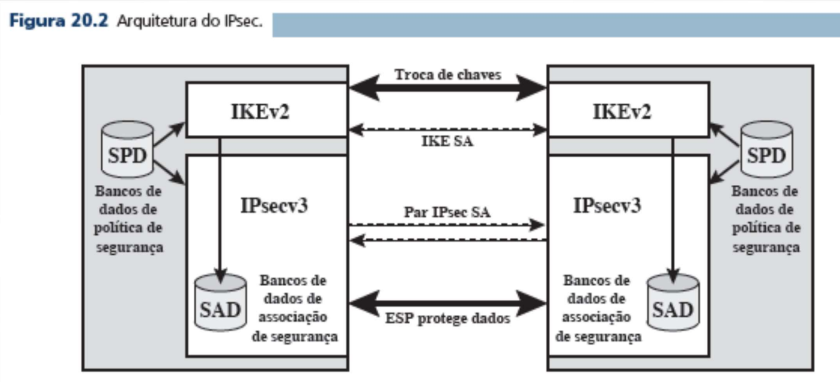
* Oferece proteção ao pacote IP inteiro. Para conseguir isso, depois que os campos AH ou ESP forem acrescentados ao pacote IP, o pacote inteiro mais os campos de segurança são tratados como o payload do novo pacote IP externo, com um novo cabeçalho IP externo. Todo o pacote interno original viaja por um túnel de um ponto de uma rede IP para outro; nenhum roteador ao longo do caminho é capaz de examinar o cabeçalho IP interno. Como o pacote original é encapsulado, o novo pacote maior pode ter endereços de origem e destino totalmente diferentes, aumentando a segurança;
* É usado quando uma ou ambas as extremidades de uma associação de segurança (SA) são um gateway de segurança, como um firewall ou roteador que implemente IPSec. Assim, diversos hospedeiros nas redes por trás de firewalls podem se engajar em comunicações seguras sem implementar IPsec.

Mesmo protocolo IP dentro de outro protocolo IP = Tunelamento/Encapsulamento.

* SA (Associação de Segurança): relacionamento de única via entre o emissor e um

receptor, que está de acordo com os serviços de segurança ao tráfego transportado

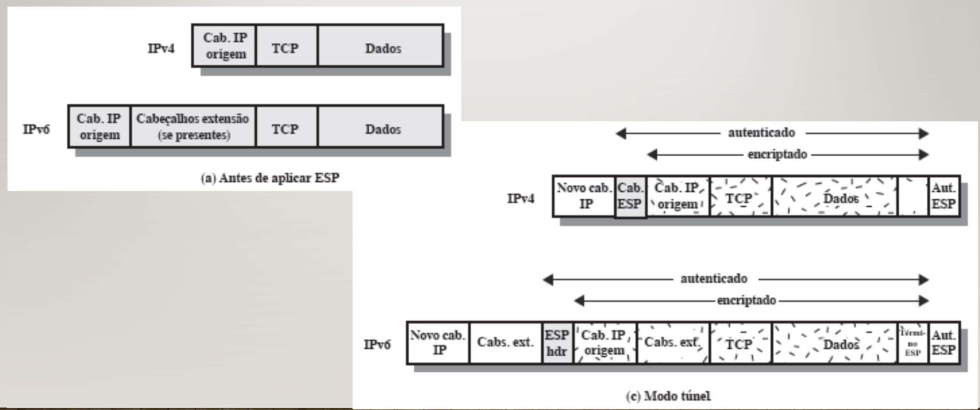
nele.

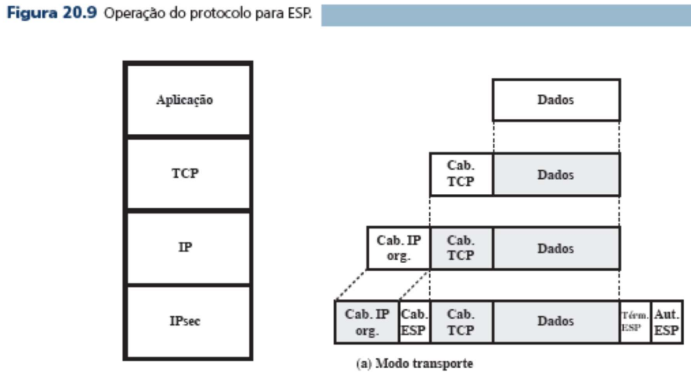
* Se um relacionamento pareado for necessário para a troca segura em duas vias, então duas associações de segurança são exigidas.
* Uma associação de segurança é identificada exclusivamente por três parâmetros:
  + Security Parameters Index (SPI): uma string de 32 bits atribuída a essa SA e tendo significado apenas local. O SPI é transportado nos cabeçalhos AH e ESP para permitir que o sistema receptor selecione a SA sob a qual um pacote recebido será processado;
  + Endereço IP de destino: atualmente, apenas endereços unicast são permitidos; esse é o endereço da extremidade de destino da SA, que pode ser um sistema de usuário final ou um sistema de rede;
  + Security Protocol Identifier (SPI): este campo do cabeçalho IP externo indica se a associação é uma associação de segurança AH ou ESP.

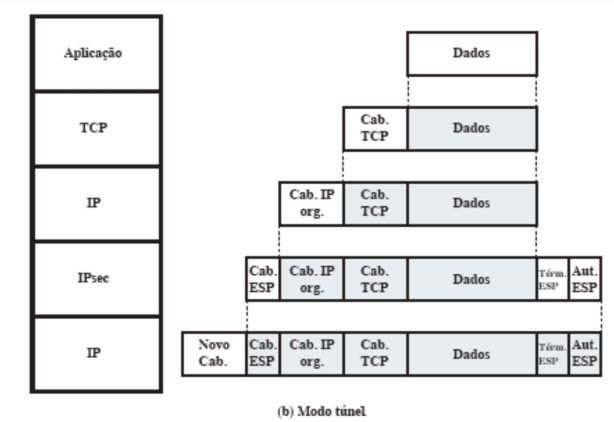
ESP pode ser usado para fornecer confidencialidade, autenticação da origem de dados,

integridade sem conexão, um serviço antirreplicação (uma forma de integridade de

sequência parcial) e confidencialidade (limitada) de fluxo de tráfego.







* VPNs podem ser estabelecidas nas camadas 2 ou 3:
* Tunelamento em Nível 2 - Enlace - (PPP sobre IP): permite transportar protocolos de nível 3, tais como o IP e IPX na Internet.
* Tunelamento em Nível 3 - Rede – Uso de IPSec.
* Para otimizar o uso dos endereços IPv4, dividiu-se os endereços em dois grupos: endereços públicos e endereços privados/privativos.
* Endereços privados: somente tem significado para equipamentos pertencentes aquela rede, ou seja, não tem validade na Internet.
* Endereços públicos: aqueles que são acessíveis e roteáveis na Internet.
* Nossa rede interna, utiliza os endereços privados nos dispositivos internos. O roteador recebe um endereço privado na interface interna e um endereço público na interface externa;

\* NAT - pega endereço público e traduz para um IP privado (normalmente no

Roteador ou Firewall).

* Existe o que chamamos de Backup Quente e Backup Frio:
* Backup Quente: cópias feitas sem interrupção do uso do sistema.
* Backup Frio: cópias feitas offline para recuperação futura caso necessária.

Uma boa estratégia de backup combina os dois tipos de ações, identificando as ações a serem tomadas para a continuidade do negócio.

Métodos de Backup Quente:

RAID (Redundant Array of Independent Disks) é um sistema de armazenamento inteligente que consolida múltiplos discos rígidos para fornecer mais performance, segurança e contingência nos dados empresariais.

Métodos de Backup Frio:

Podem ser de diversos tipos e a cópia pode ser feita em diferentes tipos de mídias que apresentarão diferenças no tempo de cópia, de recuperação e custo da mídia.

É importante que as mídias sejam armazenadas em locais diferentes para não comprometer as cópias em caso de incidentes no local onde se encontra o sistema em operação.

**Grupo de trabalho X Domínio:**

Domínio: área de gestão lógica para gerenciamento de equipamentos e usuários.

Grupos de trabalho: subdivisões do domínio.

* Com o uso de domínios, é possível definir e aplicar regras que valerão para todos os dispositivos e usuários que fazem parte do mesmo;
* O uso de domínio permite que todos os usuários que pertencem ao mesmo efetuem login em qualquer um dos computadores disponíveis sem que seja necessária a criação de uma conta local previamente.
* O controle de acesso físico aos equipamentos que proveem a infraestrutura básica do ambiente também é muito importante.
  + Equipamentos como switches, roteadores, firewall, proxy devem estar armazenados em local bem refrigerado, sem contato com umidade e acessíveis apenas às pessoas autorizadas.
* Um dos pontos mais importantes para uma rápida recuperação de rede, é a manutenção de uma documentação de topologia física e lógica atualizada.
  + Esse tipo de documentação permite uma rápida atuação em caso de erros pontuais, facilitando o reparo onde necessário.

**Gerência de erros e falhas**

Necessidade de monitoração e controle do universo de dispositivos que compõem as redes de comunicação.

Em função dessa necessidade, foram criados dois padrões de gerenciamento:

* SNMP (Simple Network Management Protocol): também chamado de Modelo Internet, possui uma abordagem genérica, podendo gerenciar diferentes tipos de sistemas, bastando apenas possuir alguns componentes elementares.
* OSI (Open Systems Interconnection): pertencente a ISO, baseia-se na teoria da orientação a objetos. Pela sua complexidade, e pela lentidão do processo de padronização, ele não é muito popular.
  + Sistema representa os recursos gerenciados através de entidades lógicas, as quais recebem a denominação de objetos gerenciados.
  + Provê uma arquitetura de gerenciamento capaz de atender à diversidade de equipamentos da rede.

**Sistema e Protocolo SNMP**

Os elementos básicos que compõem o sistema são:

* Estação de Gerenciamento: serve como interface para o gerente humano; nela são concentradas as informações enviadas pelos agentes;
* Agente de Gerenciamento: responde às solicitações de informações e de ações da estação de gerenciamento e deve também prover, assincronamente, informações importantes que não foram solicitadas por esta estação;
* Base de Informações Gerenciais (MIB): Os recursos a serem gerenciados são representados como objetos, e a coleção objetos é referenciada como MIB;
* Protocolo de Gerenciamento de Redes: o protocolo SNMP provê comunicação entre a estação de gerenciamento e o agente;
* Objeto Gerenciado: É a visão abstrata de um recurso real do sistema. Todos os recursos da rede que devem ser gerenciados são modelados e as estruturas de dados resultantes são os objetos gerenciados.
* MIB (Management Information Base): É o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede, possibilitando assim, a automatização de grande parte das tarefas de gerência;

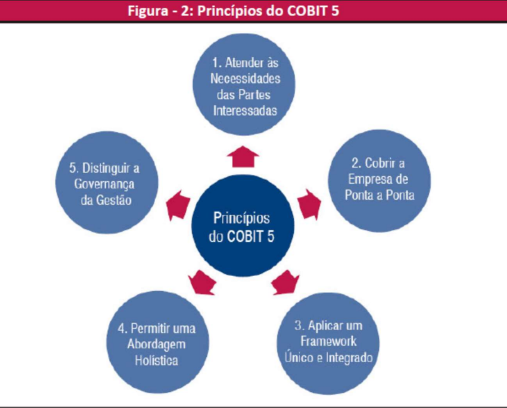
**Ainda sobre o Protocolo SNMP**

* Define mensagens, unidades de dados chamadas PDU (Protocol Data Unit), para serem trocadas durante uma comunicação entre o gerente e o agente;
* Gestão x Governança:
  + Governança: implementação de soluções TI na empresa.
  + Gestão: "Dia-a-dia" dos processos.
* Utiliza o protocolo de transporte UDP;
* É um protocolo não orientado a conexão, sendo cada troca de mensagens uma transação diferente entre o agente e a estação de gerenciamento;
* Para que um dispositivo seja gerenciável, ele precisa possuir uma MIB e ter suporte ao protocolo SNMP;

**Cobit5**

**(Control Objectives for Information and Related Technology)**

* Atualmente está na versão 5 – COBIT5;
* Fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI, ou seja, auxilia as organizações a criar valor por meio da TI mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos;
* Permite que a TI seja governada e gerida de forma holística para toda a organização, abrangendo o negócio de ponta a ponta bem como todas as áreas responsáveis pelas funções de TI, levando em consideração os interesses internos e externos relacionados com TI;
* O COBIT 5 é genérico e útil para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas.



* Juntos, esses cinco princípios permitem que a organização crie um modelo eficiente de governança e gestão otimizando os investimentos em tecnologia da informação e seu uso para o benefício das partes interessadas;
* A visão do COBIT 5 sobre esta importante distinção entre governança e gestão é:
  + Flexibilidade (permite uso de outros frameworks e/ou normas) entre governança e gestão. É um framework, não apenas um conjunto de práticas. É correlato com a ISO/IEC 27000
* Governança: garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.
* Gestão: é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos.
* Princípios:
  + Entende a necessidade da empresa (governança);
  + Cobrir a empresa de ponta a ponta;
  + Aplicar framework único e integrado;
  + Abordagens holísticas;
  + Distinguir as estruturas da empresa.
* Objetivos do COBIT5 em cima das necessidades:
  + Criação de valor para a organização através do uso eficiente e inovador de TI da organização;
  + Satisfação dos usuários de negócio com os serviços de TI;
  + Cumprimento das leis, regulamentos, acordos contratuais e políticas internas pertinentes;
  + Uma melhoria das relações entre as necessidades corporativas e os objetivos de TI.
* Objetivos de habilitador: Conjunto de ações para se atingir os objetivos de TI e sua monitoração (o que fazer? Por que fazer? O que se espera? Como medir?).
* Cascata de objetivos -> processo
* Perguntas das Partes Interessadas Internas (têm a ver com o ciclo PDCA).

.

* Com o tempo, o ciclo de vida deve ser seguido de forma interativa paralelamente à criação de uma abordagem sustentável para a governança e gestão de TI da organização

**Ciclos de vida**

Entender os problemas e quais atitudes tomar para sua solução, levando em consideração quem fará isto.

**Itil**

**v3 e v4**

* É princípio básico de uma organização buscar a gerência dos seus processos internos e também a forma de comunicação destes processos com os seus fornecedores e parceiros de negócios, que podemos chamar de processos externos à organização.
* Isso visa identificar as interfaces entre esses processos, as responsabilidades das áreas da empresa, das pessoas e o desempenho esperado medido por indicadores e metas.
* Na maioria dos casos, tendo as interfaces definidas, as responsabilidades claras entre as áreas e a mensuração do desempenho, as empresas conseguem alcançar o objetivo final que é a melhoria dos serviços devido aos ganhos de produtividade e diminuição de retrabalho além de otimização dos processos.
* O problema que se apresenta é justamente que a melhoria e evolução dos processos não tem fim, pois os negócios podem ser sempre melhorados nos requisitos de organização, eficiência e grau de automação.
* Tem como foco principal a operação e a gestão da infraestrutura de tecnologia na organização, incluindo todos os assuntos que são importantes no fornecimento dos serviços de TI. Nesse contexto, o ITIL considera que um serviço de TI é a descrição de um conjunto de recursos de TI. Os serviços de suporte ITIL auxiliam no atendimento de uma ou mais necessidades do cliente, apoiando, desta forma, aos seus objetivos de negócios.
  + O princípio básico do ITIL é o objeto de seu gerenciamento: a infraestrutura de TI. Ele descreve os processos que são necessários para dar suporte à utilização e ao gerenciamento da infraestrutura de TI;
  + Outro princípio fundamental do ITIL é o fornecimento de qualidade de serviço aos clientes de TI com custos justificáveis, isto é, relacionar os custos dos serviços de tecnologia e como estes trazem valor estratégico ao negócio.
* Gerenciamento de Infraestrutura de TIC:
* Estes processos cobrem todos os aspectos de gerenciamento de infraestrutura de TIC desde a identificação dos requisitos do negócio, passando pelo projeto e implantação até o suporte e manutenção dos componentes desse cenário. Os principais processos são:
  + Projeto e Planejamento: relacionados com a criação e melhoria da solução TIC;
  + Implantação: relacionado com a implantação da solução TIC e/ou de negócio conforme planejado e com o impacto mínimo nos processos de negócio;
  + Operação: refere-se à operação e à manutenção diária da infraestrutura de TIC;
  + Suporte Técnico: refere-se à estruturação e sustentação de outros processos para garantir os serviços implantados.
* Gerenciamento de Serviços:
* O objetivo aqui é certificar-se que os serviços de TI estão alinhados com as necessidades do negócio da empresa. Podemos subdividir esses processos em dois grupos: entrega de serviços e suporte de serviços.
* Os processos de entrega de serviços estão relacionados com a provisão de entrega de serviços aos usuários e encontram-se descritos em uma tabela.
* Os processos de suporte de serviços estão relacionados com a provisão de suporte aos serviços que sustentam o negócio da empresa e encontram-se descritos em uma tabela.

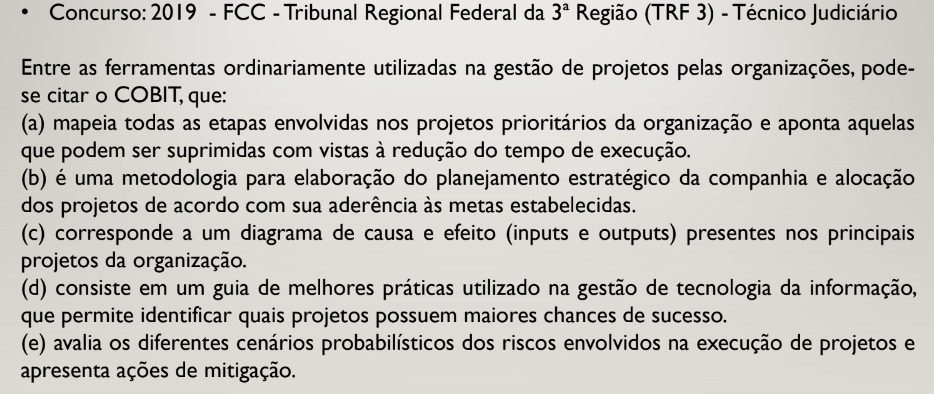
**Ainda sobre o ITIL**

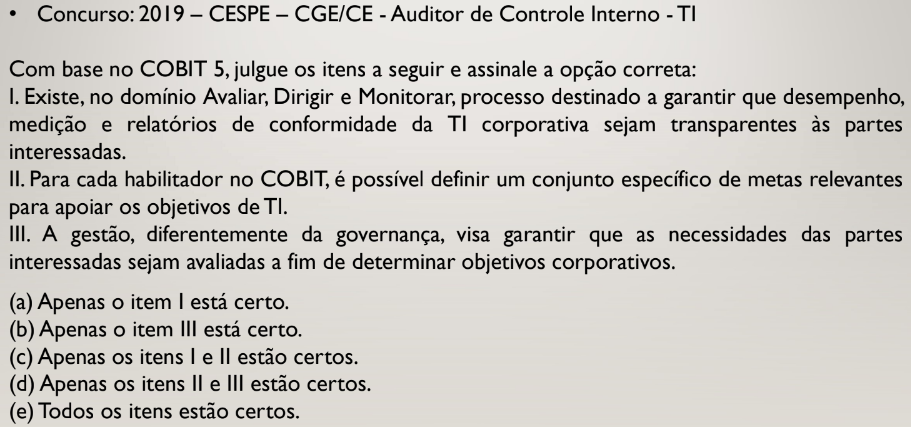
* É mais voltado para Gestão de TI, pensando em todas as etapas do processo a fim de melhorar os serviços.
* O ITILv3 é organizado em cinco elementos conhecidos como Ciclo de Vida de Serviço, cada uma com sua função específica. Os elementos são:
  + Estratégia de Serviço, define as características principais da organização e de seus serviços;
  + Design de Serviço, fornece orientação para a concepção e desenvolvimento de serviços que atenderão aos objetivos da empresa;
  + Transição de Serviço, fornece um guia para a transição de um serviço novo ou modificado em um serviço pronto para ser lançado;
  + Operação de Serviço, foca na entrega e na manutenção do serviço;
  + Aperfeiçoamento Contínuo de Serviço que cuida das práticas para avaliar e melhorar a qualidade dos serviços.
* É voltado para processos. Tinha estrutura mais estática.
* O modelo que estudamos até o momento é compatível com a versão 3 dessa biblioteca (ITILv3). Porém no mercado atualmente está sendo aplicada a versão 4 (ITILv4);
  + A nova versão (ITILv4) procura rever as boas práticas frente às mudanças tecnológicas e no mercado de trabalho;
  + Pela mudança no tratamento dos dados, é voltado para agregar valor aos projetos.
  + Acordo de Nível de Serviço (ANS ou SLA): combinado entre a parte solicitante e a contratada. Depende do produto.
  + Gestão de pessoas também se faz importante.
* Componentes do ITIL
  + Modelo de 4 dimensões para o gerenciamento de serviços:
    - Organizações e pessoas;
    - Informação e tecnologia;
    - Parceiros e fornecedores (ponto que diferencia dos outros frameworks);
    - Fluxos de valor e processos.

**Método ágil:**

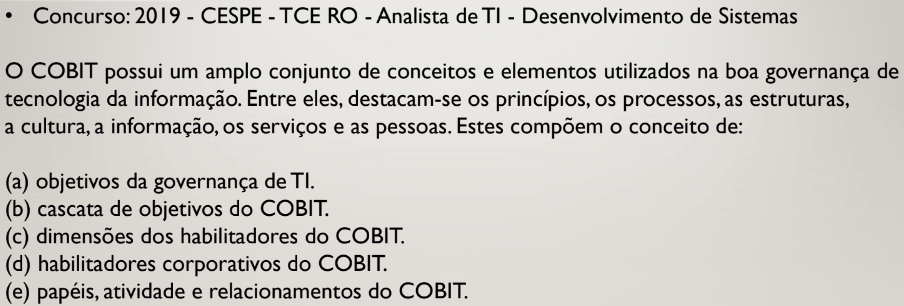
Solução para o método de cascata. Onde para eventuais surgimentos de problemas, as soluções só podem agir no fim do ciclo de vida.

* Quando o assunto é gestão e inovação, a metodologia ágil está no topo das tendências;
* Metodologia ágil é um conjunto de técnicas e práticas para gestão de projetos que oferece mais rapidez, eficiência e flexibilidade. Seu objetivo inicial era agilizar o desenvolvimento de softwares, mas esses métodos extrapolaram o setor de tecnologia e hoje revolucionam a gestão de empresas de todas as áreas;
* Basicamente, a metodologia ágil torna os processos mais simples, dinâmicos e iterativos, da concepção da ideia até o produto final;
* O conceito de metodologia ágil consiste nas correções de erros e melhorias continuas.
* Valores da Metodologia Ágil:
  + 1 - Indivíduos e interações mais que processos e ferramentas: comunicação é fundamental;
  + 2 - Software em funcionamento mais que documentação abrangente: software em pleno funcionamento é indicativo de ação e resultado;
  + 3 - Colaboração com o cliente mais que negociação de contratos: Entender as demandas do cliente. O mesmo empenho nos contratos deve ser aplicado ao cliente;
  + 4 - Responder a mudanças mais que seguir um plano: ajuste no plano de acordo com as novas necessidades. Permite interromper os processos para melhorias.
* FDD - Feature Driven Davelopmnet
  + Foco no desenvolvimento e em fases;
  + Cada atividade tem um responsável, para diminuir ramificações;
  + Planejamento incremental;
  + Desenvolvimento baseado nos requisitos funcionais do sistema;
  + Controle de qualidade em todas as fases do projeto;
  + Testes de software contínuos.
* XP - Extreme Programming
  + Agilidade no desenvolvimento da solução;
  + Economia de recursos;
  + Qualidade do produto final;
  + Equipe baseada em valores para que as atitudes e comportamentos (soft skills) levem ao sucesso do projeto

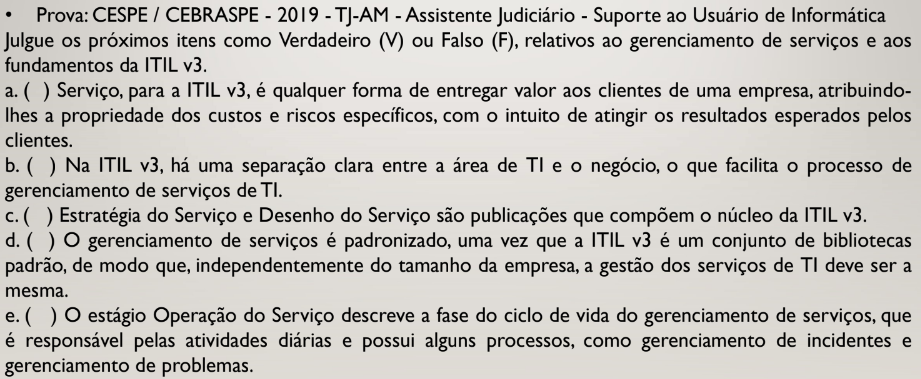
Gabarito: C.



Gabarito: C.



Gabarito: D.



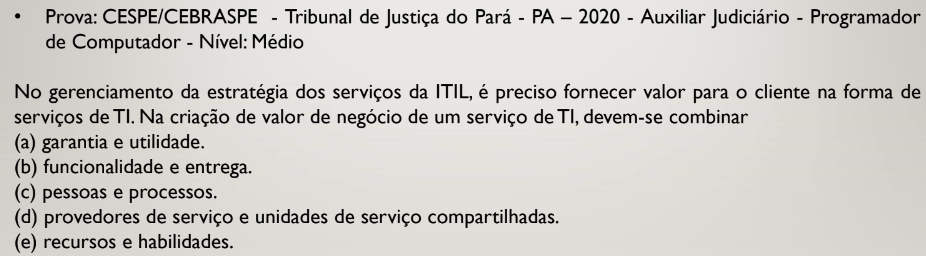
Resposta:

F.

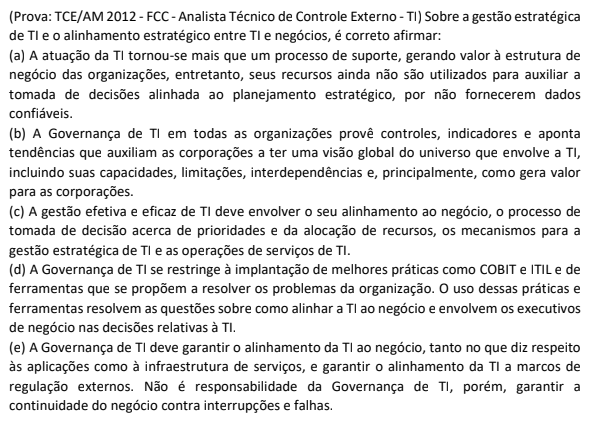
F.

V.

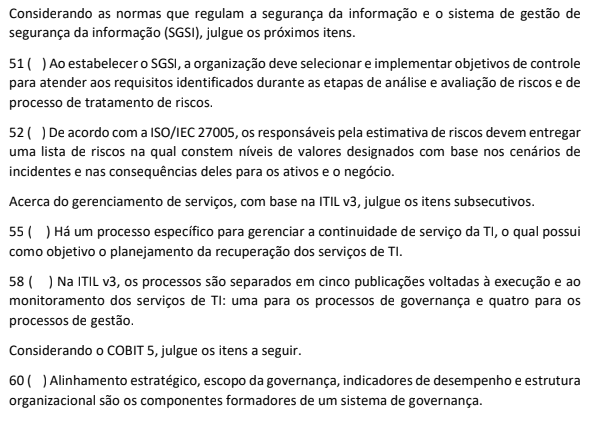
F.

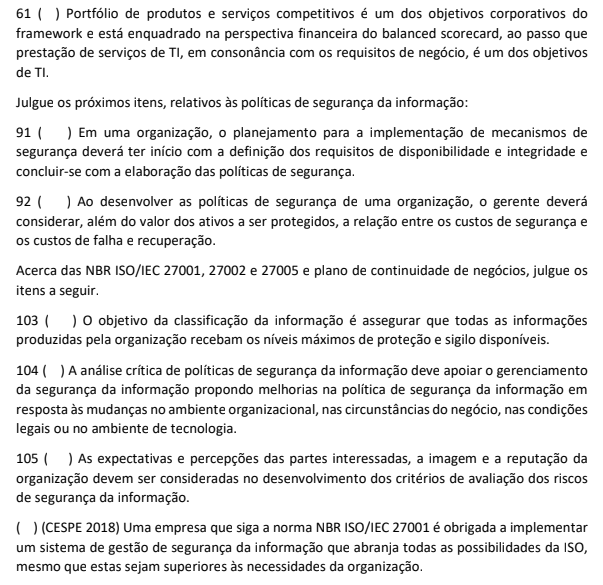
V.

Gabarito: A.



Gabarito: C.





Resposta:

V || V || V || F || F || V ||

F || V || F || V || V || F ||