Segurança da Informação

Prof. Me. Wallace Rodrigues de Santana

www.neutronica.com.br

Atribuição-NãoComercial-CompartilhaIgual 3.0 Brasil (CC BY-NC-SA 3.0)

Você tem a liberdade de:

Compartilhar — copiar, distribuir e transmitir a obra.

Remixar — criar obras derivadas.

Sob as seguintes condições:

Atribuição — Você deve creditar a obra da forma especificada pelo autor ou licenciante (mas não de maneira que sugira que estes concedem qualquer aval a você ou ao seu uso da obra).

Uso não comercial — Você não pode usar esta obra para fins comerciais.

Compartilhamento pela mesma licença — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Ficando claro que:

Renúncia — Qualquer das condições acima pode ser **renunciada** se você obtiver permissão do titular dos direitos autorais.

Domínio Público — Onde a obra ou qualquer de seus elementos estiver em **domínio público** sob o direito aplicável, esta condição não é, de maneira alguma, afetada pela licença.

Outros Direitos — Os seguintes direitos não são, de maneira alguma, afetados pela licença:

- Limitações e exceções aos direitos autorais ou quaisquer **usos livres** aplicáveis;
- Os **direitos morais** do autor;
- Direitos que outras pessoas podem ter sobre a obra ou sobre a utilização da obra, tais como **direitos de imagem** ou privacidade.

Aviso — Para qualquer reutilização ou distribuição, você deve deixar claro a terceiros os termos da licença a que se encontra submetida esta obra. A melhor maneira de fazer isso é com um link para esta página.

Módulo Zero

Apresentação da Disciplina

Objetivo geral

Capacitar os alunos na compreensão dos vários tipos de sistemas de segurança e proteção de sistemas, auditoria de sistemas e seus objetivos principais.

Objetivos específicos

- Identificar a importância da segurança computacional e o cenário atual;
- Conhecer o invasor através do estudo das principais formas de ataque;
- Conhecer as principais formas de proteção aos dados e aos recursos computacionais;
- Compreender a importância do estabelecimento de uma política de segurança;
- Identificar a necessidade de equipes de segurança e do administrador de segurança nas organizações;
- Discutir os aspectos legais e éticos no estabelecimento de segurança computacional;
- Analisar logs e estabelecer as melhores formas de mantê-lo para análises futuras;
- Auditoria em sistemas e computadores.

Módulos

PARTE I

1. Introdução à Segurança da Informação
2. Segurança e Governança
3. Melhores Práticas de Governança
4. Melhores Práticas de Entrega de Serviços
5. Guia para Certificação de Sistemas de Gestão de Segurança da Informação
6. Melhores Práticas de Segurança da Informação

Módulos

PARTE II

7. ISO/OSI Network Management Framework
8. Simple Network Management Protocol
9. Serviço de Diretório
10. Análise e Avaliação de Riscos
11. Plano de Continuidade do Negócio
12. Plano de Recuperação de Desastres

Módulos

PARTE III

13. Técnicas de Invasão, Análise e Gestão de Vulnerabilidades
14. Criptografia, Certificados Digitais e Public Key Infrastructure
15. Proteção de Redes de Computadores
16. Análise de Logs e Ferramentas de Monitoração
17. Auditoria
18. Return on Security Investiment

Módulo 1

Introdução à Segurança da Informação

Motivação

Redes de computadores nas primeiras décadas de existência eram usadas para fins acadêmicos ou para compartilhamento de recursos. Segurança não era uma prioridade.

Popularização da Internet e de outras tecnologias permitem o uso muito mais frequente de redes, com um grande incremento no número de usuários. Segurança passa a ser uma prioridade.

Fonte: TANENBAUM, A. S.; WETHERALL, D. Redes de Computadores. 5ª. ed. São Paulo: Pearson Prentice Hall, 2011.

O que é segurança?

De acordo com o **Dicionário Houaiss**:

1. ação ou efeito de tornar seguro; estabilidade, firmeza, seguração
2. ação ou efeito de assegurar e garantir alguma coisa; garantia, fiança, caução
3. estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais, afastada de todo mal
4. estado, condição ou caráter daquilo que é firme, seguro, inabalável, ou daquele com quem se pode contar ou em quem se pode confiar inteiramente
5. situação em que não há nada a temer; a tranquilidade que dela resulta
6. conjunto de processos, de dispositivos, de medidas de precaução que asseguram o sucesso de um empreendimento, do funcionamento preciso de um objeto, do cumprimento de algum plano, etc.
7. etc.

O que proteger?

De acordo com a ISO/IEC 27002:2005, **ativos alvo** de uma política de **segurança da informação** podem ser de vários tipos, incluindo:

a) **ativos de informação**: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

b) **ativos de *software***: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

c) **ativos físicos**: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

d) **serviços**: serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração;

e) **pessoas e suas qualificações**, habilidades e experiências;

f) intangíveis, tais como a **reputação e a imagem da organização**.

Fonte: NBR ISO/IEC 27002:2005

Por que proteger-se?

"A arte da guerra ensina-nos a não confiar na probabilidade do inimigo não vir, mas sim na nossa prontidão para recebê-lo; não na chance dele não atacar, mas no fato de termos feito nossa posição não assediável."

Sun Tzu, A Arte da Guerra

Definição ISO/IEC

O que é Segurança da Informação?

Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio*.

Como a Segurança da Informação é alcançada?

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware***.

Fontes: *NBR ISO/IEC 27002:2005 e **NBR ISO/IEC 27002:2013

O que é um sistema seguro?

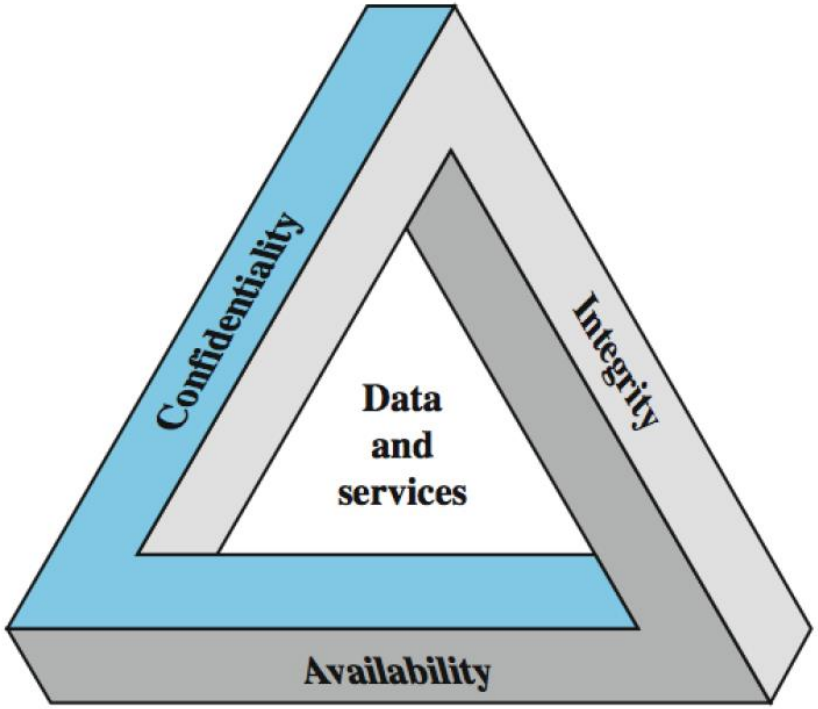
Sistema Seguro é todo sistema composto por pessoas, processos e tecnologia, que tem a capacidade de fornecer informações íntegras a todo usuário devidamente autenticado e autorizado no momento em que elas são solicitadas, sempre por meio de requisições válidas, identificadas e rastreáveis, impedindo que terceiros não autorizados interceptem, observem ou alterem estas mesmas informações.

Serviços básicos de segurança

NIST	ITU-T	Donn B. Parker
• Confidencialidade • Integridade • Disponibilidade	• Autenticação • Controle de acesso • Confidencialidade ou Privacidade • Integridade • Irretratabilidade (não repúdio)	• Confidencialidade • Integridade • Disponibilidade • Autenticidade • Posse ou Controle • Utilidade

Serviços básicos de segurança
NIST

De acordo com Stallings, o NIST (*National Institute of Standards and Technology*) define segurança da computação como uma tríade formada pela confidencialidade, integridade e disponibilidade, também conhecida como **Tríade da Segurança**.



Serviços básicos de segurança NIST

CONFIDENCIALIDADE

Garantir o acesso às informações somente a indivíduos, entidades ou processos autorizados.

INTEGRIDADE

Proteger contra modificação ou destruição inadequada das informações.

DISPONIBILIDADE

Garantir o acesso oportuno e confiável e o uso das informações.

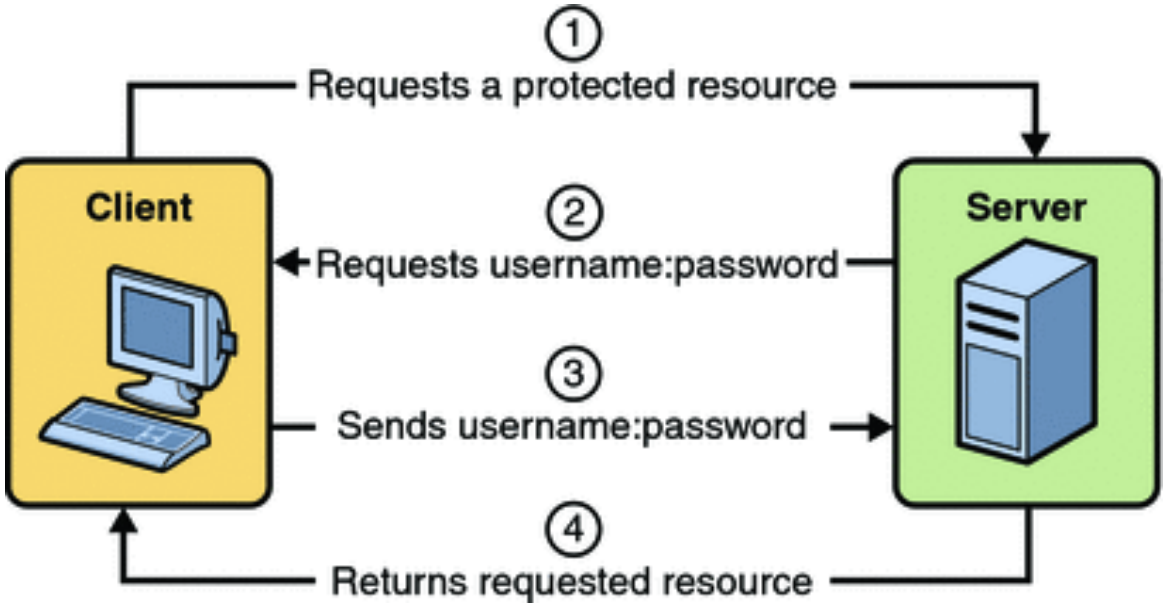
Serviços básicos de segurança ITU-T

De acordo com a Recomendação ITU-T X.800, que trata da Arquitetura de Segurança para Interconexão de Sistemas Abertos, os serviços básicos de segurança são os seguintes:

- Autenticação;
- Controle de acesso;
- Confidencialidade ou Privacidade;
- Integridade;
- Irretratabilidade (não repúdio).

Autenticação
ITU-T

A autenticação tem por objetivo garantir a identidade presumida de quem está acessando os recursos da rede.



Métodos de autenticação
ITU-T

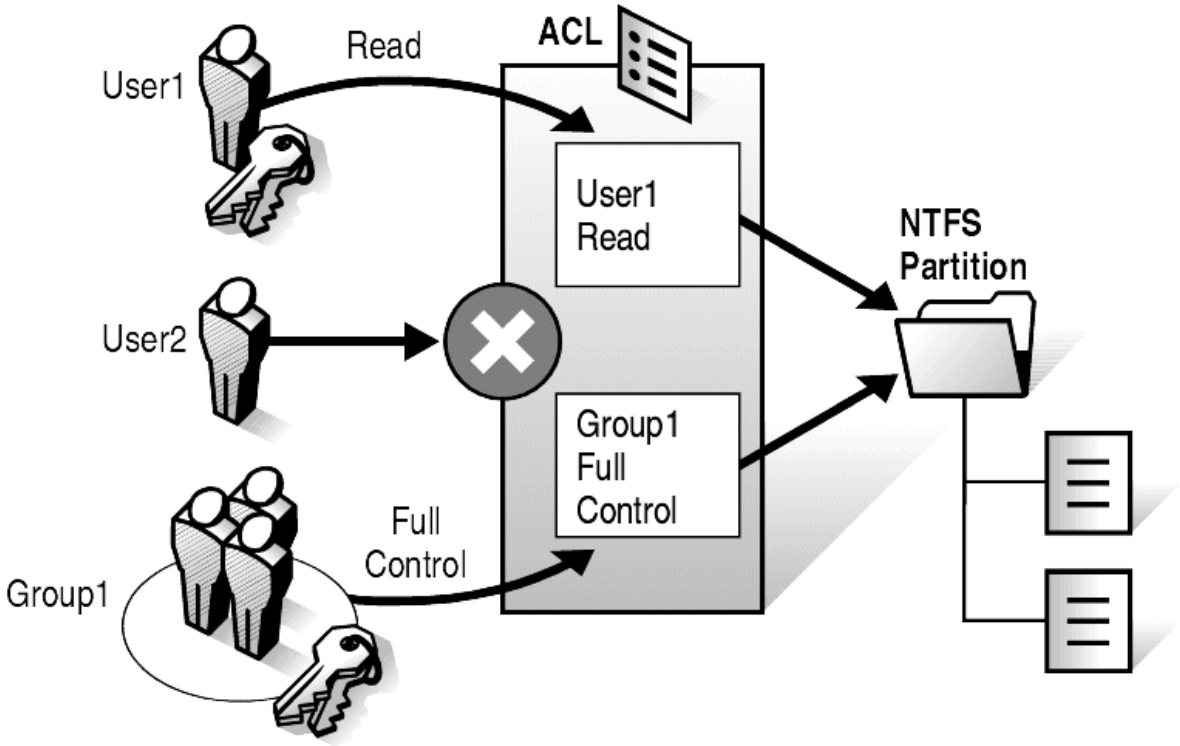
A autenticação pode ser baseada em um dos seguintes métodos:

- O que o usuário sabe (senha);
- O que o usuário tem (token);
- O que o usuário é (biometria).

A autenticação também pode ser baseada em uma combinação destes métodos.

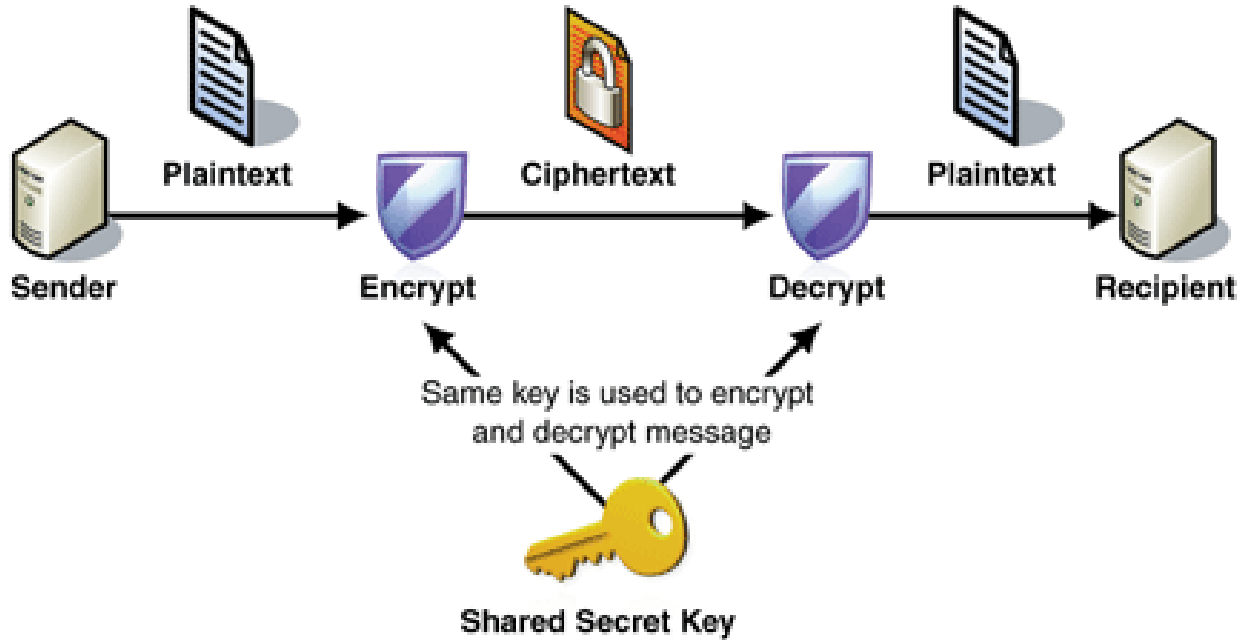
Controle de acesso
ITU-T

O controle de acesso é o mecanismo que limita o acesso a sistemas e aplicações somente a usuários autorizados.



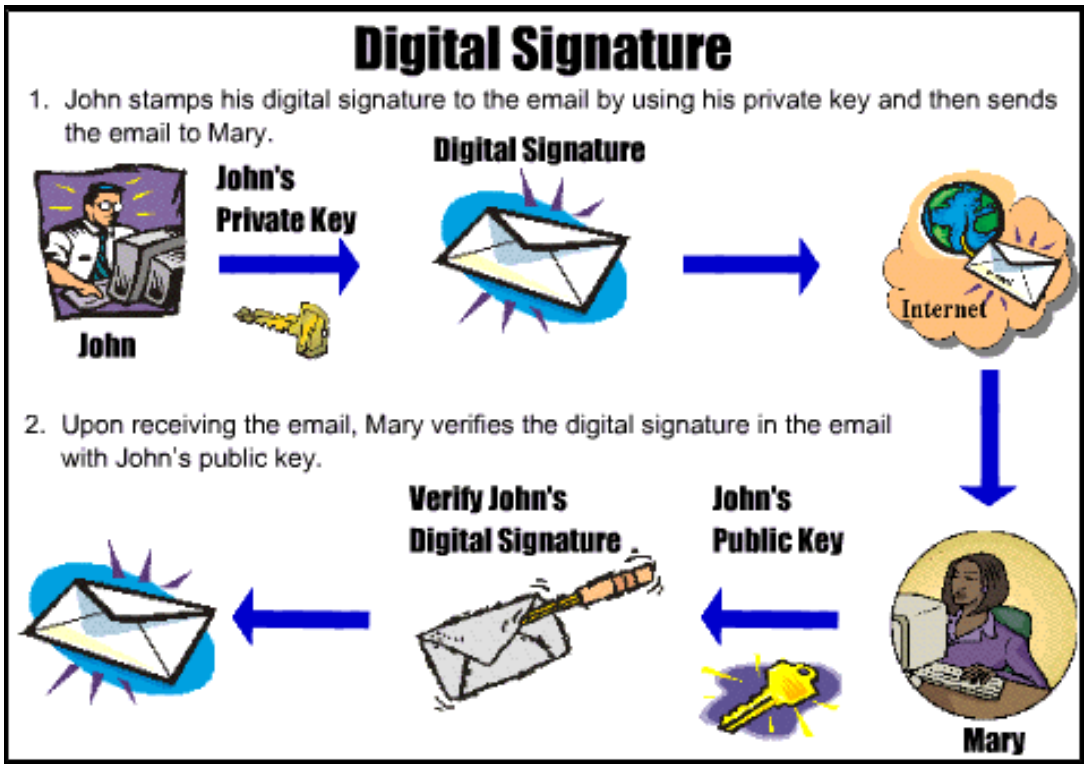
Confidencialidade
ITU-T

A confidencialidade garante que os dados ficarão protegidos contra divulgação não autorizada. Em outras palavras, impede que os dados sejam usados caso seja recuperado por terceiros.



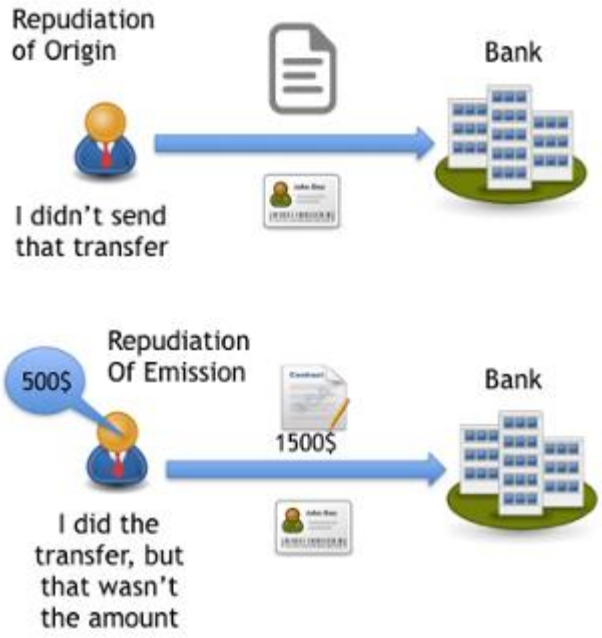
Integridade
ITU-T

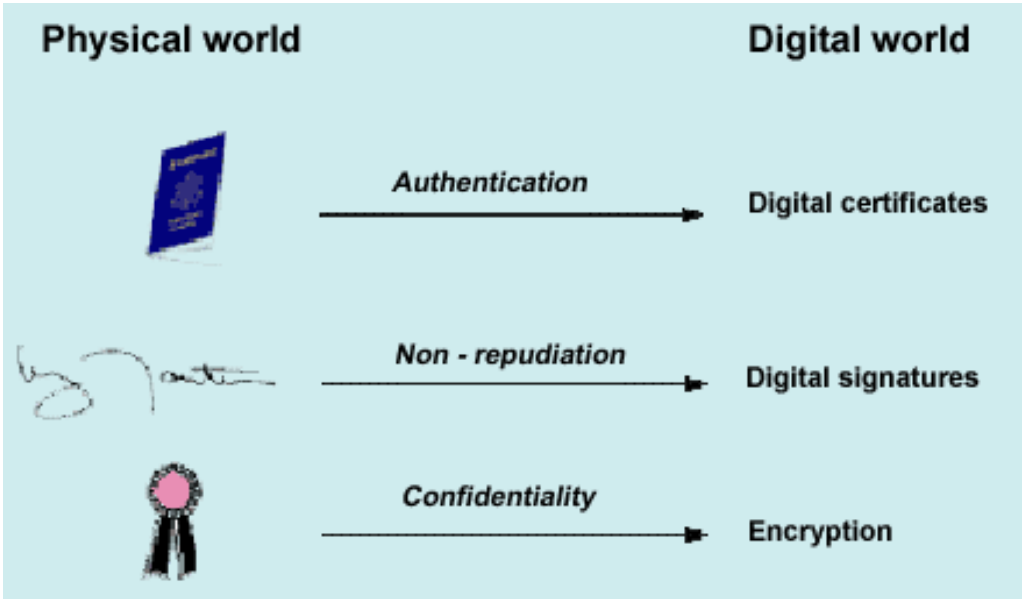
A integridade é uma garantia de que o dado ou informação não foi alterado por terceiros durante sua transmissão.



Irretratabilidade (não repúdio) ITU-T

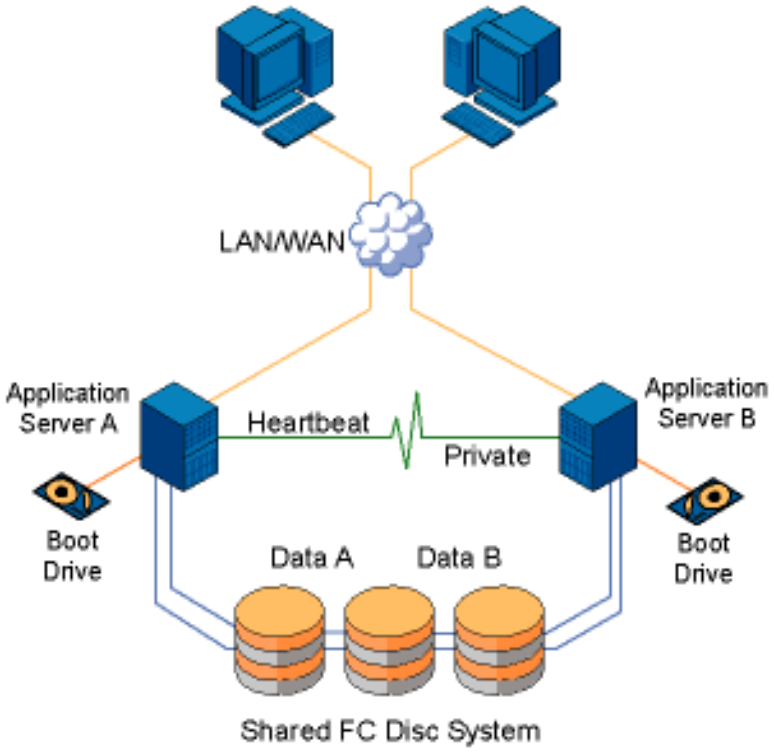
A irretratabilidade ou não repúdio impede que o emissor negue que enviou uma mensagem (irretratabilidade de origem) ou que o destinatário negue que a recebeu (irretratabilidade de destino).





Disponibilidade
ITU-T

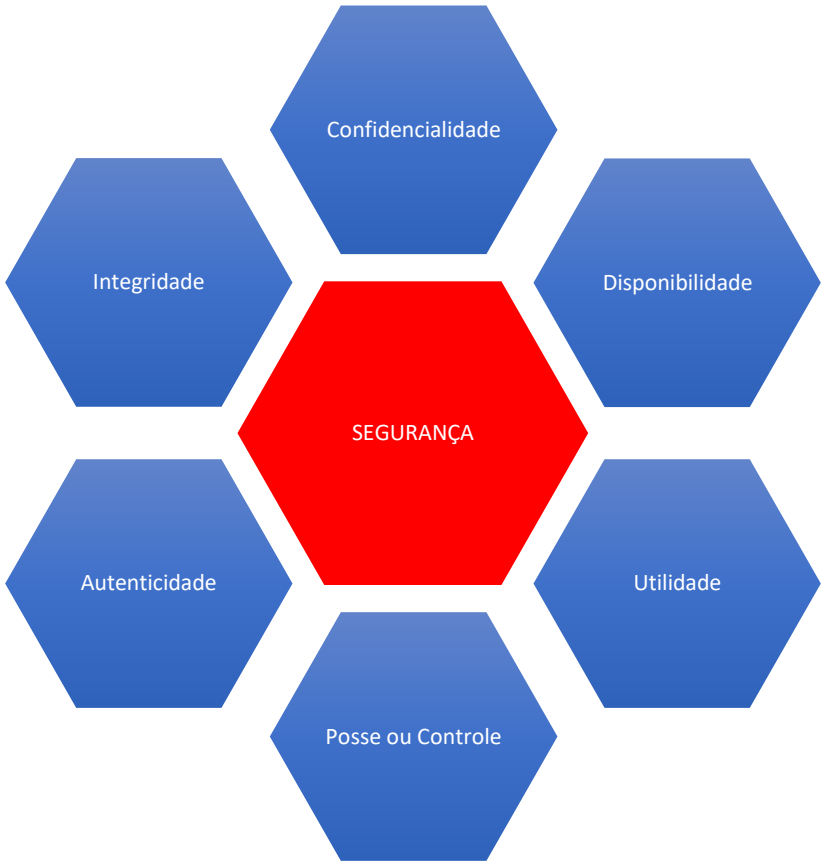
Tanto a X.800 como a RFC 2828 definem a disponibilidade como sendo a capacidade de um sistema ou recurso ser acessível a qualquer usuário autorizado a utilizá-lo.



Serviços Básicos de Segurança
Hexagrama Parkeriano

O Hexagrama Parkeriano (Parkerian Hexad) foi proposto por Donn B. Parker e visa expandir os atributos da Tríade de Segurança:

- Autenticidade – busca verificar a veracidade quanto à alegação de origem ou autoria de um dado documento ou informação, que poderia ser aferida com o uso de assinatura digital;
- Posse ou Controle – quando o dado, informação ou sistema esta na posse de quem o controle ou utiliza. Um cartão de banco roubado pode ser usado sem o consentimento de seu proprietário, que perdeu assim o controle e a posse sobre o cartão;
- Utilidade – diz respeito ao proveito que o usuário pode fazer de dados, informações ou sistemas. Um arquivo criptografado cuja chave foi perdida tem sua utilidade comprometida.



Vulnerabilidades

Vulnerabilidade é uma **fraqueza** que um ativo possui ou apresenta e que poderia ser potencialmente explorada por uma ou mais ameaças. São os elementos que, uma vez expostos e explorados pelas ameaças, afetam a confidencialidade, a integridade e a disponibilidade dos ativos.

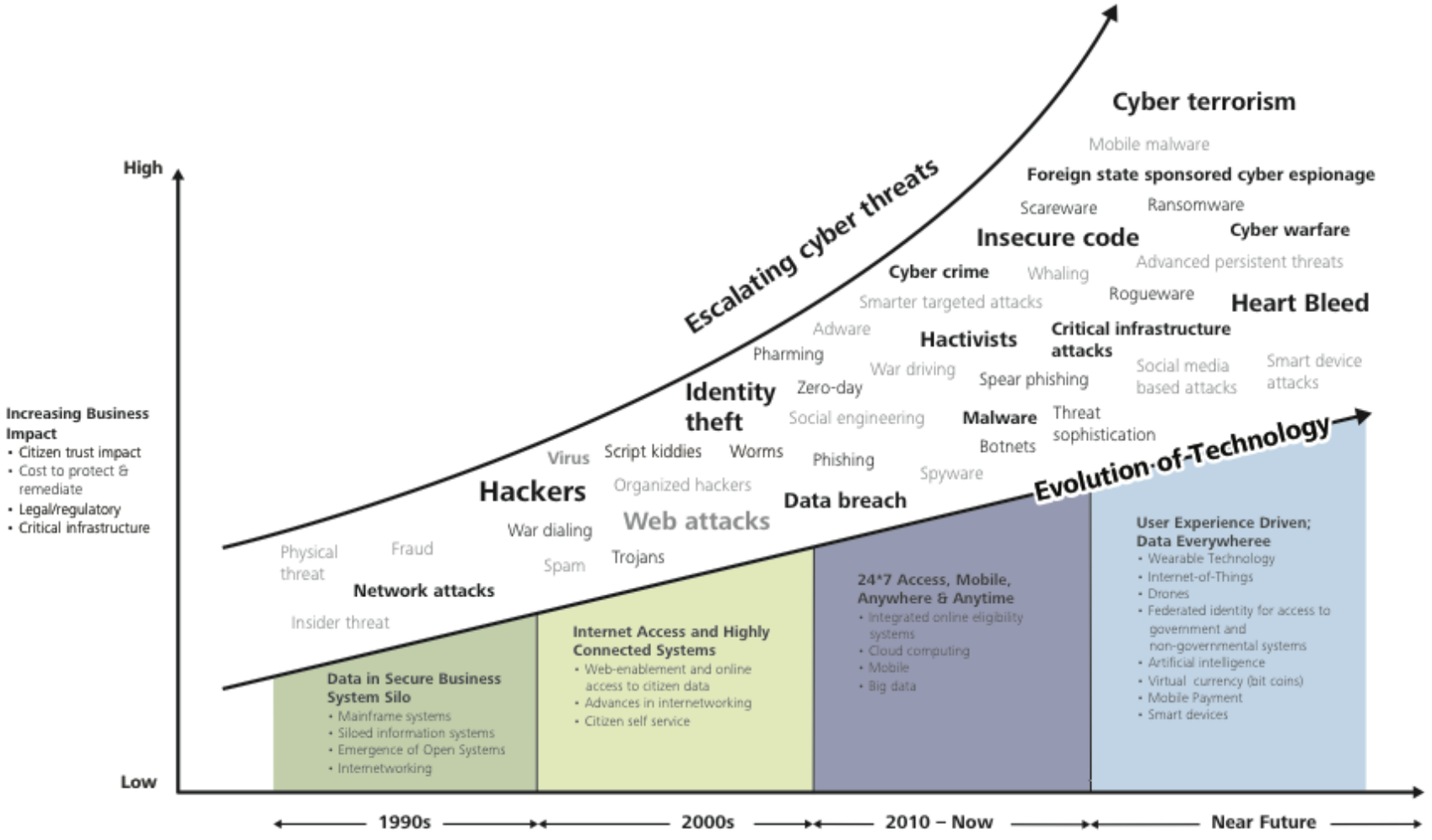
Ameaças

Ameaça é toda e qualquer **causa potencial** de um incidente indesejado que pode causar perdas e danos aos ativos da organização e afetar seus negócios.

Um sistema pode ser comprometido por ameaças do tipo:

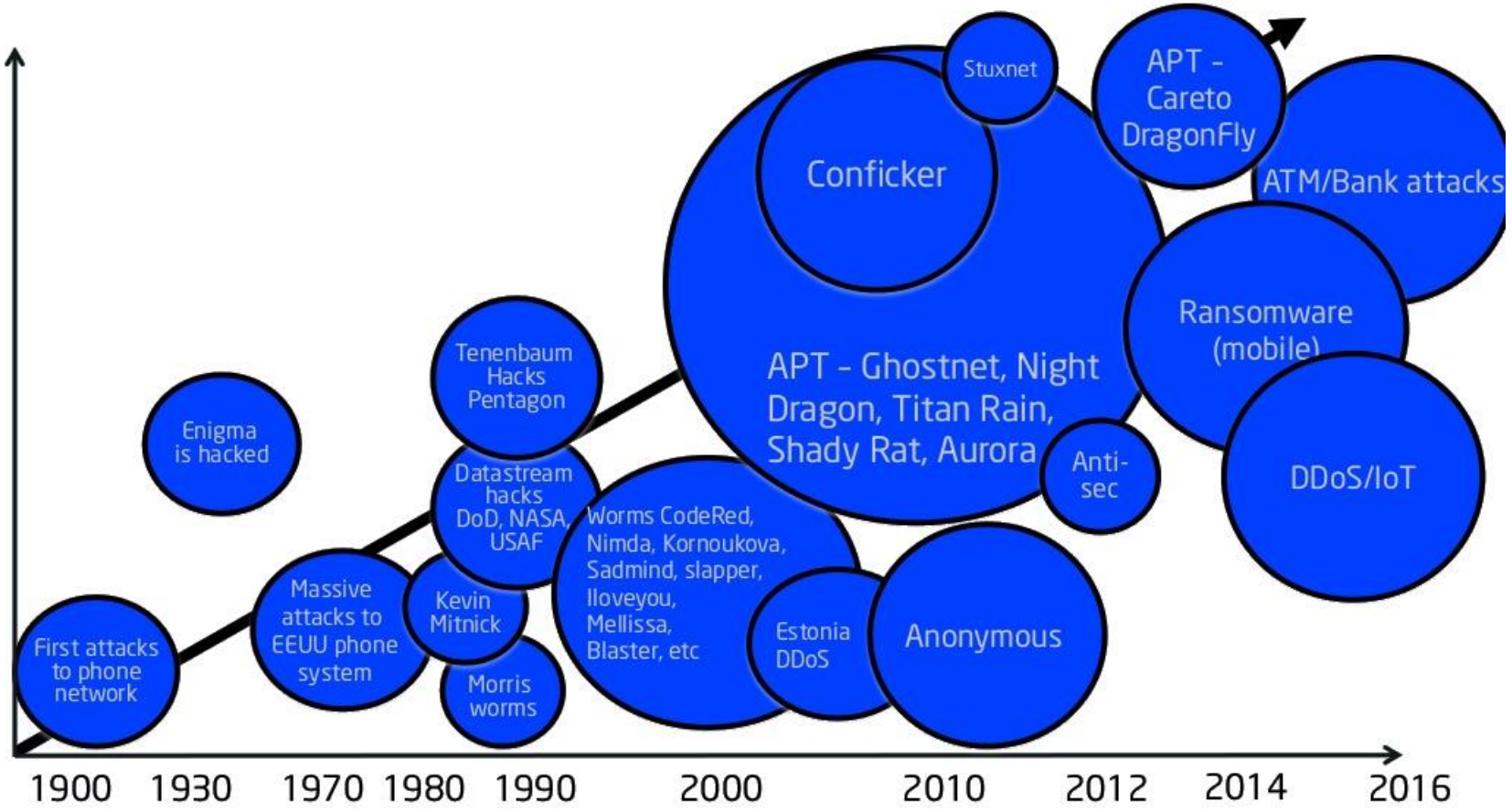
- Física;
- Lógica;
- Humana.

Escalada e evolução das ameaças cibernéticas



Fonte: Deloitte-NASCIO Cybersecurity Study, 2014

Escalada e evolução das ameaças cibernéticas



Fonte: Jorge Lopez Hernandez-Ardieta. **Cyber ranges: The (r)evolution in cybersecurity training**, 2016

Tipos de ataque

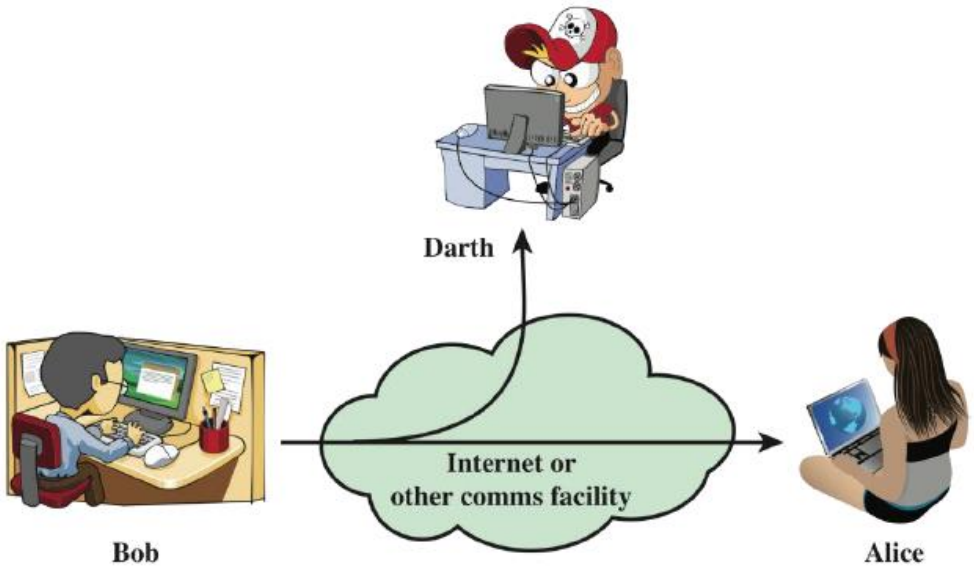
De acordo com Stallings, um meio de classificar ataques de segurança, usado tanto na X.800 quanto na RFC 4949, é em termos de ataques passivos e ataques ativos.

Um **ataque passivo** tenta aprender ou usar informações do sistema, mas não afeta os seus recursos, sendo assim mais difícil de se detectar.

Já um **ataque ativo** tenta alterar os recursos do sistema ou afetar a sua operação, sendo mais fácil de se detectar.

Ataque passivo

Os ataques passivos tem a natureza de espionagem ou de monitoramento de transmissões. O objetivo é obter informações que estão sendo transmitidas. Podem ser do tipo vazamento de conteúdo ou análise de tráfego.



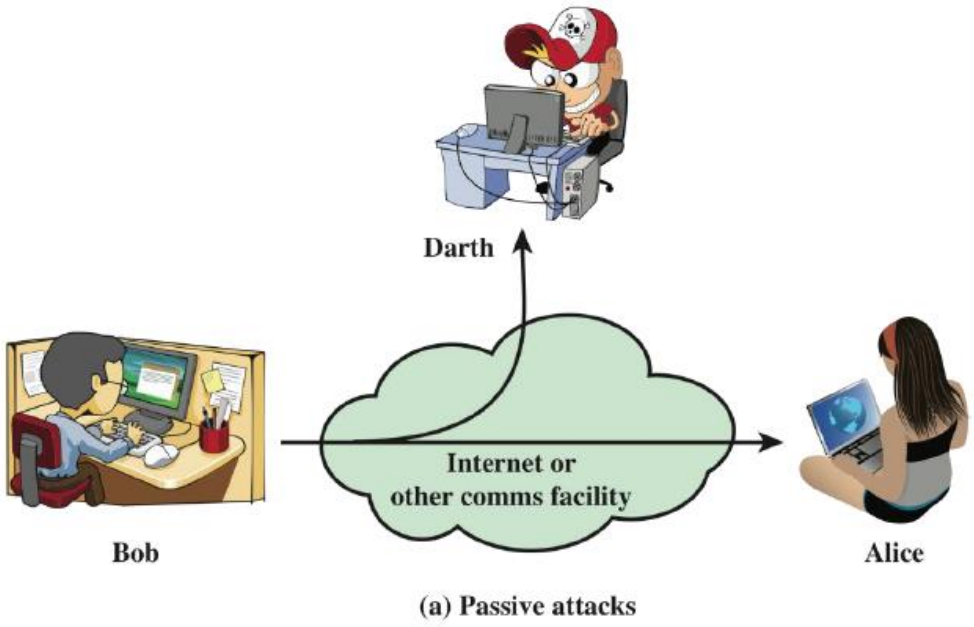
(a) Passive attacks

Fonte: Stallings

Ataque passivo – continuação

No vazamento de conteúdo o oponente procura obter informações sensíveis e confidenciais.

Na análise de tráfego o objetivo é obter o padrão de tráfego e determinar o local e a identidade dos interlocutores.

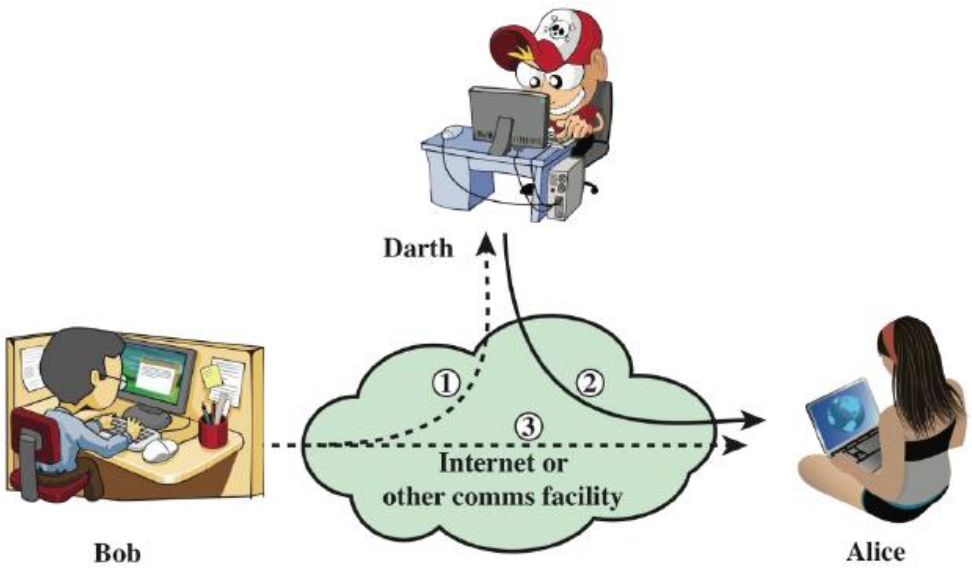


(a) Passive attacks

Fonte: Stallings

Ataque ativo

Os ataques ativos envolvem algum tipo de modificação do conteúdo ou do fluxo de dados ou a criação de um fluxo falso. Podem ser do tipo mascaramento ou disfarce (masquerade), repasse (replay), modificação de mensagens ou negação de serviço (denial of service).



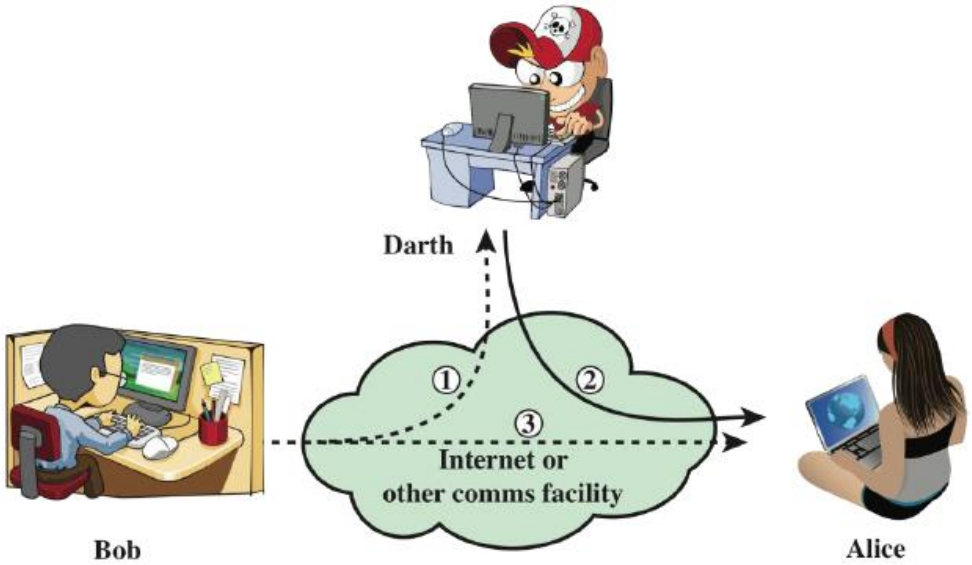
(b) Active attacks

Fonte: Stallings

Ataque ativo – continuação

O disfarce ocorre quando uma entidade finge ser outra diferente (2).

O repasse envolve a captura passiva de uma unidade de dados e sua subsequente retransmissão para produzir um efeito não autorizado (1, 2 e 3).

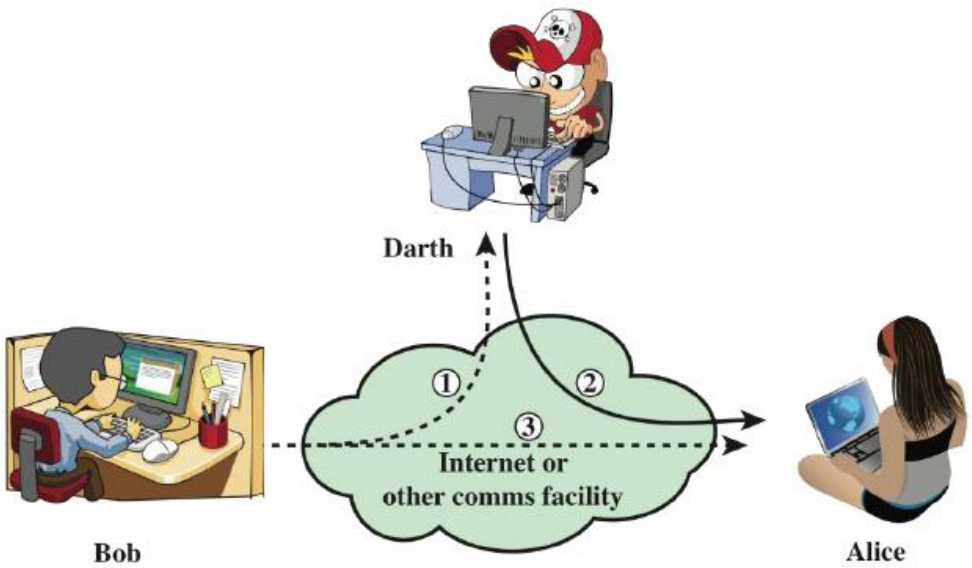


(b) Active attacks

Fonte: Stallings

Ataque ativo – continuação

A modificação de mensagens significa que parte de uma mensagem legítima é alterada, ou que as mensagens são atrasadas ou reordenadas, para produzir um efeito não autorizado (1 e 2).

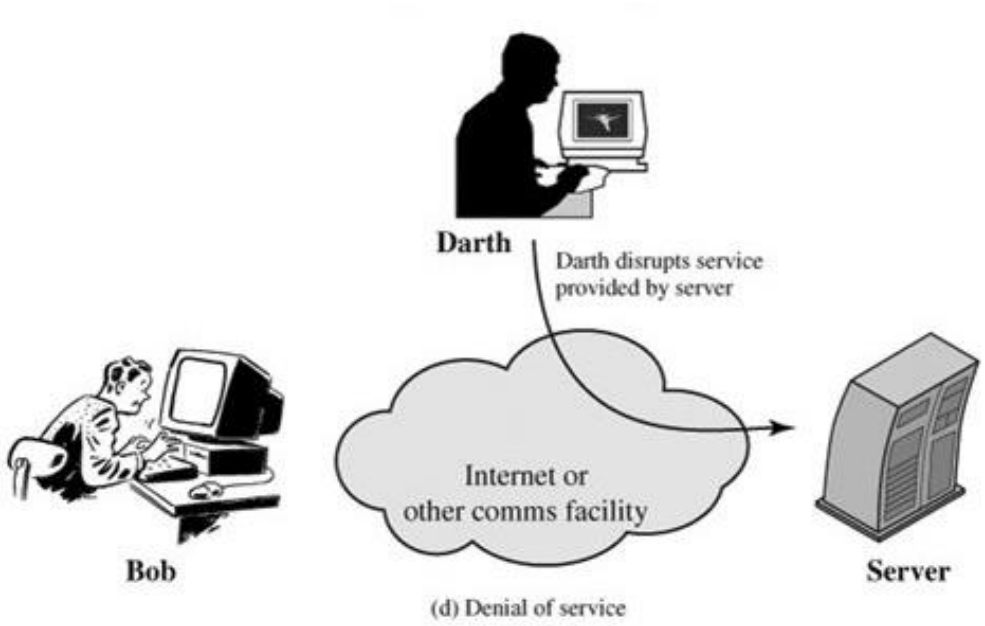


(b) Active attacks

Fonte: Stallings

Ataque ativo – continuação

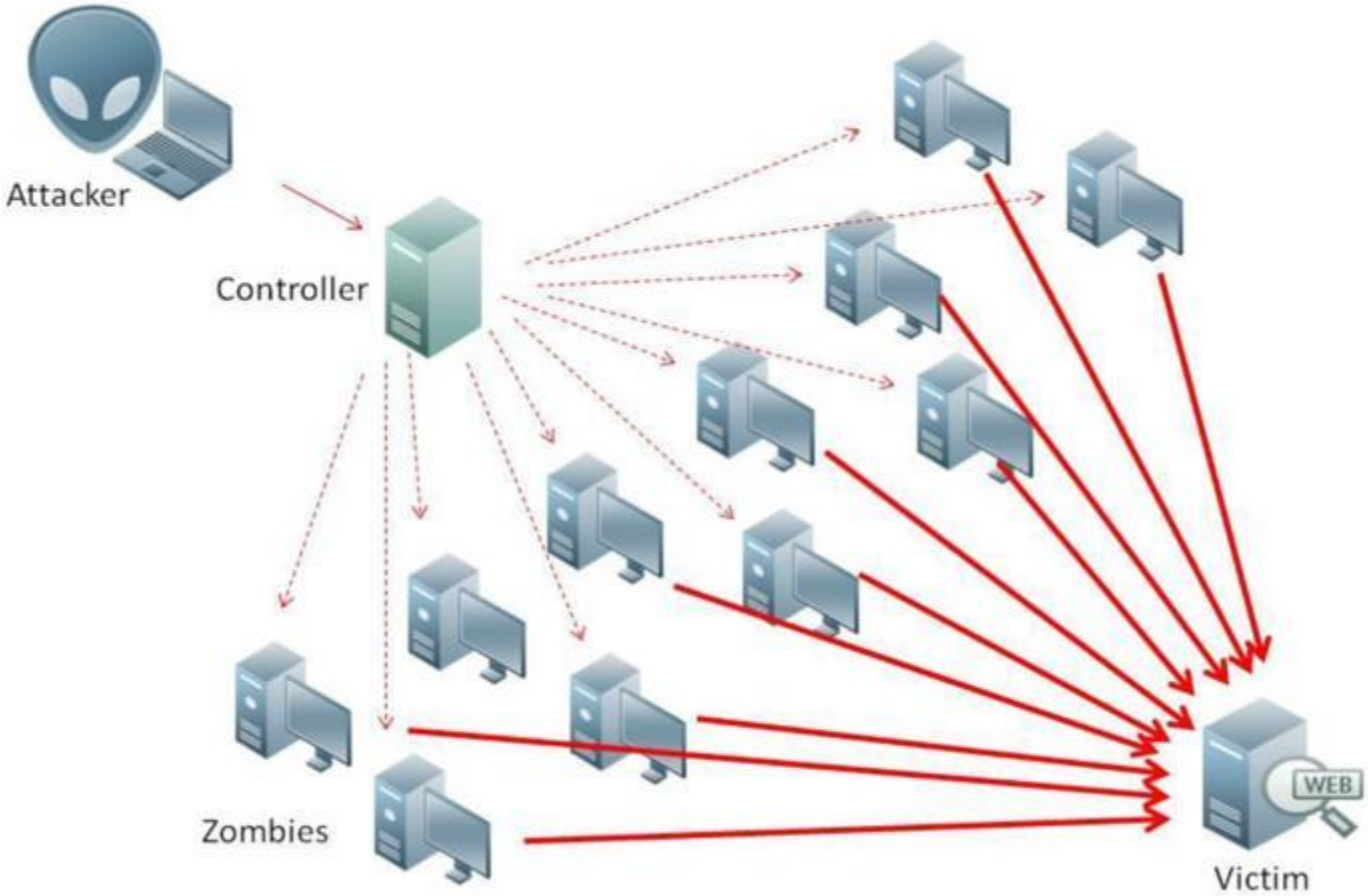
A negação de serviço impede ou inibe o uso normal ou o gerenciamento das instalações de comunicações. Outra forma de negação de serviço é a interrupção de uma rede inteira, seja desativando a rede ou sobrecarregando-a com mensagens para degradar o desempenho.



(d) Denial of service

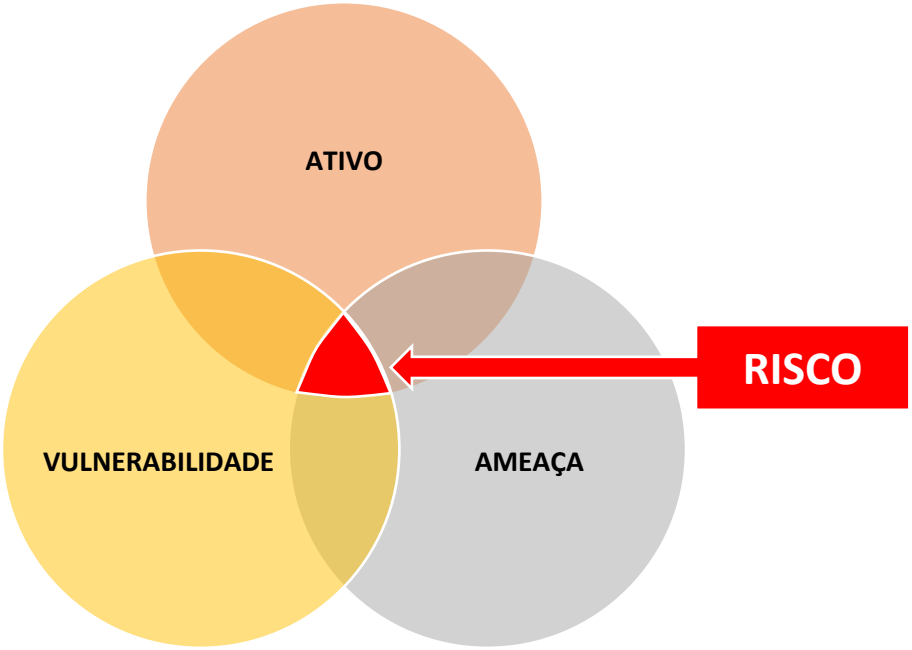
Fonte: Stallings

DDoS – distributed denial of service



Riscos

Risco é a probabilidade de que as ameaças explorem as vulnerabilidades e comprometam os ativos.



OBS.: quando a exploração da vulnerabilidade é concretizada, temos um incidente.

Proteção

Para que os ativos possam ser protegidos, deve-se tomar as seguintes medidas:

- Identificar o que se quer proteger;
- Avaliar os riscos;
- Desenvolver medidas de segurança e/ou remediação.

Proteção

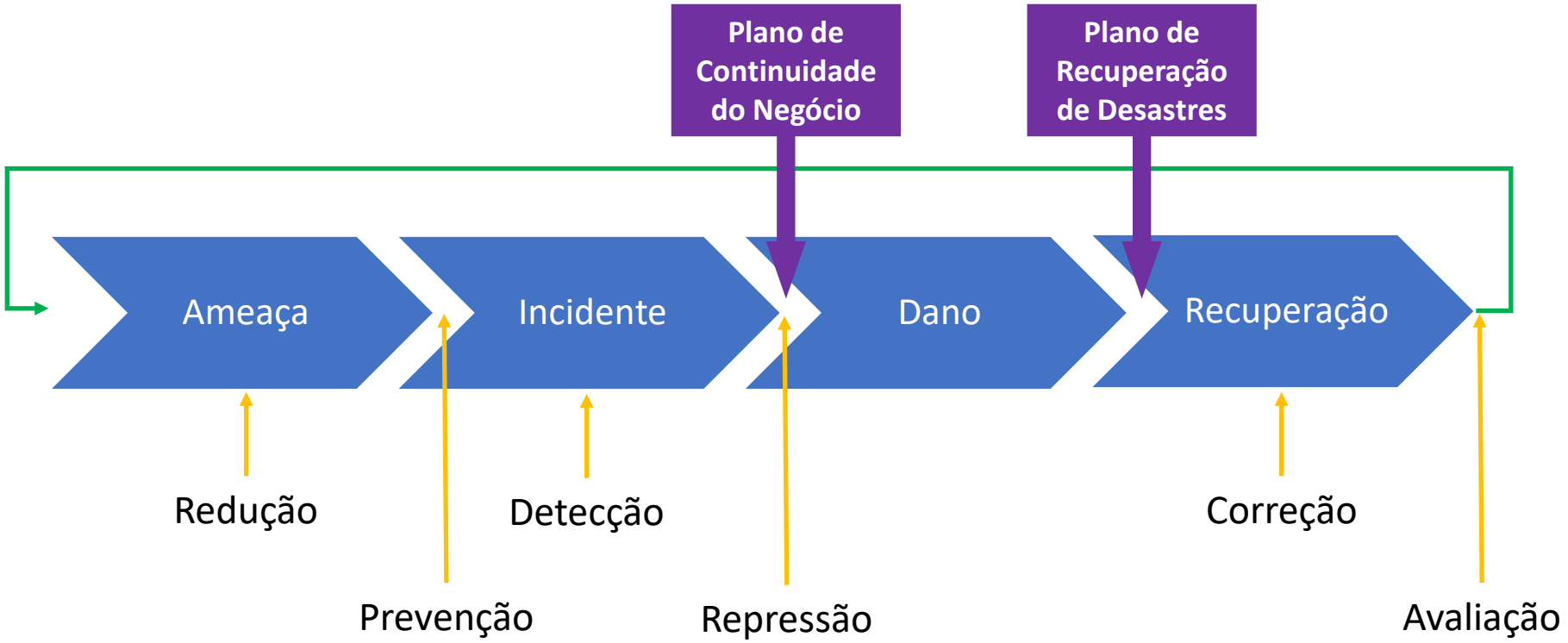
CONTROLE

*A criptonita em si é uma ameaça. A vulnerabilidade do Superman é a sensibilidade ou “alergia” que ele tem da radiação emitida por ela.

Resposta aos riscos

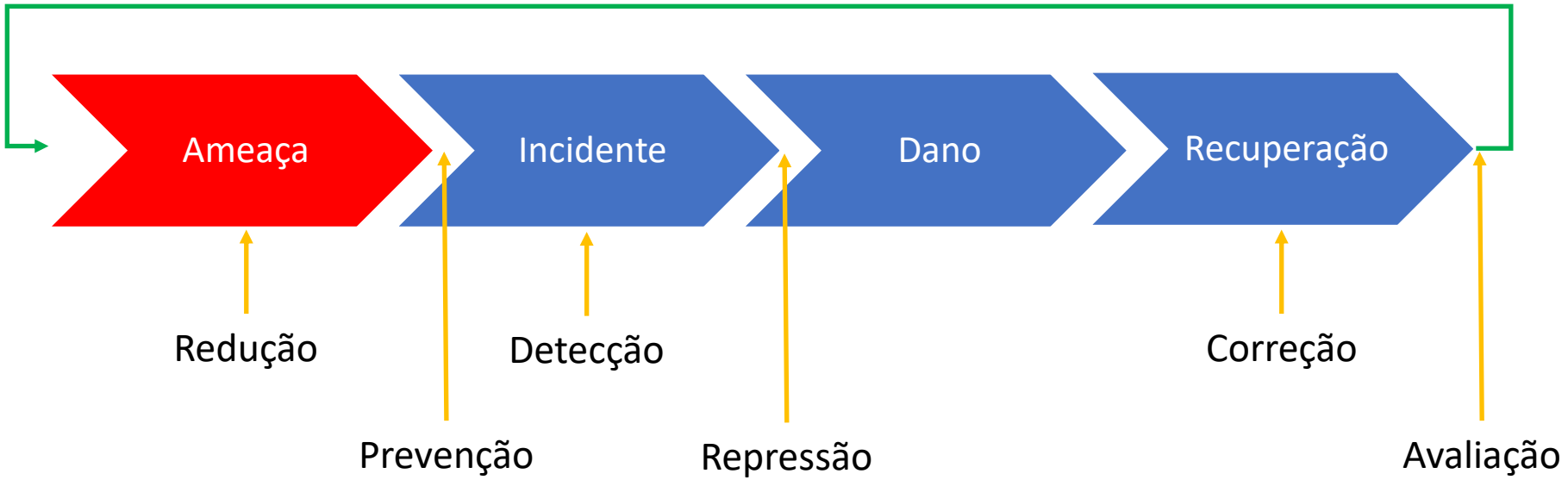
Evitar, prevenir ou eliminar	• Elimina a causa raiz do problema a fim de evitar a exposição ao risco. **Pode afetar a utilidade do ativo.**
Transferir	• Não trata o risco, apenas transfere o ônus para um terceiro, de modo parcial ou total, como num seguro. **Há a necessidade de se pagar um prêmio para a parte que assume o risco.**
Mitigar	• Reduz a probabilidade de ocorrência de um incidente ou o seu impacto até um nível aceitável.
Aceitar	• Quando a probabilidade de ocorrência e o impacto são baixos ou quando não é possível aplicar nenhuma estratégia e decide-se arcar com as consequências.

Ciclo de vida de um incidente de segurança



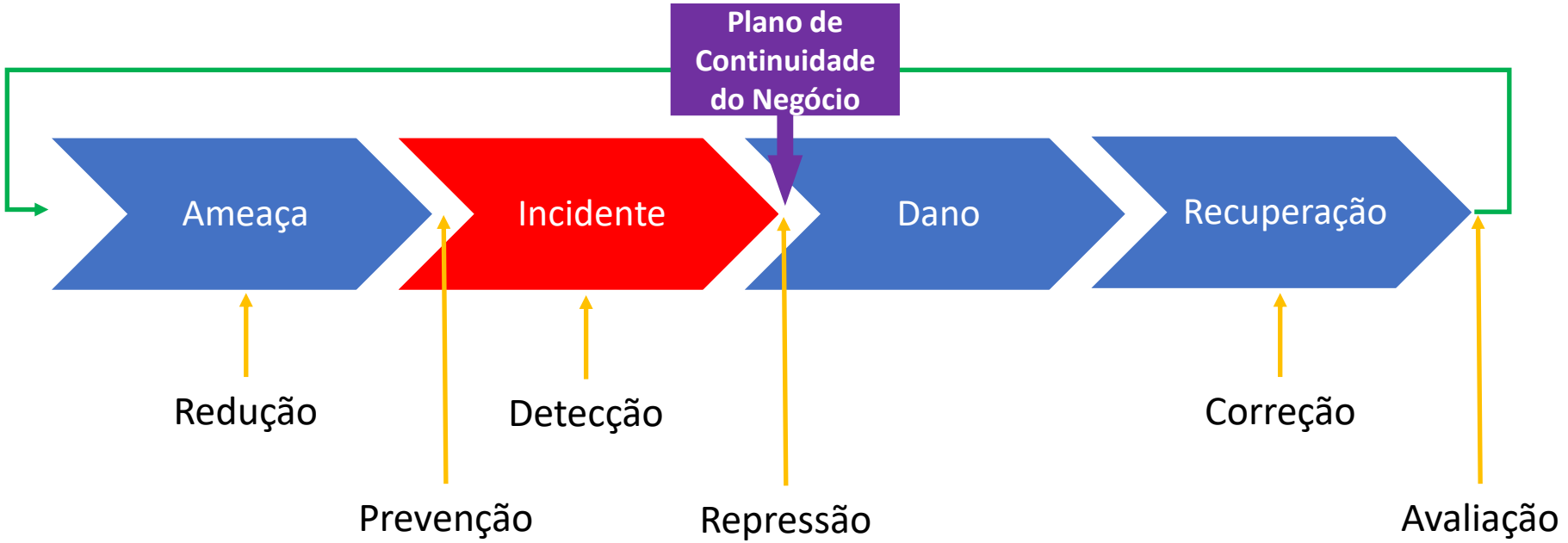
Ciclo de vida de um incidente de segurança

- Ameaça – todo ativo alvo da segurança da informação possui vulnerabilidades e está sujeito a ameaças que as explorem. O gerenciamento de riscos permite que se conheçam tais vulnerabilidades e ameaças e que medidas de redução e de prevenção das ameaças possam ser adotadas.



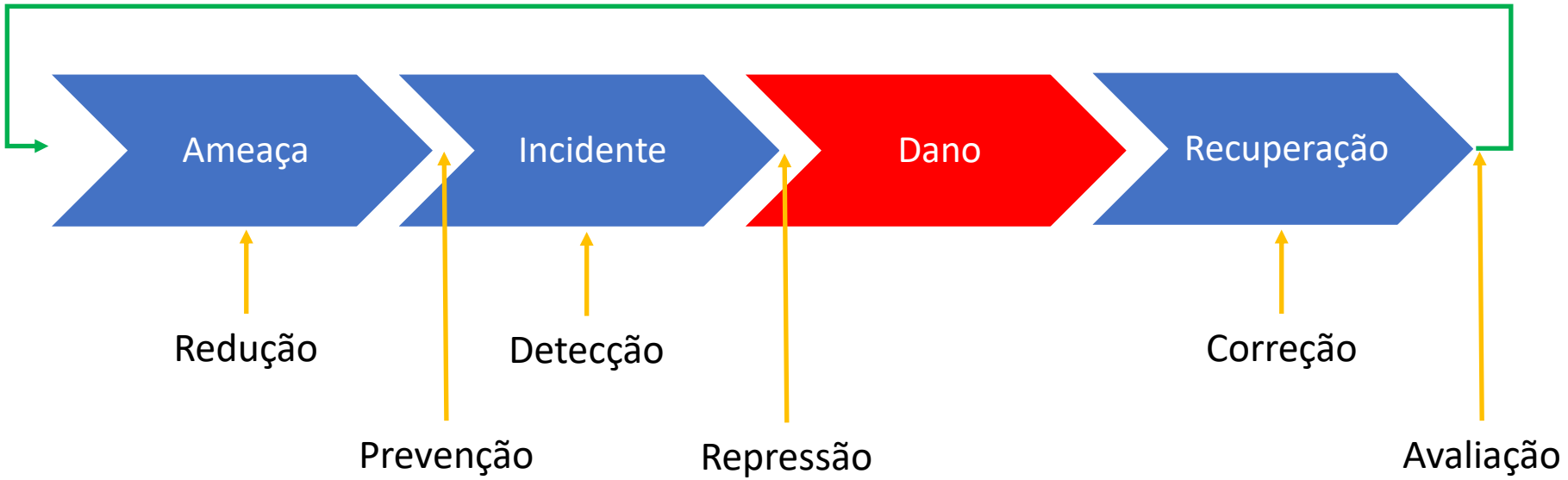
Ciclo de vida de um incidente de segurança

- Incidente – ainda que as medidas de redução e prevenção de ameaças sejam adotadas, um incidente pode ocorrer. Neste caso é importante que o mesmo seja detectado o quanto antes de modo a causar o menor dano possível. As medidas repressivas, como um Plano de Continuidade do Negócio, podem ser acionadas para reprimir o dano a sua menor intensidade possível.



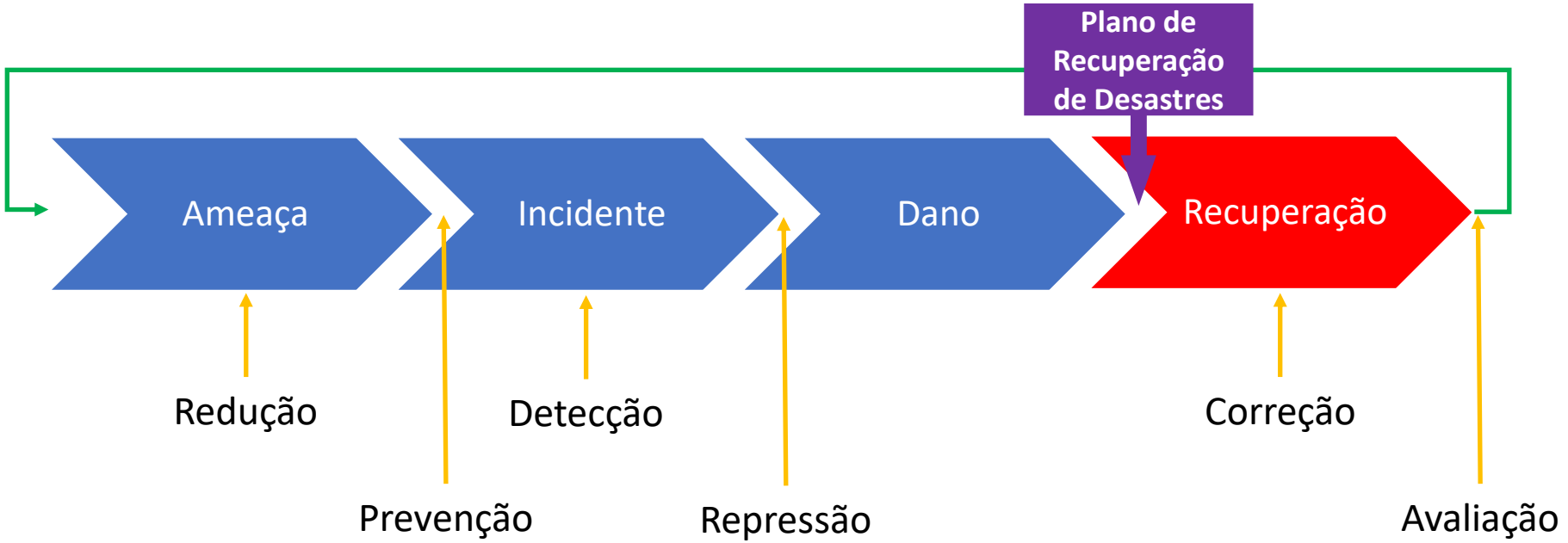
Ciclo de vida de um incidente de segurança

- Dano – nesta etapa a organização deve avaliar os danos causados pelo incidente e confrontá-los com a análise de impacto realizada no gerenciamento de riscos. O objetivo aqui é avaliar se os controles de segurança adotados eram adequados ou não e se devem ser refinados.



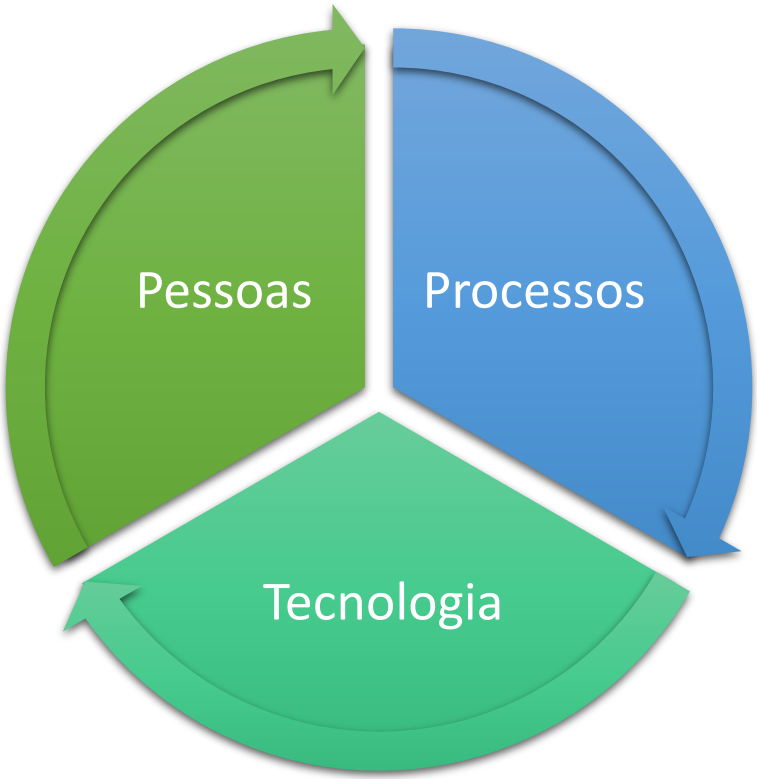
Ciclo de vida de um incidente de segurança

- Recuperação – durante a etapa de recuperação, a partir do Plano de Recuperação de Desastres e quando há o retorno à operação normal, medidas corretivas e avaliativas devem ser adotadas para evitar que incidentes como o que provocou a descontinuidade da operação não voltem a ocorrer. As medidas avaliativas são extremamente importantes no processo de melhoria contínua.



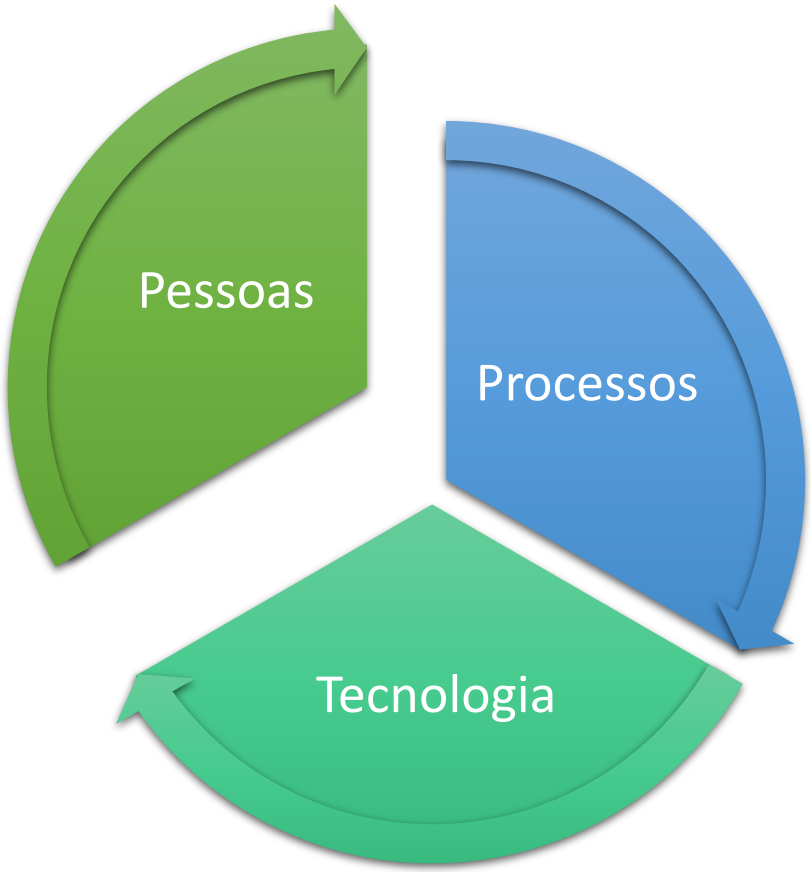
Pessoas, processos e tecnologia

O pilar de implementação de um sistema de gestão da segurança da informação (SGSI) é a tríade pessoas, processos e tecnologia. Não há como pensar a segurança da informação dentro das organizações sem levar em consideração estes três componentes.



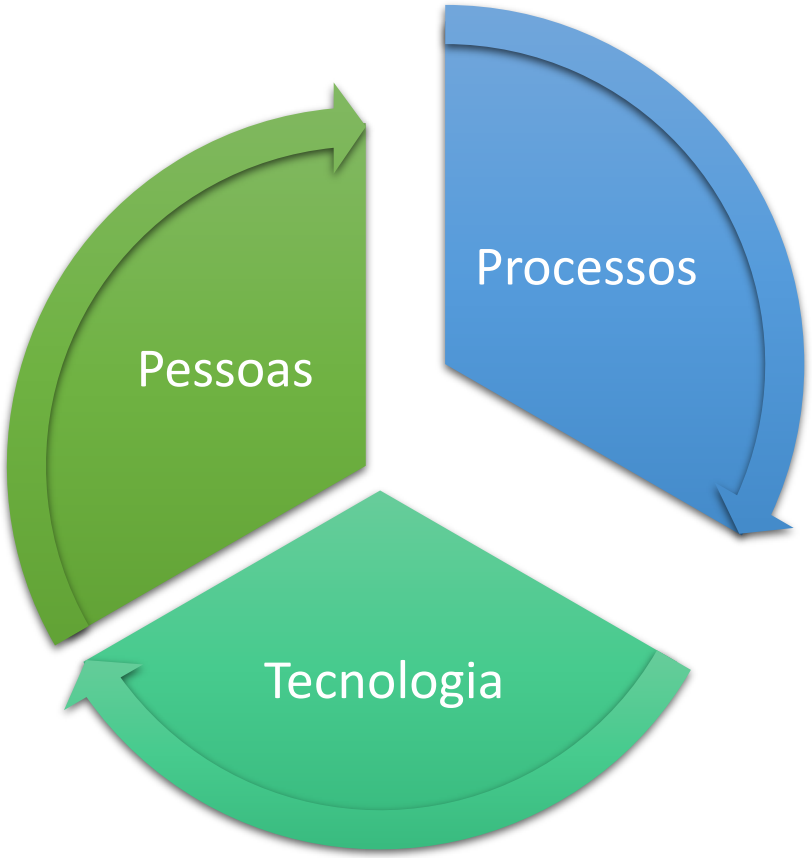
Pessoas, processos e tecnologia

- Pessoas – são ao mesmo tempo o elo mais fraco da cadeia de segurança (engenharia social) e ao mesmo tempo a essência da organizações, pois são elas que planejam, executam e suportam os processos de negócio e de segurança. São valorizados aspectos como conscientização (porque fazer), cultura (o que fazer) e capacitação (como fazer).



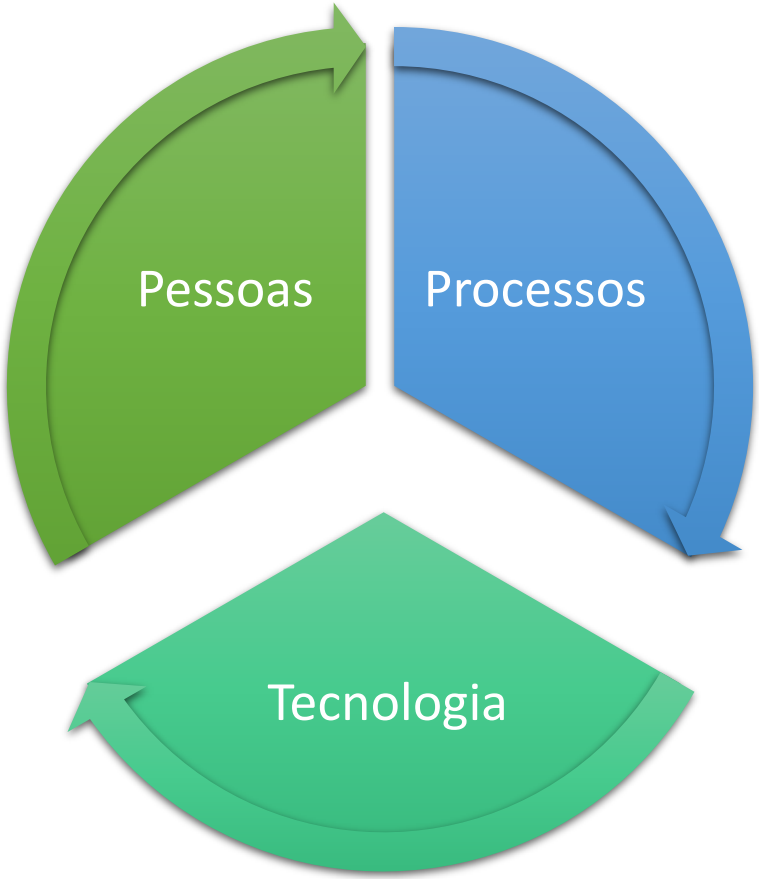
Pessoas, processos e tecnologia

- Processos – compreende o modelo de negócios e seus objetivos, a identificação dos ativos que se quer proteger e a estratégia de segurança para tal; a definição das políticas de segurança e sua implementação, as normas, os procedimentos e a metodologia adotados para manter e melhorar o SGSI. Inclui também as normas, documentações e padrões de conformidade. Os processos devem ser flexíveis tanto quanto possível, de tal modo que a organização não perca a sua dinâmica e agilidade para responder aos desafios diários.



Pessoas, processos e tecnologia

- Tecnologia – são as ferramentas e soluções de segurança adotadas para suportar a estratégia de segurança da informação dos ativos identificados. Devem estar de acordo com a Política de Segurança da Informação, as demais normas e processos definidos para o seu cumprimento.



Segurança física

De acordo com a norma NBR ISO/IEC 27002, o projeto de implantação de um *Datacenter* deve contemplar uma série de características únicas, de forma que sejam projetadas e aplicadas proteção física contra sinistros.

De forma geral, deve-se garantir proteção:

- contra acesso não autorizado por meio de dispositivos de segurança;
- contra incêndios e demais intempéries, por meio de implantação de salas cofre;
- equipamentos de contingência e mídias de backup devem ficar armazenadas em local diverso;
- etc.

Segurança lógica

A segurança lógica pode ser implementada com o uso de proteção nos seguintes níveis:

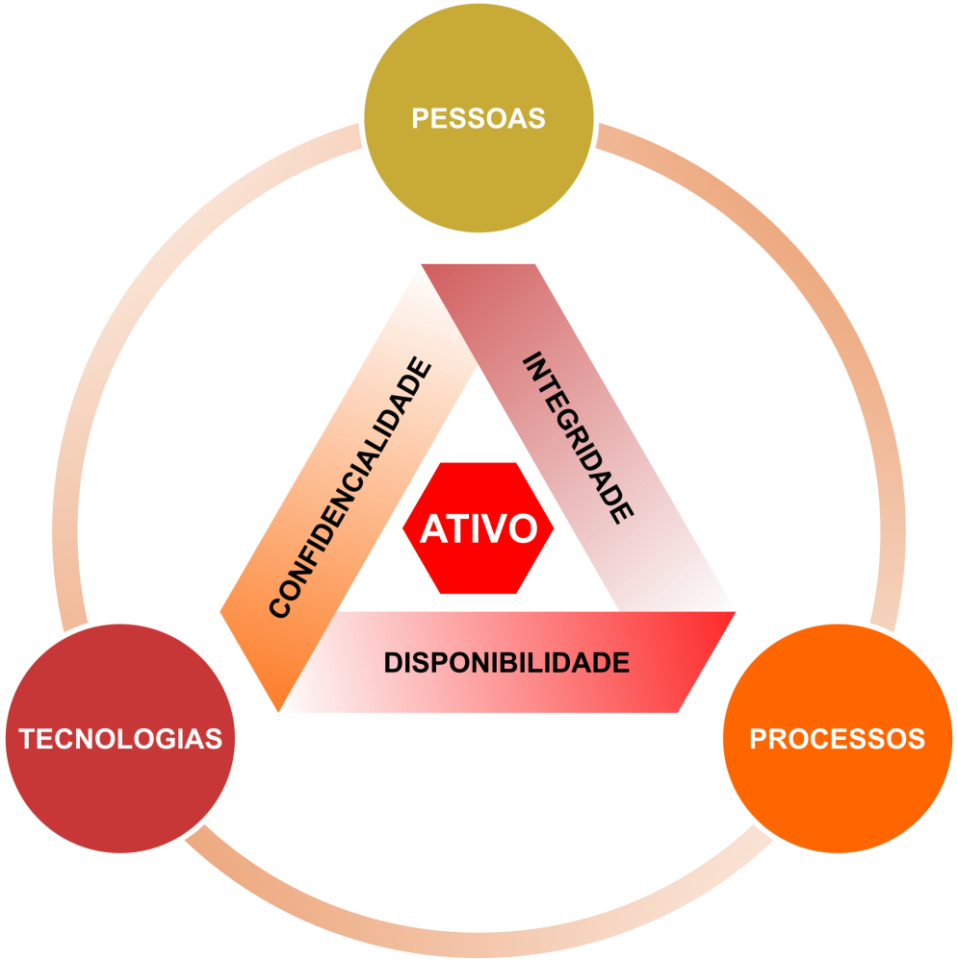
- na borda da rede – por meio do uso de firewall e snort;
- no interior da rede – por meio do uso de antivírus e antispam e outros mecanismos para controle de acesso;
- etc.

Segurança em recursos humanos

A segurança em recursos humanos pode ser implementada da seguinte forma:

- cuidados na contratação e dispensa de pessoal;
- documentação de procedimentos quanto ao uso de recursos;
- etc.

Segurança – resumo



Fonte: Xxxxxxxxxxxxxxxxxxxxxxxx

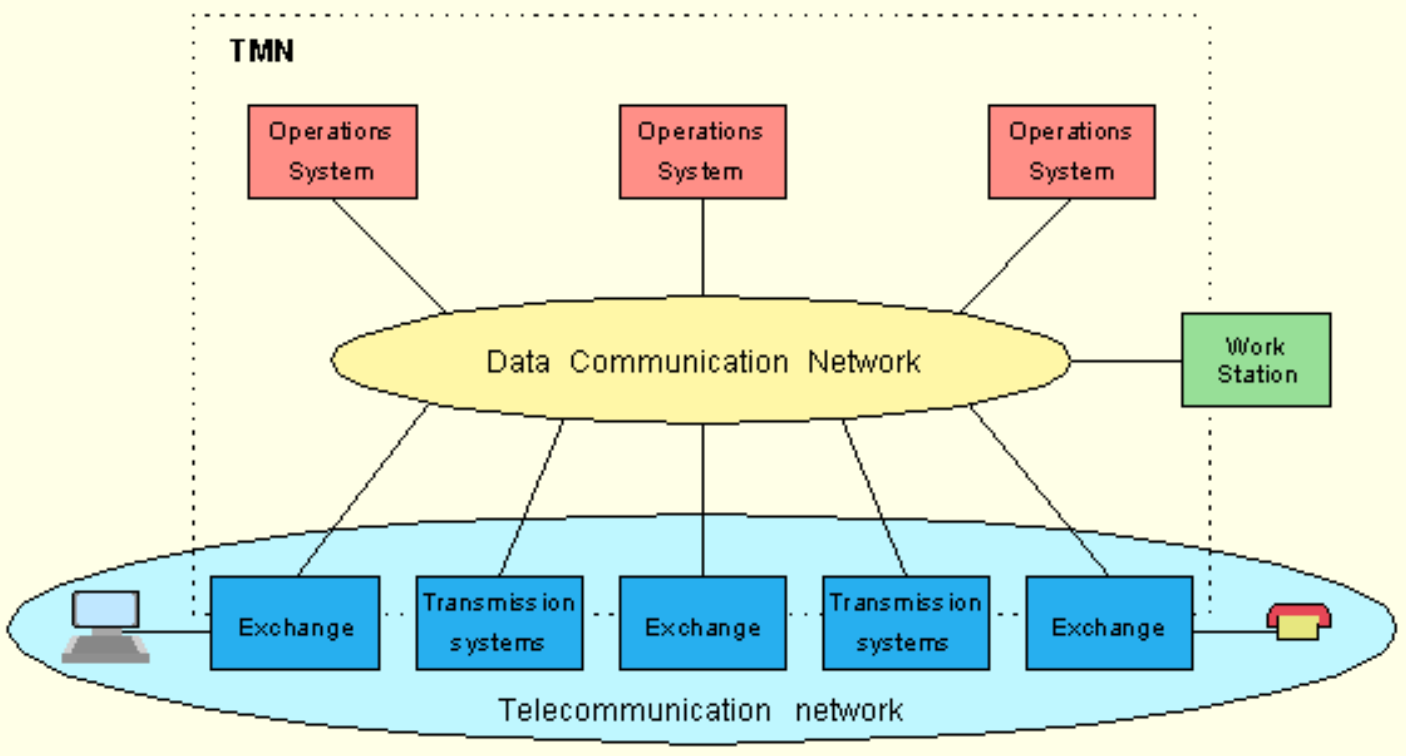
Segurança e gerência de redes

Gerência de Redes é a disciplina que trata da forma como uma rede ou sistema pode ser monitorada, gerenciada e administrada.

Dentre os modelos podemos destacar TMN (*Telecomunications Management Network*) da ITU-T e o FCAPS (*Fault, Configuration, Accounting, Performance e Security*) da ISO.

TMN

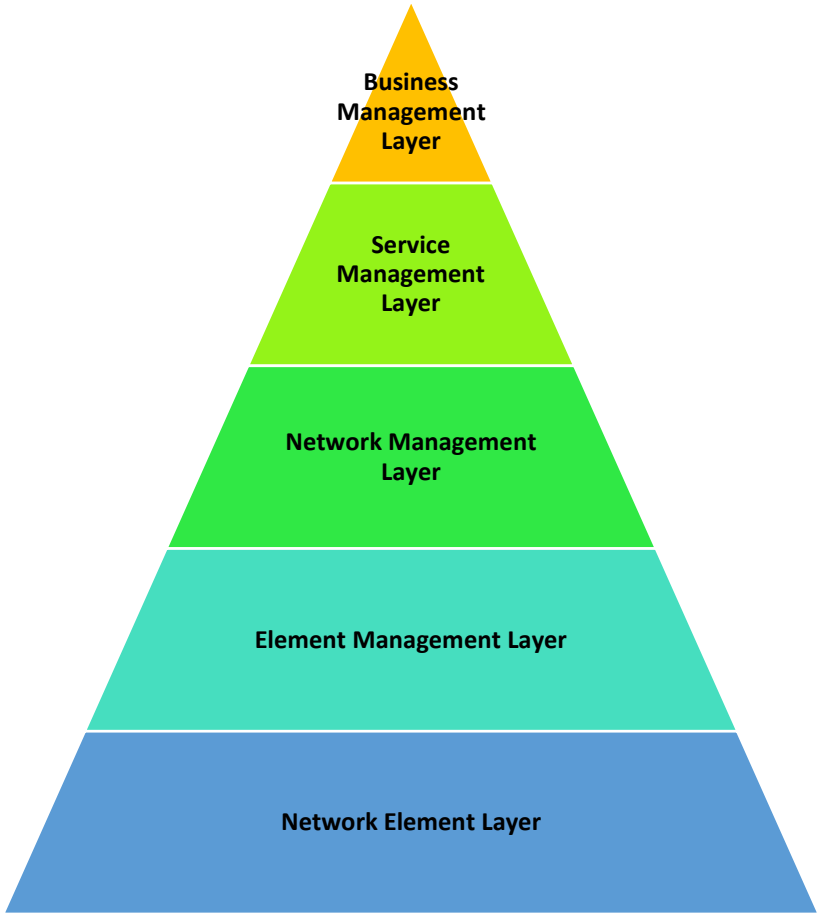
O modelo TMN é um conjunto de recomendações editados pela ITU em 1988 com o objetivo de prover uma metodologia para gerenciar redes, serviços e equipamentos de telecomunicações.



TMN – arquitetura lógica

A arquitetura lógica ou LLA (Logical Layered Architecture) tem por objetivo restringir atividades de gerência em camadas. São cinco as camadas:

- Camada de gerência de negócios
- Camada de gerência de serviços
- Camada de gerência de rede
- Camada de gerência de elementos de rede
- Camada de elementos de rede



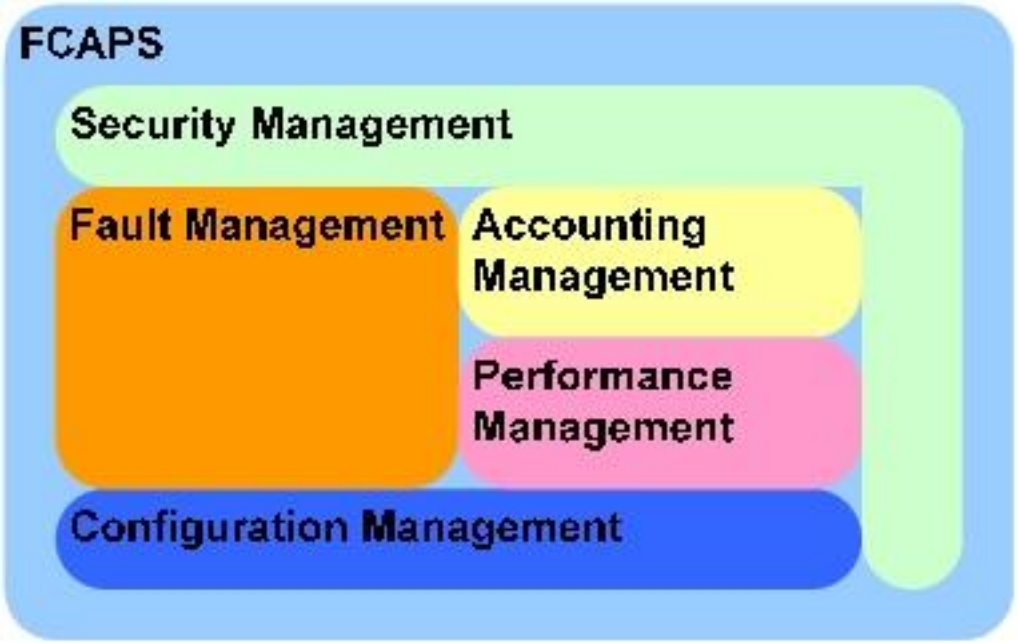
FCAPS

Neste modelo de gerenciamento de redes a ISO identificou um conjunto de cinco áreas críticas, que ficou conhecido pela sigla FCAPS, um acrônimo para *fault* (falha), *configuration* (configuração), *accounting* (contabilidade), *performance* (desempenho) e *security* (segurança).

Em organizações que não possuem tarifação, a área de *accounting* pode ser substituída por *administration* (administração).

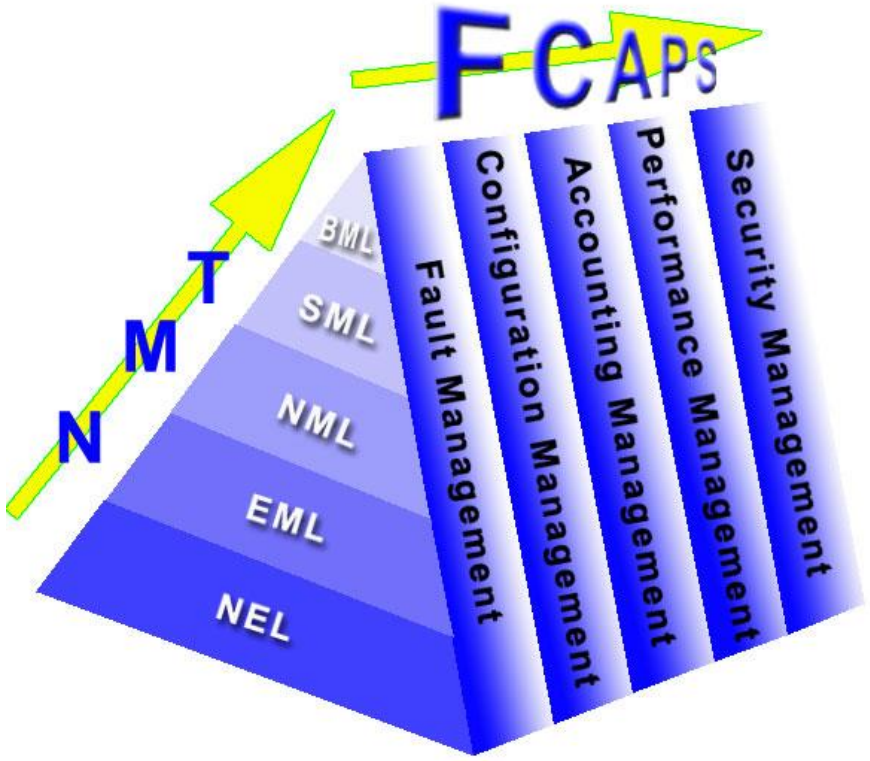
FCAPS

De acordo com a Cisco, as cinco áreas do modelo de gerenciamento de redes OSI/ISO se relacionam da seguinte forma:



FCAPS versus TMN

O modelo FCAPS da ISO e o modelo TMN da ITU-T podem ser relacionados de acordo com a figura abaixo:



Normas de segurança

A ISO propôs duas normas de segurança da informação. São elas:

- ISO 27001 : Information Security Management Systems - Requirements
- ISO 27002 : Code of practice for information security management

A ISO 27001 é um conjunto de requerimentos para sistema de gestão de segurança da informação, onde é possível que a empresa obtenha a certificação após atender todos os itens obrigatórios. Somente a ISO 27001 pode ser auditada.

Já a ISO 27002 é um código de boas práticas que contém os controles que podem ser usados em alinhamento com o processo de tratamento de riscos de segurança da informação.

Para saber mais...

... leia o capítulo 3 do livro Fundamentos de segurança da informação com base na ISO 27001 e na ISO 27002, de Jule Hintzbergen

... leia o capítulo 1 do livro Criptografia e segurança de redes: princípios e práticas, de William Stallings

Módulo 2

Segurança e Governança

Introdução

"Política de Segurança é composta por um **conjunto de regras e padrões** sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente, de modo a garantir a sua confidencialidade, integridade e disponibilidade"

Scott Barman apud Fernando Nicolau Freitas Ferreira

Fonte: FERREIRA, F. N. F.; ARAÚJO, M. T. D. **Política de Segurança da Informação**. 2ª. ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

Premissas

- Estabelecer o conceito de que as informações são um ativo importante para a organização
- Envolver a alta administração da organização
- Responsabilizar formalmente os colaboradores sobre a salvaguarda dos recursos da informação, definindo o conceito de irrevogabilidade
- Estabelecer padrões para a manutenção da Segurança da Informação

Fonte: FERREIRA, F. N. F.; ARAÚJO, M. T. D. **Política de Segurança da Informação**. 2ª. ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

Definições

- Ativos – toda e qualquer informação identificada como elemento essencial para os negócios de uma organização, que devem ser protegidos por um período de tempo pré-determinado de acordo com sua importância;
- Ameaças – toda e qualquer causa potencial de um incidente indesejado que pode causar perdas e danos aos ativos da organização e afetar seus negócios;
- Vulnerabilidades – são os elementos que, uma vez expostos e explorados pelas ameaças, afetam a confidencialidade, a integridade e a disponibilidade dos ativos;
- Riscos – é a probabilidade de que as ameaças explorem as vulnerabilidades;
- Medidas de segurança – são as ações orientadas para a eliminação ou redução das vulnerabilidades;

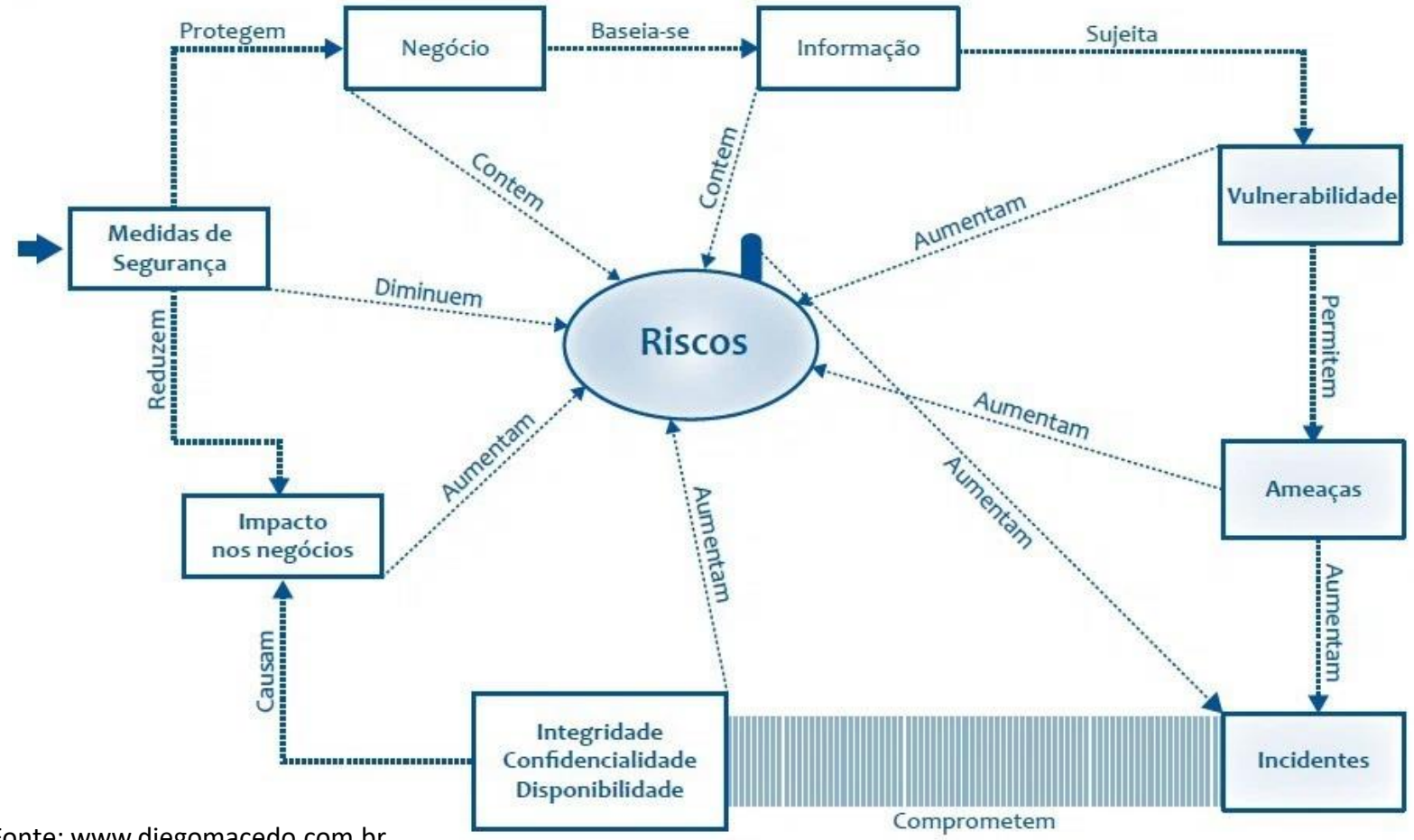
Definições – continuação

- Confidencialidade – garantia de que a informação é acessível somente por pessoas autorizadas;
- Integridade – garantia de que a informação não foi alterada. É salvaguarda da exatidão da informação;
- Disponibilidade – garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

Definições – continuação

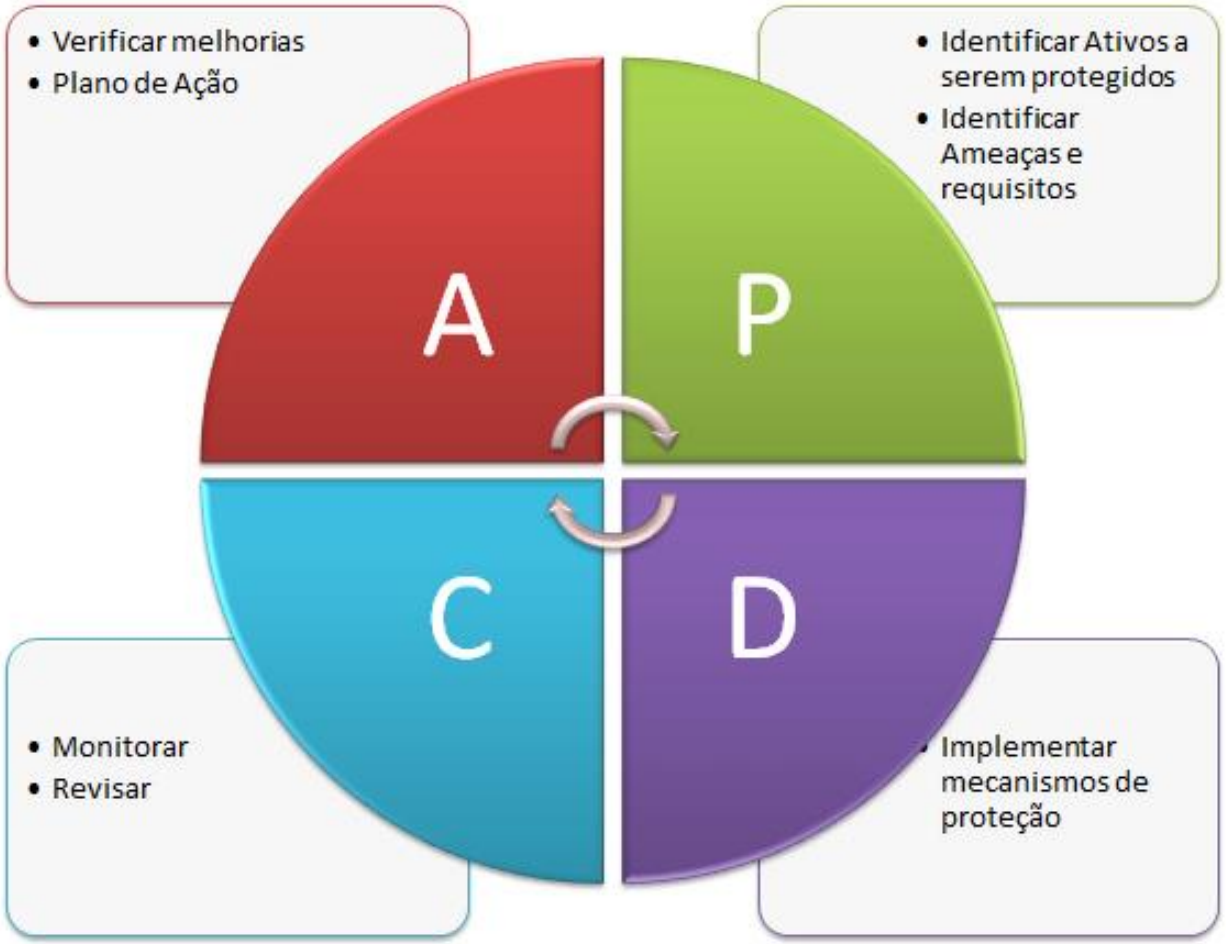
- Autenticidade – garantia que os dados fornecidos são verdadeiros e provêm de fonte legítima;
- Legalidade – o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos;
- Auditabilidade – o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação;
- Não repúdio – o usuário que gerou ou alterou a informação não pode negar o fato, pois existem mecanismos que garantem sua autoria.

Ciclo de segurança da informação



Fonte: www.diegomacedo.com.br

Implantação



Fonte: www.devmedia.com.br

Ciclo de Deming para Segurança da Informação

Governança

"A Governança Corporativa é o sistema pelo qual as organizações são dirigidas e controladas"

NBR ISO/IEC 38500:2009

"A Governança Corporativa de TI é o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar planos. Inclui a estratégia e as políticas de uso da TI dentro da organização"

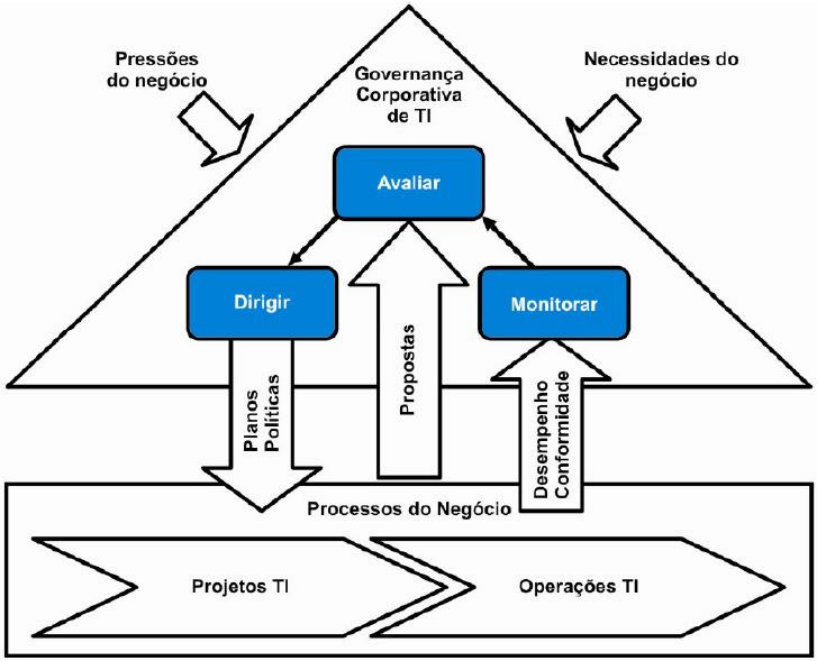
NBR ISO/IEC 38500:2009

"A Governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e os objetivos da organização"

IT Governance Institute

Governança

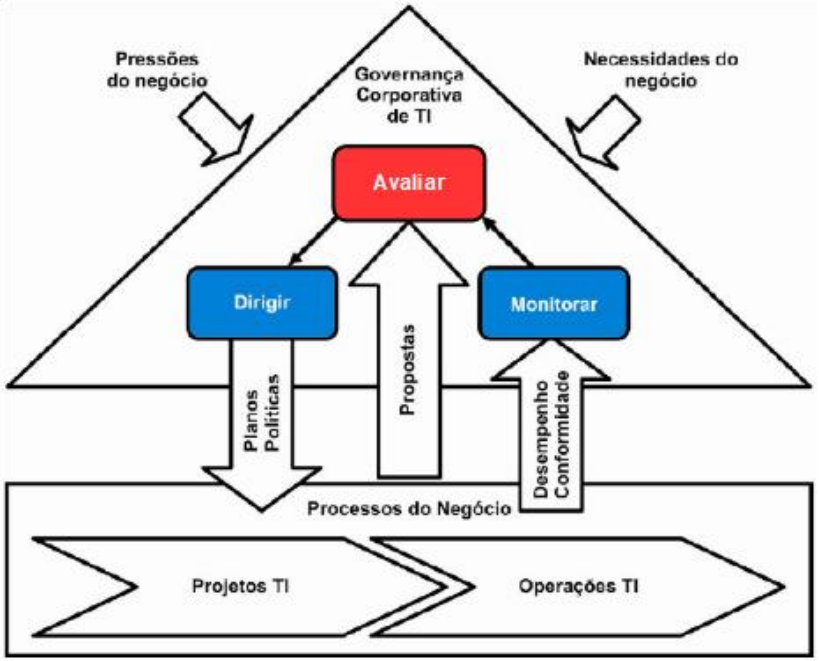
A norma ISO/IEC 38500 oferece ao corpo diretivo das organizações princípios para orientar sobre o uso eficaz, eficiente e aceitável da TI e se aplica aos processos de gerenciamento da governança relacionados aos serviços de informação e comunicação. A norma orienta ainda que estes dirigentes governem a TI por meio de três tarefas: Avaliar, Dirigir e Monitorar.



Fonte: NBR ISO/IEC 38500:2009

Governança

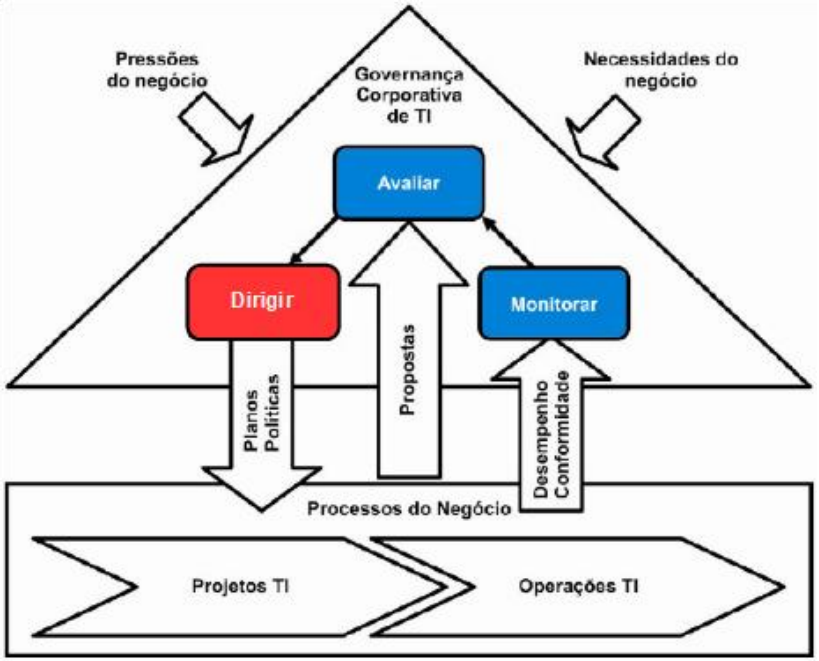
Avaliar – os dirigentes devem avaliar o uso atual e futuro da TI, incluindo estratégias, propostas e arranjos de fornecimento. Devem também considerar as pressões externas e internas que influenciam o negócio, tais como mudanças tecnológicas, tendências econômicas e sociais e influências políticas, e levem em conta as necessidades atuais e futuras do negócio.



Fonte: NBR ISO/IEC 38500:2009

Governança

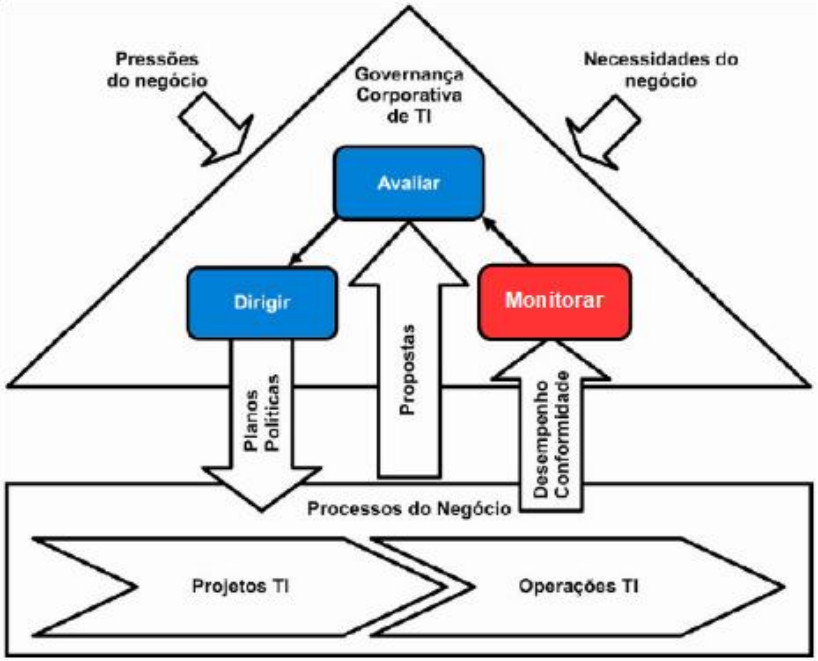
Dirigir – os dirigentes devem designar responsabilidade e exigir a preparação e implementação dos planos e políticas que estabeleçam o direcionamento dos investimentos nos projetos e operações de TI. Os dirigentes devem assegurar também que a transição e implantação dos projetos seja corretamente planejada e gerenciada, levando em conta os impactos nos negócios e nas práticas operacionais.



Fonte: NBR ISO/IEC 38500:2009

Governança

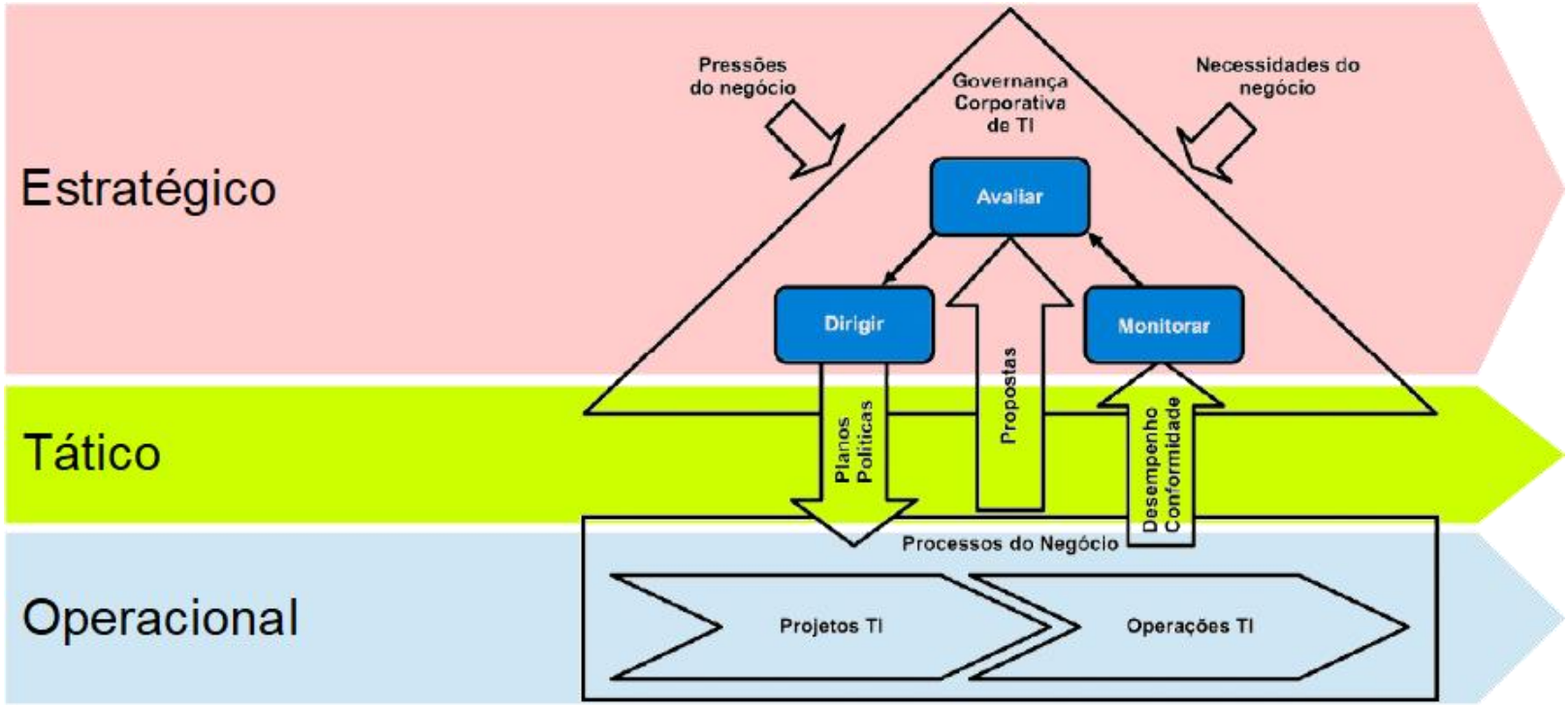
Monitorar – os dirigentes devem monitorar o desempenho da TI por meio de sistemas de mensuração apropriados, certificando-se de que o desempenho esteja de acordo com os planos e objetivos corporativos e que a TI esteja em conformidade com as obrigações externas e práticas internas de trabalho.



Fonte: NBR ISO/IEC 38500:2009

Governança versus gestão

A Governança de TI administra a Gestão de TI por meio dos níveis estratégico e tático, enquanto a Gestão de TI administra os projetos de TI e suas operações no nível operacional.



Governança versus gestão

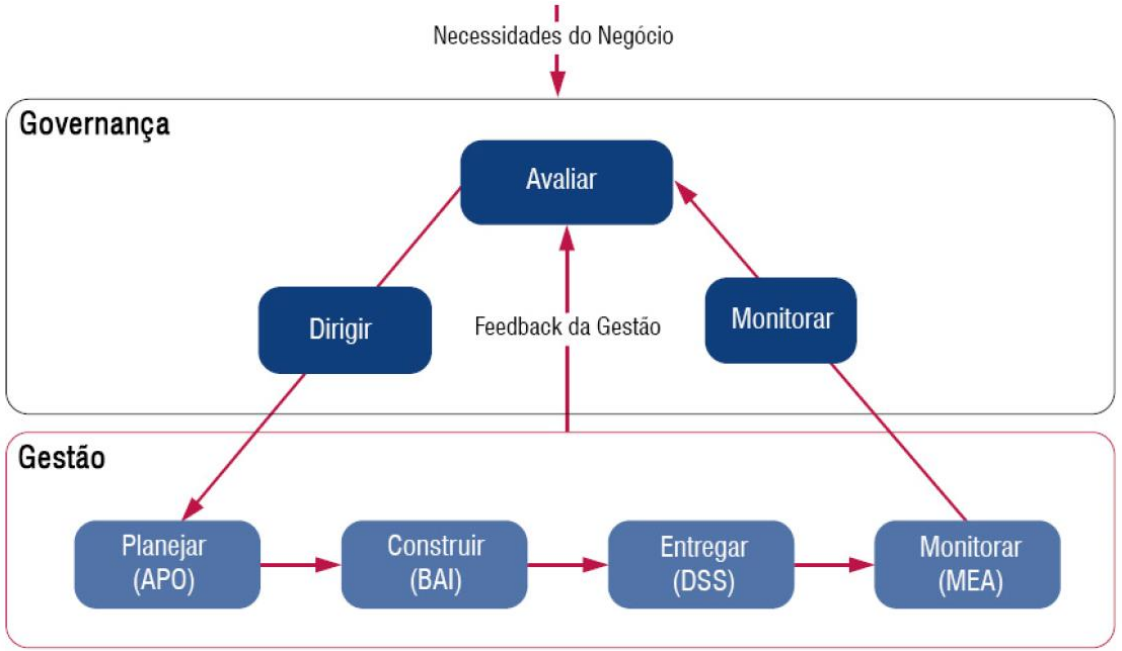
De acordo com o COBIT5:

- 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 – A 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.

De acordo com Abreu e Fernandes, a Governança Corporativa de TI está inserida na Governança Corporativa da organização, sendo dirigida por esta e buscando o direcionamento da TI para atender ao negócio e o monitoramento para verificar a conformidade com o direcionamento tomado pela administração da organização, ao passo que a Gestão de TI implica a utilização sensata de meios (recursos, pessoas, processos, práticas) pra alcançar um objetivo. Atua no planejamento, construção, organização e controle das atividades operacionais e se alinha com a direção definida pela organização.

Normas e guias de boas práticas

COBIT (Control Objectives for Information and related Technology) é um modelo de estrutura de controles internos orientado para o entendimento e o gerenciamento dos riscos associados ao uso da TI, bem como o alinhamento da TI ao negócio.



Áreas chaves da Governança e do Gerenciamento

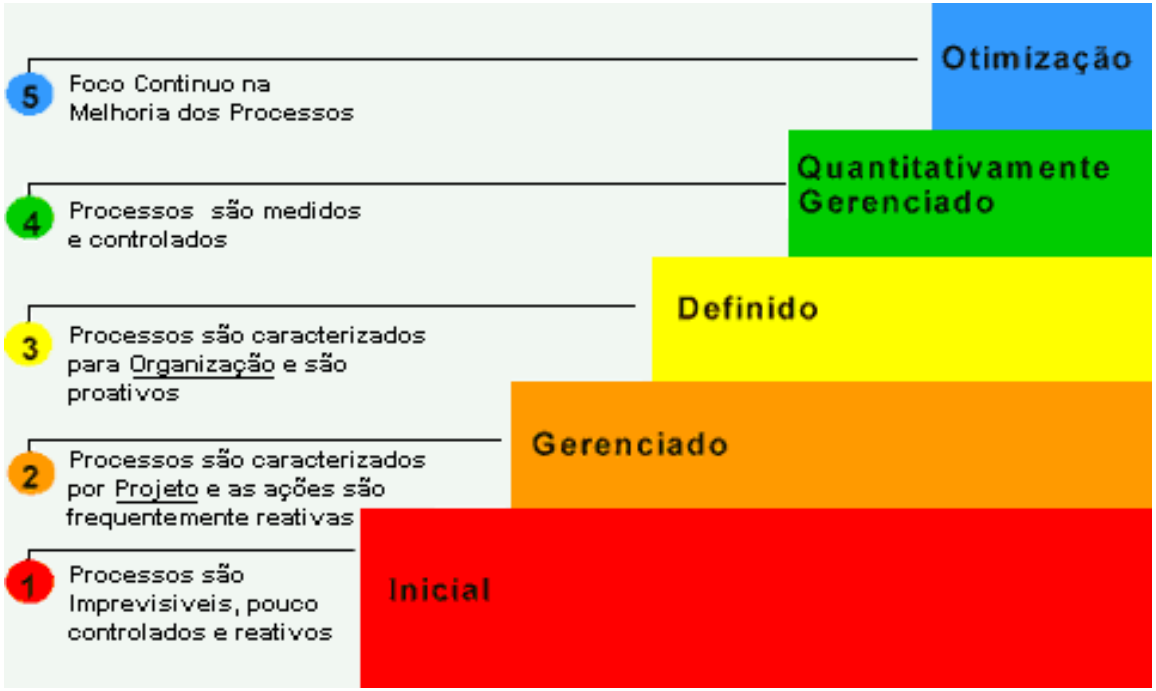
Normas e guias de boas práticas

ITIL (Information Technology Infrastructure Library) é um conjunto de melhores práticas para gestão de serviços em TI.

Ciclo de vida de serviços

Normas e guias de boas práticas

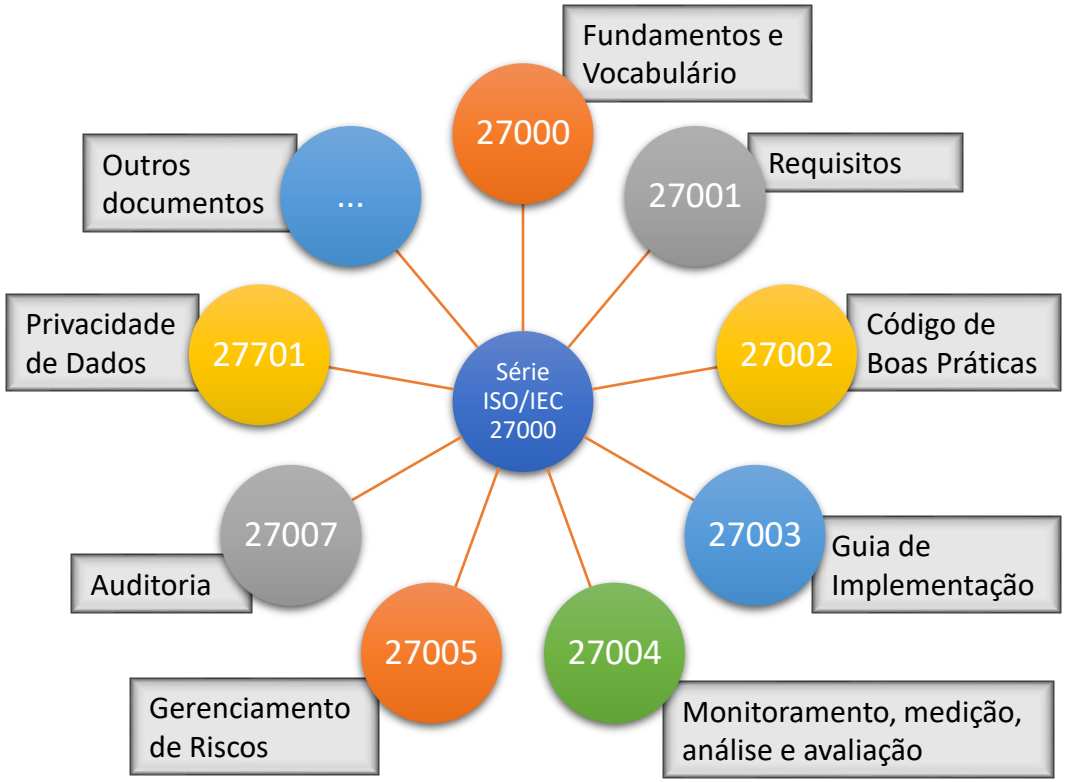
CMM (Capability Maturity Model) é um conjunto de melhores práticas para avaliação de maturidade do processo de desenvolvimento de *software* dentro de uma organização.



Níveis de maturidade

Normas e guias de boas práticas

A família ISO/IEC 27000 é uma série abrangente de normas para o gerenciamento da segurança da informação, dos riscos e dos controles. A série possui ao todo 47 documentos.



Normas e guias de boas práticas

PMBOK (Project Management Body of Knowledge) e PRINCE2 (PRojects IN Controlled Environments) são guias de boas práticas para gerenciamento de projetos de qualquer natureza, independente de tamanho, escopo, tipo de organização, entre outros.

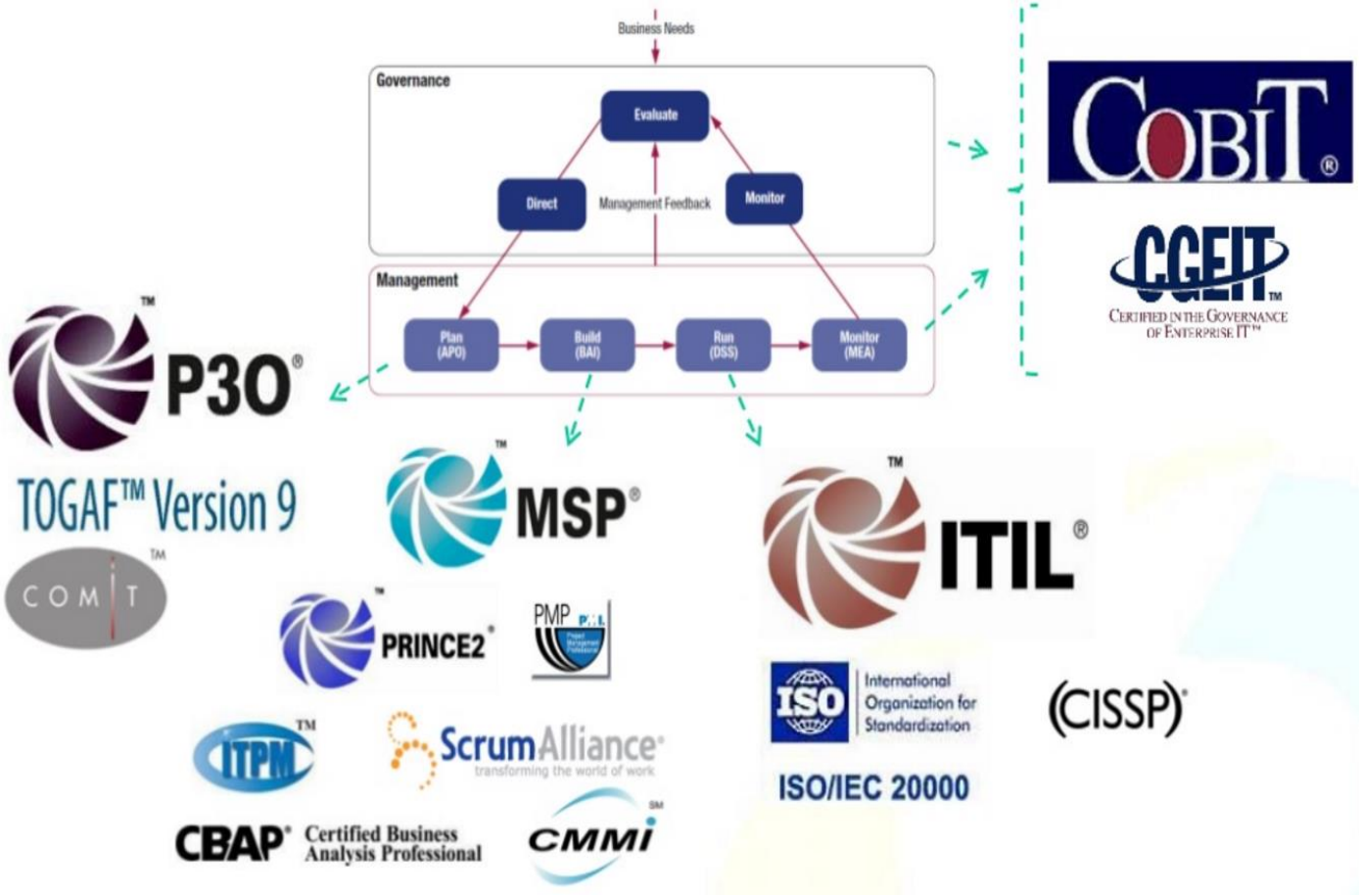
Fases da gestão de projetos

Governança – resumo

COBIT – governança de TI:

- ITIL – entrega de serviços;
- CMM – entrega de soluções;
- ISO/IEC 27000 – segurança da informação;
- PMBOK ou PRINCE2 – gerenciamento de projetos.

Governança – resumo



Para saber mais...

... leia os capítulos 1 e 2 do livro Governança de segurança da informação, de Sergio da Silva Manoel

Módulo 3

Melhores Práticas de Governança

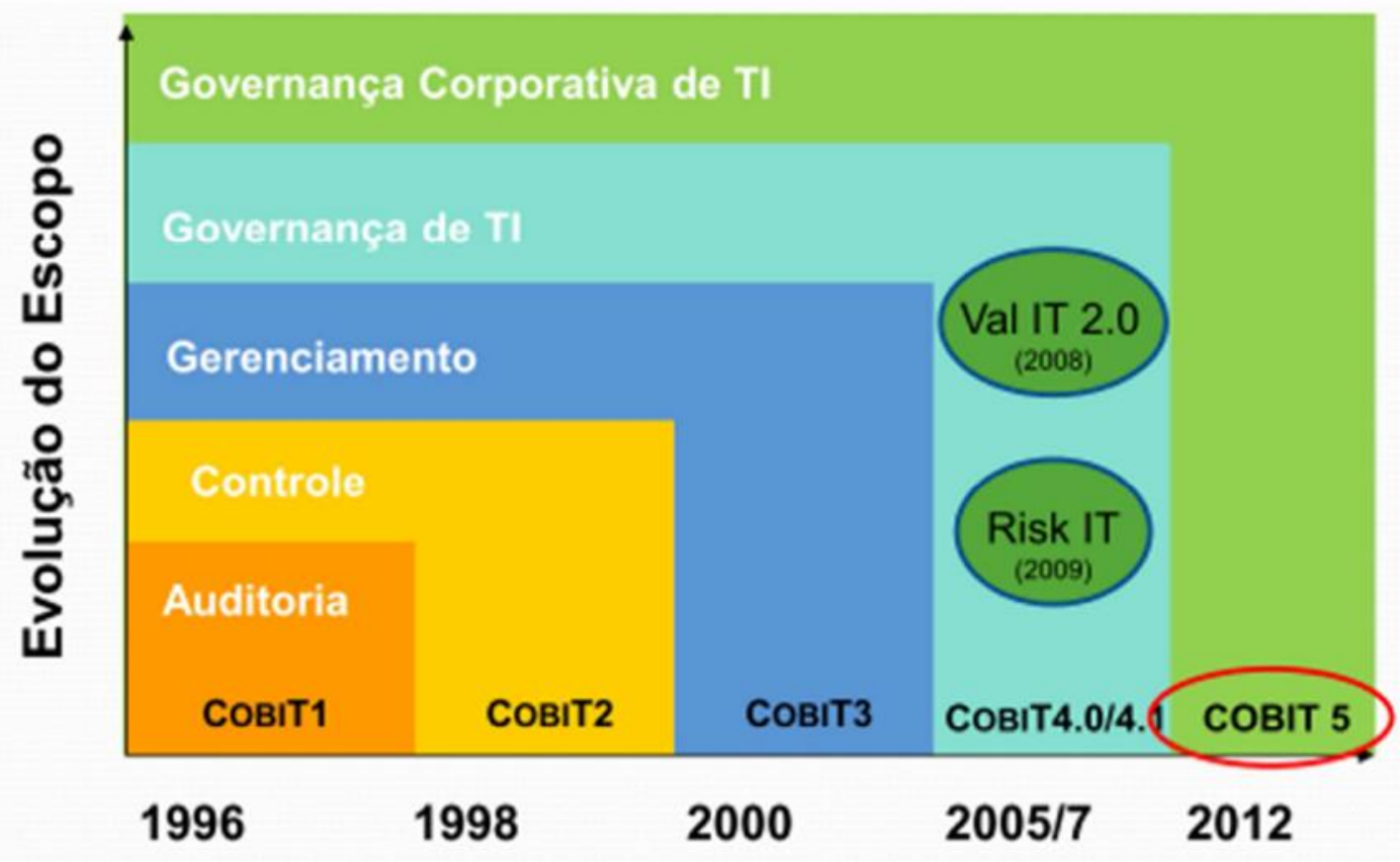
COBIT – introdução

O COBIT 5 fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI, ajudando-as a criar valor por meio da TI e mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos. Permite ainda que a TI seja governada e gerida de forma holística para toda a organização, 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.

Princípios do COBIT 5

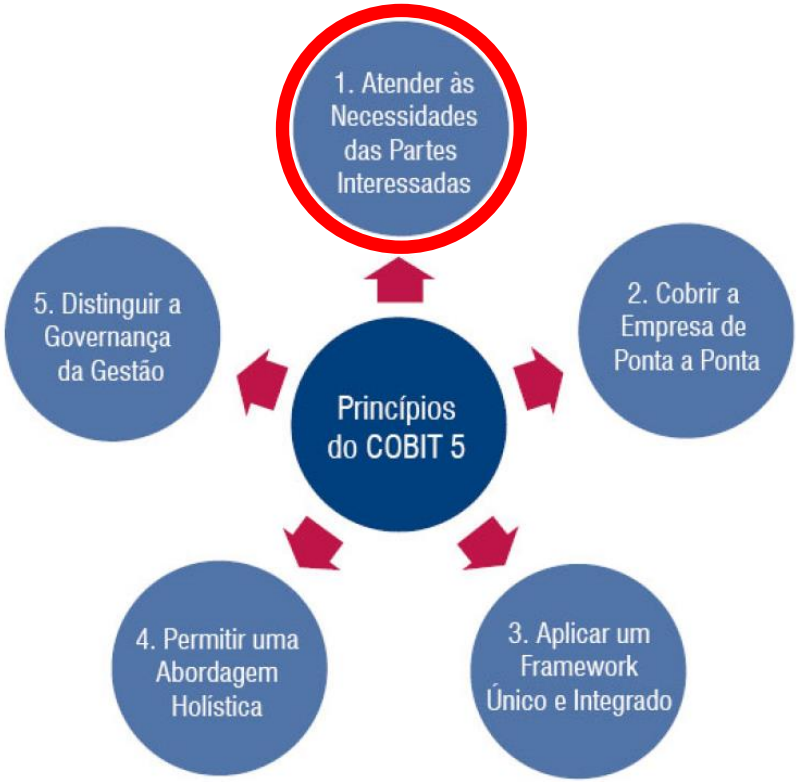
Fonte: COBIT 5 Framework

COBIT – evolução



COBIT – introdução

1. As organizações existem para criar valor para suas Partes Interessadas*, mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos. O COBIT 5 fornece todos os processos necessários e demais habilitadores para apoiar a criação de valor para a organização com o uso de TI, traduzindo os objetivos corporativos de alto nível em objetivos de TI específicos e gerenciáveis, mapeando-os em práticas e processos específicos.



Fonte: COBIT 5 Framework

*NOTA: De acordo com a NBR ISO/IEC 38500:2009 – Governança Corporativa de Tecnologia da Informação, Parte Interessada ou stakholder é "Qualquer indivíduo, grupo ou organização que possa afetar, ser afetado, ou ter a percepção de que será afetado por uma decisão ou atividade (ISO/IEC Guia 73)".

COBIT – introdução

2. O COBIT 5 integra a governança corporativa de TI da organização à governança corporativa. Cobre todas as funções e processos corporativos, não concentrando-se apenas na “função de TI”, mas considerando a Tecnologia da Informação e tecnologias relacionadas como ativos que devem ser tratados como qualquer outro ativo por todos na organização. Considera todos os habilitadores de governança e gestão de TI aplicáveis em toda a organização, incluindo tudo e todos - interna e externamente - que forem considerados relevantes para a governança e gestão das informações e de TI da organização.

Fonte: COBIT 5 Framework

COBIT – introdução

3. Há muitas normas e boas práticas relacionadas a TI, cada qual provê orientações para um conjunto específico de atividades de TI. O COBIT 5 se alinha a outros padrões e modelos importantes em um alto nível e, portanto, pode servir como um modelo unificado para a governança e gestão de TI da organização*.

Fonte: COBIT 5 Framework

COBIT – introdução

4. Governança e gestão eficiente e eficaz de TI da organização requer uma abordagem holística, levando em conta seus diversos componentes interligados. O COBIT 5 define um conjunto de habilitadores para apoiar a implementação de um sistema abrangente de gestão e governança de TI da organização. Habilitadores são geralmente definidos como qualquer coisa que possa ajudar a atingir os objetivos corporativos.

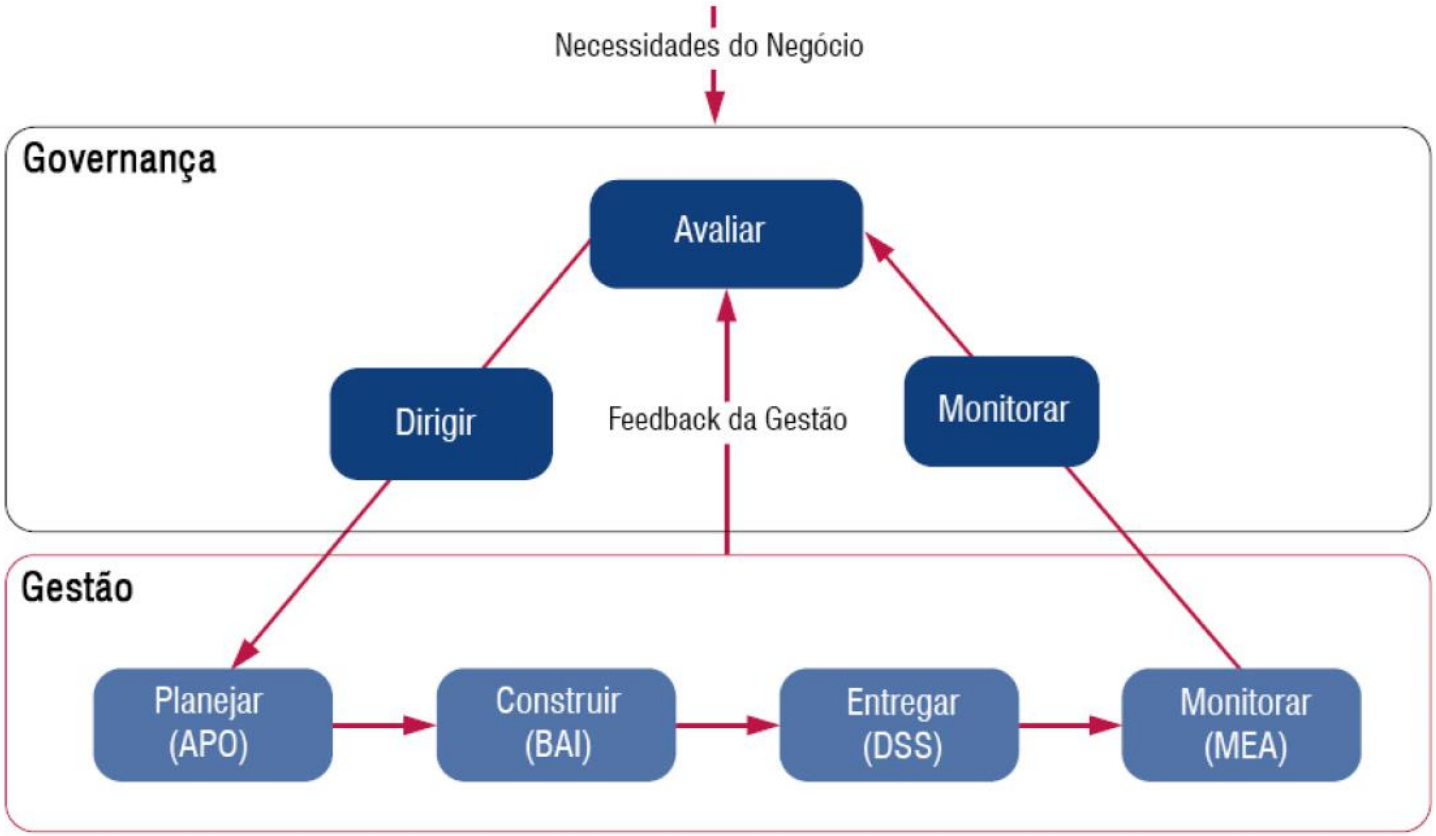
Fonte: COBIT 5 Framework

COBIT – introdução

5. O modelo do COBIT 5 faz uma clara distinção entre governança e gestão. Essas duas disciplinas compreendem diferentes tipos de atividades, exigem modelos organizacionais diferenciados e servem a propósitos diferentes.

Fonte: COBIT 5 Framework

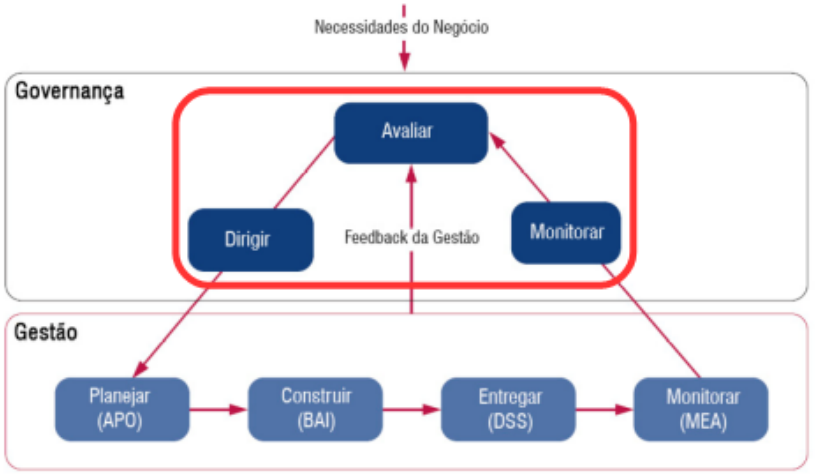
COBIT – áreas chaves



Áreas chaves da Governança e do Gerenciamento

COBIT – áreas chaves

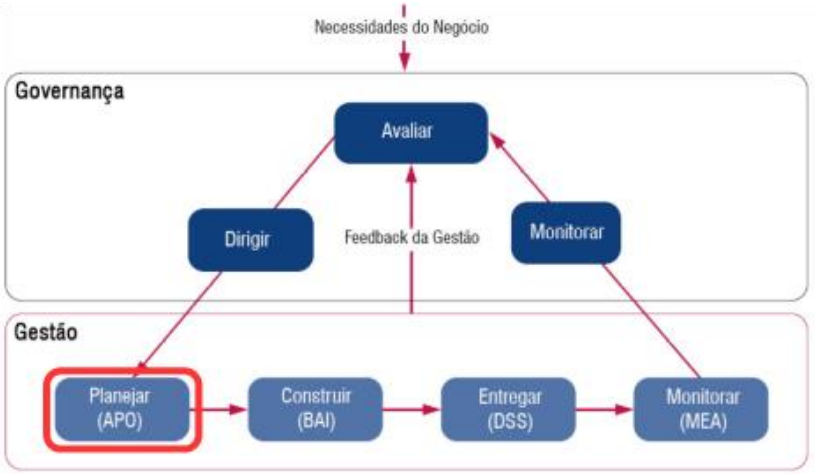
O domínio Avaliar, Dirigir e Monitorar (Evaluate, Direct and Monitor – EDM) possui cinco processos de governança, os quais ditam as responsabilidades da alta direção para a avaliação, direcionamento e monitoração do uso dos ativos de TI para a criação de valor. Este domínio cobre a definição de um framework de governança, o estabelecimento das responsabilidades em termos de valor para a organização, fatores de risco e recursos, além da transparência da TI para as partes interessadas.



Fonte: GAEA apud Luzia Dourado

COBIT – áreas chaves

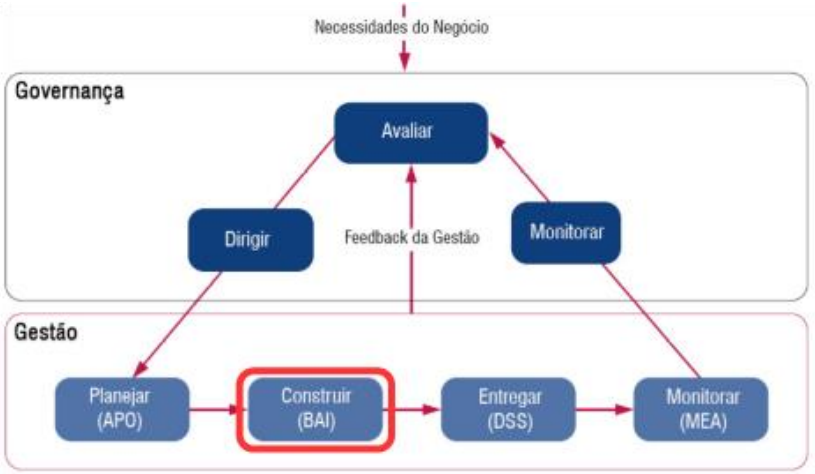
O domínio Alinhar, Planejar e Organizar (Align, Plan and Organize – APO) possui treze processos, os quais dizem respeito à identificação de como a TI pode contribuir melhor com os objetivos corporativos. Processos específicos deste domínio estão relacionados com a estratégia e táticas de TI, arquitetura corporativa, inovação e gerenciamento de portfólio, orçamento, qualidade, riscos e segurança.



Fonte: GAEA apud Luzia Dourado

COBIT – áreas chaves

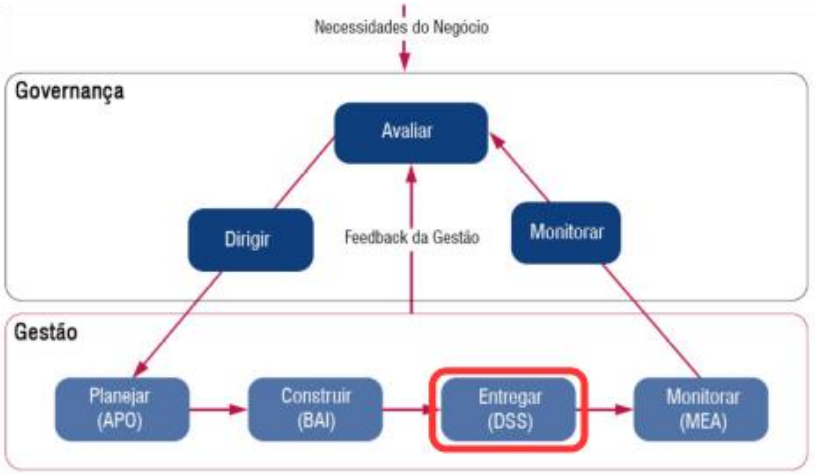
O domínio Construir, Adquirir e Implementar (Build, Acquire and Implement – BAI) possui dez processos, que tornam a estratégia de TI concreta, identificando os requisitos para a TI e gerenciando o programa de investimentos em TI e projetos associados. Este domínio também endereça o gerenciamento da disponibilidade e capacidade; mudança organizacional; gerenciamento de mudanças (TI); aceite e transição; e gerenciamento de ativos, configuração e conhecimento.



Fonte: GAEA apud Luzia Dourado

COBIT – áreas chaves

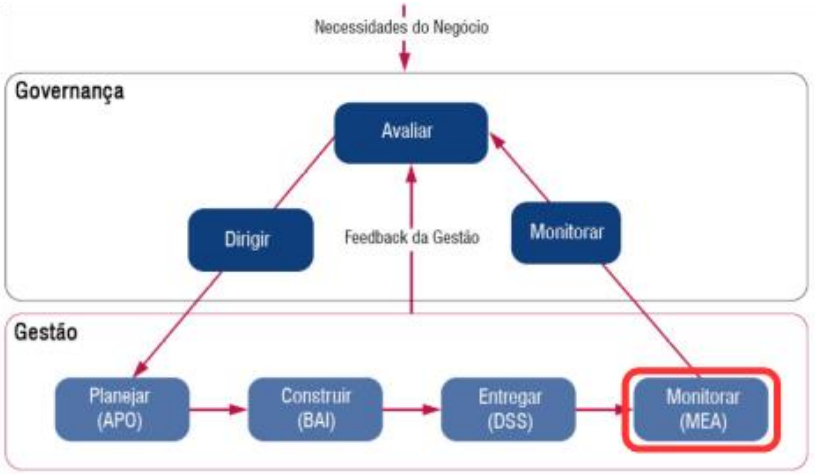
O domínio Entregar, Serviço e Suporte (Deliver, Service and Support – DSS) possui seis processos, que se referem à entrega dos serviços de TI necessários para atender aos planos táticos e estratégicos. O domínio inclui processos para gerenciar operações, requisições de serviços e incidentes, assim como o gerenciamento de problemas, continuidade, serviços de segurança e controle de processos de negócio.



Fonte: GAEA apud Luzia Dourado

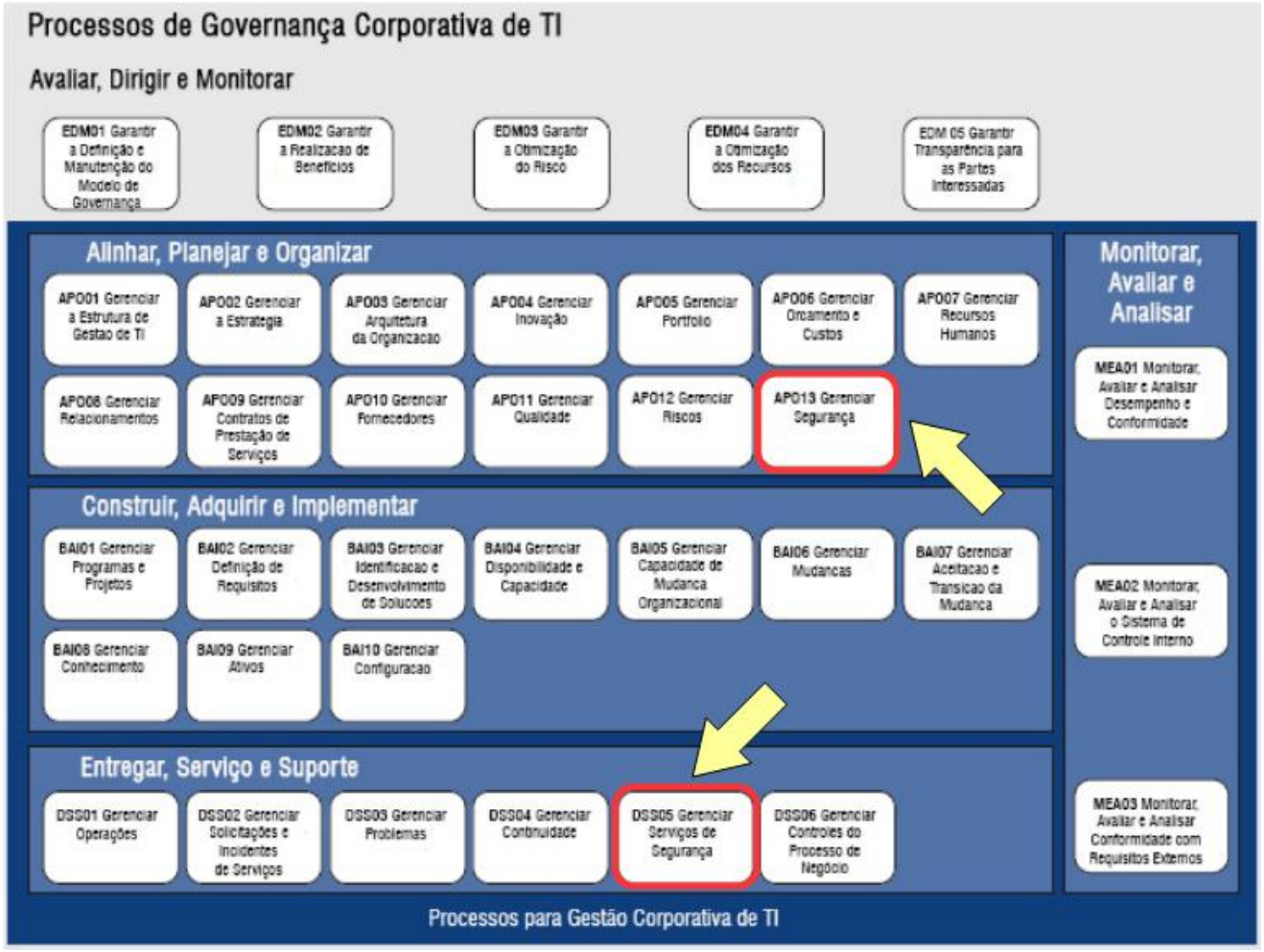
COBIT – áreas chaves

O domínio Monitorar, Avaliar e Analisar (Monitor, Evaluate and Assess – MEA) possui três processos, que visam monitorar o desempenho dos processos de TI, avaliando a conformidade com os objetivos e com os requisitos externos.



Fonte: GAEA apud Luzia Dourado

COBIT – modelo de referência



Modelo de referência de processos

COBIT – habilitador de processos

- APO13 – Gerenciar a Segurança: Definir, operar e monitorar um sistema de gestão de Segurança da Informação. Manter o impacto e a ocorrência de incidentes de segurança da informação dentro dos níveis aceitáveis de risco acordados pela organização.
- DSS05 – Gerenciar Serviços de Segurança: Proteger os ativos da empresa para manter os níveis aceitáveis de risco que estejam de acordo com a política de segurança. Estabelecer e manter as funções de segurança da informação e privilégios de acesso e realizar o monitoramento da segurança. Minimizar o impacto no negócio proveniente de vulnerabilidades e incidentes de segurança de informação.

Matriz de responsabilidade RACI

R

Responsible (Executor ou Responsável pela execução)

É quem executa a tarefa e efetivamente trabalha na atividade, mesmo que não tenha autoridade final sobre sua aprovação. Uma ou mais pessoas podem ser designadas.

A

Accountable (Decisor ou com Autoridade para aprovar)

É quem aprova a execução e dá o aceite formal da tarefa ou produto entregue. Responde ainda pelos resultados e consequências da tarefa realizada pelo executor, ou seja, é o prestador de contas. Apenas um decisor pode ser atribuído por atividade.

C

Consulted (Consultado)

São pessoas com conhecimento sobre determinados assuntos que podem contribuir com a execução das tarefas e são responsáveis por fornecerem informações úteis para sua conclusão. A comunicação com esse grupo será em duas vias.

I

Informed (Informado)

São pessoas informadas sobre o progresso e situação das tarefas, mas não precisam estar envolvidos no processo de tomada de decisão. A comunicação com esse grupo será em mão única.

Matriz de responsabilidade RACI – APO13

APO13 RACI Chart																									
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO13.01 Establish and maintain an ISMS.		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Define and manage an information security risk treatment plan.		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Monitor and review the ISMS.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Apenas um decisor (accountable) por atividade.

Matriz de responsabilidade RACI – DSS05

DSS05 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS05.01 Protect against malware.						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Manage network and connectivity security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Manage endpoint security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Manage user identity and logical access.						R					C	A			I	C	C	C	I	C	R		I	R		C

Apenas um decisor (accountable) por atividade.

Para saber mais...

… leia a apostila COBIT 5 – Framework de Governança e Gestão Corporativa de TI – v1.2, de Luiza Dourado.

… veja o processo COBIT 5 – APO13 Manage Security Process.

… veja o processo COBIT 5 – DSS05 Manage Security Services Process.

Módulo 4

Melhores Práticas de Entrega de Serviços

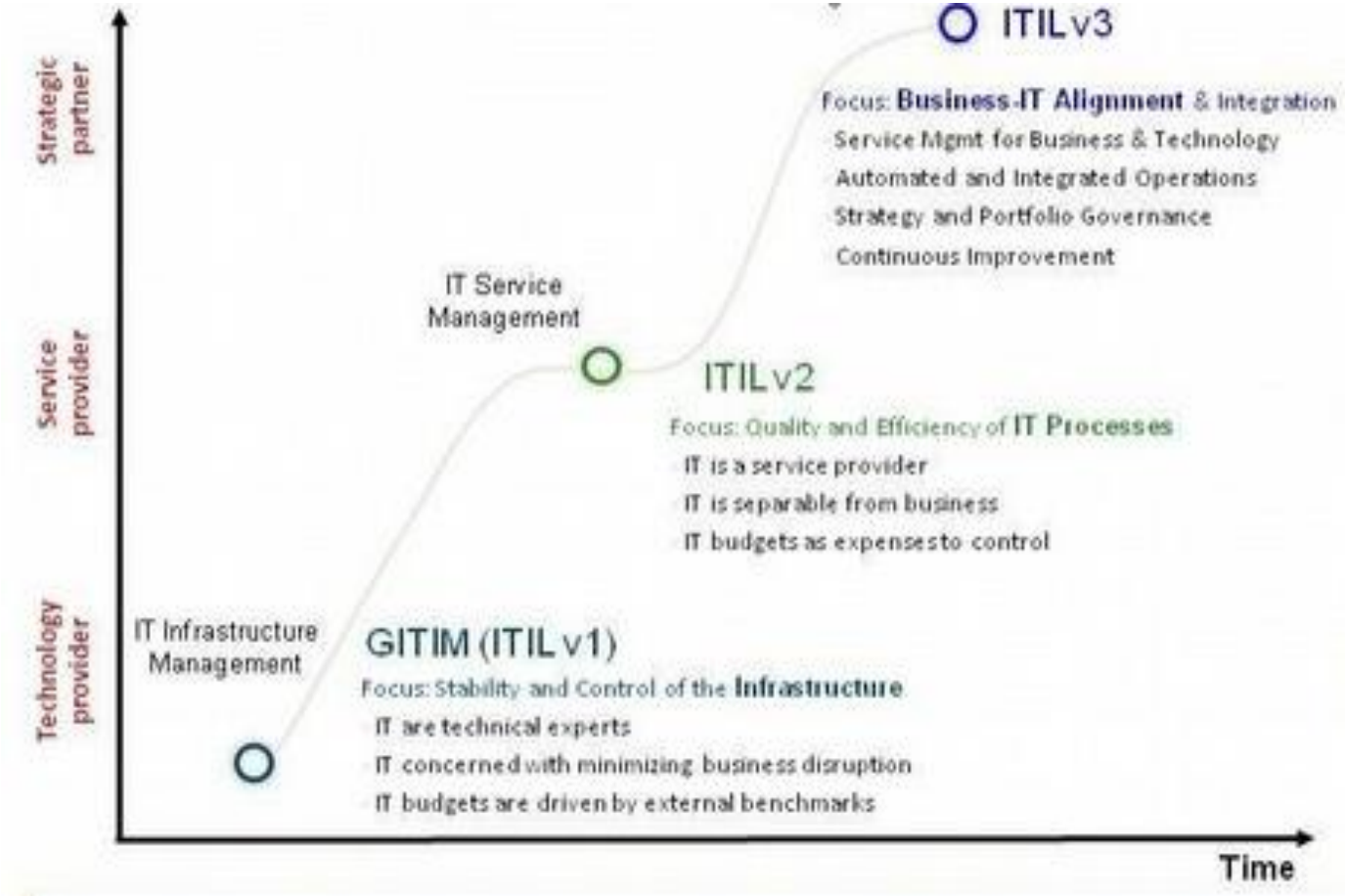
ITIL – introdução

ITIL é um conjunto de melhores práticas para a gestão de serviços de TI. Ela fornece orientação para os prestadores de serviços no provisionamento de serviços de TI de qualidade, e também sobre os processos, funções e outros recursos necessários para apoiá-los. ITIL é usado por muitas organizações para criar valor para o prestador de serviços e seus clientes.

Ciclo de vida de serviços

Fonte: ITIL 3 Service Strategy

ITIL – evolução



ITIL – serviço

- Serviço: Um meio de entregar valor aos clientes de modo que os resultados possam ser alcançados sem que os clientes tenham a propriedade dos custos e riscos específicos.
- Serviços de TI: Um serviço prestado por um fornecedor de serviços de TI. Um serviço de TI é composto por um combinação de tecnologia da informação, pessoas e processos. Um serviço de TI voltado para o cliente apoia diretamente seus processos de negócio e suas metas de nível de serviço devem ser definidos em um acordo de nível de serviço. Outros serviços de TI, chamados serviços de apoio e suporte, não são diretamente utilizados pela organização, mas são requeridos pelo fornecedor de serviços para entregar serviços voltados para o cliente.

Fonte: ITIL 3 Service Strategy

ITIL – criação de valor

O valor de um serviço pode ser considerado como o nível em que o serviço atende as expectativas de um cliente. Muitas vezes é medido pelo quanto o cliente está disposto a pagar pelo serviço, ao invés do custo do serviço ou qualquer outro atributo intrínseco do próprio serviço. O valor precisa ser definido em termo de três áreas: os resultados alcançados pelo negócio, as preferências do cliente e a percepção do cliente sobre o que foi entregue.

Fonte: ITIL 3 Service Strategy

ITIL – criação de valor

O resultado do negócio é alcançado quando o serviço facilita a realização das tarefas dos processos de negócios;

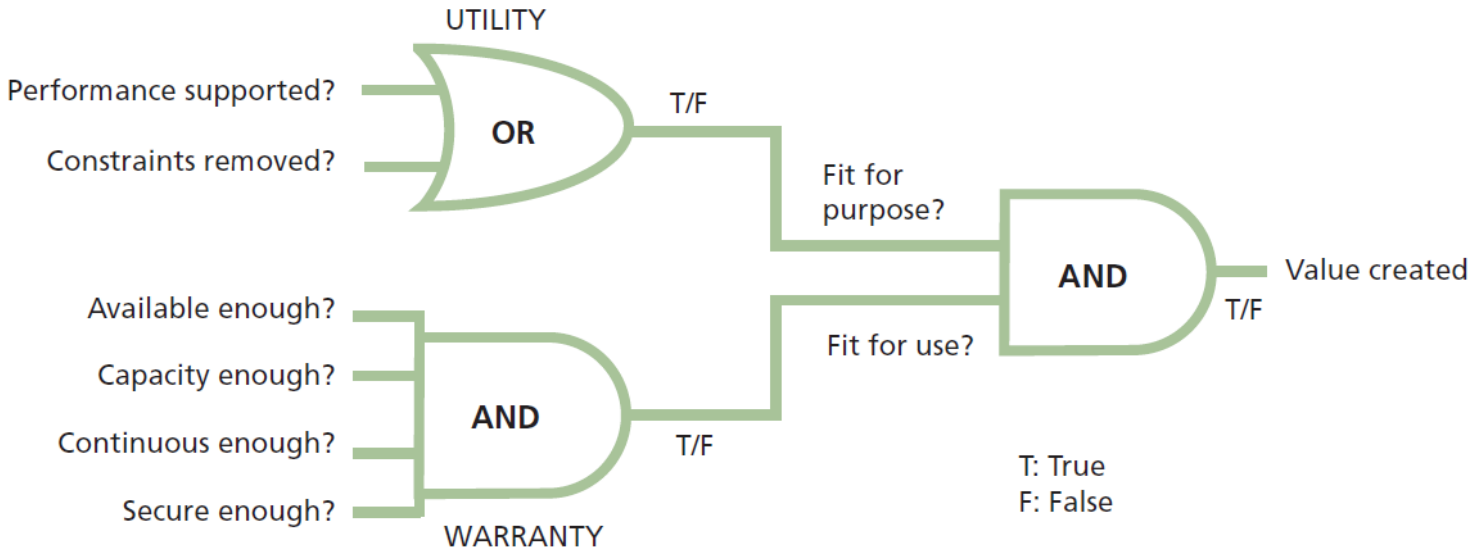
A preferência do cliente é influenciada pela sua percepção, que forma um filtro de qualidade e ajuda a escolher o prestador de serviço adequado;

Já as percepções se baseiam em atributos do serviço que possam ser medidos e/ou comparados com a concorrência.

Fonte: ITIL 3 Service Strategy

ITIL – valor de serviço

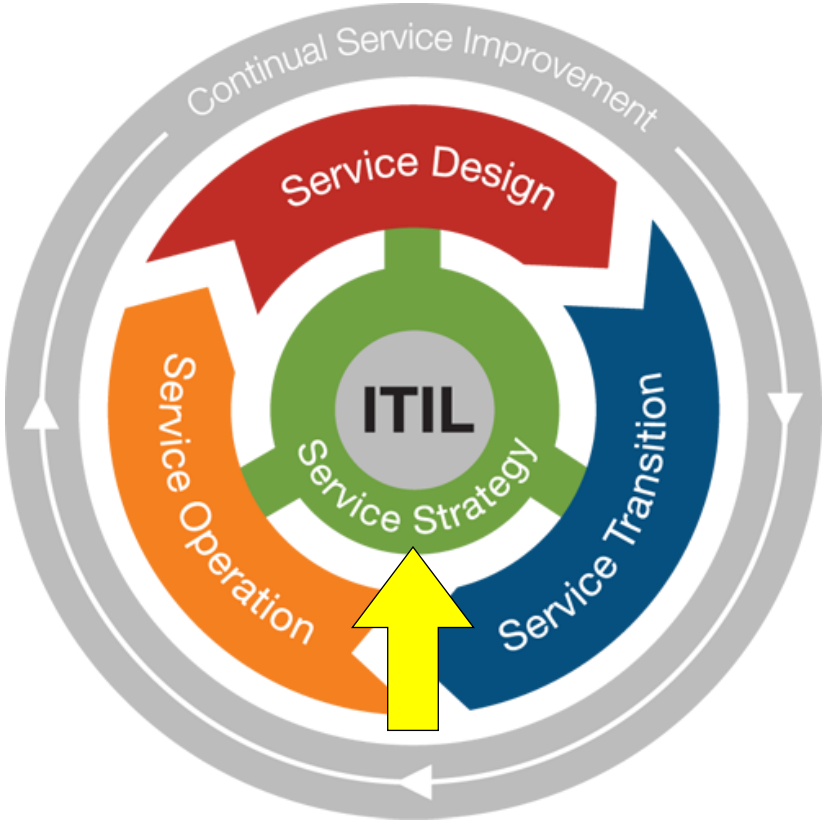
- Utilidade (Utility) – é a funcionalidade oferecida pelo produto ou serviço que atende uma necessidade em particular.
- Garantia (Warranty) – é a salvaguarda ou a certeza de que o produto ou serviço irá atender os requisitos acordados.



Fonte: ITIL 3 Service Strategy

ITIL – ciclo de vida

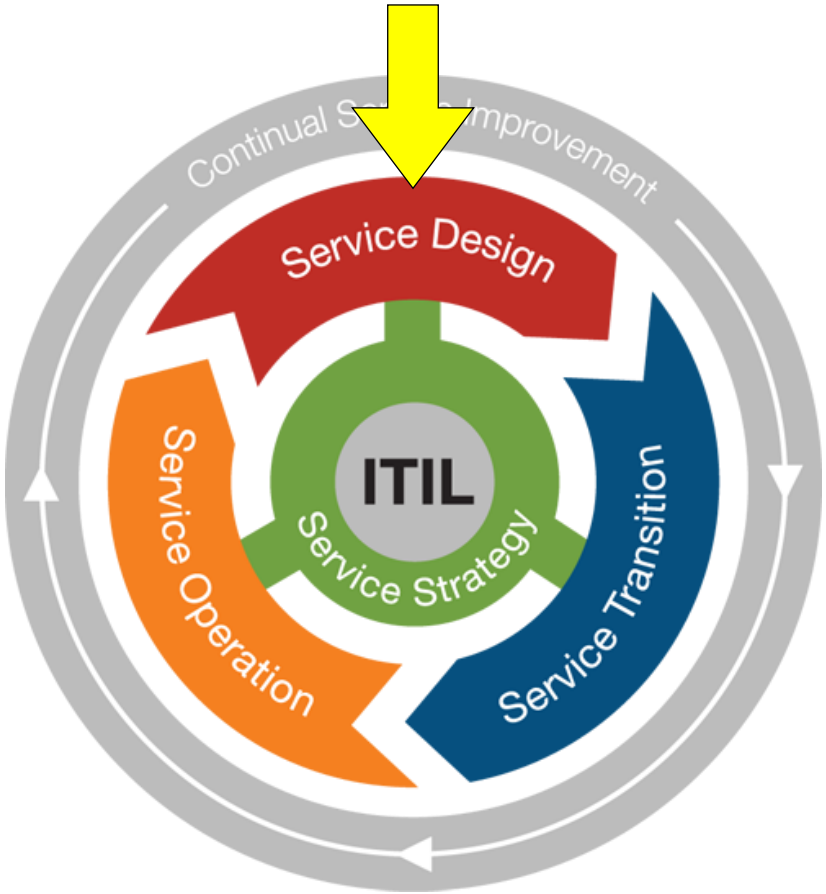
A Estratégia de Serviço fornece orientação sobre como visualizar o gerenciamento de serviços não só como uma capacidade organizacional, mas como um ativo estratégico. Ela descreve os princípios que sustentam a prática da gestão de serviços que são úteis para o desenvolvimento de políticas de gerenciamento de serviços, orientações e processos em todo o ciclo de vida de serviços.



Fonte: ITIL 3 Service Strategy

ITIL – ciclo de vida

O Desenho de Serviço fornece orientação para a concepção e desenvolvimento de serviços e práticas de gerenciamento de serviços. Abrange princípios e métodos de desenho para a conversão de objetivos estratégicos em catálogos de serviços e ativos de serviços. O escopo do Desenho de Serviço ITIL não se limita a novos serviços. Ele inclui as mudanças e melhorias necessárias para aumentar ou manter o valor aos clientes ao longo do ciclo de vida dos serviços, a continuidade dos serviços, obtenção de níveis de serviço e de conformidade a normas e regulamentos. Ele orienta as organizações sobre como desenvolver capacidades de desenho para gerenciamento de serviços.



Fonte: ITIL 3 Service Strategy

ITIL – ciclo de vida

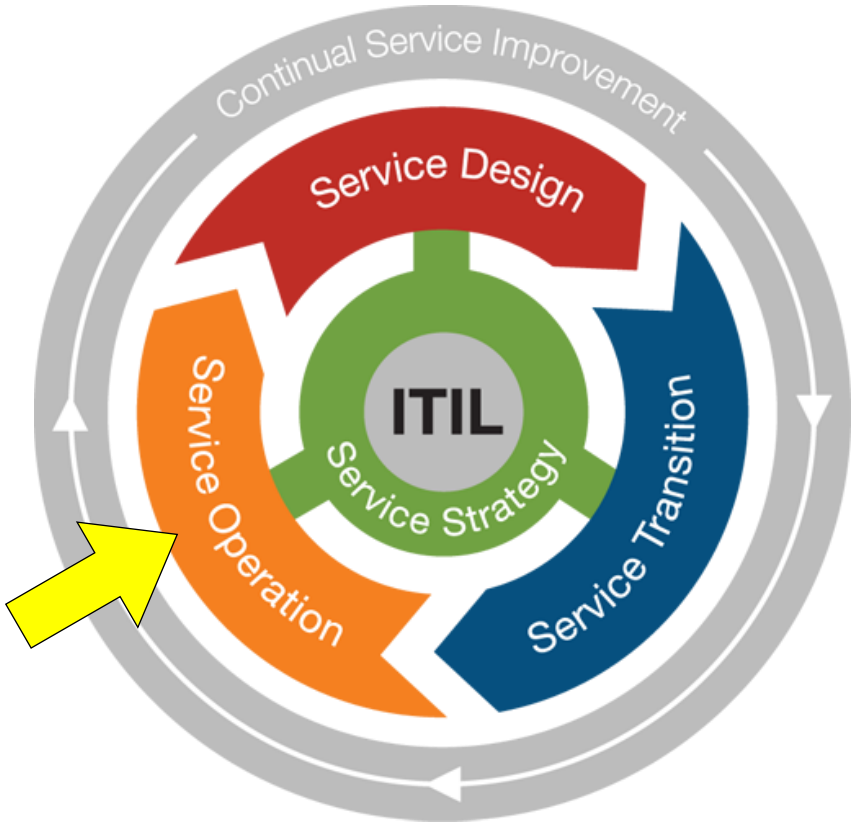
A Transição de Serviço fornece orientação para o desenvolvimento e melhoramento das capacidades para a introdução de serviços novos e modificados em ambientes suportados. Ela descreve como fazer a transição de uma organização de um estado para outro, enquanto controla o risco e apoia o conhecimento organizacional para suporte à decisão. Ela assegura que o valor identificado na estratégia de serviço, e codificado em desenho de serviço, seja efetivamente implementado e possa ser utilizado na operação de serviço.

Fonte: ITIL 3 Service Strategy

ITIL – ciclo de vida

A Operação de Serviço descreve as melhores práticas para o gerenciamento de serviços em ambientes suportados. Ela inclui orientações sobre como alcançar a eficácia e a eficiência na entrega e suporte de serviços para garantir valor ao cliente, usuários e prestadores do serviço.

continua...

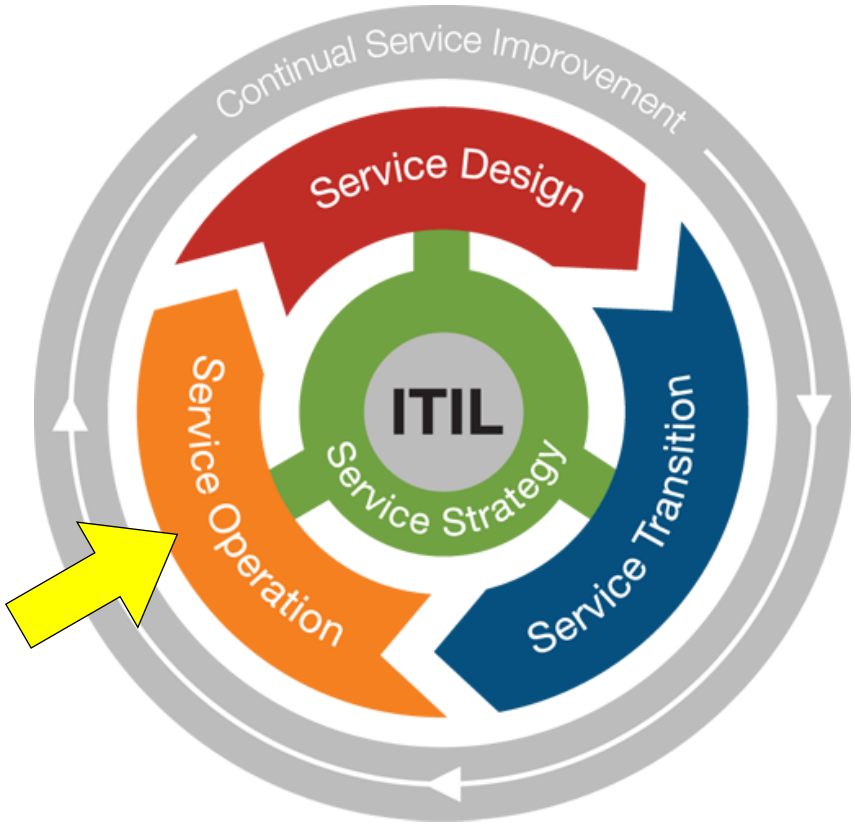


Fonte: ITIL 3 Service Strategy

ITIL – ciclo de vida

... continuação

Os objetivos estratégicos são, em última análise, realizada através de operação de serviço. Ela fornece também orientação sobre como manter a estabilidade na operação do serviço, permitindo mudanças no desenho, escala, escopo e níveis de serviços. A Operação de Serviço fornece processos detalhados, diretrizes, métodos e ferramentas para uso em duas grandes perspectivas de controle: reativas e proativas. A Operação de Serviço fornece ferramentas que permitem tomar melhores decisões em áreas como a gestão da disponibilidade de serviços, controle da demanda, otimização da capacidade, agendamento de operações, gestão de incidentes e gerenciamento de problemas.

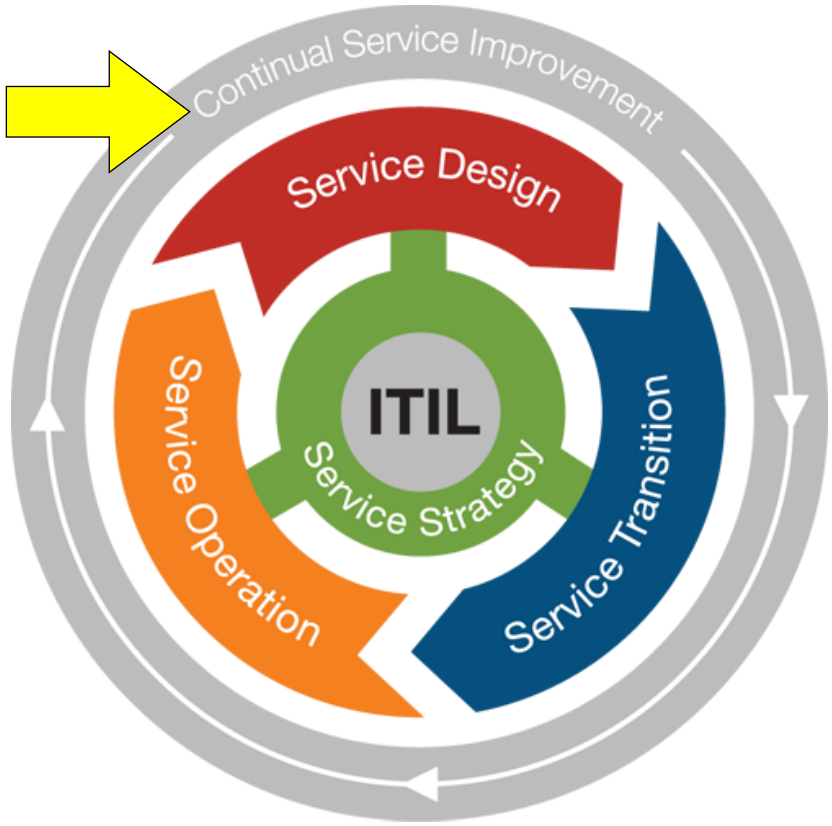


Fonte: ITIL 3 Service Strategy

ITIL – ciclo de vida

A Melhoria Contínua de Serviço fornece orientações sobre a criação e manutenção de valor para os clientes através de uma melhor estratégia, desenho, transição e operação de serviços. Ela combina princípios, práticas e métodos de gestão da qualidade, gestão da mudança e melhoria da capacidade.

continua...



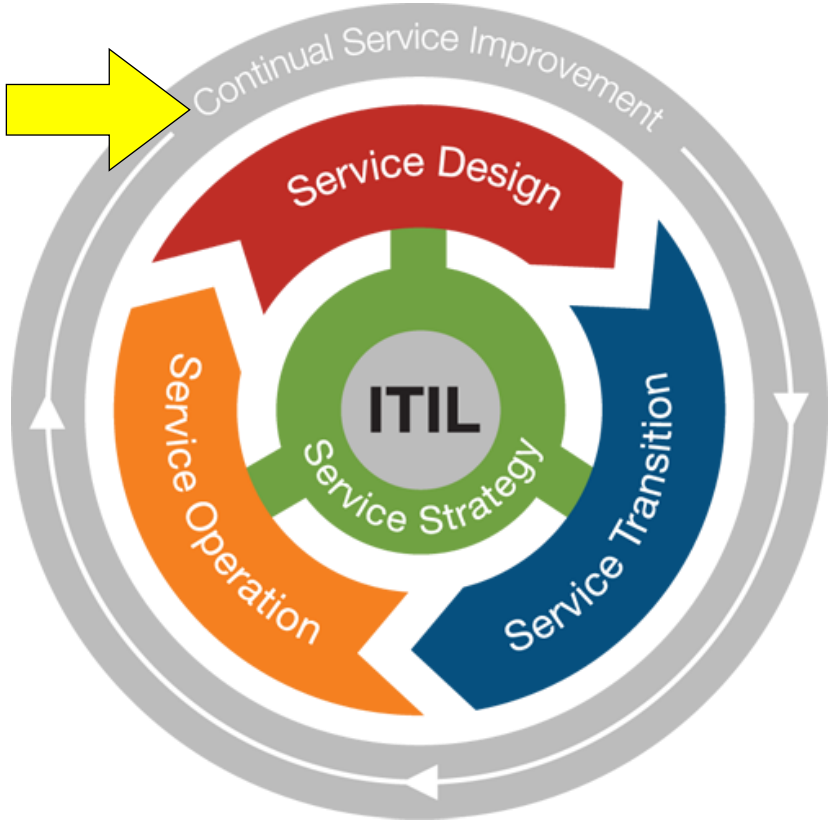
Fonte: ITIL 3 Service Strategy

ITIL – ciclo de vida

… continuação

A Melhoria Contínua de Serviço descreve ainda as melhores práticas para a obtenção de melhorias incrementais e em grande escala na qualidade do serviço, a eficiência operacional e continuidade de negócios, e assegura que o catálogo de serviços continua alinhado às necessidades do negócio.

Ela permite também conectar os esforços de melhoria e resultados com estratégia de serviço, desenho, transição e operação.



Fonte: ITIL 3 Service Strategy

ITIL – processos

ITIL – processos

A finalidade do processo de gestão de segurança da informação é alinhar a segurança de TI com a política de segurança da informação da organização e assegurar que a confidencialidade, integridade e disponibilidade dos ativos, informações, dados da organização e serviços de TI sempre correspondam às necessidades acordadas do negócio.

O objetivo da gestão da segurança da informação é a de proteger os interesses daqueles que se baseiam em informações e nos sistemas de comunicações que as fornecem de qualquer dano resultante de falhas de confidencialidade, integridade e disponibilidade.

Fonte: ITIL 3 Service Strategy

Para saber mais...

… veja o Processo ITIL v3 – Information Security Management Process.

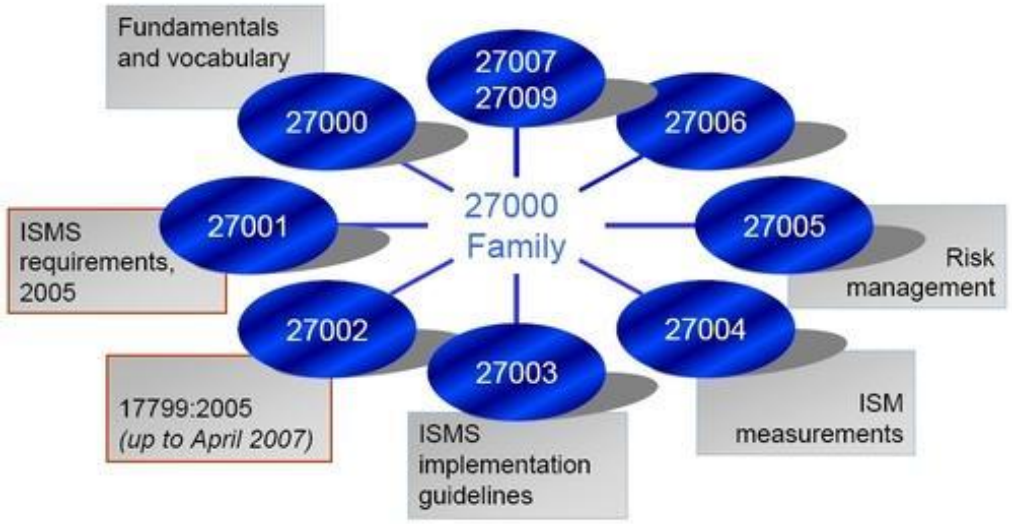
Módulo 5

Guia para Certificação de Sistemas de Gestão de Segurança da Informação

ISO/IEC 27000 – série

ISO/IEC 27000 é uma série abrangente de boas práticas para o gerenciamento da segurança da informação, dos riscos e dos controles:

- ISO/IEC 27001 – guia para certificação de sistemas de gestão de segurança da informação;
- ISO/IEC 27002 (antiga ISO/IEC 17799) – código de boas práticas.



Família de padrões ISO/IEC para Sistemas de Gerenciamento de Segurança da Informação

ISO/IEC 27001 – introdução

A ISO/IEC 27001:2013 foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). A sua adoção deve ser uma decisão estratégica da organização. O estabelecimento e a implementação do SGSI de uma organização são influenciados por:

a) suas necessidades e objetivos;

b) requisitos de segurança;

c) processos organizacionais; e

d) tamanho e estrutura da organização.

O SGSI preserva a confiabilidade (confidencialidade, integridade e disponibilidade) da informação por meio da aplicação de um processo de gestão de riscos, fornecendo a garantia necessária para as partes interessadas de que os riscos são adequadamente gerenciados.

É importante que o SGSI esteja integrado aos processos da organização!

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – processos

Processo é um conjunto de atividades que faz uso de recursos (humanos, materiais, financeiros, etc.) e que são gerenciados de forma a se obter um resultado.

De acordo com a ISO/IEC 27001:2006, a aplicação de um sistema de processos dentro de uma organização, junto com a identificação e interações destes processos, e a sua gestão podem ser consideradas como "abordagem de processo".

Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

Atualização da versão

A ISO/IEC 27001:2006 indicava claramente que o modelo “Plan-Do-Check-Act” (PDCA) era o que deveria ser aplicado por padrão para estruturar todos os processos do SGSI.

Já a nova versão da ISO/IEC 27001:2013 não especifica nenhum modelo de processo em particular. Ela exige apenas que seja utilizado um processo de melhoria contínua, a critério da organização.

Implicações para a transição

Para organizações com um SGSI já existente não há a necessidade de mudança, pois o modelo PDCA ainda é válido.

Já as organizações que estejam iniciando um SGSI baseado na ISO/IEC 27001:2013, devem identificar o melhor processo de melhoria contínua para o seu negócio.

ISO/IEC 27001 – abordagem

A abordagem de processo para a gestão da segurança da informação descrito na ISO/IEC 27001:2006 encoraja que seus usuários enfatizem a importância dos seguintes aspectos:

a) entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;

b) implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;

c) monitoração e análise crítica do desempenho e eficácia do SGSI;

d) melhoria contínua baseada em medições objetivas.

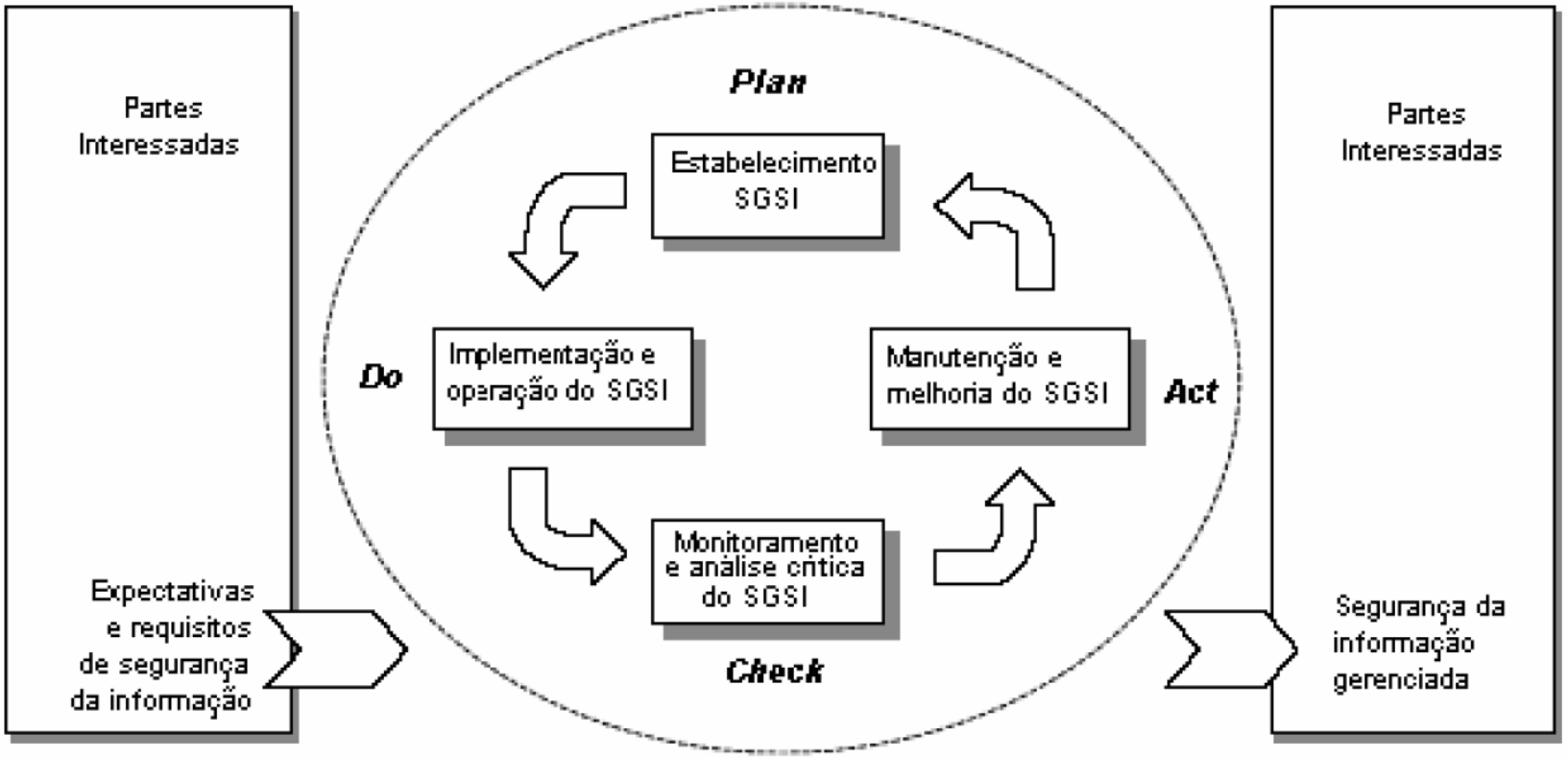
Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

A ISO/IEC 27001:2006 adota o modelo “Plan-Do-Check-Act” (PDCA), que é aplicado para estruturar todos os processos do SGSI. A figura abaixo ilustra como um SGSI considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas.

Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

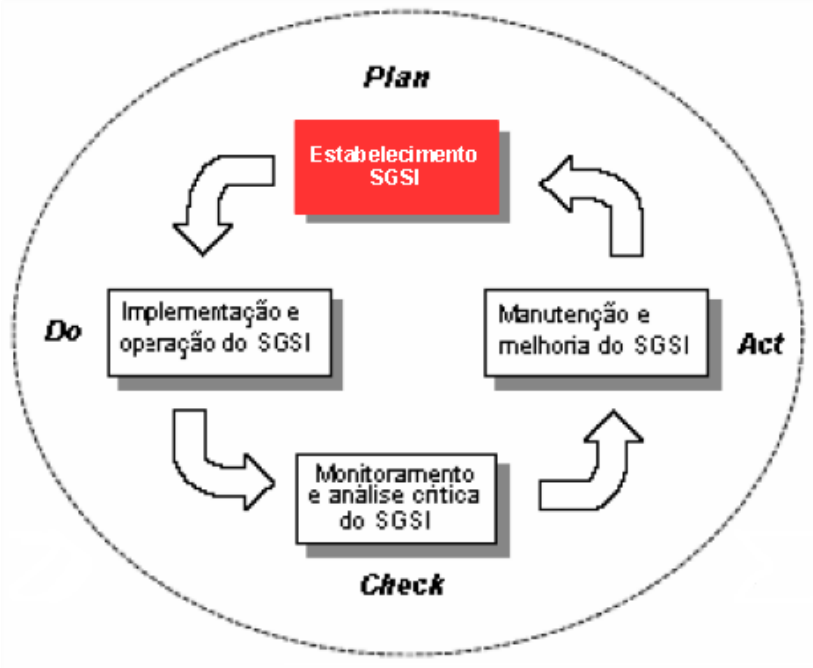


Modelo PDCA aplicado aos processos do SGSI

Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

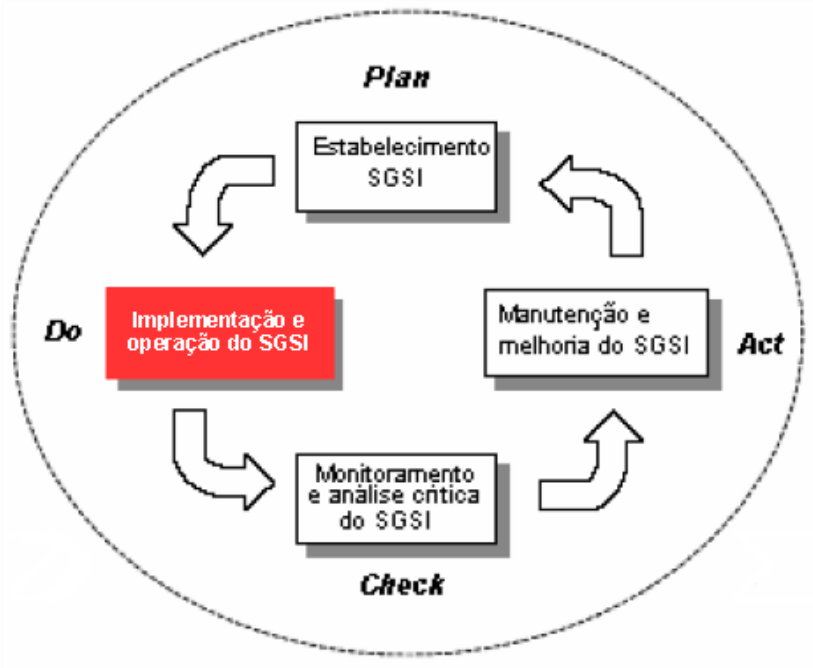
Plan – Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.



Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

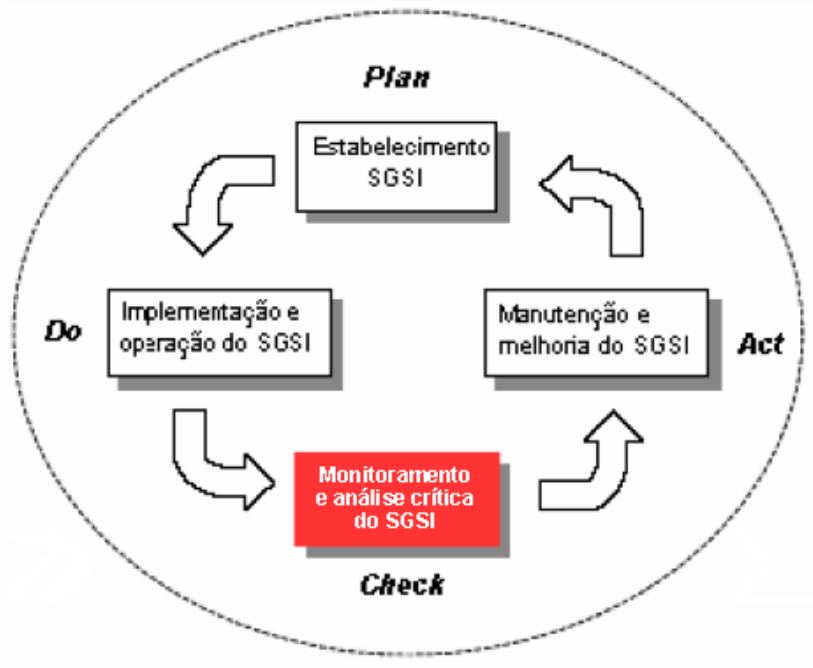
Do – Implementar e operar a política, controles, processos e procedimentos do SGSI.



Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

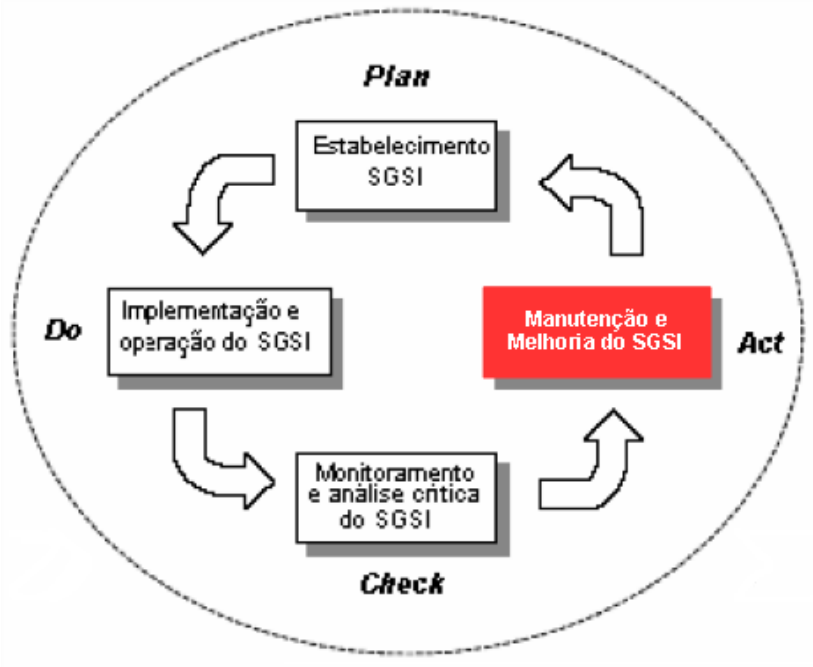
Check – Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.



Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

Act – Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.



Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – escopo

A ISO/IEC 27001:2013 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

Esta norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

Os requisitos definidos nesta norma são genéricos e são pretendidos para serem aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.

A exclusão de quaisquer dos requisitos especificados nas seções Contexto da Organização, Liderança, Planejamento, Apoio, Operação, Avaliação do Desempenho e Melhoria não é aceitável quando a organização busca a conformidade com esta norma**.

Para estes casos, deve-se aplicar a Declaração de Aplicabilidade, que é uma declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da organização, pois ela provê um resumo das decisões relativas ao tratamento de riscos. A justificativa das exclusões provê ainda uma checagem cruzada de que nenhum controle foi omitido inadvertidamente*.

Fontes: *NBR ISO/IEC 27001:2006 e **NBR ISO/IEC 27001:2013

ISO/IEC 27001 – contexto da organização

Entendendo a organização e seu contexto

A organização deve determinar as questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação**.

Entendendo as necessidades e as expectativas das partes interessadas

A organização deve determinar:

a) as partes interessadas que são relevantes para o sistema de gestão da segurança da informação; e

b) os requisitos dessas partes interessadas relevantes para a segurança da informação.

**NOTA: Para determinar as questões referentes ao estabelecimento do contexto interno e externo da organização, verificar o item 5.3 da NBR ISO 31000:2009, Gestão de riscos – Princípios e diretrizes.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – contexto da organização

Determinando o escopo do sistema de gestão da segurança da informação

A organização deve determinar os limites e a aplicabilidade do SGSI para estabelecer o seu escopo. Deve-se levar em consideração as questões internas e externas relevantes; os requisitos referenciados pelas partes interessadas, que podem incluir requisitos legais e regulamentares, bem como obrigações contratuais; e as interfaces e dependências entre as atividades desempenhadas pela organização e aquelas desempenhadas por outras organizações.

O escopo deve estar documentado.

Sistema de gestão da segurança da informação

A organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação, de acordo com os requisitos desta norma.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – liderança

Liderança e comprometimento

A alta direção da organização deve demonstrar sua liderança e comprometimento em relação ao SGSI pelos seguintes meios:

a) assegurando que a política de segurança da informação e seus objetivos estão estabelecidos e são compatíveis com a estratégia da organização;

b) garantindo a integração dos requisitos do SGSI dentro dos processos da organização;

c) assegurando que os recursos necessários para o SGSI estão disponíveis;

d) comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do SGSI;

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – liderança

Liderança e comprometimento – continuação...

e) assegurando que o SGSI alcança seus resultados pretendidos;

f) orientando e apoiando pessoas que contribuam para eficácia do SGSI;

g) promovendo a melhoria contínua; e

h) apoiando outros papéis relevantes da gestão para demonstrar como sua liderança se aplica às áreas sob sua responsabilidade

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – liderança

Política

A alta direção deve estabelecer uma política de segurança da informação que:

a) seja apropriada ao propósito da organização;

b) inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação;

c) inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação;

d) inclua o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

A política de segurança da informação deve ainda estar disponível como informação documentada, ser comunicada dentro da organização e estar disponível para as partes interessadas.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – liderança

Autoridades, responsabilidades e papéis organizacionais

A alta direção deve assegurar que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados.

A atribuição de responsabilidades e autoridade devem:

a) assegurar que o SGSI está em conformidade com os requisitos desta norma;

b) relatar sobre o desempenho do SGSI para a alta direção.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – planejamento

Ações para contemplar riscos e oportunidades – Geral

Quando do planejamento do SGSI, a organização deve levar em consideração as questões referenciadas no Contexto da Organização para determinar os riscos e oportunidades que precisam ser consideradas para assegurar que o SGSI possa alcançar os resultados pretendidos, mitigar os efeitos indesejados e promover a melhoria contínua.

A organização deve ainda planejar as ações para considerar estes riscos e oportunidades e promover a integração destas ações dentro dos processos do seu SGSI e avaliar a sua eficácia.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – planejamento

Ações para contemplar riscos e oportunidades – Avaliação de riscos

A organização deve definir e aplicar um processo de avaliação de riscos de segurança da informação que:

a) estabeleça e mantenha critérios de riscos de segurança da informação que incluam os critérios de aceitação do risco e os critérios para o desempenho das avaliações dos riscos de segurança da informação;

b) assegure que as contínuas avaliações de riscos de segurança da informação produzam resultados comparáveis, válidos e consistentes;

c) identifique os riscos de segurança da informação aplicando o processo de avaliação do risco de segurança da informação para identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade da informação dentro do escopo do sistema de gestão da segurança da informação e identificando os responsáveis dos riscos;

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – planejamento

Ações para contemplar riscos e oportunidades – Avaliação de riscos – cont....

d) analise os riscos de segurança da informação, avaliando as consequências potenciais que podem resultar se os riscos identificados forem materializados, avaliando a probabilidade realística da ocorrência dos riscos identificados e determinando os níveis de risco;

e) avalie os riscos de segurança da informação, comparando os resultados da análise dos riscos com os critérios de riscos estabelecidos e priorizando os riscos analisados para o tratamento do risco.

O processo de avaliação de riscos de segurança da informação deve ser documentado.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – planejamento

Ações para contemplar riscos e oportunidades – Tratamento de riscos

A organização deve definir e aplicar um processo de tratamento dos riscos de segurança da informação para:

a) selecionar, de forma apropriada, as opções de tratamento dos riscos de segurança da informação, levando em consideração os resultados da avaliação do risco;

b) determinar todos os controles que são necessários para implementar as opções escolhidas do tratamento do risco da segurança da informação;

c) comparar os controles necessários para implementar as opções de tratamento dos riscos de segurança da informação com aqueles constantes da Tabela de Referência aos Controles e Objetivos de Controle e verificar se algum controle necessário foi omitido;

d) elaborar uma declaração de aplicabilidade que contenha os controles necessários e a justificativa para inclusões, sejam eles implementados ou não, bem como a justificativa para a exclusão dos controles da Tabela de Referência aos Controles e Objetivos de Controle;

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – planejamento

Ações para contemplar riscos e oportunidades – Tratamento de riscos – cont....

e) preparar um plano para tratamento dos riscos de segurança da informação; e

f) obter a aprovação dos responsáveis pelos riscos do plano de tratamento dos riscos de segurança da informação e a aceitação dos riscos residuais de segurança da informação.

O processo de tratamento dos riscos de segurança da informação deve ser documentado.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – planejamento

Objetivo de segurança da informação e planejamento para alcançá-los

A organização deve estabelecer os objetivos de segurança da informação para as funções e níveis relevantes.

Os objetivos de segurança da informação devem ser consistentes com a política de segurança da informação, ser mensuráveis (quando aplicável), levar em conta os requisitos de segurança da informação aplicáveis e os resultados da avaliação e tratamento dos riscos, comunicados e atualizados, conforme apropriado.

Quando do planejamento para alcançar os seus objetivos de segurança da informação, a organização deve determinar o que será feito, quais recursos serão necessários, quem será responsável, quando estará concluído e como os resultados serão avaliados.

Os objetivos de segurança da informação devem ser documentados.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Recursos

A organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI.

Competência

A organização deve:

a) determinar a competência necessária das pessoas que realizam trabalho sob o seu controle e que afeta o desempenho da segurança da informação;

b) assegurar que essas pessoas são competentes, com base na educação, treinamento ou experiência apropriados;

c) onde aplicável, tomar ações para adquirir a competência necessária e avaliar a eficácia das ações tomadas; e

d) reter informação documentada apropriada como evidência da competência.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Conscientização

Pessoas que realizam trabalho sob o controle da organização devem estar cientes da:

a) política de segurança da informação;

b) suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e

c) implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Comunicação

A organização deve determinar as comunicações internas e externas relevantes para o sistema de gestão da segurança da informação incluindo:

a) o que comunicar;

b) quando comunicar;

c) quem comunicar;

d) quem será comunicado; e

e) o processo pelo qual a comunicação será realizada.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Informação documentada – Geral

O sistema de gestão da segurança da informação da organização deve incluir:

a) informação documentada requerida pela ISO/IEC 27001:2013;

b) informação documentada determinada pela organização como sendo necessária para a eficácia do SGSI.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Informação documentada – Criando e atualizando

Quando da criação e atualização da informação documentada, a organização deve assegurar, de forma apropriada:

a) identificação e descrição (por exemplo, título, data, autor ou um número de referência);

b) formato (por exemplo, linguagem, versão do software, gráficos) e o seu meio (por exemplo, papel, eletrônico); e

c) análise crítica e aprovação para pertinência e adequação.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Informação documentada – Controle

A informação documentada requerida pelo SGSI deve ser controlada para assegurar os requisitos de confiabilidade, ou seja, confidencialidade, integridade e disponibilidade.

Para o controle da informação documentada, a organização deve considerar as seguintes atividades, conforme aplicadas:

a) distribuição, acesso, recuperação e uso;

b) armazenagem e preservação, incluindo a preservação da legibilidade;

c) controle de mudanças (por exemplo, controle de versão);

d) retenção e disposição.

A informação documentada de origem externa, determinada pela organização como necessária para o planejamento e operação do SGSI, deve ser identificada e controlada.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – operação

Planejamento operacional e controle

A organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos de segurança da informação e para implementar as ações para contemplar riscos e oportunidades. A organização deve também implementar planos para alcançar os objetivos de segurança da informação, que devem ser consistentes com a política de segurança, mensuráveis, comunicados e atualizados, entre outros.

A organização deve manter a informação documentada, controlar as mudanças planejadas e analisar criticamente as consequências de mudanças não previstas, tomando ações para mitigar quaisquer efeitos adversos, conforme necessário.

A organização deve também assegurar que os processos terceirizados são controlados.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – operação

Avaliação de riscos de segurança da informação

A organização deve realizar avaliações de riscos de segurança da informação a intervalos planejados, ou quando mudanças significativas são propostas ou ocorrem, levando em conta os critérios de aceitação do risco.

Os resultados das avaliações de risco de segurança da informação devem ser documentados.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – operação

Tratamento de riscos de segurança da informação

A organização deve implementar o plano de tratamento de riscos de segurança da informação.

Os resultados do tratamento dos riscos de segurança da informação devem ser documentados.

OBS.: O "Tratamento de Riscos" é uma etapa do processo de "Gestão de Riscos" que é posterior a etapa de "Avaliação de Riscos", conforme a ISO/IEC 27005:2013. Na etapa de "Avaliação de Riscos", os riscos são identificados e os que não são aceitáveis devem ser selecionados. Na etapa de "Tratamento de Riscos" são selecionados um ou mais controles para tratar cada risco inaceitável de modo a mitigar todos eles.

O "Plano de Tratamento de Riscos" é uma espécie de plano de ação, onde são definidos quem, como, em qual prazo, com qual orçamento, etc, cada controle será implementado.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – avaliação de desempenho

Monitoramento, medição, análise e avaliação

A organização deve avaliar o desempenho da segurança da informação e a eficácia do SGSI. Ela deve determinar:

a) o que precisa ser monitorado e medido;

b) os métodos para monitoramento, medição, análise e avaliação, conforme aplicável, para assegurar resultados válidos;

c) quando o monitoramento e a medição devem ser realizados;

d) o que deve ser monitorado e medido;

e) quando os resultados do monitoramento e da medição devem ser analisados e avaliados e por quem.

A evidência do monitoramento e dos resultados da medição devem ser documentados.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – avaliação de desempenho

Auditoria interna

A organização deve conduzir auditorias internas a intervalos planejados para prover informações sobre o quanto o SGSI está em conformidade com os próprios requisitos da organização e os requisitos da ISO/IEC 27001:2013, bem como se está efetivamente implementado e mantido. A organização deve:

a) planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos pertinentes e os resultados de auditorias anteriores;

b) definir os critérios e o escopo da auditoria, para cada auditoria;

c) selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria;

d) assegurar que os resultados das auditorias são relatados para a direção pertinente.

Os programas de auditoria e seus resultados devem ser documentados.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – avaliação de desempenho

Análise crítica pela Direção

A alta direção deve analisar criticamente o SGSI da organização a intervalos planejados, para assegurar a sua contínua adequação, pertinência e eficácia.

A análise crítica pela direção deve incluir:

a) a situação das ações de análises críticas anteriores, realizadas pela direção;

b) as mudanças nas questões internas e externas, que sejam relevantes para o SGSI;

c) realimentação sobre o desempenho da segurança da informação, incluindo tendências em não conformidades e ações corretivas, monitoramento e resultados da medição, resultados de auditorias e cumprimento dos objetivos de segurança da informação;

d) realimentação das partes interessadas;

e) os resultados da avaliação dos riscos e situação do plano de tratamento dos riscos; e

f) as oportunidades para melhoria contínua.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – avaliação de desempenho

Análise crítica pela Direção – continuação...

Os resultados da análise crítica pela direção devem incluir decisões relativas a oportunidades para melhoria contínua e quaisquer necessidades para mudanças do SGSI.

Os resultados das análises críticas pela direção devem ser documentados.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – melhoria

Não conformidade e ação corretiva

Quando uma não conformidade ocorre, a organização deve:

a) reagir a não conformidade, tomando ações para controlá-la, corrigi-la e tratar com as consequências;

b) avaliar a necessidade de ações para eliminar as causas de não conformidade de modo a evitar sua repetição ou ocorrência, seja por um meio de sua análise crítica ou da determinação de suas causas;

c) implementar quaisquer ações necessárias;

d) analisar criticamente a eficácia de quaisquer ações corretivas tomadas; e

e) realizar mudanças no SGSI, quando necessário.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – melhoria

As ações corretivas devem ser apropriadas aos efeitos das não conformidades encontradas.

As não conformidades e os resultados de qualquer ação corretiva devem ser documentados.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – melhoria

Melhoria contínua

A organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão da segurança da informação.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – controles

Os objetivos de controle e controles apresentados na norma são derivados diretamente e estão alinhados com a ISO/IEC 27002:2013, e devem ser usados em alinhamento com o processo de tratamento de riscos de segurança da informação.

Ao todo são 14 (quatorze) categorias, 35 (trinta e cinco) objetivos de controle e 114 (cento e quatorze) controles.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – exemplos

A.5 Políticas de segurança da informação		
A.5.1 Orientação da Direção para segurança da informação		
Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.		
A.5.1.1	Políticas para segurança da informação	*Controle* Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela Direção, publicado e comunicado para os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica das políticas para segurança da informação	*Controle* As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – exemplos

A.8 Gestão de ativos		
A.8.1. Responsabilidade pelos ativos		
Objetivo: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.		
A.8.1.1	Inventário dos ativos	*Controle* Os ativos associados com informação e com os recursos e processamento da informação devem ser identificados, e um inventário destes ativos deve ser estruturado e mantido.
A.8.1.2	Proprietário dos ativos	*Controle* Os ativos mantidos no inventário devem ter um proprietário.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – exemplos

A.11 Segurança física e do ambiente		
A.11.1 Áreas seguras		
Objetivo: Prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização.		
A.11.1.1	Perímetro de segurança física	*Controle* Perímetros de segurança devem ser definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.
A.11.1.2	Controles de entrada física	*Controle* As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – exemplos

A.12.3 Cópias de segurança		
Objetivo: Proteger contra a perda de dados.		
A.12.3.1	Cópias de segurança das informações	*Controle* Cópias de segurança das informações, *softwares* e das imagens do sistema devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

Fonte: NBR ISO/IEC 27001:2013

Para saber mais...

… veja os Objetivos de Controle e Controles da ABNT NBR ISO/IEC 27001:2013.

Módulo 6

Melhores Práticas de Segurança da Informação

ISO/IEC 27002 – introdução

O que é Segurança da Informação?

Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio*.

Como a Segurança da Informação é alcançada?

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. Um sistema de gestão da segurança da informação (SGSI), a exemplo do especificado na ABNT NBR ISO/IEC 27001, considera uma visão holística e coordenada dos riscos de segurança da informação da organização, para implementar um conjunto de controles de segurança da informação detalhado, com base na estrutura global de um sistema de gestão coerente**.

Fontes: *NBR ISO/IEC 27002:2005 e **NBR ISO/IEC 27002:2013

ISO/IEC 27002 – introdução

Como estabelecer requisitos de segurança da informação?

É essencial que uma organização identifique os seus requisitos de segurança da informação. Existem três fontes principais de requisitos de segurança da informação:

1. A avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.
2. A legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.
3. Os conjuntos particulares de princípios, objetivos e os requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

A ABNT NBR ISO/IEC 27005 fornece diretrizes sobre gestão de riscos de segurança da informação, incluindo orientações sobre avaliação de riscos, tratamentos de riscos, aceitação de riscos, comunicação de riscos, monitoramento e análise crítica dos riscos.

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – análise de riscos

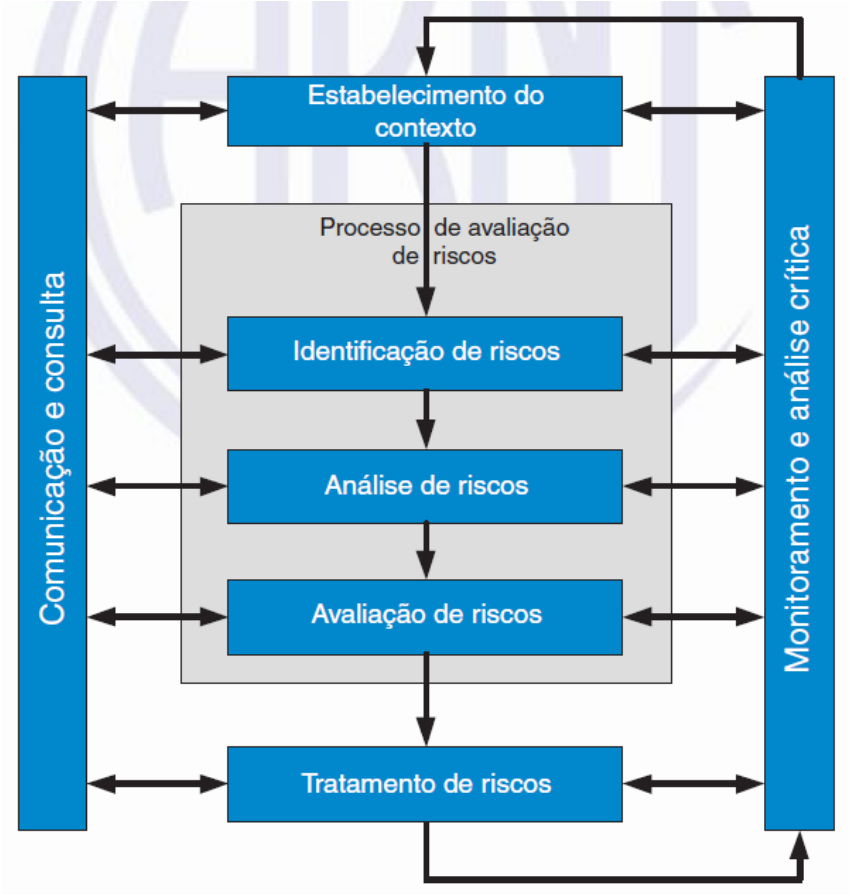
Analisando/avaliando os riscos de segurança da informação

As análises/avaliações de riscos devem:

- Identificar, quantificar e priorizar os riscos com base em critérios para aceitação dos mesmos, para orientar e determinar as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação;
- Incluir um enfoque sistemático para estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco);
- Ser realizadas periodicamente para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco. Essas análises/avaliações de riscos devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.
- Ter um escopo claramente definido para ser eficaz e incluir os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário.

Fonte: NBR ISO/IEC 27002:2005

ISO/IEC 27005 – gestão de riscos



Processo de Gestão de Riscos

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27002 – controles

Seleção de controles

Controles podem ser selecionados desta norma ou de outros conjuntos de controles, ou novos controles podem ser projetados para atender às necessidades específicas, conforme apropriado.

A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização, e convém que a seleção destes controles também esteja sujeita a todas as legislações e regulamentações nacionais e internacionais relevantes. A seleção de controles também depende da maneira pela qual os controles interagem para prover uma proteção segura.

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – estrutura

Estrutura da norma

Contém 14 seções de controles de segurança da informação, que juntas totalizam 35 categorias principais de segurança ou objetivos de controle, 114 controles e uma seção introdutória . Cada seção contém um número de categorias principais de segurança da informação, conforme listadas abaixo:

a) Políticas de Segurança da Informação (1 categoria e/ou objetivo de controle e 2 controles);

b) Organização da Segurança da Informação (2 categorias e/ou objetivos de controle e 7 controles);

c) Segurança em Recursos Humanos (3 categorias e/ou objetivos de controle e 6 controles);

d) Gestão de Ativos (3 categorias e/ou objetivos de controle e 10 controles);

e) Controle de Acessos (4 categorias e/ou objetivos de controle e 14 controles);

f) Criptografia (1 categoria e/ou objetivo de controle e 2 controles);

g) Segurança Física e do Ambiente (2 categorias e/ou objetivos de controle e 15 controles);

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – estrutura

Estrutura da norma – continuação...

h) Segurança nas Operações (7 categorias e/ou objetivos de controle e 14 controles);

i) Segurança nas Comunicações (2 categorias e/ou objetivos de controle e 7 controles);

j) Aquisição, Desenvolvimento e Manutenção de Sistemas (3 categorias e/ou objetivos de controle e 13 controles);

k) Relacionamento na Cadeia de Suprimento (2 categorias e/ou objetivos de controle e 5 controles);

l) Gestão de Incidentes de Segurança da Informação (1 categoria e/ou objetivo de controle e 7 controles);

m) Aspectos da Segurança da Informação e Gestão da Continuidade do Negócio (2 categorias e/ou objetivos de controle e 4 controles);

n) Conformidade (2 categorias e/ou objetivos de controle e 8 controles).

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – estrutura

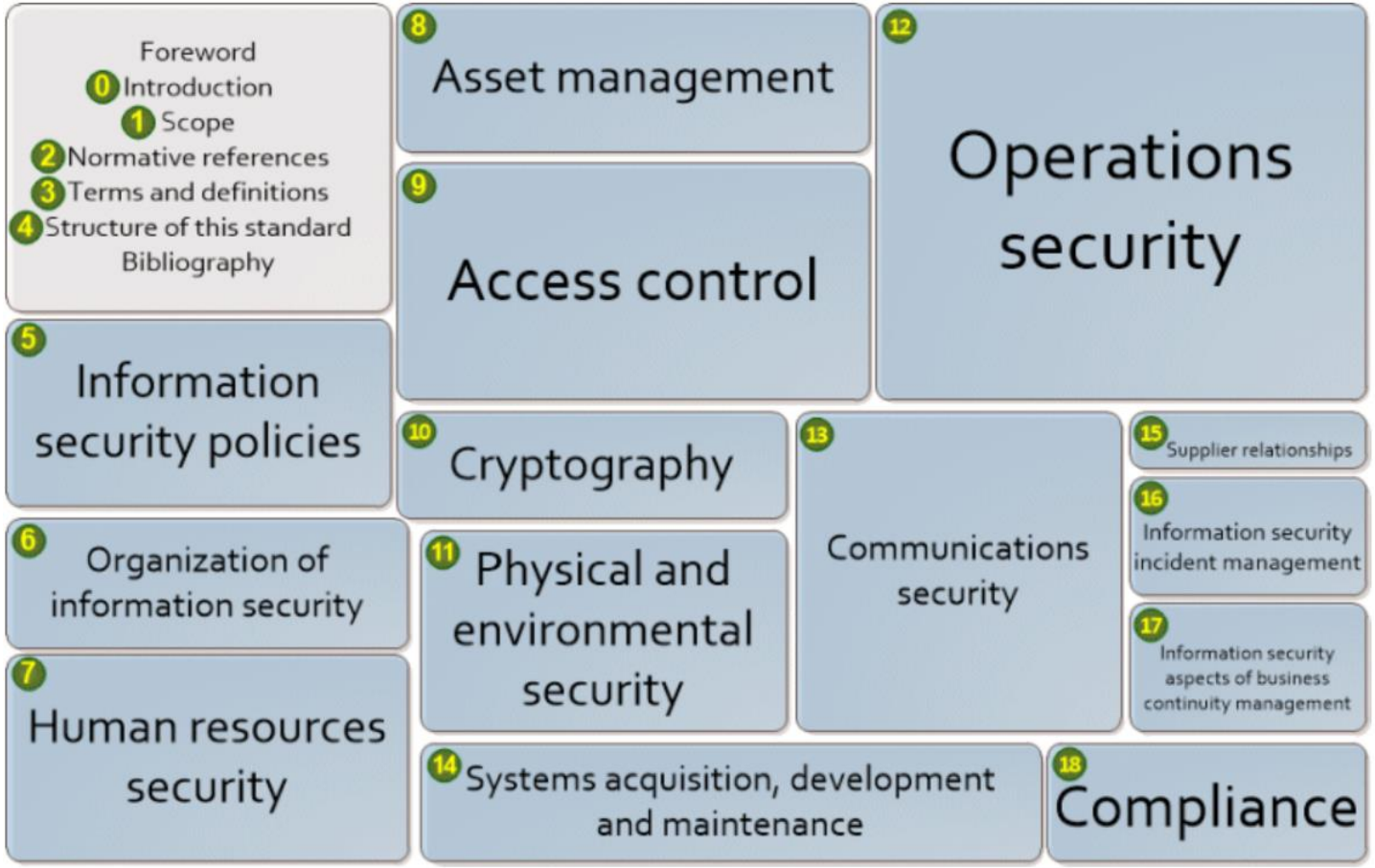
Estrutura da norma – continuação...

Cada seção principal contém:

- Um objetivo de controle declarando o que se espera que seja alcançado; e
- Um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.
  a) Controle – define a declaração específica do controle, para atender ao objetivo de controle.
  b) Diretrizes para implementação – apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle. As diretrizes podem não ser totalmente adequadas ou suficientes em todas as situações e podem, portanto, não atender completamente aos requisitos de controle específicos da organização.
  c) Informações adicionais – apresenta mais dados que podem ser considerados, como por exemplo, questões legais e referências normativas. Se não existirem informações adicionais, esta parte não é mostrada no controle.

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – resumo



Fonte: NBR ISO/IEC 27002:2013

Para saber mais...

… leia o Módulo 1 da apostila Introdução à ABNT NBR ISO/IEC 17799:2005, de Arthur Roberto dos Santos Jr., Fernando Sérgio Santos Fonseca e Paulo Eustáquio Soares Coelho, da Microsoft Technet.

FIM