POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Prof. Me. Wallace Rodrigues de Santana

www.neutronica.com.br

Versão 1.0

Parte 1 de 2

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.

Apresentação da disciplina

Objetivo Geral

- Compreender a necessidade da definição de Políticas de Segurança da Informação nas organizações e quais as possíveis consequências da falta de seu planejamento e implementação;
- Conhecer e ser capaz de interpretar as principais normas brasileiras e internacionais utilizadas na definição de Políticas de Segurança da Informação;
- Definir Políticas de Segurança da Informação para ambientes diversos, baseando-se em melhores práticas e normas adotadas pelo mercado e na realidade da organização.

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Ementa

- Apresentar a importância e a relevância da formulação de políticas como instrumento norteador da Segurança da Informação dentro das organizações.
- Introduzir métodos baseados em práticas adequadas para a elaboração e implementação dessas políticas, além de serem discutidas medidas que podem ser tomadas para sua divulgação na organização e conscientização de seus integrantes.

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Referências

BÁSICAS

BARMAN, Scott. **Writing Information Security Policies**. New Riders Publishing, 2001.

FERREIRA, Fernando Nicolau; ARAUJO, Marcio. **Política de Segurança da Informação**. 2.ed. Rio de Janeiro: Ciência Moderna, 2008.

PELTIER, Thomas R. **Information Security Policies and Procedures: A Practitioner's Reference**, Second Edition. 2.ed. Auerbach Publications, 2004.

COMPLEMENTAR

WOOD, Charles Cresson. **Information Security Policies Made Easy**, 11th Edition. Information Shield, 2009.

Referências

ADICIONAIS

ABREU, Vladimir Ferraz de; FERNANDES, Aguinaldo Aragon. **Implantando a Governança de TI: da estratégia à gestão dos processos e serviços**. Rio de Janeiro: Brasport, 2006.

SANTOS Jr, Arthur Roberto dos; FONSECA, Fernando Sérgio Santos; COELHO, Paulo Estáquio Soares. **Academia Latino Americana de Segurança da Informação – Introdução à ABNT NBR ISO/IEC 17799:2005**. Microsoft Technet, 2006.

Módulos

PARTE I

- Módulo 1 – Introdução
- Módulo 2 – Melhores Práticas de Governança
- Módulo 3 – Melhores Práticas de Entrega de Serviços
- Módulo 4 – Guia para Certificação de Sistemas de Gestão de Segurança da Informação
- Módulo 5 – Melhores Práticas de Segurança da Informação

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Módulos – continuação...

PARTE II

- Módulo 6 – Política de Segurança da Informação
- Módulo 7 – Organizando a Segurança da Informação
- Módulo 8 – Gestão de Ativos
- Módulo 9 – Segurança em Recursos Humanos
- Módulo 10 – Segurança Física e do Ambiente
- Módulo 11 – Gerenciamento das Operações e Comunicações
- Módulo 12 – Controle de Acessos

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Módulos – continuação...

- Módulo 13 – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
- Módulo 14 – Gestão de Incidentes de Segurança da Informação
- Módulo 15 – Gestão da Continuidade do Negócio
- Módulo 16 – Conformidade

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

PARTE I

Módulo 1

Introdução

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 Ferreira

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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.

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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 ameças explorem as vulnerabilidades;
- Medidas de segurança – são as ações orientadas para a eliminação ou redução das vulnerabilidades;

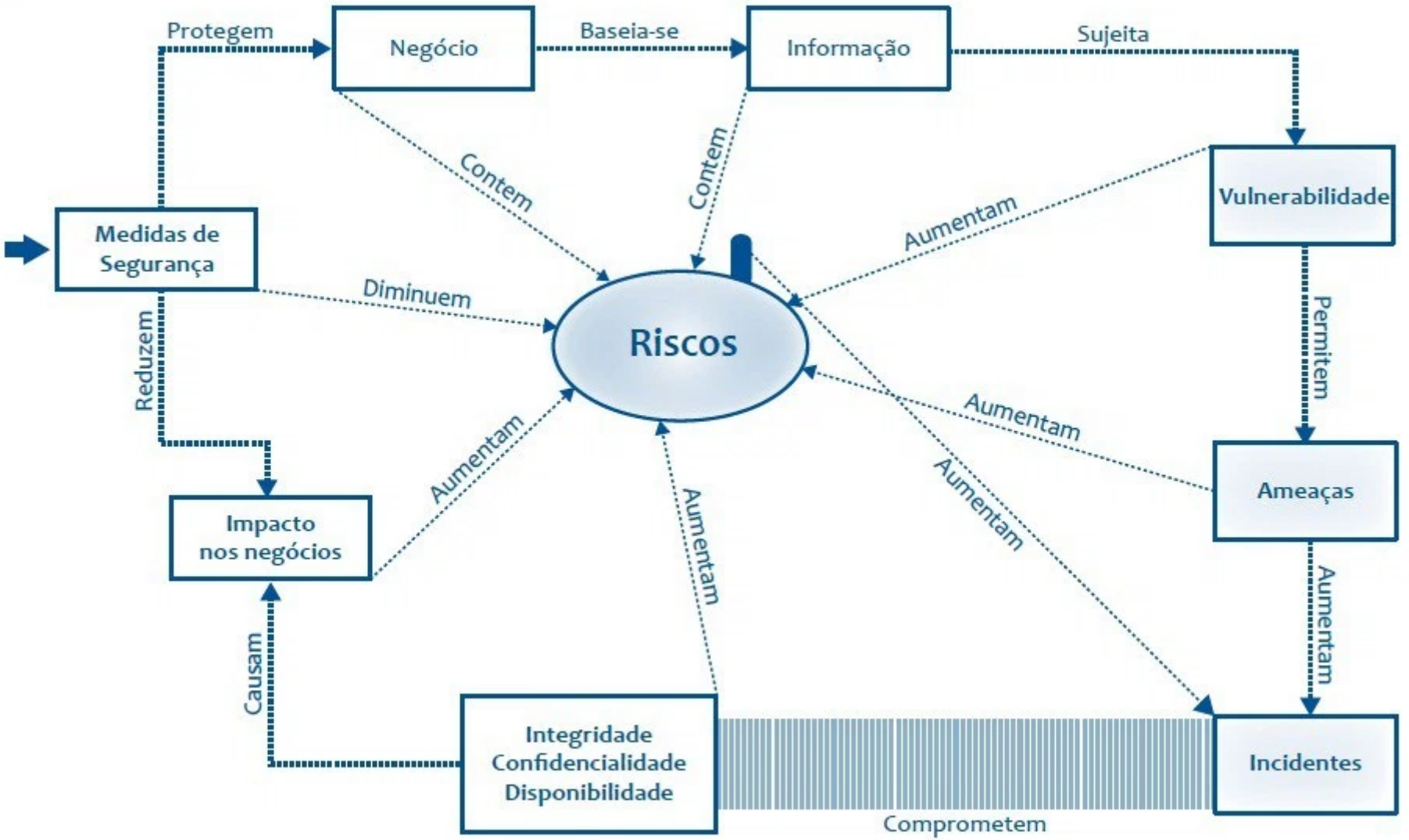
Definições – continuação

- 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

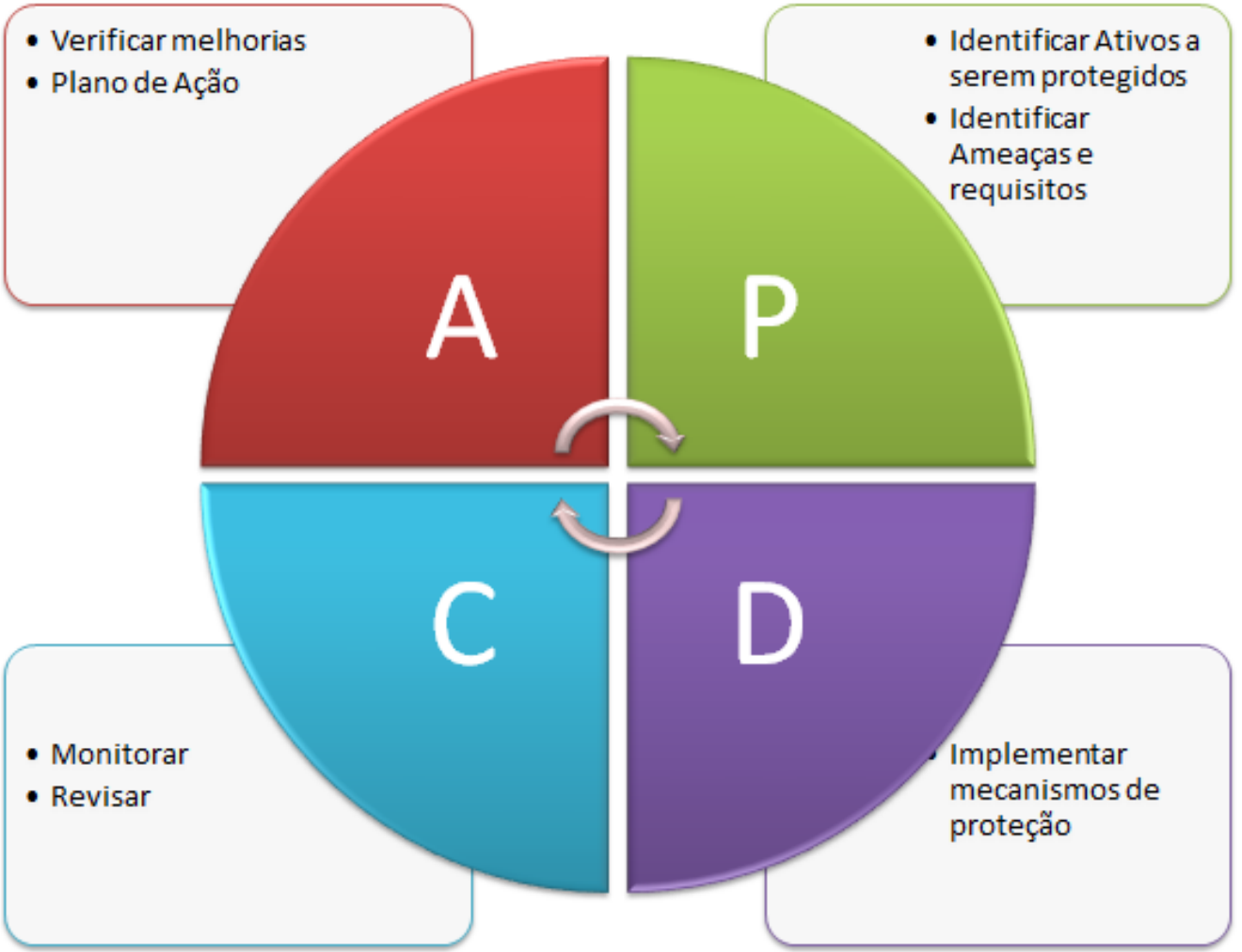
- Autenticidade – garantia que os dados fornecidos são verdadeiros e provêm de fonte legítima;
- Legalidade – o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos;
- Auditabilidade – o acesso e o uso da informação devem ser registrados, possibilitando a 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



Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Implantação



Ciclo de Deming para Segurança da Informação

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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"

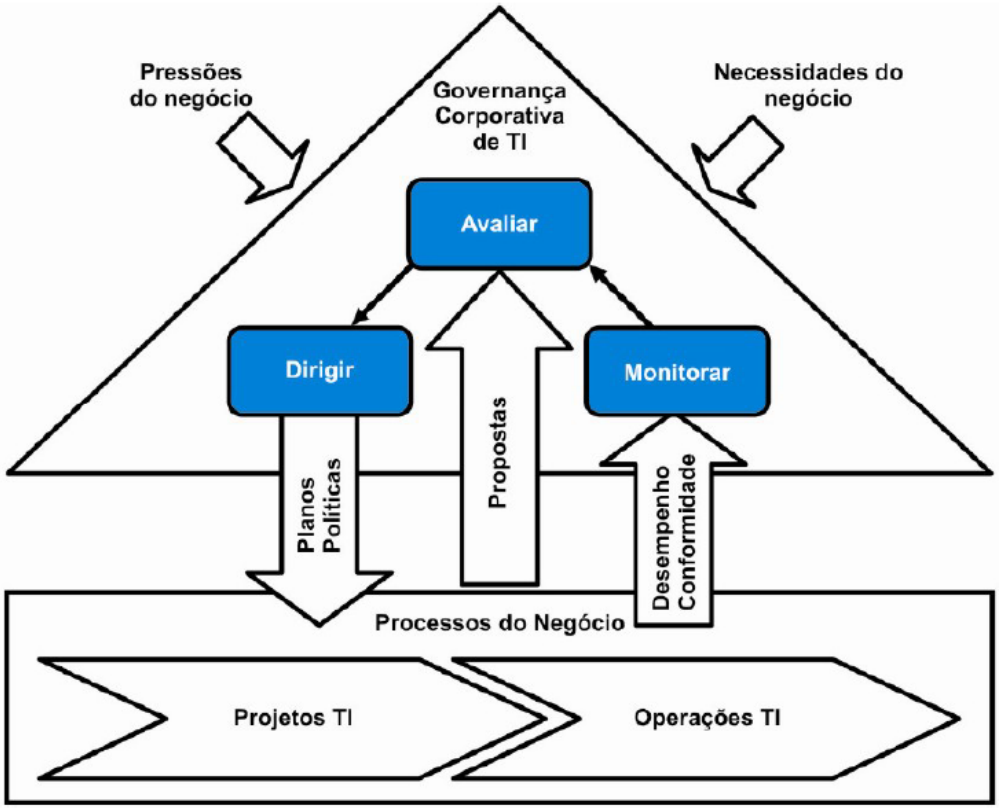
NBR ISO/IEC 38500:2009

"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.

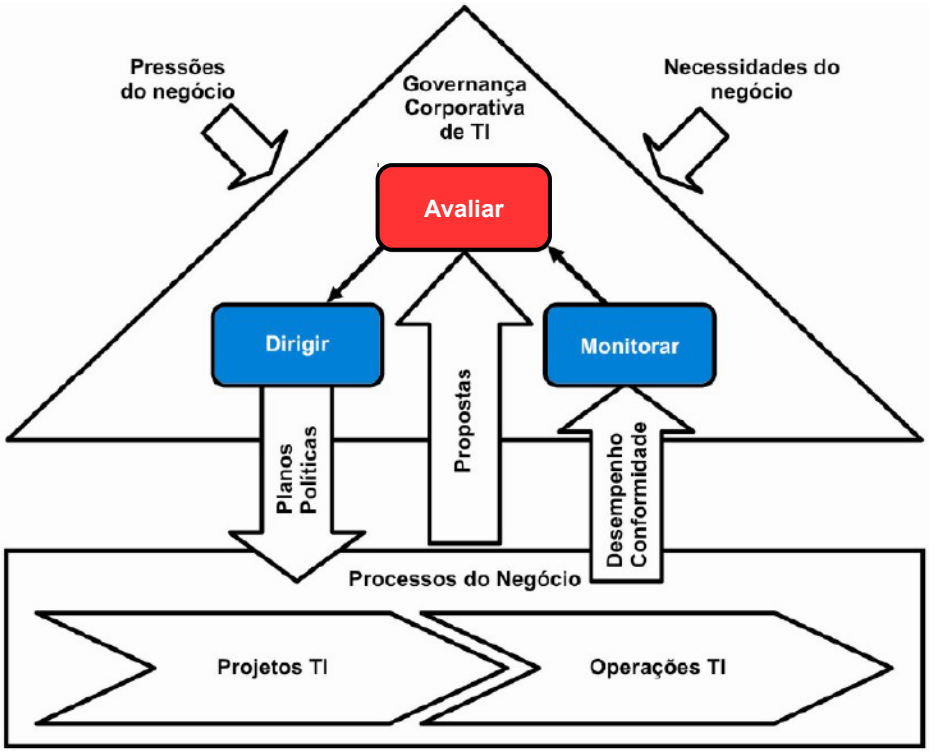


Modelo de Governança Corporativa de TI

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.

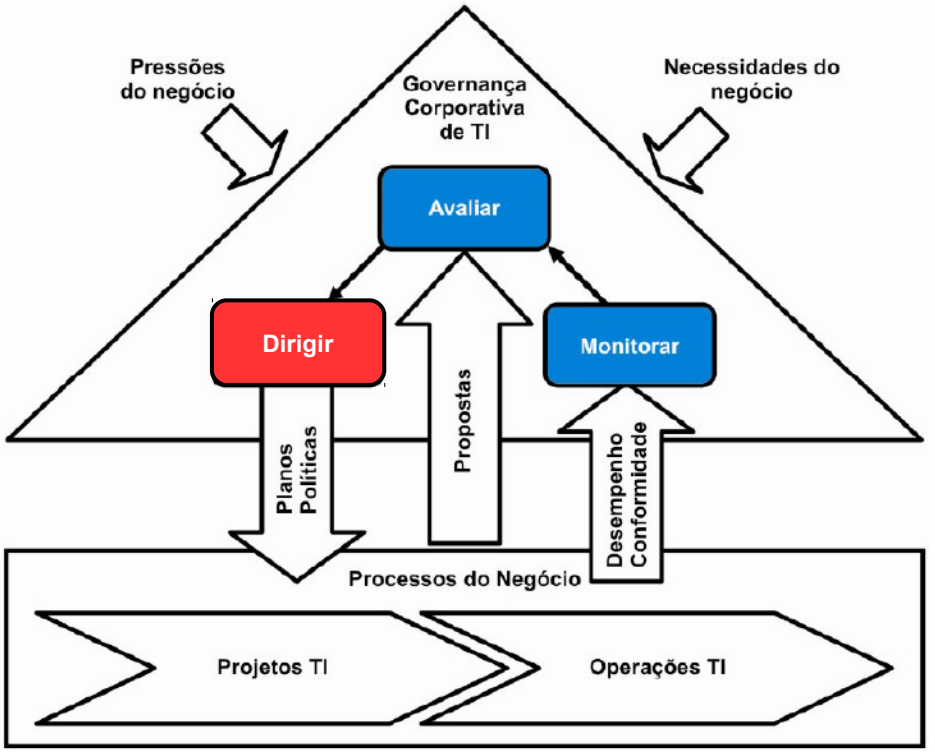


*NBR ISO/IEC 38500:2009

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Governança

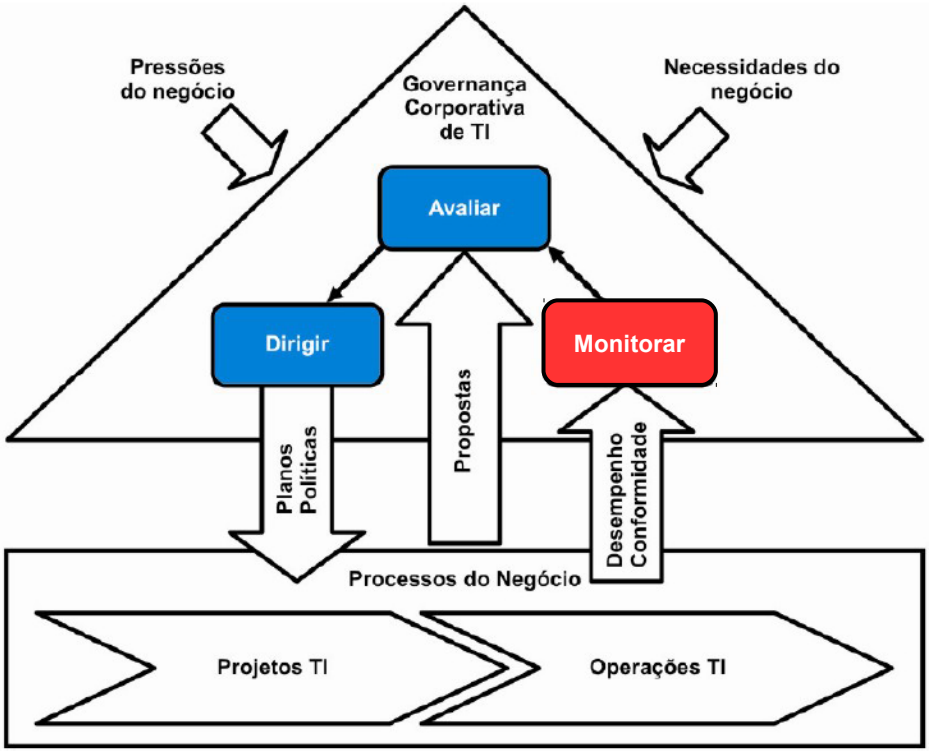
Dirigir – os dirigentes devem designar responsabilidade e exigir a preparação e implementação dos planos e políticas que estabeleçam o direcionamento dos investimentos nos projetos e operações de TI. Os dirigentes devem assegurar também que a transição e implantação dos projetos seja corretamente planejada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



*NBR ISO/IEC 38500:2009

Governança

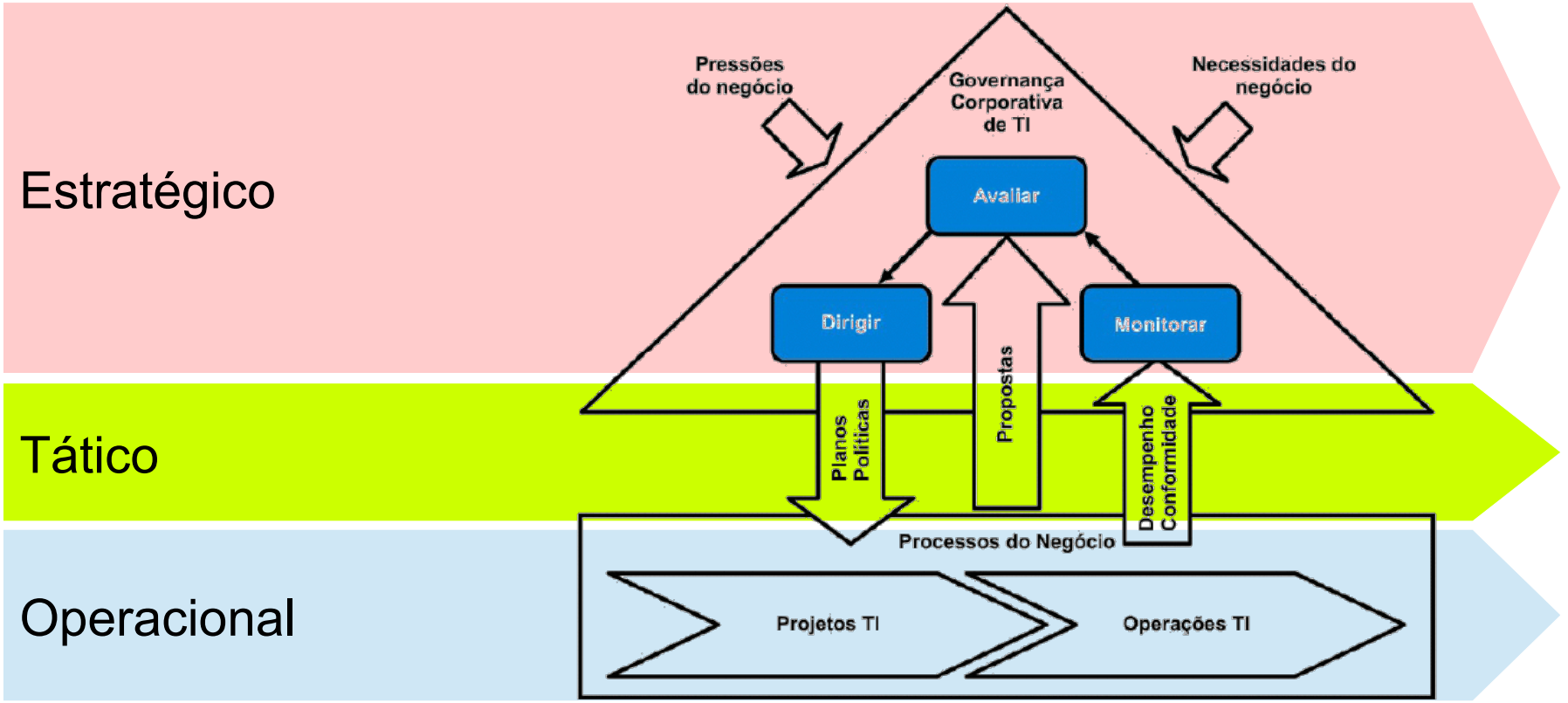
Monitorar – os dirigentes devem monitorar o desempenho da TI por meio de sistemas de mensuração apropriados, certificando-se de que o desempenho esteja de acordo com os planos e objetivos corporativos e que a TI esteja em conformidade com as obrigações externas e práticas internas de trabalho*.



*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.



Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Governança *versus* Gestão

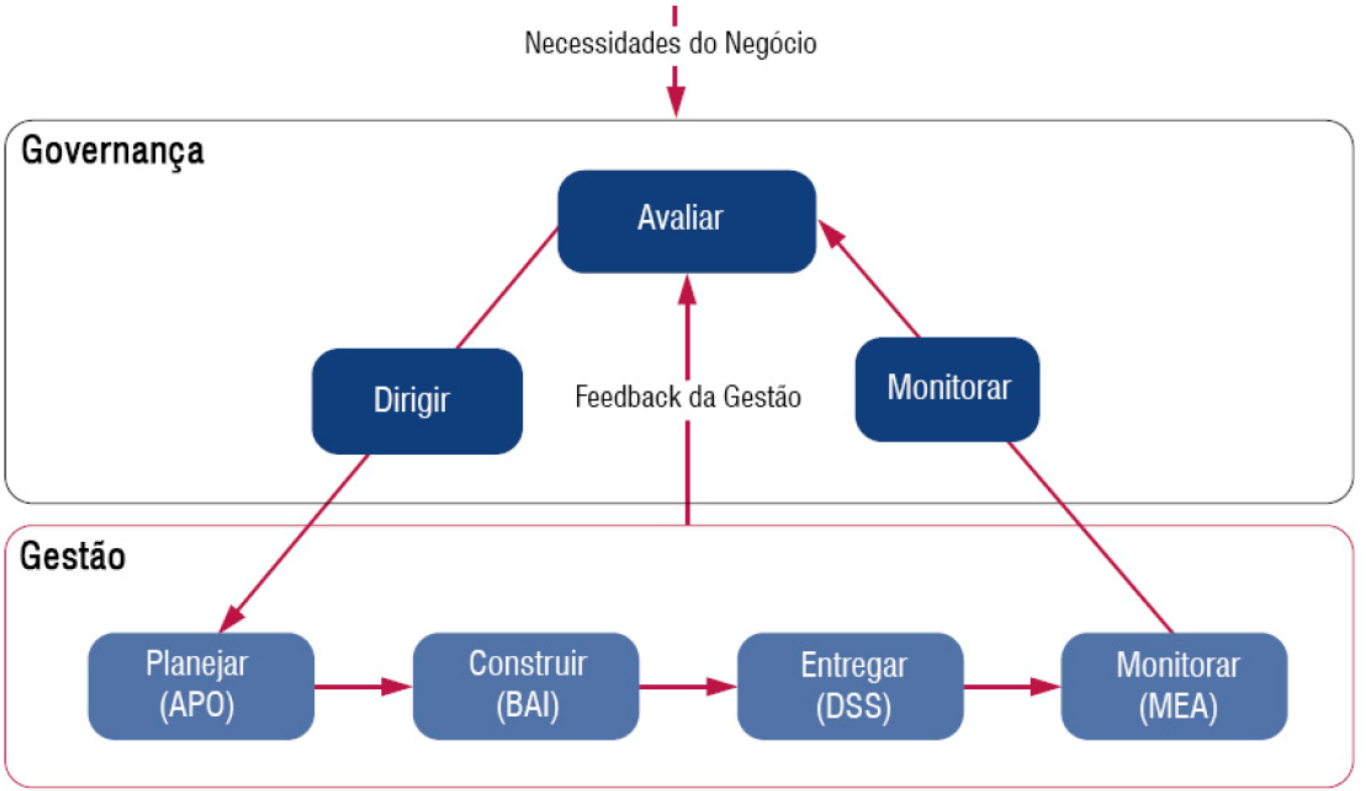
De acordo com o COBIT5:

- 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

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Normas e Guias de Boas Práticas

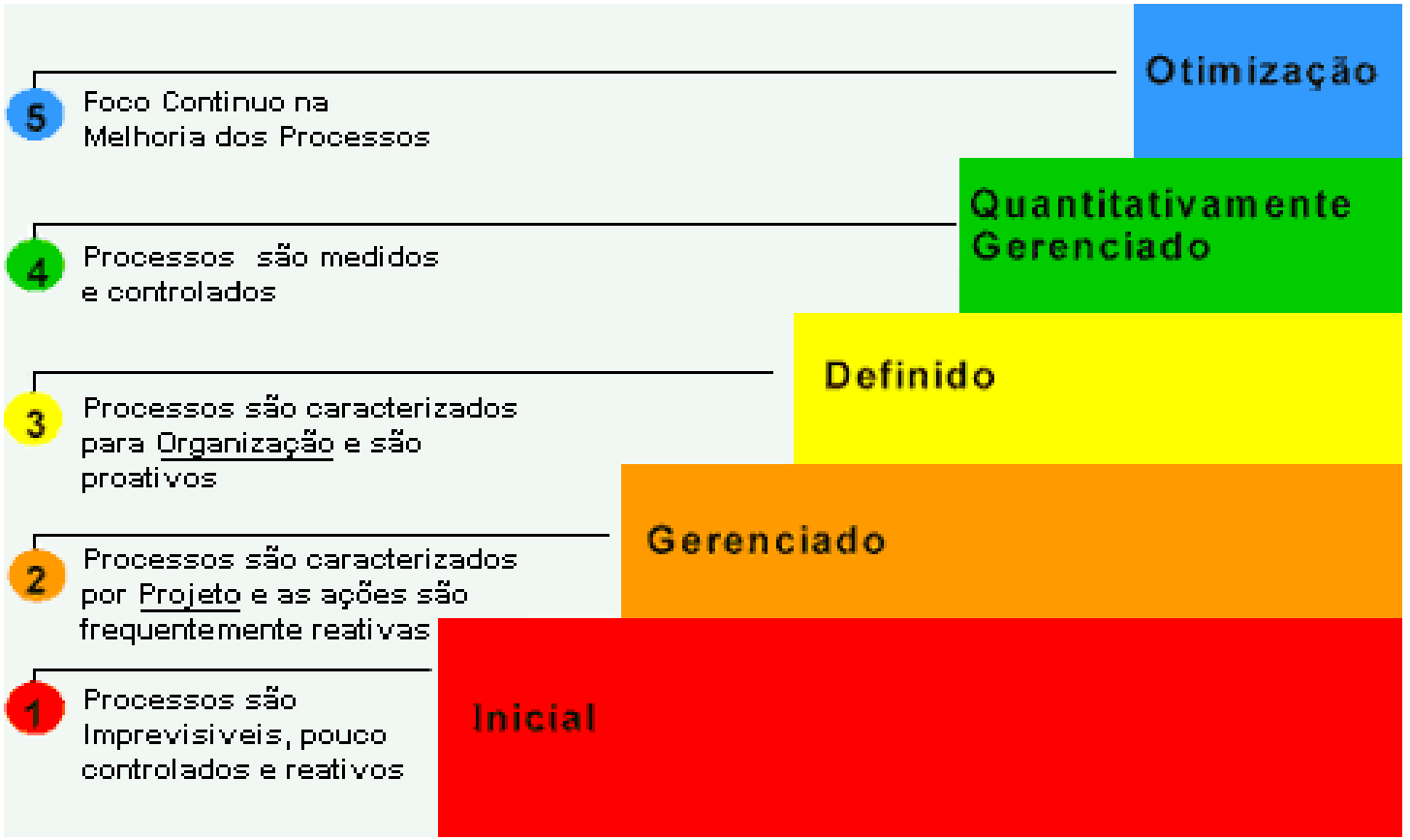
ITIL (Information Technology Infrastructure Library) é um conjunto de melhores práticas para gestão de serviços em TI.

Ciclo de vida de serviços

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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.



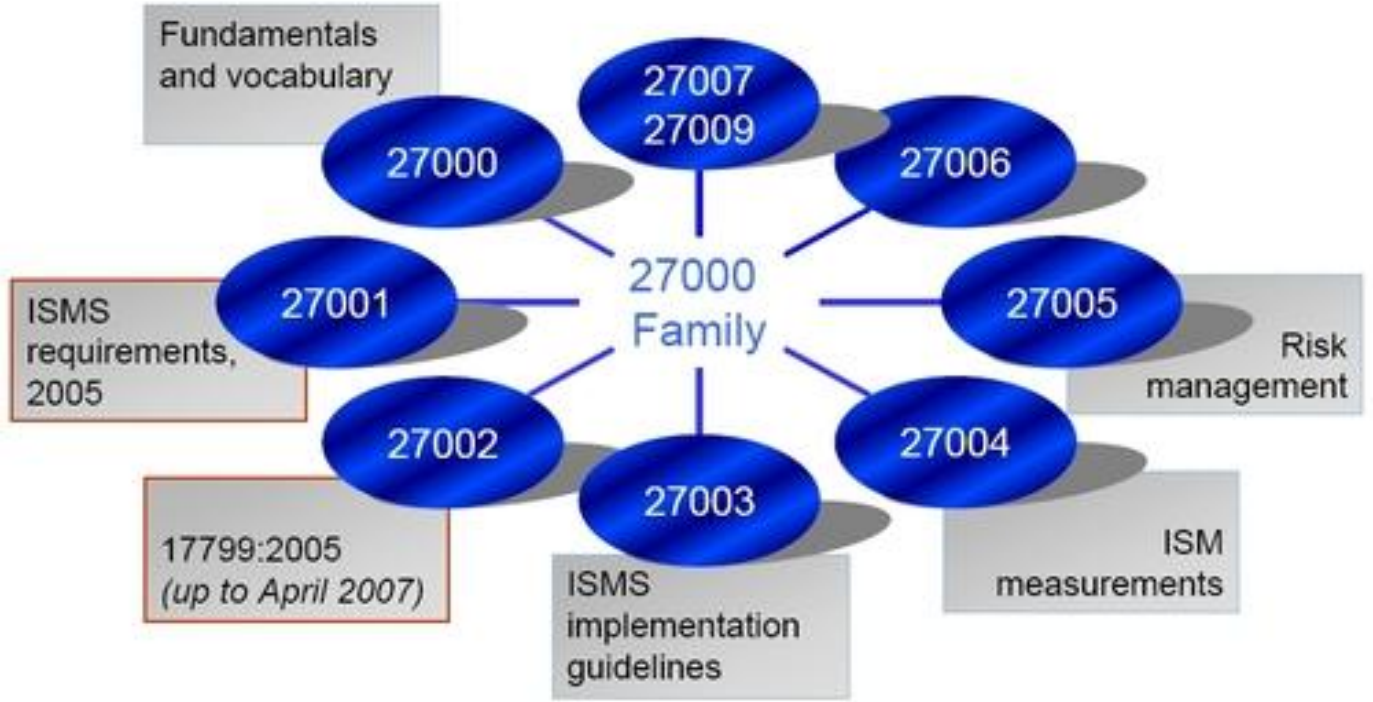
Níveis de maturidade

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Normas e Guias de Boas Práticas

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.

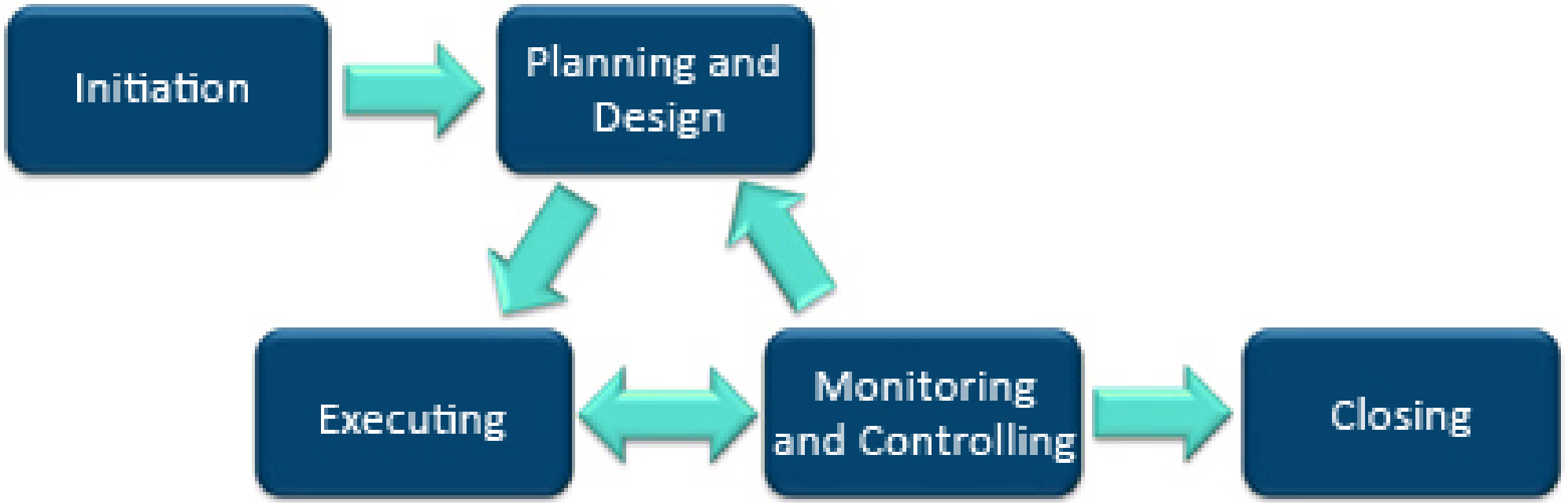


Família de padrões ISO/IEC para Sistemas de Gerenciamento de Segurança da Informação

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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

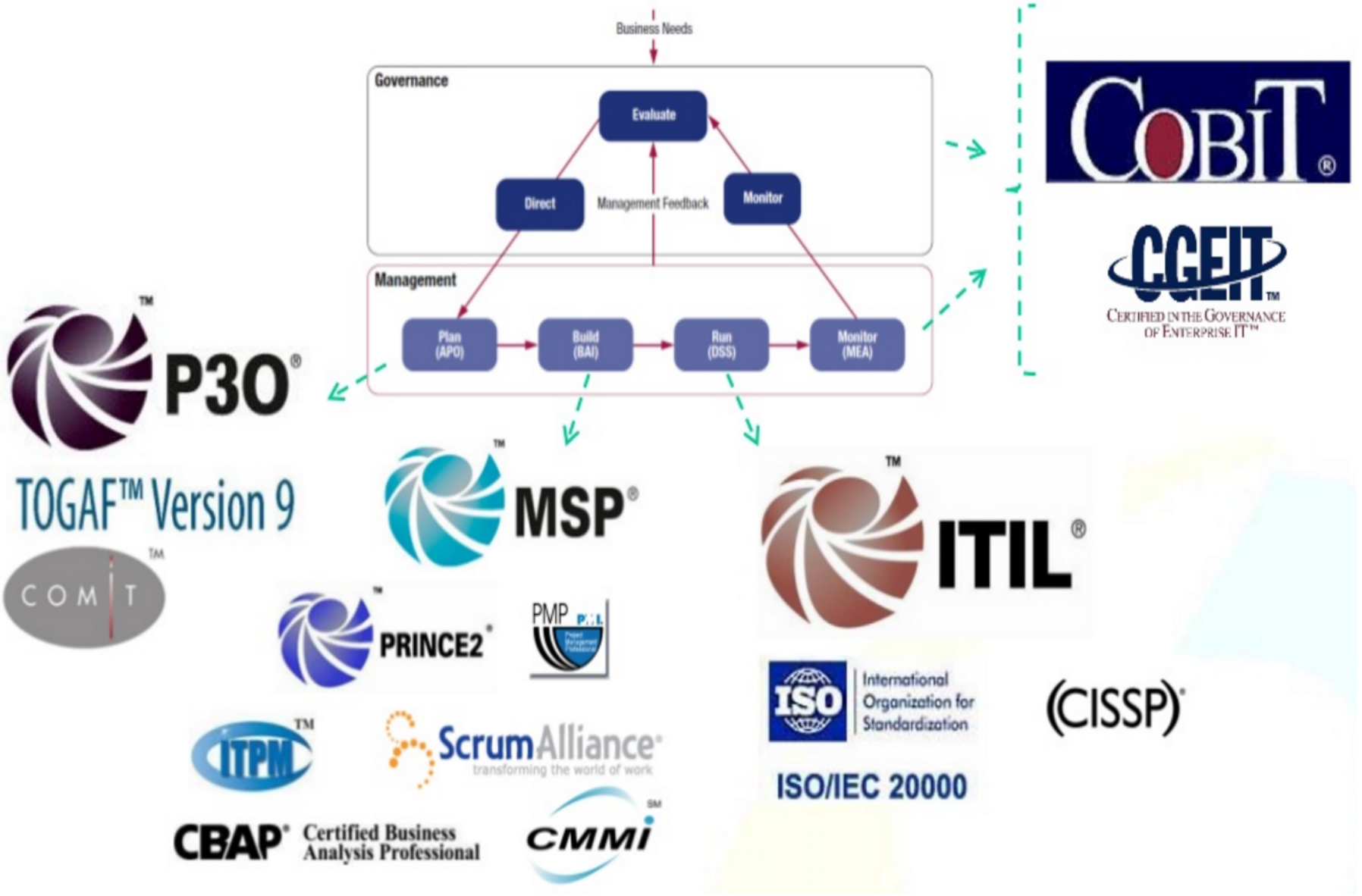
Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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.

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Governança – resumo



Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Para saber mais...

… leia o Capítulo 1 do livro Política de Segurança da Informação, de Fernando Nicolau Ferreira e Márcio Araújo, editado pela Editora Ciência Moderna.

Módulo 2

Melhores Práticas de Governança

COBIT – Introdução

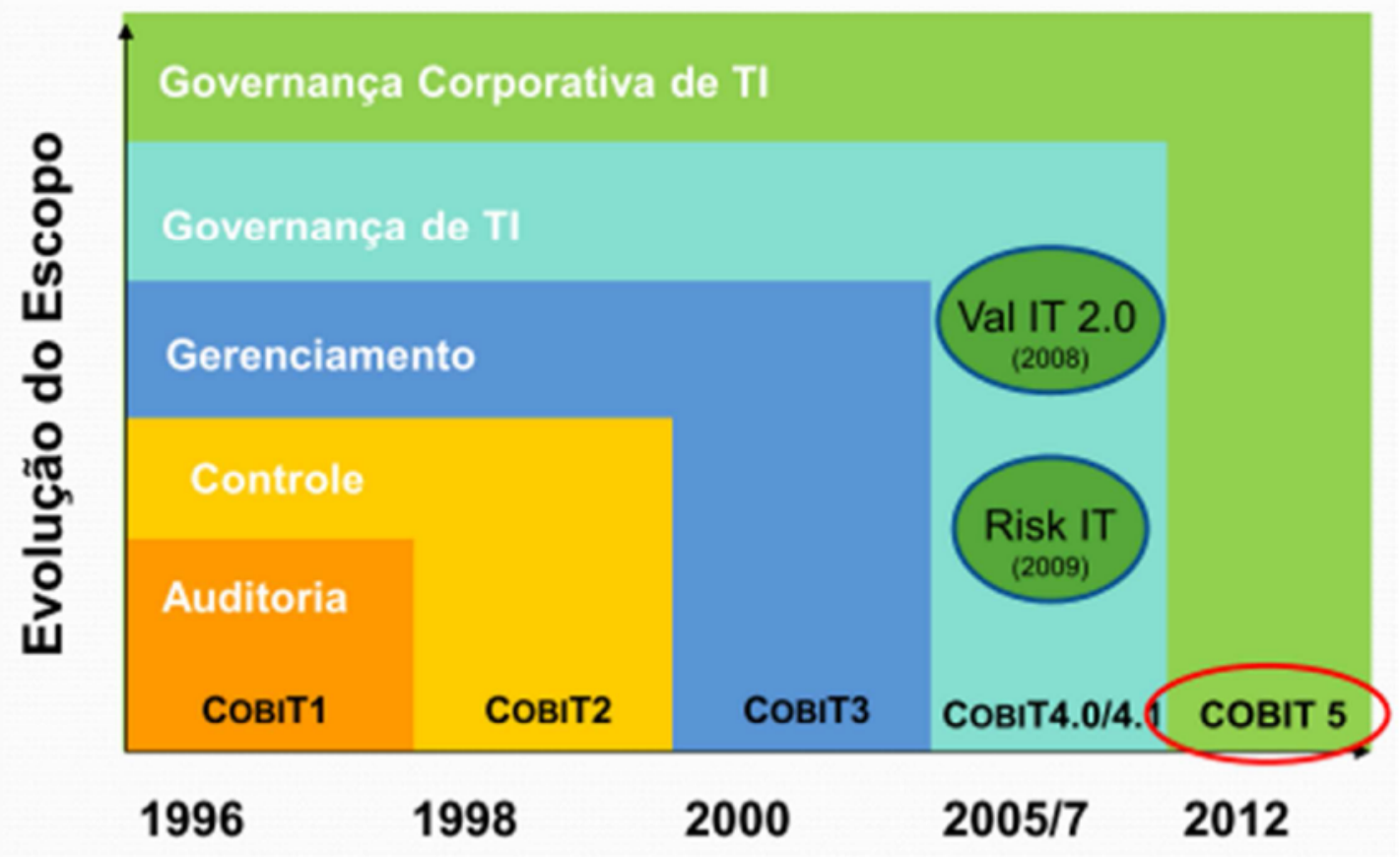
O COBIT 5 fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI, ajudando-as a criar valor por meio da TI e mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos. Permite ainda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

***COBIT 5 Framework**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

COBIT – Evolução



Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

COBIT – Princípios

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*.

**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 5 Framework

COBIT – Princípios

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*.

***COBIT 5 Framework**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

COBIT – Princípios

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*.

*COBIT 5 Framework

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

COBIT – Princípios

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*.

*COBIT 5 Framework

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

COBIT – Princípios

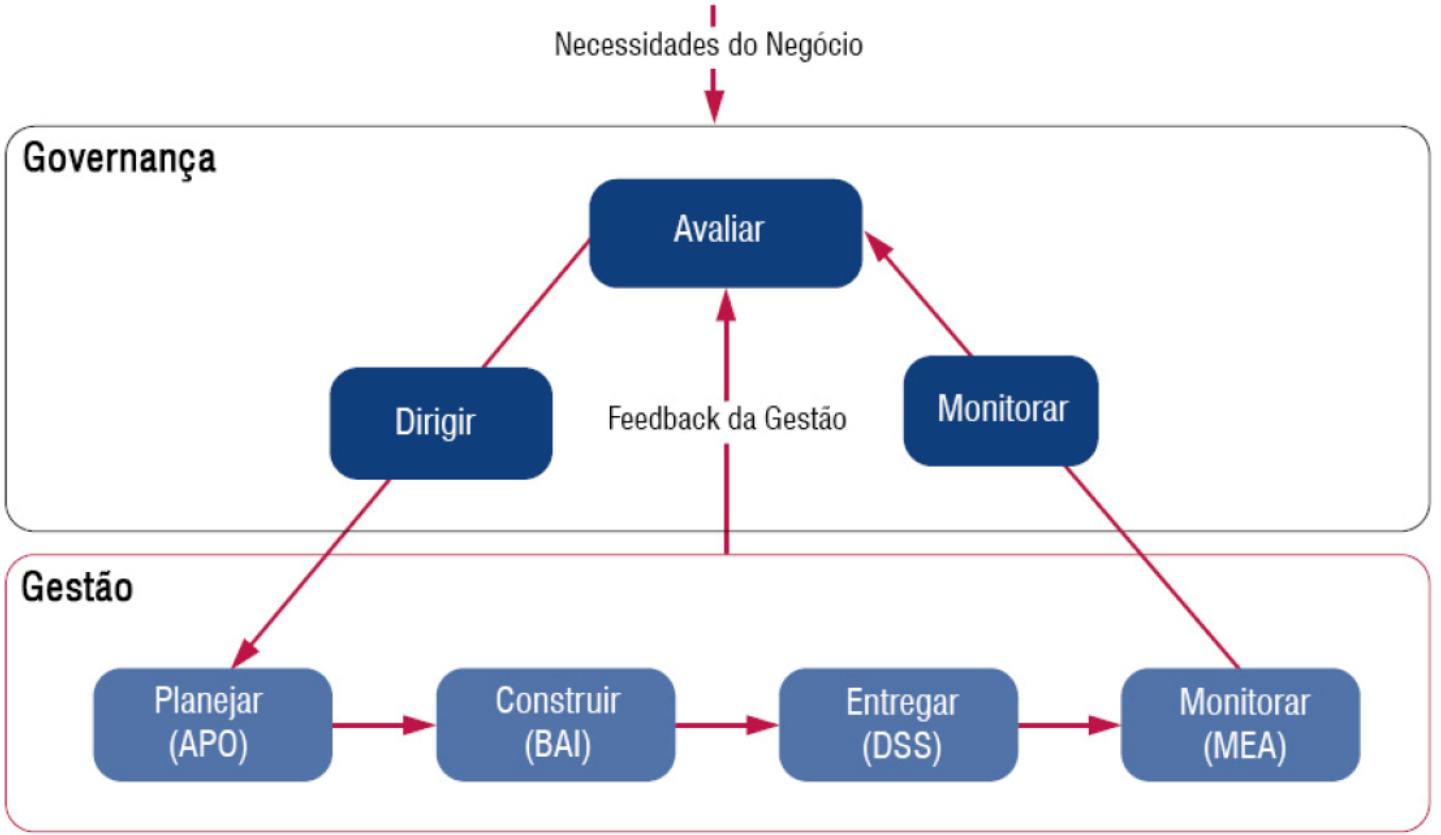
5. O modelo do COBIT 5 faz uma clara distinção entre governança e gestão. Essas duas disciplinas compreendem diferentes tipos de atividades, exigem modelos organizacionais diferenciados e servem a propósitos diferentes*.

*COBIT 5 Framework

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

COBIT – Áreas Chaves

O modelo de referência de processos do COBIT 5 possui um domínio de governança, com cinco processos; e quatro domínios de gestão, com 32 processos.

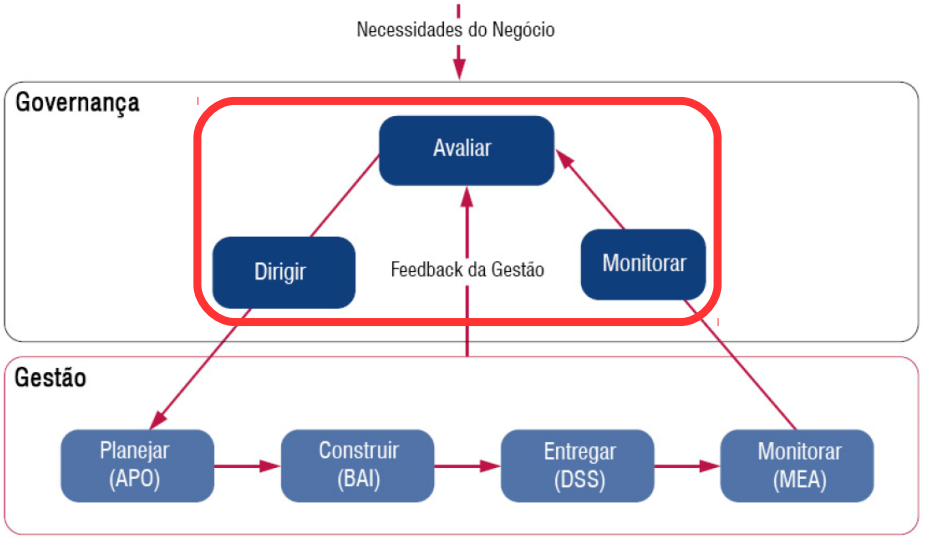


Áreas chaves da Governança e do Gerenciamento

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.

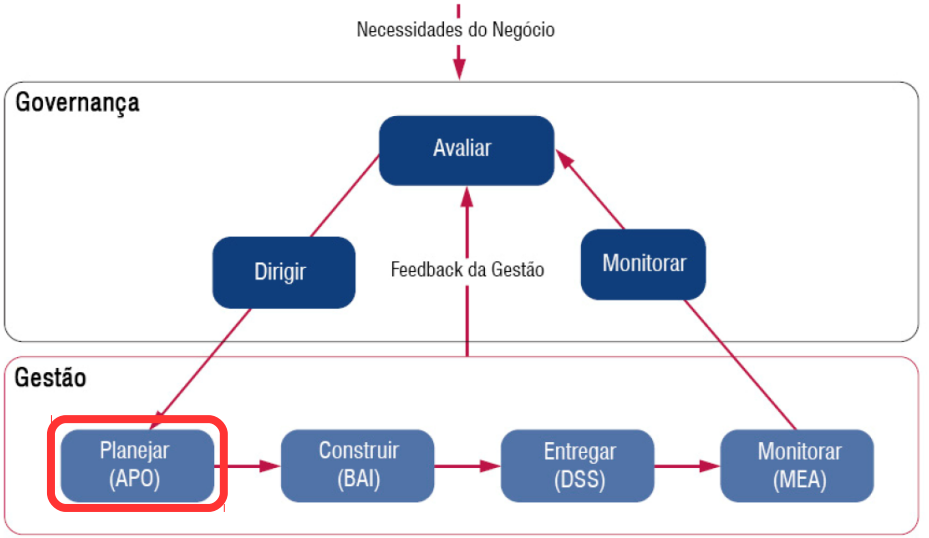


***GAEA apud Luzia Dourado**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.

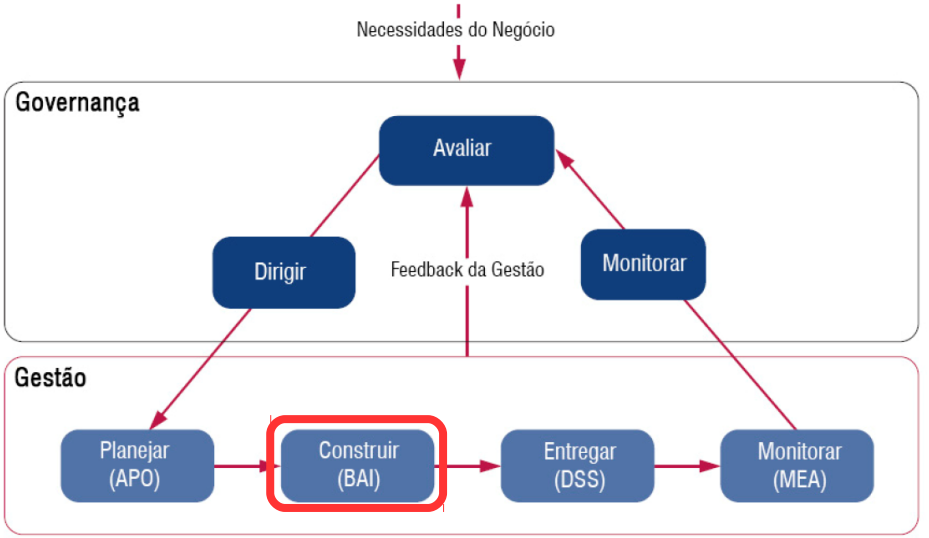


***GAEA apud Luzia Dourado**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

COBIT – Áreas Chaves

O domínio Construir, Adquirir e Implementar (Build, Acquire and Implement – BAI) possui dez processos, quem 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*.

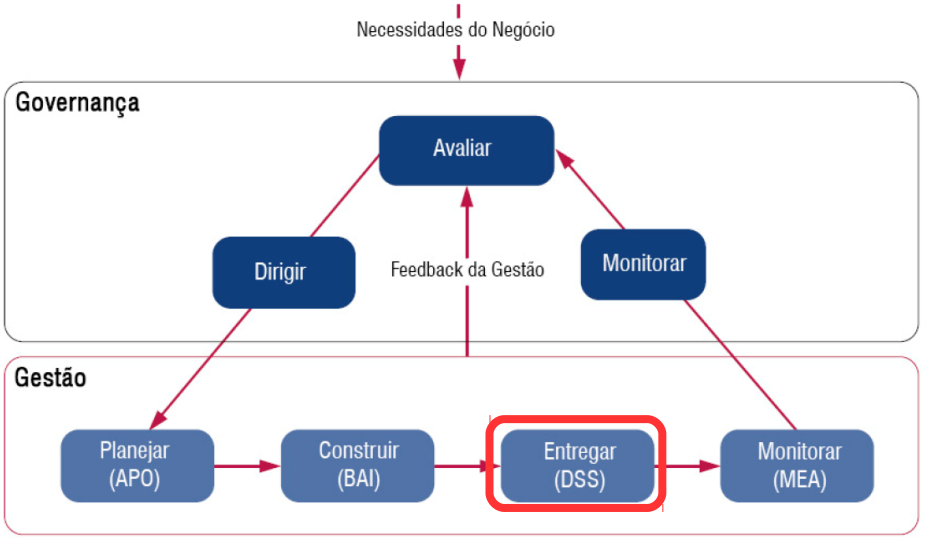


***GAEA apud Luzia Dourado**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.

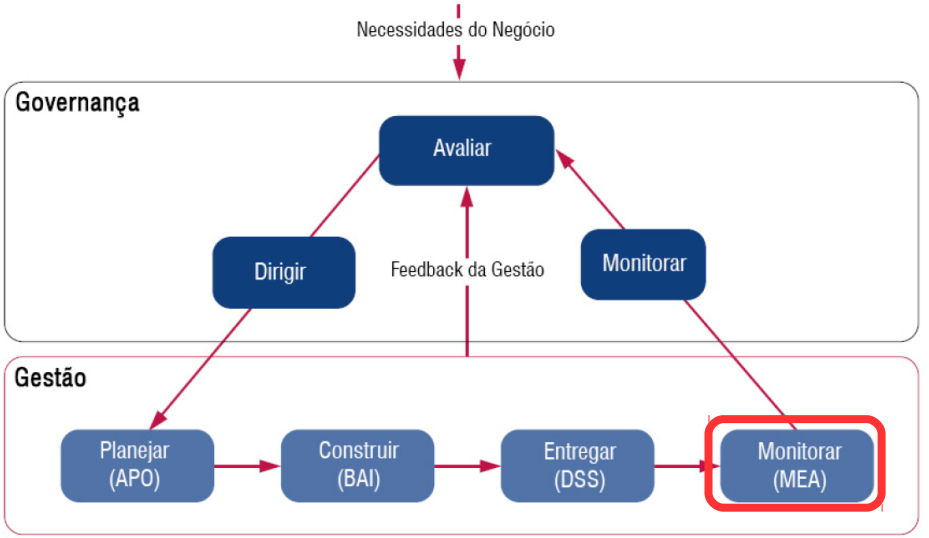


***GAEA apud Luzia Dourado**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

COBIT – Áreas Chaves

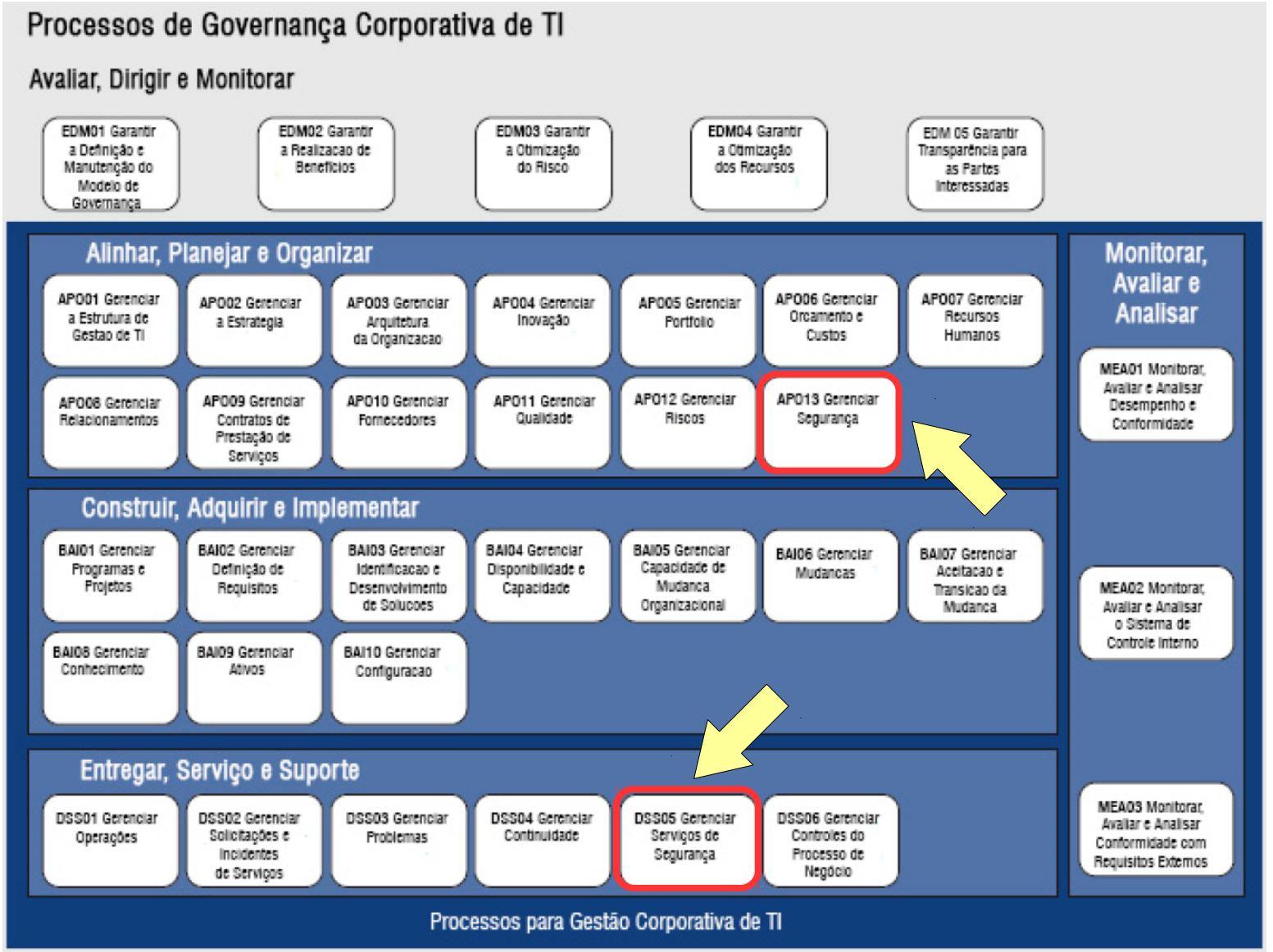
O domínio Monitorar, Avaliar e Analisar (Monitor, Evaluate and Assess – MEA) possui três processos, que visam monitorar o desempenho dos processos de TI, avaliando a conformidade com os objetivos e com os requisitos externos*.



***GAEA apud Luzia Dourado**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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.

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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.

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Módulo 3

Melhores Práticas de Entrega de Serviços

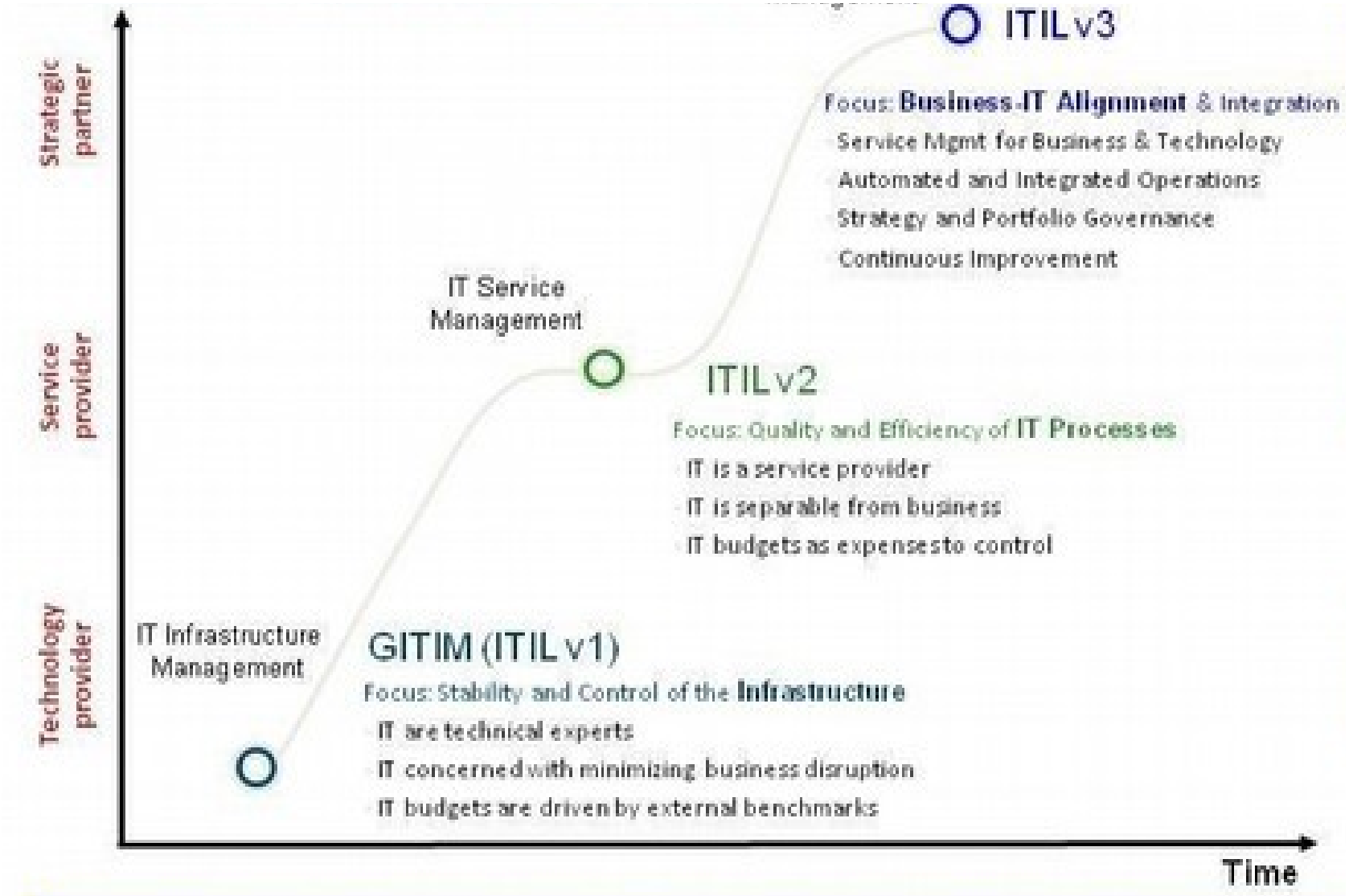
ITIL – Introdução

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

***ITIL 3 Service Strategy**

ITIL – Evolução



Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.

***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*.

*ITIL 3 Service Strategy

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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;

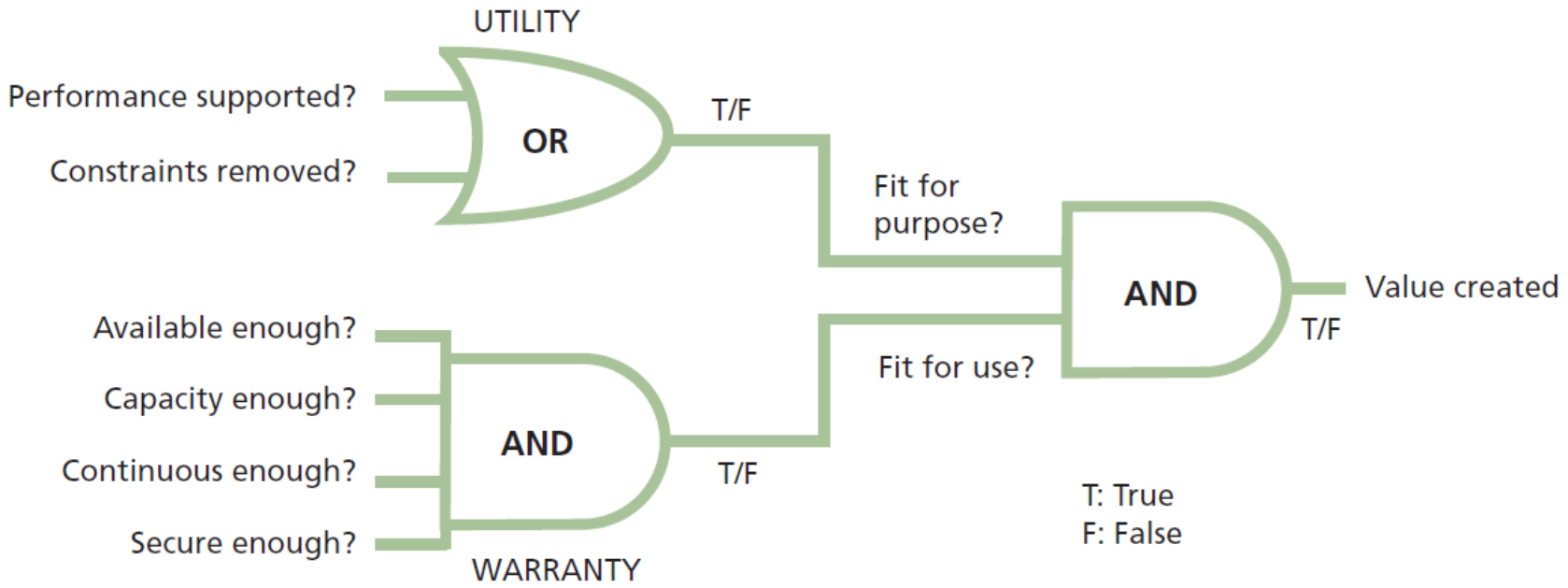
Já as percepções se baseiam em atributos do serviço que possam ser medidos e/ou comparados com a concorrência*.

*ITIL 3 Service Strategy

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

ITIL – Valor de Serviço

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

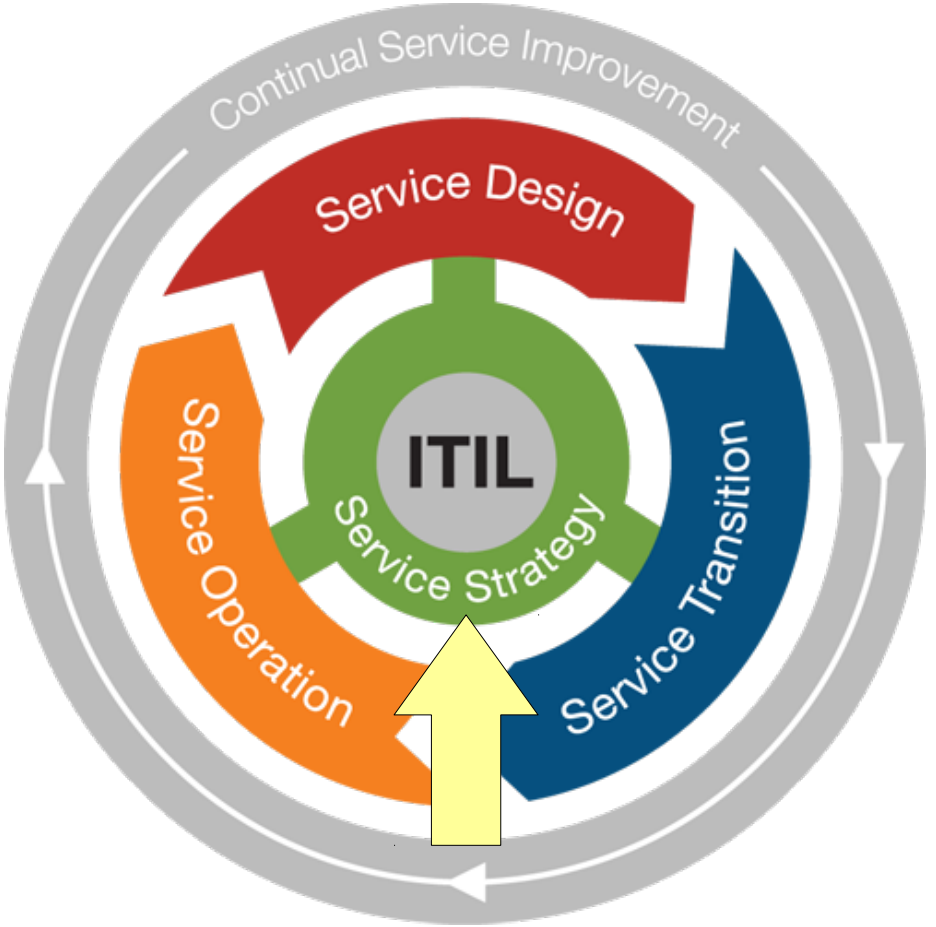


*ITIL 3 Service Strategy

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.

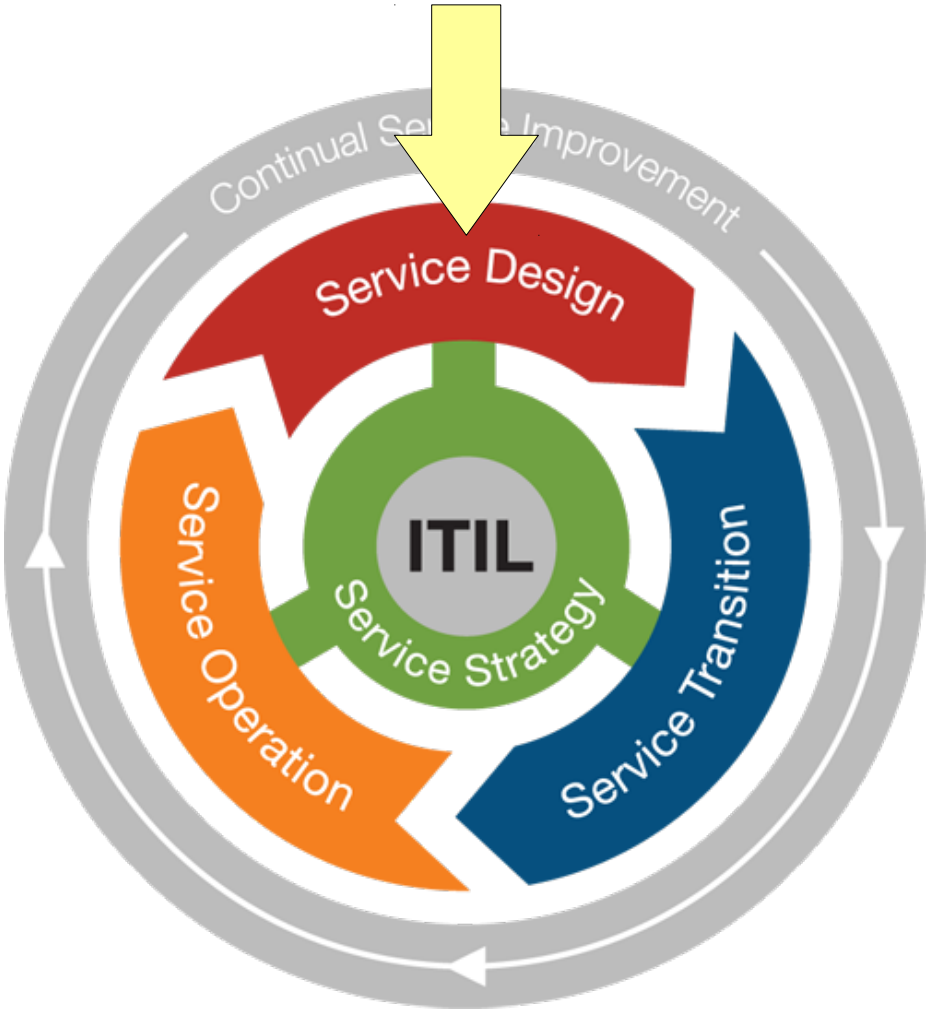


*ITIL 3 Service Strategy

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.



***ITIL 3 Service Strategy**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.

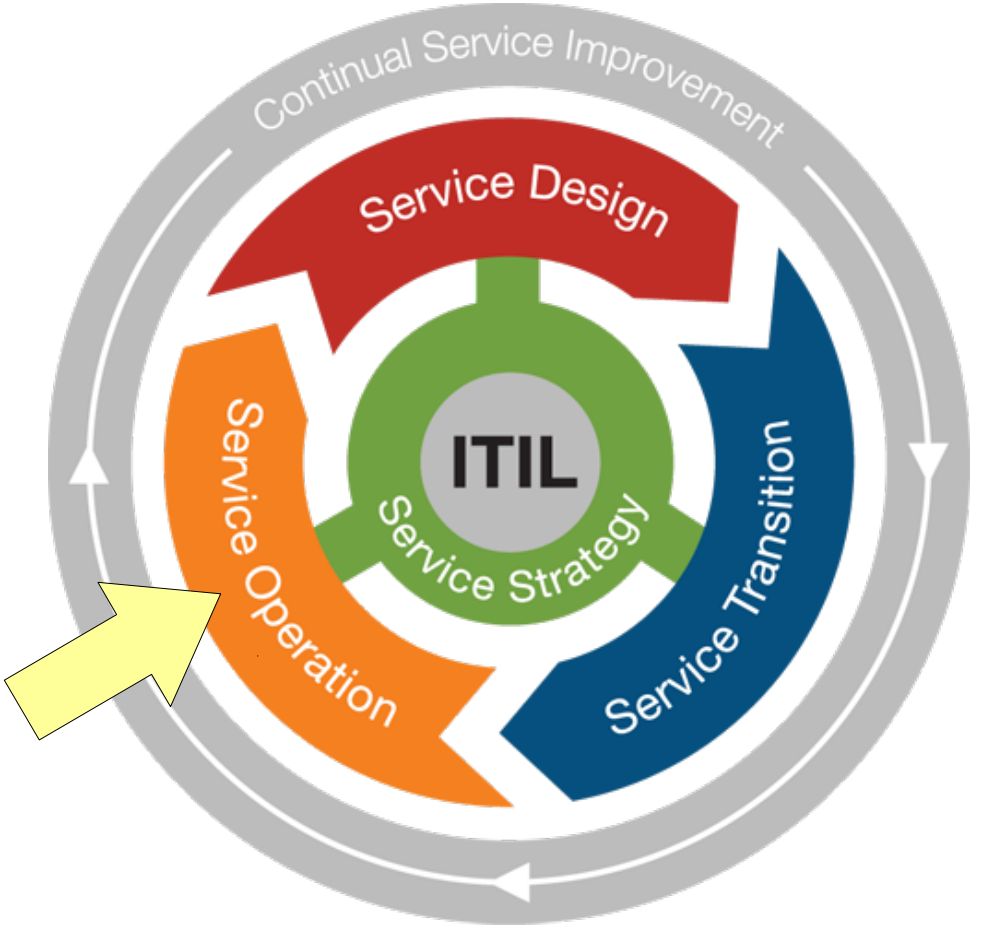
*ITIL 3 Service Strategy

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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...



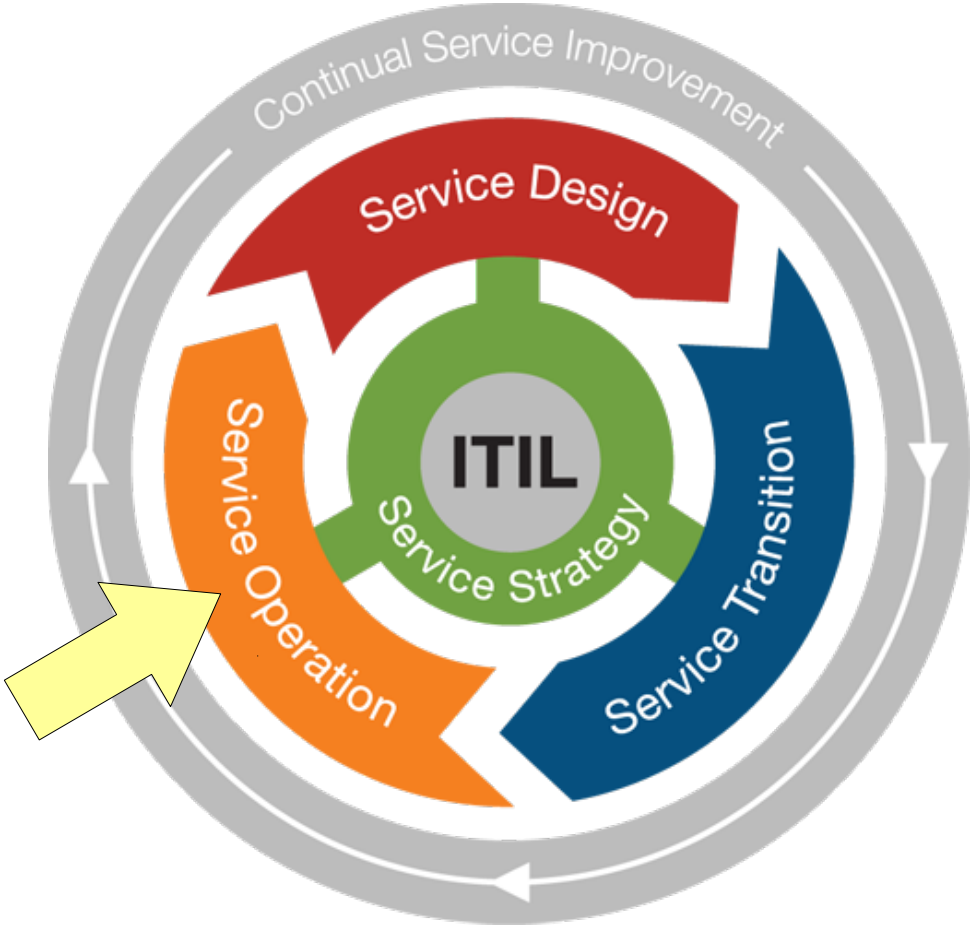
*ITIL 3 Service Strategy

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.



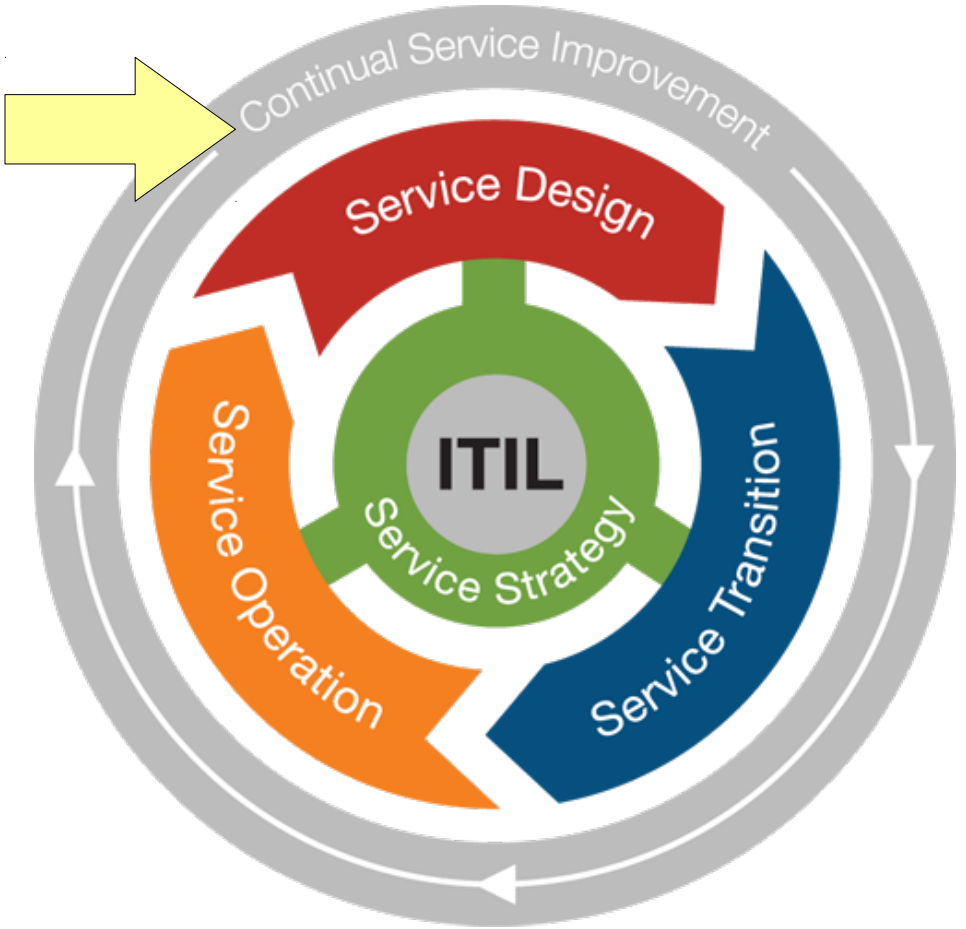
***ITIL 3 Service Strategy**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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...



***ITIL 3 Service Strategy**

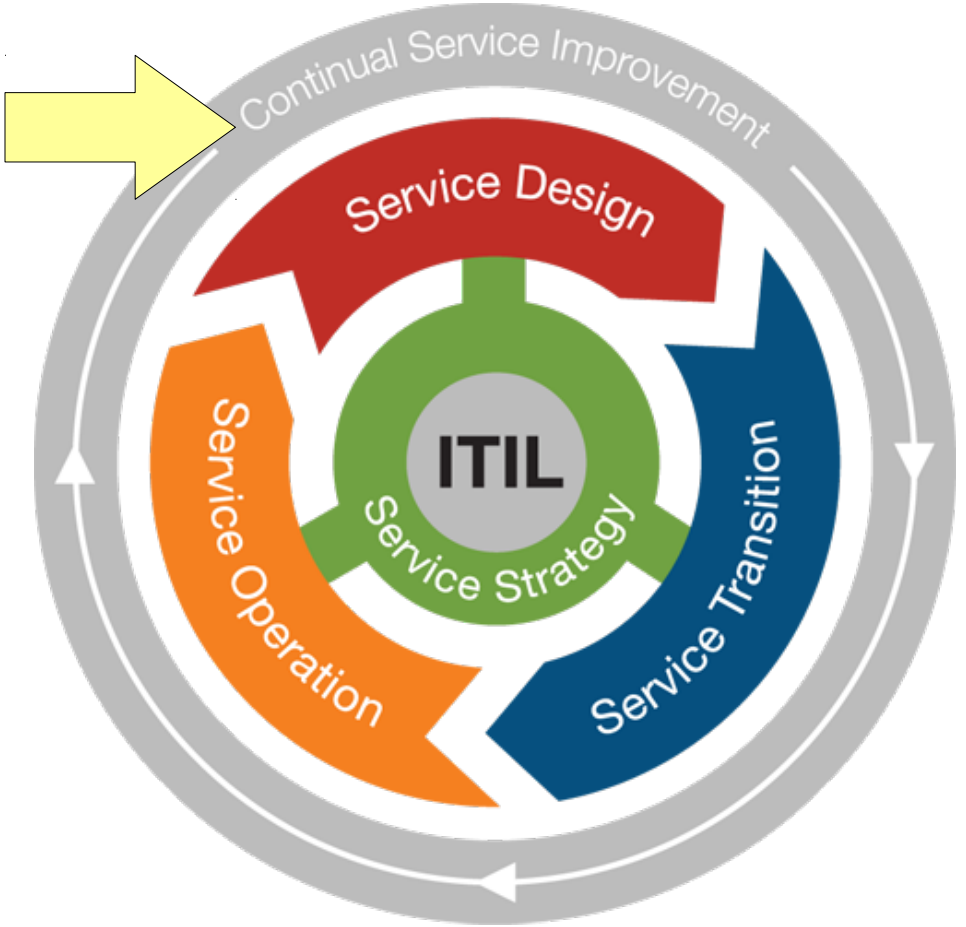
Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.



***ITIL 3 Service Strategy**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

ITIL – Processos

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

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*.

***ITIL 3 Service Design**

Para saber mais...

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

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

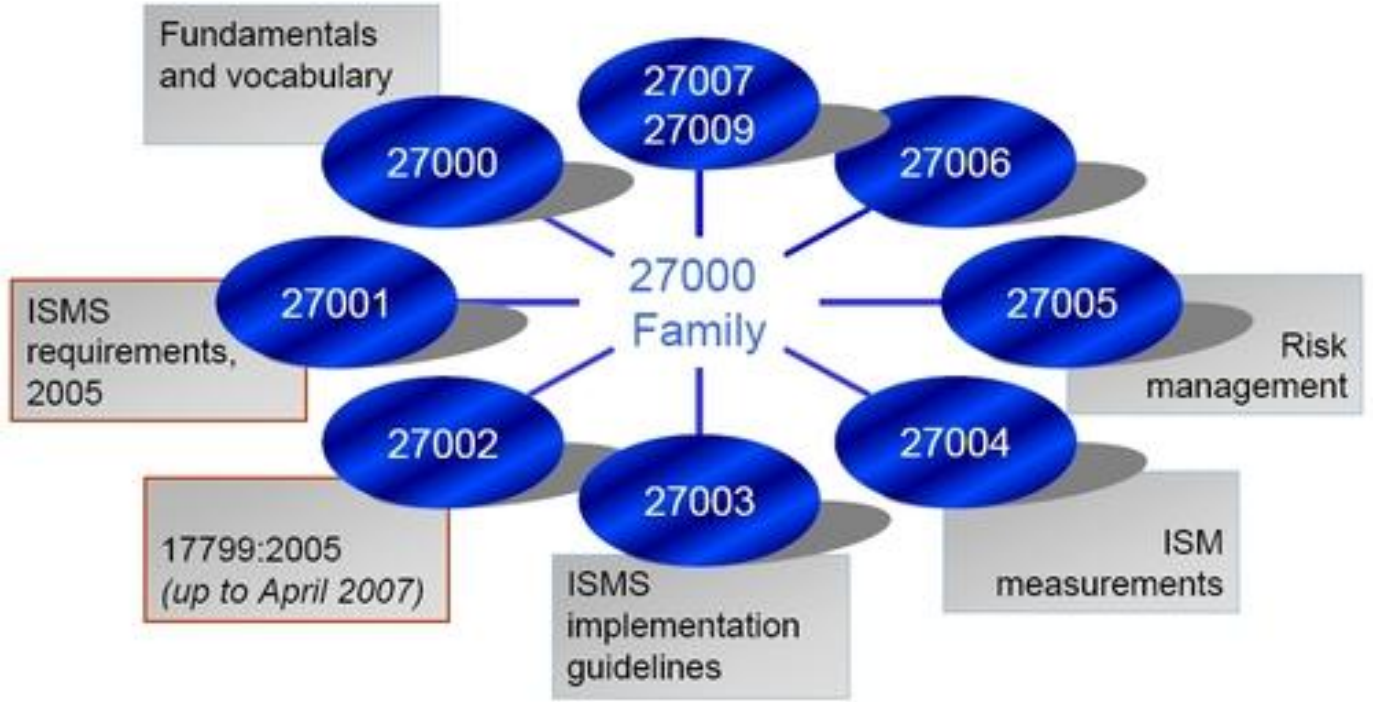
Módulo 4

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

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Introdução

Esta norma tem por objetivo prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Sua adoção deve ser uma decisão estratégica da organização, pois sua especificação e implementação são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Abordagem

A organização precisa identificar e gerenciar muitas atividades para funcionar efetivamente. A atividade que faz o uso de recursos e os gerencia para obter um resultado pode ser considerada um processo. Assim, 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".

A abordagem de processo para a gestão da segurança da informação desta norma 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;

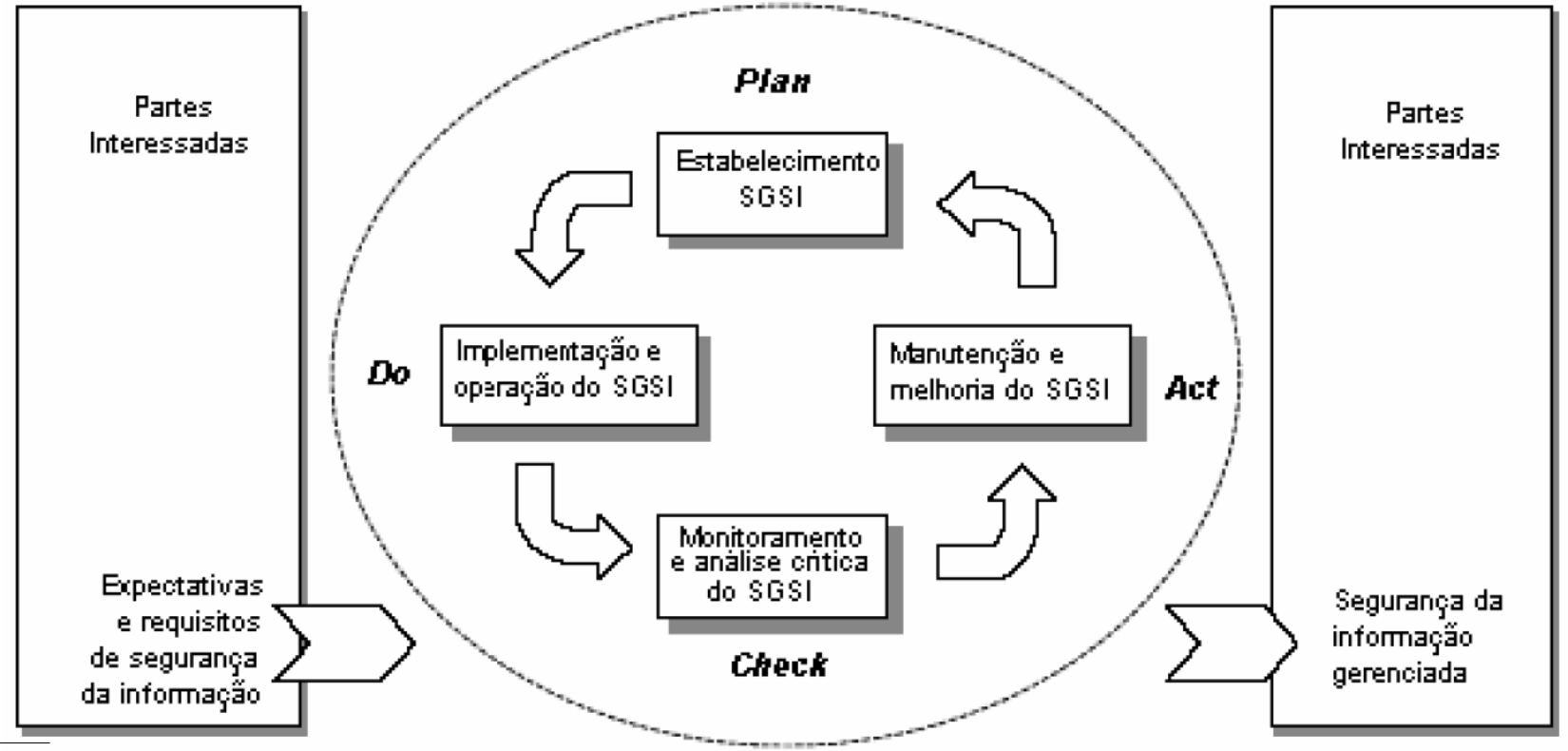
d) melhoria contínua baseada em medições objetivas*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Abordagem

Esta norma 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*.



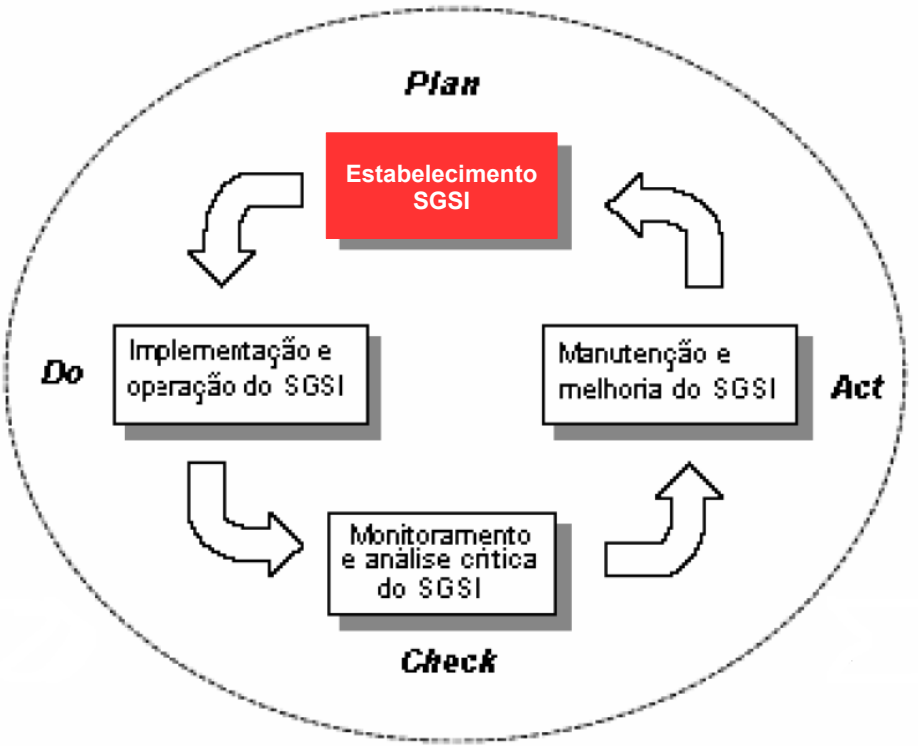
*NBR ISO/IEC 27001:2006

Modelo PDCA aplicado aos processos do SGSI

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR 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*.

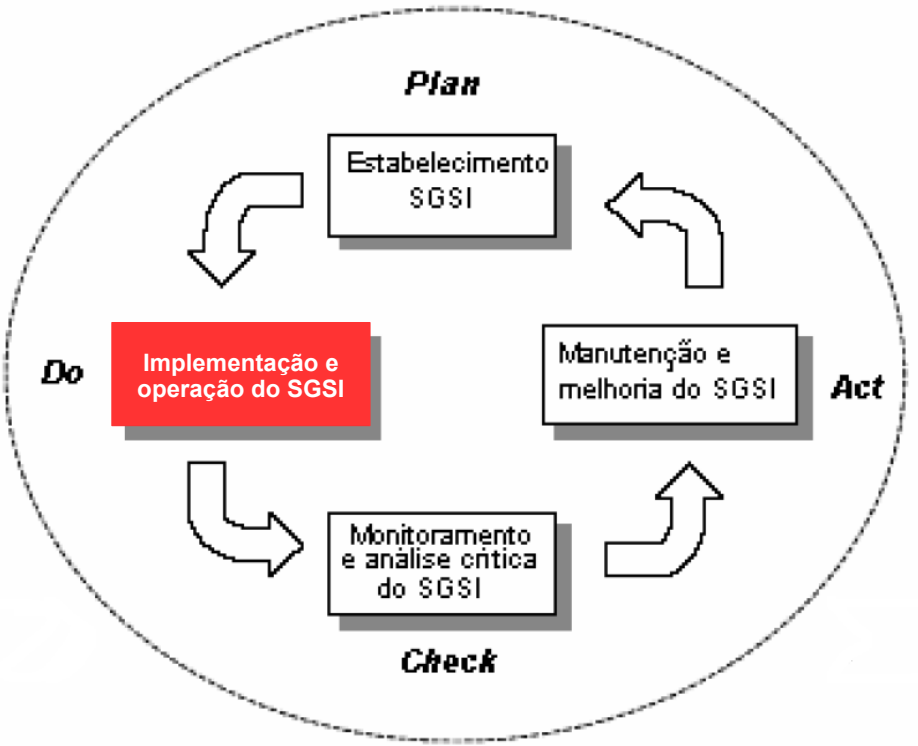


*NBR ISO/IEC 27001:2006

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Abordagem

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

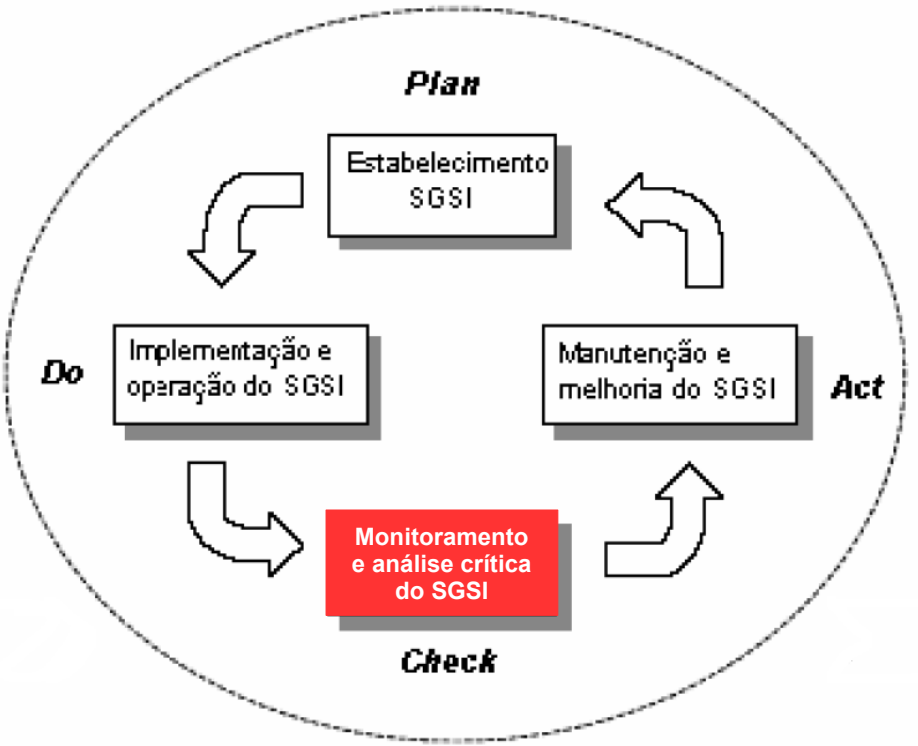


*NBR ISO/IEC 27001:2006

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR 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*.

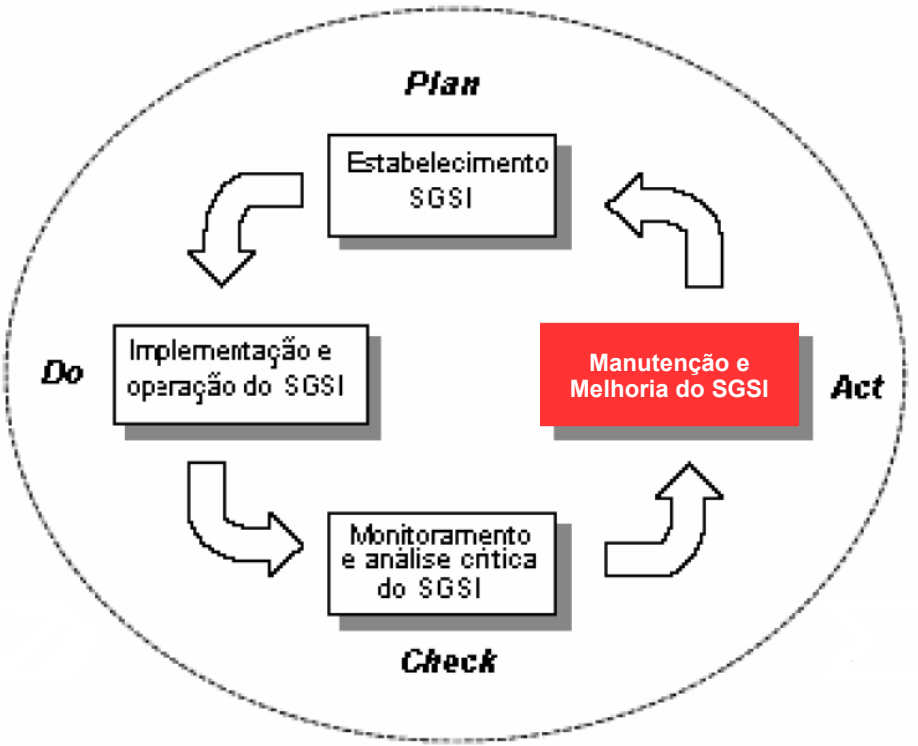


*NBR ISO/IEC 27001:2006

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR 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*.



*NBR ISO/IEC 27001:2006

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Objetivo

Geral

Esta norma cobre todos os tipos de organizações (por exemplo, empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos) e especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.

O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Objetivo

Aplicação

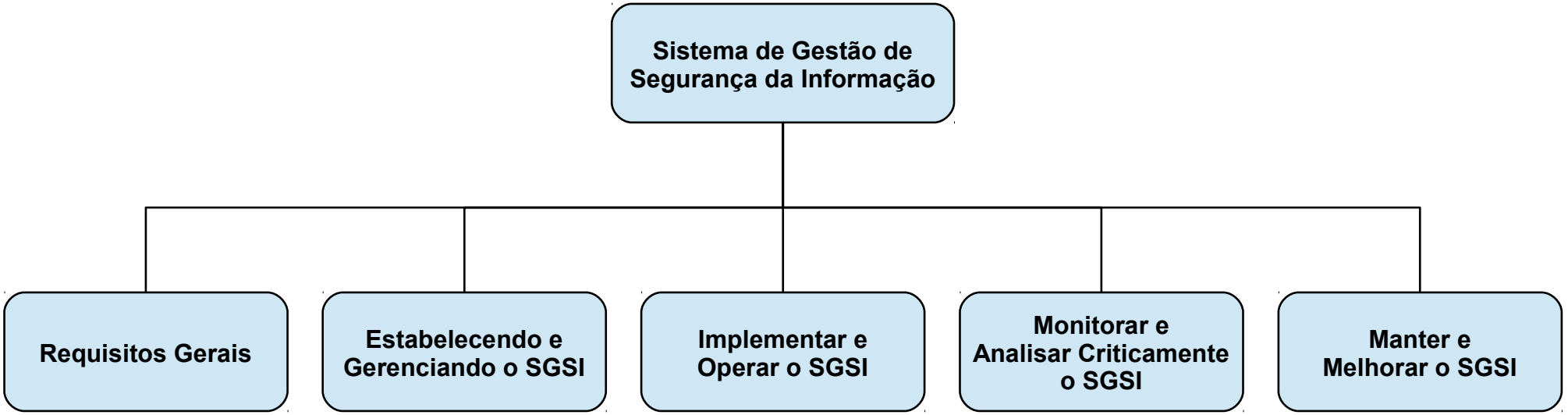
Os requisitos definidos nesta norma são genéricos e é pretendido que sejam aplicáveis a todas as organizações, independentemente de tipo, tamanho e natureza. A exclusão de quaisquer dos requisitos especificados não é aceitável quando uma organização reivindica conformidade com esta Norma.

Qualquer exclusão de controles considerados necessários para satisfazer aos critérios de aceitação de riscos precisa ser justificada e as evidências de que os riscos associados foram aceitos pelas pessoas responsáveis precisam ser fornecidas. Onde quaisquer controles sejam excluídos, reivindicações de conformidade a esta norma não são aceitáveis, a menos que tais exclusões não afetem a capacidade da organização, e/ou responsabilidade de prover segurança da informação que atenda os requisitos de segurança determinados pela análise/avaliação de riscos e por requisitos legais e regulamentares aplicáveis*.

***NBR ISO/IEC 27001:2006**

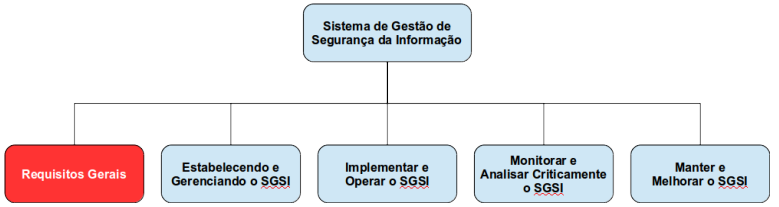
NBR ISO/IEC 27001 – SGSI

O Sistema de Gestão de Segurança da Informação (SGSI) é a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação*.



***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – SGSI



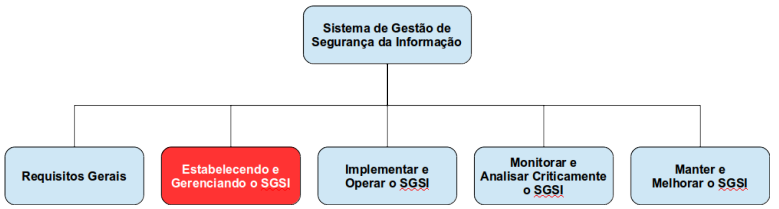
Requisitos gerais

A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – SGSI



Estabelecendo e gerenciando o SGSI

Para estabelecer o SGSI, a organização deve:

a) Definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo;

b) Definir uma política do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia;

c) Definir a abordagem de análise/avaliação de riscos da organização**;

d) Identificar os riscos;

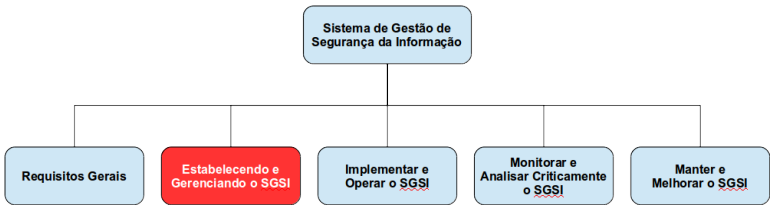
e) Analisar e avaliar os riscos;

*NBR ISO/IEC 27001:2006

**NOTA: Existem diferentes metodologias para análise/avaliação de riscos. São discutidos exemplos de metodologias de análise/avaliação de riscos na ISO/IEC TR 13335-3, *Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT security*.

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – SGSI



Estabelecendo e gerenciando o SGSI – continuação...

f) Identificar e avaliar as opções para o tratamento de riscos;

g) Selecionar objetivos de controle e controles para o tratamento de riscos;

h) Obter aprovação da direção dos riscos residuais propostos;

i) Obter autorização da direção para implementar e operar o SGSI;

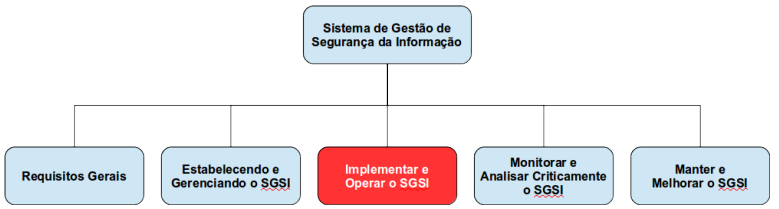
j) Preparar uma Declaração de Aplicabilidade**.

**NOTA: A Declaração de Aplicabilidade provê um resumo das decisões relativas ao tratamento de riscos. A justificativa das exclusões provê uma checagem cruzada de que nenhum controle foi omitido inadvertidamente.

*NBR ISO/IEC 27001:2006

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – SGSI



Implementar e operar o SGSI

Para implementar e operar o SGSI, a organização deve:

a) Formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança;

b) Implementar o plano de tratamento de riscos para alcançar os objetivos de controle identificados, que inclua considerações de financiamentos e atribuição de papéis e responsabilidades;

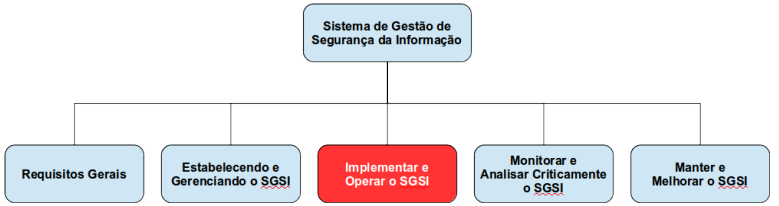
c) Implementar os controles para o tratamento de riscos de modo a atender aos objetivos de controle;

d) Definir como medir a eficácia dos controles ou grupos de controles selecionados, e especificar como estas medidas devem ser usadas para avaliar a eficácia dos controles de modo a produzir resultados comparáveis e reproduzíveis;

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – SGSI



Implementar e operar o SGSI – continuação...

e)Implementar programas de conscientização e treinamento;

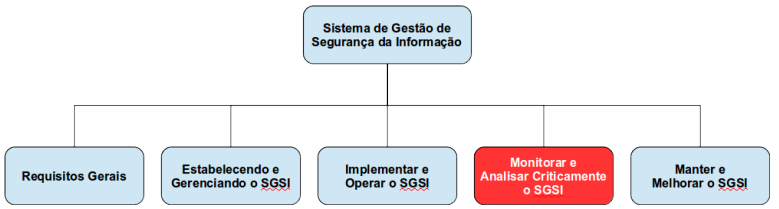
f)Gerenciar as operações do SGSI;

g)Gerenciar os recursos para o SGSI;

h)Implementar procedimentos e outros controles capazes de permitir a pronta detecção de eventos de segurança da informação e resposta a incidentes de segurança da informação*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – SGSI



Monitorar e analisar criticamente o SGSI

Para monitorar e analisar o SGSI, a organização deve:

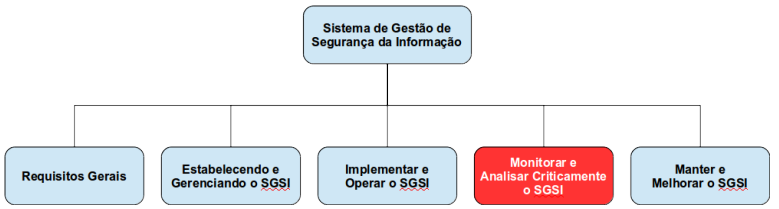
a) Executar procedimentos de monitoração e análise crítica e outros controles para:

1. prontamente detectar erros nos resultados de processamento;
2. prontamente identificar tentativas e violações de segurança bem-sucedidas, e incidentes de segurança da informação;
3. permitir à direção determinar se as atividades de segurança da informação delegadas a pessoas ou implementadas por meio de tecnologias de informação são executadas conforme esperado;
4. ajudar a detectar eventos de segurança da informação e assim prevenir incidentes de segurança da informação pelo uso de indicadores; e
5. determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – SGSI



Monitorar e analisar criticamente o SGSI – continuação...

b) Realizar análises críticas regulares da eficácia do SGSI (incluindo o atendimento da política e dos objetivos do SGSI, e a análise crítica de controles de segurança), levando em consideração os resultados de auditorias de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas;

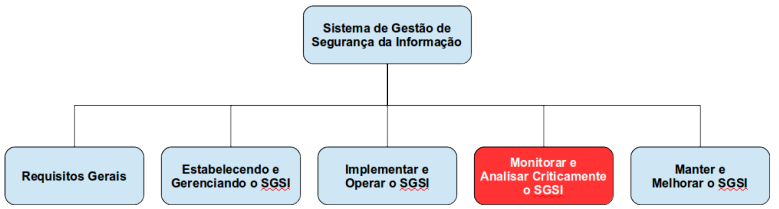
c) Medir a eficácia dos controles para verificar que os requisitos de segurança da informação foram atendidos;

d) Analisar criticamente as análises/avaliações de riscos a intervalos planejados e analisar criticamente os riscos residuais e os níveis de riscos aceitáveis identificados, levando em consideração mudanças relativas a organização, tecnologias, objetivos e processos de negócio, ameaças identificadas, eficácia dos controles implementados e eventos externos, tais como mudanças nos ambientes legais ou regulamentares, alterações das obrigações contratuais e mudanças na conjuntura social;

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – SGSI



Monitorar e analisar criticamente o SGSI – continuação...

e) Conduzir auditorias internas do SGSI a intervalos planejados;

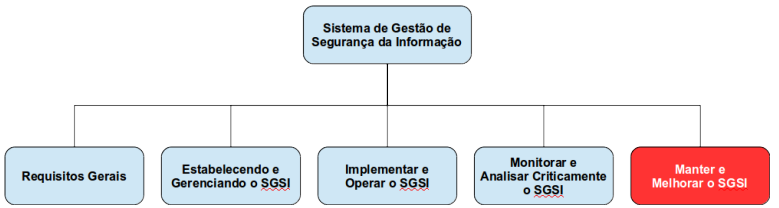
f) Realizar uma análise crítica do SGSI pela direção em bases regulares para assegurar que o escopo permanece adequado e que são identificadas melhorias nos processos do SGSI;

g) Atualizar os planos de segurança da informação para levar em consideração os resultados das atividades de monitoramento e análise crítica;

h) Registrar ações e eventos que possam ter um impacto na eficácia ou no desempenho do SGSI*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – SGSI



Manter e melhorar o SGSI

A organização deve, regularmente:

a) Implementar as melhorias identificadas no SGSI;

b) Executar as ações preventivas e corretivas apropriadas e aplicar as lições aprendidas de experiências de segurança da informação de outras organizações e aquelas da própria organização;

c) Comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe apropriado às circunstâncias e, se relevante, obter a concordância sobre como proceder;

d) Assegurar-se de que as melhorias atinjam os objetivos pretendidos*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Documentação

A documentação deve incluir registros de decisões da direção, assegurar que as ações sejam rastreáveis às políticas e decisões da direção, e assegurar que os resultados registrados sejam reproduzíveis.

É importante que se possa demonstrar a relação dos controles selecionados com os resultados da análise/avaliação de riscos e do processo de tratamento de riscos, e consequentemente com a política e objetivos do SGSI*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Documentação

A documentação do SGSI deve incluir:

a) declarações documentadas da política e objetivos do SGSI;

b) o escopo do SGSI;

c) procedimentos e controles que apoiam o SGSI;

d) uma descrição da metodologia de análise/avaliação de riscos;

e) o relatório de análise/avaliação de riscos;

f) o plano de tratamento de riscos;

g) procedimentos documentados requeridos pela organização para assegurar o planejamento efetivo, a operação e o controle de seus processos de segurança de informação e para descrever como medir a eficácia dos controles;

h) registros requeridos por esta norma;

i) a Declaração de Aplicabilidade*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Documentação

Declaração de Aplicabilidade é uma declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da organização.

OBS.: Os objetivos de controle e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Responsabilidades

Comprometimento da direção

A direção deve fornecer evidência do seu comprometimento com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do SGSI mediante:

a) o estabelecimento da política do SGSI;

b) a garantia de que são estabelecidos os planos e objetivos do SGSI;

c) o estabelecimento de papéis e responsabilidades pela segurança de informação;

d) a comunicação à organização da importância em atender aos objetivos de segurança da informação e a conformidade com a política de segurança de informação, suas responsabilidades perante a lei e a necessidade para melhoria contínua;

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Responsabilidades

Provisão de recursos

A organização deve determinar e prover os recursos necessários para:

a) estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI;

b) assegurar que os procedimentos de segurança da informação apoiam os requisitos de negócio;

c) identificar e tratar os requisitos legais e regulamentares e obrigações contratuais de segurança da informação;

d) manter a segurança da informação adequada pela aplicação correta de todos os controles implementados;

e) realizar análises críticas, quando necessário, e reagir adequadamente aos resultados destas análises críticas;

f) onde requerido, melhorar a eficácia do SGSI*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Responsabilidades

Treinamento, conscientização e competência

A organização deve assegurar que todo o pessoal que tem responsabilidades atribuídas definidas no SGSI seja competente para desempenhar as tarefas requeridas:

a) determinando as competências necessárias para o pessoal que executa trabalhos que afetam o SGSI;

b) fornecendo treinamento ou executando outras ações (por exemplo, contratar pessoal competente) para satisfazer essas necessidades;

c) avaliando a eficácia das ações executadas;

d) mantendo registros de educação, treinamento, habilidades, experiências e qualificações*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Auditorias

A organização deve conduzir auditorias internas do SGSI a intervalos planejados para determinar se os objetivos de controle, controles, processos e procedimentos do seu SGSI:

a) atendem aos requisitos desta norma e à legislação ou regulamentações pertinentes;

b) atendem aos requisitos de segurança da informação identificados;

c) estão mantidos e implementados eficazmente;

d) são executados conforme esperado*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Análise Crítica

A direção deve analisar criticamente o SGSI da organização a intervalos planejados (pelo menos uma vez por ano) para assegurar a sua contínua pertinência, adequação e eficácia.

Esta análise crítica deve incluir a avaliação de oportunidades para melhoria e a necessidade de mudanças do SGSI, incluindo a política de segurança da informação e objetivos de segurança da informação.

Os resultados dessas análises críticas devem ser claramente documentados e os registros devem ser mantidos*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Análise Crítica

Entradas para a análise crítica

As entradas para a análise crítica pela direção devem incluir:

a) resultados de auditorias do SGSI e análises críticas;

b) realimentação das partes interessadas;

c) técnicas, produtos ou procedimentos que podem ser usados na organização para melhorar o desempenho e a eficácia do SGSI;

d) situação das ações preventivas e corretivas;

e) vulnerabilidades ou ameaças não contempladas adequadamente nas análises/avaliações de risco anteriores;

f) acompanhamento das ações oriundas de análises críticas anteriores pela direção;

g) quaisquer mudanças que possam afetar o SGSI;

h) recomendações para melhoria*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Análise Crítica

Saídas para a análise crítica

As saídas da análise crítica pela direção devem incluir quaisquer decisões e ações relacionadas a:

a) melhoria da eficácia do SGSI;

b) atualização da análise/avaliação de riscos e do plano de tratamento de riscos;

c) modificação de procedimentos e controles que afetem a segurança da informação, quando necessário, para responder a eventos internos ou externos que possam impactar no SGSI, incluindo mudanças de requisitos de negócio, requisitos de segurança da informação, processos de negócio que afetem os requisitos de negócio existentes, requisitos legais ou regulamentares, obrigações contratuais e níveis de riscos e/ou critérios de aceitação de riscos;

d) necessidade de recursos;

e) melhoria de como a eficácia dos controles está sendo medida*.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Melhoria Contínua

A organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análises de eventos monitorados, ações corretivas e preventivas e análise crítica pela direção*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Melhoria Contínua

Ação corretiva

A organização deve executar ações para eliminar as causas de não-conformidades com os requisitos do SGSI, de forma a evitar a sua repetição. O procedimento documentado para ação corretiva deve definir requisitos para:

a) identificar não-conformidades;

b) determinar as causas de não-conformidades;

c) avaliar a necessidade de ações para assegurar que aquelas não-conformidades não ocorram novamente;

d) determinar e implementar as ações corretivas necessárias;

e) registrar os resultados das ações executadas;

f) analisar criticamente as ações corretivas executadas*.

*NBR ISO/IEC 27001:2006

NBR ISO/IEC 27001 – Melhoria Contínua

Ação preventiva

A organização deve determinar ações para eliminar as causas de não-conformidades potenciais com os requisitos do SGSI, de forma a evitar a sua ocorrência. As ações preventivas tomadas devem ser apropriadas aos impactos dos potenciais problemas. O procedimento documentado para ação preventiva deve definir requisitos para:

a) identificar não-conformidades potenciais e suas causas;

b) avaliar a necessidade de ações para evitar a ocorrência de não-conformidades;

c) determinar e implementar as ações preventivas necessárias;

d) registrar os resultados de ações executadas;

e) analisar criticamente as ações preventivas executadas*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Controles

Os objetivos de controle e controles apresentados na norma são derivados e estão alinhados com a ISO/IEC 27002. Esta lista não é exaustiva e uma organização pode considerar que objetivos de controle e controles adicionais sejam necessários.

Os objetivos de controle e controles desta lista devem ser selecionados como parte do processo de SGSI especificado em Estabelecer e Gerenciar o SGSI.

Ao todo são 11 (onze) categorias, 39 (trinta e nove) objetivos de controle e 133 (cento e trinta e três) controles*.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Exemplos

A.5 Política de segurança		
A.5.1 Política de segurança da informação *Objetivo:* Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.		
A.5.1.1	Documento da política de segurança da informação	*Controle* Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica da política de segurança da informação	*Controle* A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Exemplos

A.7 Gestão de ativos		
A.7.1 Responsabilidade pelos ativos *Objetivo:* Alcançar e manter a proteção adequada dos ativos da organização.		
A.7.1.1	Inventário dos ativos	*Controle* Todos os ativos devem ser claramente identificados e um inventário de todos os ativos importantes deve ser estruturado e mantido.
A.7.1.2	Proprietário dos ativos	*Controle* Todas as informações e ativos associados com os recursos de processamento da informação devem ter um "proprietário"[3)] designado por uma parte definida da organização.
A.7.1.3	Uso aceitável dos ativos	*Controle* Devem ser identificadas, documentadas e implementadas regras para que seja permitido o uso de informações e de ativos associados aos recursos de processamento da informação.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Exemplos

A.9 Segurança física e do ambiente		
A.9.1 Áreas seguras *Objetivo:* Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.		
A.9.1.1	Perímetro de segurança física	*Controle* Devem ser utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e recursos de processamento da informação.
A.9.1.2	Controles de entrada física	*Controle* As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.
A.9.1.3	Segurança em escritórios salas e instalações	*Controle* Deve ser projetada e aplicada segurança física para escritórios, salas e instalações.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Exemplos

A.10.5 Cópias de segurança		
Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.		
A.10.5.1	Cópias de segurança das informações	*Controle* Cópias de segurança das informações e dos *softwares* devem ser efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Exemplos

A.10.6 Gerenciamento da segurança em redes *Objetivo:* Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte.		
A.10.6.1	Controles de redes	*Controle* Redes devem ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito.
A.10.6.2	Segurança dos serviços de rede	*Controle* Características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Exemplos

A.10.9 Serviços de comércio eletrônico *Objetivo:* Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.		
A.10.9.1	Comércio eletrônico	*Controle* As informações envolvidas em comércio eletrônico transitando sobre redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas.
A.10.9.2	Transações *on-line*	*Controle* Informações envolvidas em transações *on-line* devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
A.10.9.3	Informações publicamente disponíveis	*Controle* A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida, para prevenir modificações não autorizadas.

***NBR ISO/IEC 27001:2006**

NBR ISO/IEC 27001 – Exemplos

A.11.2 Gerenciamento de acesso do usuário *Objetivo:* Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.		
A.11.2.1	Registro de usuário	*Controle* Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.
A.11.2.2	Gerenciamento de privilégios	*Controle* A concessão e o uso de privilégios devem ser restritos e controlados.
A.11.2.3	Gerenciamento de senha do usuário	*Controle* A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27001 – Exemplos

A.11.3 Responsabilidades dos usuários *Objetivo:* Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.		
A.11.3.1	Uso de senhas	*Controle* Os usuários devem ser orientados a seguir boas práticas de segurança da informação na seleção e uso de senhas.
A.11.3.2	Equipamento de usuário sem monitoração	*Controle* Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada.
A.11.3.3	Política de mesa limpa e tela limpa	*Controle* Deve ser adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

***NBR ISO/IEC 27001:2006**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Para saber mais...

… veja os Objetivos de Controle e Controles da ABNT NBR ISO/IEC 27001:2005.

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

Módulo 5

Melhores Práticas de Segurança da Informação

NBR 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*.

Por que a Segurança da Informação é necessária?

A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (*e-gov*) ou o comércio eletrônico (*e-business*), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado*.

***NBR ISO/IEC 27002:2005**

NBR 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. Uma fonte é obtida a partir da análise/avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da análise/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. Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço tem que atender, além do seu ambiente sociocultural.

3. A terceira fonte é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações*.

***NBR ISO/IEC 27002:2005**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27002 – Análise de Riscos

Analisando/avaliando os riscos de segurança da informação

Os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação. Os gastos com os controles precisam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação.

Os resultados da análise/avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação, e para a implementação dos controles selecionados para a proteção contra estes riscos.

Convém que a análise/avaliação de riscos seja repetida periodicamente para contemplar quaisquer mudanças que possam influenciar os resultados desta análise/avaliação*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Análise de Riscos

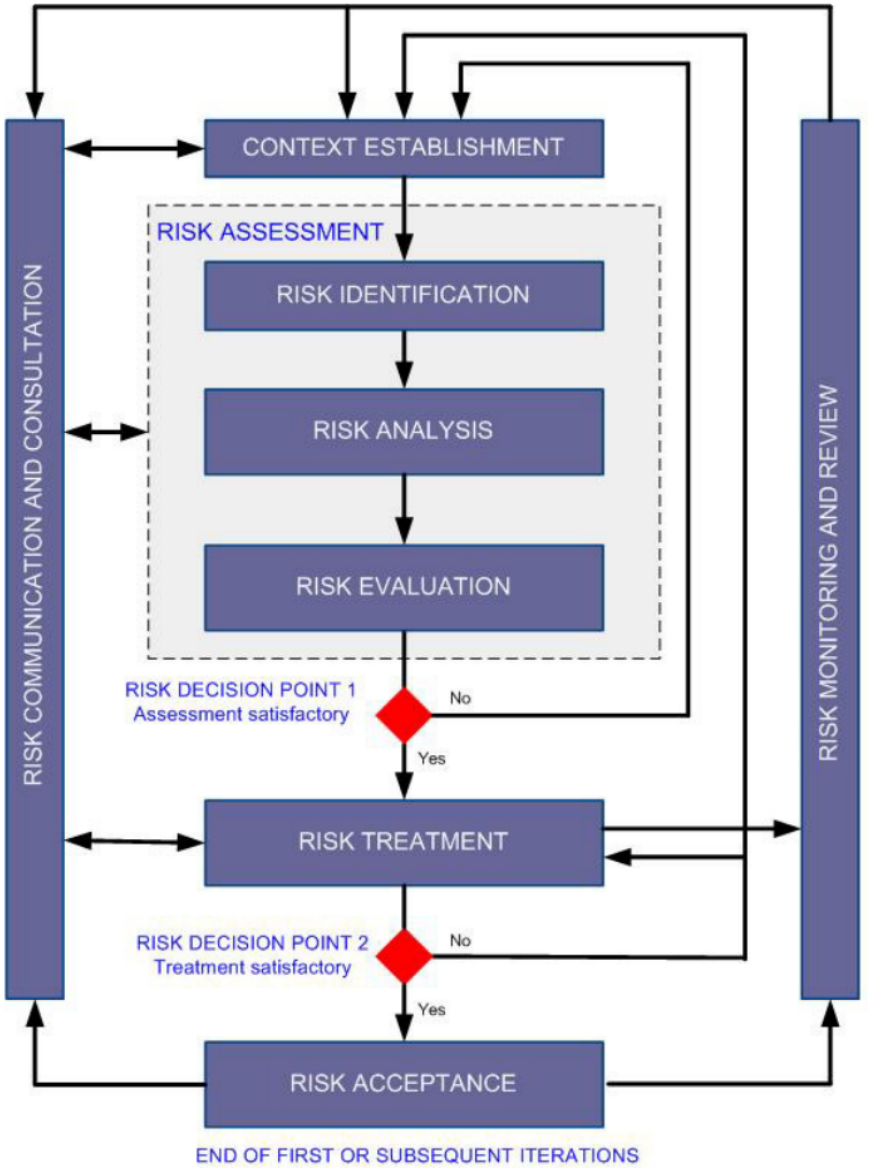
Analisando/avaliando os riscos de segurança da informação – continuação...

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*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Análise de Riscos



*ISO/IEC 27005:2011

Processo de Gerenciamento de Risco de Segurança da Informação*

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27002 – Controles

Seleção de controles

Uma vez que os requisitos de segurança da informação e os riscos tenham sido identificados e as decisões para o tratamento dos riscos tenham sido tomadas, convém que controles apropriados sejam selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável. Os controles podem ser selecionados a partir desta norma ou de um outro conjunto de controles ou novos controles podem ser desenvolvidos 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 também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais relevantes.

Alguns dos controles nesta norma podem ser considerados como princípios básicos para a gestão da segurança da informação e podem ser aplicados na maioria das organizações*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Tratamento de Riscos

Tratando os riscos de segurança da informação

Convém que, antes de considerar o tratamento de um risco, a organização defina os critérios para determinar se os riscos podem ser ou não aceitos. Riscos podem ser aceitos se, por exemplo, for avaliado que o risco é baixo ou que o custo do tratamento não é economicamente viável para a organização.

Para cada um dos riscos identificados, seguindo a análise/avaliação de riscos, uma decisão sobre o tratamento do risco precisa ser tomada. Possíveis opções para o tratamento do risco incluem:

a) aplicar controles apropriados para reduzir os riscos;

b) conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente a política da organização e aos critérios para a aceitação de risco;

c) evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;

d) transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Tratamento de Riscos

Tratando os riscos de segurança da informação – continuação...

Convém que, para aqueles riscos onde a decisão de tratamento do risco seja a de aplicar os controles apropriados, esses controles sejam selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos. Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável, levando-se em conta:

a) os requisitos e restrições de legislações e regulamentações nacionais e internacionais;

b) os objetivos organizacionais;

c) os requisitos e restrições operacionais;

d) custo de implementação e a operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais às restrições e requisitos da organização;

e) a necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Tratamento de Riscos

Tratando os riscos de segurança da informação – continuação...

Os controles podem ser selecionados desta norma ou de outros conjuntos de controles, ou novos controles podem ser considerados para atender às necessidades específicas da organização. É importante reconhecer que alguns controles podem não ser aplicáveis a todos os sistemas de informação ou ambientes, e podem não ser praticáveis para todas as organizações.

Convém que os controles de segurança da informação sejam considerados na especificação dos requisitos e nos estágios iniciais dos projetos e sistemas. Caso isso não seja realizado, pode acarretar custos adicionais e soluções menos efetivas, ou mesmo, no pior caso, incapacidade de se alcançar a segurança necessária.

Convém que seja lembrado que nenhum conjunto de controles pode conseguir a segurança completa, e que uma ação gerencial adicional deve ser implementada para monitorar, avaliar e melhorar a eficiência e eficácia dos controles de segurança da informação, para apoiar as metas da organização*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Ponto de Partida

Ponto de partida para a Segurança da Informação

Um certo número de controles pode ser considerado um bom ponto de partida para a implementação da segurança da informação. Estes controles são baseados tanto em requisitos legais como nas melhores práticas de segurança da informação normalmente usadas.

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem, dependendo da legislação aplicável:

a) proteção de dados e privacidade de informações pessoais;

b) proteção de registros organizacionais;

c) direitos de propriedade intelectual*.

***NBR ISO/IEC 27002:2005**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27002 – Ponto de Partida

Ponto de partida para a Segurança da Informação – continuação...

Os controles considerados práticas para a segurança da informação incluem:

a) documento da política de segurança da informação;

b) atribuição de responsabilidades para a segurança da informação;

c) conscientização, educação e treinamento em segurança da informação;

d) processamento correto nas aplicações;

e) gestão de vulnerabilidades técnicas;

f) gestão da continuidade do negócio;

g) gestão de incidentes de segurança da informação e melhorias*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Ponto de Partida

Ponto de partida para a Segurança da Informação – continuação...

Esses controles se aplicam para a maioria das organizações e na maioria dos ambientes.

Convém observar que, embora todos os controles nesta norma sejam importantes e devam ser considerados, a relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta. Por isto, embora o enfoque acima seja considerado um bom ponto de partida, ele não substitui a seleção de controles baseado na análise/avaliação de riscos*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Fatores de Sucesso

Fatores críticos de sucesso

A experiência tem mostrado que os seguintes fatores são geralmente críticos para o sucesso da implementação da segurança da informação dentro de uma organização:

a) política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;

b) uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;

c) comprometimento e apoio visível de todos os níveis gerenciais;

d) um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;

e) divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Fatores de Sucesso

Fatores críticos de sucesso – continuação...

f) distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;

g) provisão de recursos financeiros para as atividades da gestão de segurança da informação;

h) provisão de conscientização, treinamento e educação adequados;

i) estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;

j) implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria*.

***NBR ISO/IEC 27002:2005**

Prof. Me. Wallace Rodrigues de Santana
www.neutronica.com.br

NBR ISO/IEC 27002 – Estrutura

Estrutura da norma

Contém 11 seções de controles de segurança da informação, que juntas totalizam 39 categorias principais de segurança ou objetivos de controle, 133 controles e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos. Cada seção contém um número de categorias principais de segurança da informação, conforme listadas abaixo:

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

b) Organizando a Segurança da Informação (2 categorias e/ou objetivos de controle e 11 controles);

c) Gestão de Ativos (2 categorias e/ou objetivos de controle e 5 controles);

d) Segurança em Recursos Humanos (3 categorias e/ou objetivos de controle e 9 controles);

e) Segurança Física e do Ambiente (2 categorias e/ou objetivos de controle e 13 controles);

f) Gerenciamento das Operações e Comunicações (10 categorias e/ou objetivos de controle e 32 controles)*;

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Estrutura

Estrutura da norma – continuação...

g) Controle de Acessos (7 categorias e/ou objetivos de controle e 25 controles);

h) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (6 categorias e/ou objetivos de controle e 16 controles);

i) Gestão de Incidentes de Segurança da Informação (2 categorias e/ou objetivos de controle e 5 controles);

j) Gestão da Continuidade do Negócio (1 categoria e/ou objetivo de controle e 5 controles);

k) Conformidade (3 categorias e/ou objetivos de controle e 10 controles)*.

***NBR ISO/IEC 27002:2005**

NBR ISO/IEC 27002 – Estrutura

Estrutura da norma – continuação...

Cada categoria principal de segurança da informação contém:

- Um objetivo de controle que define o que deve ser alcançado; e
- Um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle:

a) Controle – define qual o controle específico para atender ao objetivo do controle.

b) Diretrizes para a implementação – contém informações mais detalhadas para apoiar a implementação do controle e atender ao objetivo de controle. Algumas destas diretrizes podem não ser adequadas em todos os casos e assim outras formas de implementação do controle podem ser mais apropriadas;

c) Informações adicionais – contém informações adicionais que podem ser consideradas, como, por exemplo, considerações legais e referências a outras normas*.

***NBR ISO/IEC 27002:2005**

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