Marisangila Alves, MSc
marisangila.alves@gmail.com

UDESC
Universidade do Estado de Santa Catarina

Segurança da Informação
Normas

Sumário

Conceitos

Normas

Para que a segurança não seja algo empírico, surgiram as **normas** que permitem padronização e análise.

- **Norma**: aprovada por órgão reconhecido e deve ser seguida para alcançar conformidade.
- **Regulamento**: publicado ou definido por alguma organização; nem sempre é norma.
- **Política**: define a direção a ser alcançada, baseada em norma.
- **Procedimento**: meios pelos quais os atos devem ser realizados para cumprir norma/polític

História

Histórico das Principais Normas e Regulamentos I

- **BS 7799** – Publicada pela BSI *(British Standards Institution)* em **1995**.
- **ISO/IEC 17799** – Publicada pela ISO/IEC em **2000**.
- **NBR ISO/IEC 17799** – Publicada pela ABNT em **2001**.
- **ISO/IEC 17799:2005** – Revisada e publicada pela ISO/IEC em **2005**.
- **ISO/IEC 27002** – Renomeada e publicada pela ISO/IEC em **2007**.
- **ISO/IEC 27001** – Publicada pela ISO/IEC em **2005**.
- **COBIT** – Publicada pela ISACA *Information Systems Audit and Control Association* em **1996**.
- **ITIL** – Publicada pela OGC *(Office of Government Commerce)* em **1989**, atualizada em versões subsequentes.

Histórico das Principais Normas e Regulamentos II

Regulamentos Relacionados:

- **FIPS** – *Federal Information Processing Standards* Publicado pelo NIST (EUA) em **1973**.
- **HIPAA** – *Health Insurance Portability and Accountability Act* Publicado pelo HHS (EUA) em **1996**.
- **GDPR** – *General Data Protection Regulation* Regulamento da União Europeia, adotado em **2016**.
- **LGPD** – Lei Geral da Proteção de Ddos brasiliera, sancionada em **2018**.

BS 7799

Norma britânica pioneira que define diretrizes para a gestão da segurança da informação. Publicada em 1995, foi a precursora da **ISO/IEC 27001** e estabeleceu as bases para implementação de práticas de proteção de dados nas organizações.

Evolução da ISO/IEC 17799 → 27002 I

Contexto: A ISO/IEC 17799 (2000) é a versão original como código de prática para gestão de segurança da informação, baseada na BS 7799-1.

Evolução da ISO/IEC 17799 → 27002 II

Evolução da ISO/IEC 17799 → 27002 III

- BS 7799-1 (1995) – Primeira norma britânica sobre gestão de segurança; fundamentos e boas práticas.
- ISO/IEC 17799 (2000) – Versão internacional baseada na BS 7799-1; código de prática de controles de segurança.
- ISO/IEC 27002 (2007) – Atualização da ISO 17799; guia de controles alinhado à família ISO 27000.

Família ISO 27000

Família de Normas ISO 27000

- ISO/IEC 27000 — Visão geral e vocabulário.
- ISO/IEC 27001 — Requisitos para SGSI.
- ISO/IEC 27002 — Código de prática para gestão de segurança.
- ISO/IEC 27003 — Guia de implementação.
- ISO/IEC 27004 — Medição e monitoramento de segurança.
- ISO/IEC 27005 — Gestão de riscos.
- ISO/IEC 27006 — Auditoria e certificação.

Comparativo de Normas ISO 27000

Norma	Objetivo	Foco Principal
ISO/IEC 27001	Definir requisitos para SGSI	Norma certificável; estabelece gestão da segurança da informação.
ISO/IEC 27002	Fornecer diretrizes práticas	Guia de implementação dos controles (políticas, processos, tecnologia, pessoas e físico).
ISO/IEC 27003	Orientar implementação do SGSI	Guia passo a passo do planejamento e operação.
ISO/IEC 27004	Medir e monitorar SGSI	Métricas, indicadores e métodos para avaliar resultados de segurança.
ISO/IEC 27005	Gerenciar riscos	Identificação, análise, tratamento e monitoramento de riscos.

ISO/IEC 27001 — Cláusulas Principais I

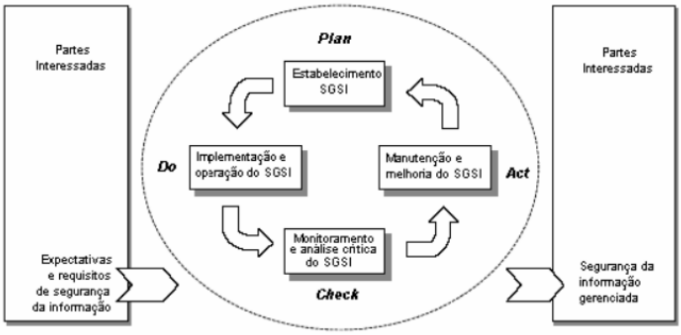
ISO/IEC 27001 — Cláusulas Principais II

Objetivos

Estabelecer requisitos para um **Sistema de Gestão de Segurança da Informação (SGSI)**, baseada no ciclo PDCA (*Plan-Do-Check-Act*).

ISO/IEC 27001 — Cláusulas Principais III

ISO/IEC 27001 — Cláusulas Principais IV



ISO/IEC 27001 — Cláusulas Principais V

- **Cláusula 4 — Contexto da Organização:** escopo, requisitos legais, partes interessadas.
- **Cláusula 5 — Liderança:** política de segurança, papéis e responsabilidades, apoio da direção.
- **Cláusula 6 — Planejamento:** avaliação de riscos, tratamento de riscos, objetivos de segurança.
- **Cláusula 7 — Apoio:** recursos, treinamento, comunicação, documentação.
- **Cláusula 8 — Operação:** execução de controles, gestão de riscos no dia a dia.
- **Cláusula 9 — Avaliação de Desempenho:** auditorias, métricas, análise crítica.
- **Cláusula 10 — Melhoria:** ações corretivas, lições aprendidas, melhoria contínua.

ISO/IEC 27001 — Cláusulas Principais VI

Itens da ISO9001:2015 – 10, 10.1, 10.2 e 10.3.	Itens da ISO9001:2015 – 6, 6.1, 6.2 e 6.3.
Itens da ISO9001:2015 – 9, 9.1, 9.1.1, 9.1.2, 9.1.3, 9.2, 9.3, 9.3.1, 9.3.2, 9.3.3.	Itens da ISO9001:2015 – 7, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.5.1, 7.1.5.2, 7.1.6, 7.2, 7.3, 7.4, 7.5, 7.5.1, 7.5.2, 7.5.3, 8, 8.1, 8.2, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.3, 8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6, 8.4, 8.4.1, 8.4.2, 8.4.3, 8.5, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.5, 8.5.6, 8.6 e 8.7.

:ontinuously improve the ISMS.

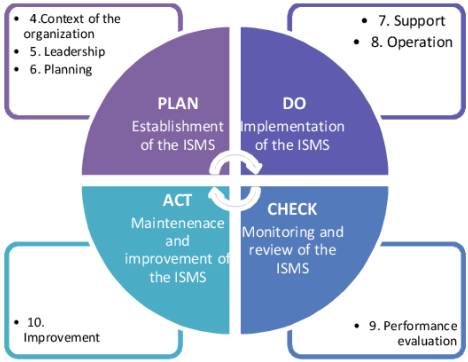


Figure 1 - PDCA cycle and the NP ISO/IEC 27001:2013 4 to 10 clauses (adapted from [18, p. 13])

ISO/IEC 27001 — Anexo A (Controles de Segurança)

- A.5 Políticas de segurança
- A.6 Organização da segurança
- A.7 Recursos humanos
- A.8 Gestão de ativos
- A.9 Controle de acesso
- A.10 Criptografia
- A.11 Segurança física e ambiental
- A.12 Operações
- A.13 Segurança das comunicações
- A.14 Desenvolvimento e manutenção
- A.15 Fornecedores
- A.16 Gestão de incidentes
- A.17 Continuidade do negócio
- A.18 Conformidade

Obs.: Versão 2022 possui 93 controles distribuídos nessas seções.

ISO/IEC 27001 — Documentos do Ciclo PDCA

Plan (Planejar):

- Política de Segurança da Informação, Escopo do SGSI
- Metodologia e Relatório de Riscos
- Plano de Tratamento de Riscos, Declaração de Aplicabilidade
- Objetivos de segurança

Do (Executar):

- Procedimentos operacionais, planos de resposta a incidentes
- Documentos: Plano de Continuidade do Negócio e Plano de Recuperação de Desastres, registros de treinamentos
- Controles técnicos aplicados (firewalls, IDS/IPS, backups)

ISO/IEC 27001 — Documentos do Ciclo PDCA (continuação) I

Check (Verificar):

- Relatórios de auditorias internas
- Registros de monitoramento e métricas
- Relatórios de análise crítica da direção
- Resultados de testes de continuidade

Act (Agir):

- Ações corretivas documentadas
- Revisão e atualização da política
- Atualização da matriz de riscos
- Implementação de melhorias

ISO/IEC 27002 — Detalhes por Seção I

Objetivos

Fornecer diretrizes para implementação de controles de segurança.

ISO/IEC 27002 — Detalhes por Seção II

Seção	O que diz	Exemplo
Políticas de Segurança	Diretrizes, responsabilidades e objetivos	Criar política formal, aprovada, comunicada e revisada anualmente
Organização da Segurança	Papéis e governança	Definir CISO, comitês e responsabilidades para TI, RH e áreas de negócio
Segurança RH	Controle de pessoal, treinamento	Treinar sobre phishing, acordo de confidencialidade, política de senhas; gerenciar desligamentos
Gestão de Ativos	Inventário e proteção de ativos	Mapear ativos críticos, classificar dados e aplicar controles físicos/lógicos
Controle de Acesso	Autenticação e privilégios	Implementar controle de acesso baseado em papéis, MFA, senhas fortes e revisão periódica
Criptografia	Proteção de dados	Criptografar dados em trânsito (TLS) e repouso (AES-256); gestão de chaves
Segurança Física	Proteção física	Controle de acesso, câmeras, alarmes, climatização e redundância
Segurança em Operações	Sistemas e backup	Atualizações, antivírus, monitoramento, backup rotativo e logs centralizados
Segurança das Comunicações	Proteção da rede	VPN, firewalls, segmentação, DMZ, auditoria de tráfego
Desenvolvimento de Sistemas	Ciclo de vida seguro	Revisão de código, testes, desenvolvimento seguro, mudanças controladas
Fornecedores	Terceirização	Contratos, cláusulas de confidencialidade, auditorias críticas
Gestão de Incidentes	Resposta a incidentes	Plano de resposta, equipe SOC, registro e investigação
Continuidade do Negócio	Contingência	DRP, redundância, backup offsite, testes periódicos
Conformidade	Auditoria e legislação	Auditorias internas, LGPD, GDPR, ISO 27001

ISO/IEC 27003 — Detalhes por Seção I

Objetivos

Transformar requisitos da ISO 27001 em ações práticas.

ISO/IEC 27003 — Detalhes por Seção II

Seção	O que diz	Exemplo
Introdução e Escopo	Contextualiza SGSI	Mapear escopo, definir processos e limites
Planejamento do SGSI	Políticas e objetivos	Criar plano, definir metas e cronogramas
Contexto da Organização	Ambiente interno/externo	Identificar stakeholders, requisitos legais, recursos, ameaças
Avaliação e Tratamento de Riscos	Analisar/priorizar riscos	Usar ISO 27005, calcular probabilidade $\times$ impacto, priorizar mitigação
Implementação de Controles	Controles do Anexo A	Selecionar controles ISO 27002, configurar firewalls, IDS/IPS, backups, MFA
Integração de Processos	Alinhar SGSI	Sincronizar com ITIL, COBIT, ISO 22301 e processos corporativos
Treinamento e Conscientização	Preparar equipe	Workshops, simulados de phishing, treinamentos periódicos
Monitoramento e Revisão	Auditorias e métricas	Revisão de KPIs, auditorias internas/externas, logs periódicos
Melhoria Contínua	Feedback e ajustes	Aprender com incidentes, atualizar políticas, implementar novos controles

ISO/IEC 27004 — Detalhes por Seção I

Objetivos

Avaliar eficácia do SGSI via métricas.

ISO/IEC 27004 — Detalhes por Seção II

Seção	O que diz	Exemplo
Introdução e Escopo	Importância de medir SGSI	Estabelecer métricas alinhadas a objetivos estratégicos
Planejamento da Medição	Escolher métricas	Definir KPIs: tempo de resposta, vulnerabilidades críticas, disponibilidade
Desenvolvimento de Métricas	Quantitativas/qualitativas	Número de incidentes, tempo médio de resolução, % de conformidade de backups
Coleta de Dados	Logs e eventos	SIEM, IDS/IPS, logs centralizados, auditorias periódicas
Análise de Métricas	Avaliar eficácia dos controles	Comparar métricas com objetivos, identificar gaps de segurança
Relatórios e Comunicação	Comunicar resultados	Dashboards, relatórios gerenciais, alertas a CISO e direção
Melhoria Contínua	Ajustar controles/processos	Revisar políticas, atualizar procedimentos, treinamento contínuo

ISO/IEC 27005 — Detalhes por Seção I

Objetivos

Estabelecer metodologia de análise e tratamento de riscos.

ISO/IEC 27005 — Detalhes por Seção II

Seção	O que diz	Exemplo
Introdução e Conceitos	Define termos e escopo de riscos	Criar glossário interno, explicar conceitos à equipe
Estabelecimento do Contexto	Contexto organizacional	Identificar escopo, regulamentações, tolerância a risco, objetivos estratégicos
Identificação de Riscos	Ativos, ameaças e vulnerabilidades	Inventariar ativos, mapear ameaças externas/internas, avaliar vulnerabilidades
Análise de Riscos	Probabilidade x impacto	Avaliar riscos quantitativa/qualitativamente, calcular severidade
Avaliação de Riscos	Priorização	Definir riscos críticos que demandam tratamento imediato
Tratamento de Riscos	Mitigação, aceitação, transferência	Implementar controles, seguros, contratos ou aceitar risco residual
Aceitação e Comunicação	Aprovar riscos e informar stakeholders	Relatórios de riscos, aprovação da direção, comunicação transparente
Monitoramento e Revisão	Revisão contínua de riscos	Auditorias periódicas, testes de penetração, revisão de matrizes de risco

COBIT

Definição

O **COBIT (Control Objectives for Information and Related Technologies)** é um **guia de boas práticas** criado pela ISACA e pelo IT Governance Institute, voltado ao **gerenciamento e controle da Tecnologia da Informação**.

- Foco no **uso eficaz dos recursos de TI** e na geração de valor para o negócio;
- Baseado em metodologias que visam o **alinhamento estratégico** e a **governança de TI**;
- Define processos, responsabilidades e controles de gestão;
- Evoluiu ao longo de cinco versões principais.

- alinhamento entre TI e metas do negócio;
- gestão de riscos e conformidade normativa;
- otimização de recursos de tecnologia;
- melhoria contínua e adaptação das práticas à realidade da organização.

O Cubo do COBIT I

O **Cubo do COBIT** é uma representação gráfica que demonstra a **relação entre os recursos de TI, os processos e os critérios de informação**. Ele ilustra como o COBIT integra a governança e o gerenciamento de tecnologia da informação em três dimensões:

- **Critérios de Informação** — qualidade, eficácia, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade;
- **Recursos de TI** — aplicações, informações, infraestrutura e pessoas;
- **Processos de TI** — organizados nos quatro domínios: PO, AI, DS e ME.

O Cubo do COBIT II

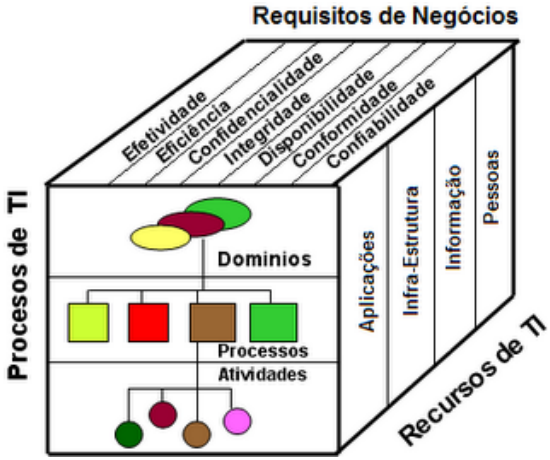


Figure: O Cubo do COBIT.

O Cubo do COBIT III

Information

O cubo mostra que a **governança de TI** deve considerar simultaneamente **os objetivos de informação**, **os recursos de TI** e **os processos de controle**, garantindo valor e desempenho organizacional.

Evolução I

O COBIT possui uma trajetória de evolução com foco crescente na integração entre **negócio, governança e tecnologia**.

- Cinco versões lançadas até o COBIT 2019;
- Estrutura baseada em **domínios e processos de TI**;
- Apoia-se em ferramentas como a **Matriz RACI** e nos **níveis de maturidade**;
- Permite medir e acompanhar o grau de maturidade da organização.

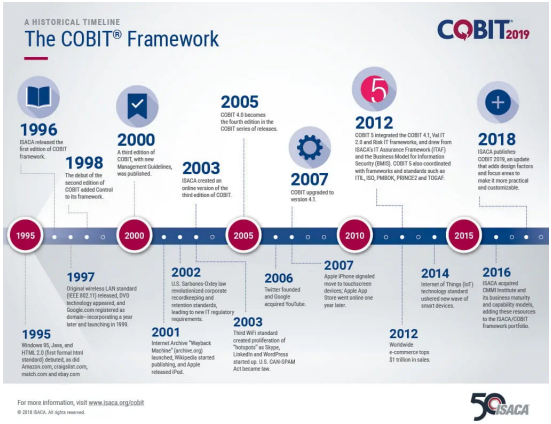


Figure: Evolução e estrutura conceitual do COBIT.

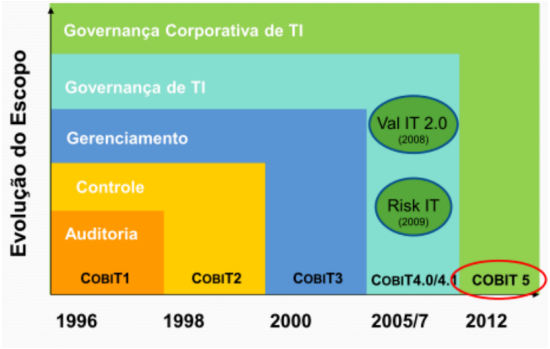


Figure: Evolução de escopo.

Áreas de Governança de TI I

O COBIT define **cinco áreas de Governança de TI** que direcionam a gestão e o controle organizacional:

- **Alinhamento Estratégico** – garantir que TI e negócio compartilhem os mesmos objetivos;
- **Entrega de Valor** – assegurar que os investimentos em TI gerem retorno;
- **Gestão de Riscos** – reduzir incertezas e impactos operacionais;
- **Gestão de Recursos** – otimizar o uso de pessoas, infraestrutura e informações;
- **Mensuração de Desempenho** – acompanhar resultados e promover a melhoria contínua.

Áreas de Governança de TI II

Domínios o Ciclo PDCA I

- O COBIT® divide a atuação da TI em:
  - 4 domínios
  - 34 áreas de processos
  - 210 atividades
- Objetivo: promover a **melhoria contínua** das organizações.
- A melhoria contínua ocorre de acordo com o **ciclo PDCA**:
  - **Planejar e Organizar (PO)** ⇒ Plan
  - **Adquirir e Implementar (AI)** ⇒ Do
  - **Entregar e Suportar (DS)** ⇒ Check
  - **Monitorar e Avaliar (ME)** ⇒ Act
- As 34 áreas de processos estão distribuídas entre os 4 domínios, obedecendo à filosofia de melhoria contínua.

Domínios o Ciclo PDCA II

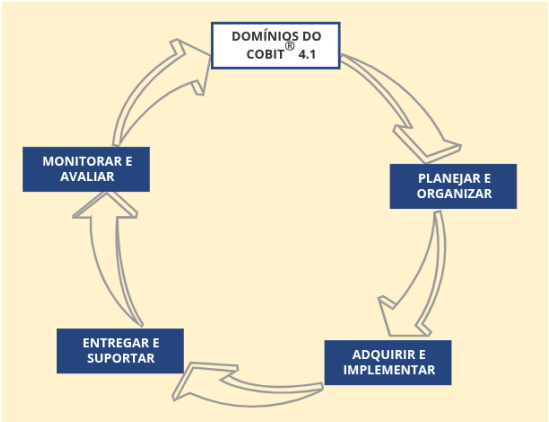


Figure: Os cinco domínios do COBIT 4.1

Domínios o Ciclo PDCA III

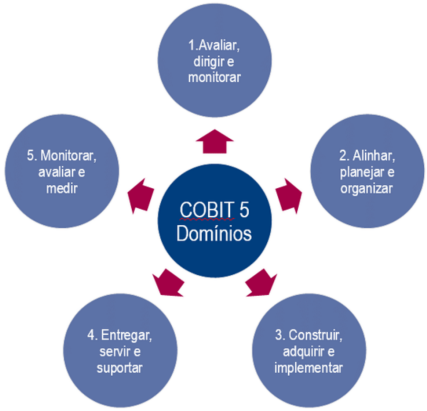


Figure: Os cinco domínios do COBIT 5.

Domínios o Ciclo PDCA IV

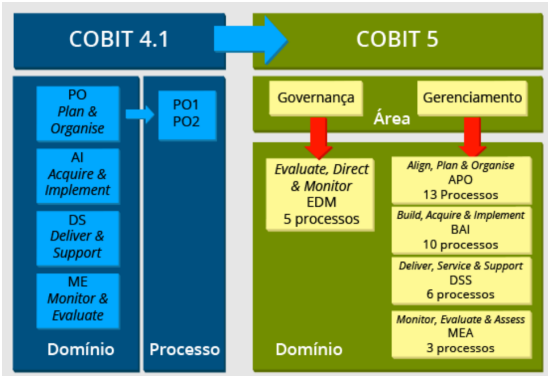


Figure: 4 domínios e 5 domínios.

Domínio 1 – Planejar e Organizar (PO) I

O domínio **Planejar e Organizar** estabelece a base estratégica da governança de TI.

- Definir plano estratégico e arquitetura da informação;
- Determinar posição tecnológica e processos de TI;
- Gerenciar investimentos e recursos humanos de TI;
- Comunicar objetivos e diretrizes de gestão;
- Avaliar riscos e garantir a qualidade;
- Gerenciar projetos e processos de melhoria contínua.

Nota:

O foco do domínio PO é alinhar a estratégia de TI com as metas de negócio e assegurar que a organização possua direção e políticas claras.

Domínio 2 – Adquirir e Implementar (AI) I

O domínio **Adquirir e Implementar** trata da transformação do planejamento em soluções e sistemas práticos.

- Identificar soluções automatizadas e comprar recursos de TI;
- Adquirir e manter infraestrutura e software;
- Gerenciar mudanças e homologar implementações;
- Habilitar a operação de uso e assegurar integração.

Nota:

Este domínio garante que os novos sistemas e processos sejam entregues com qualidade, segurança e alinhamento aos requisitos definidos em PO.

Domínio 3 – Entregar e Suportar (DS) I

O domínio **Entregar e Suportar** foca na entrega dos serviços e no suporte às operações de TI.

- Definir e gerenciar níveis de serviço;
- Garantir continuidade e segurança;
- Gerenciar central de serviços, incidentes e problemas;
- Controlar desempenho, capacidade e custos;
- Treinar usuários e administrar ambiente físico e lógico.

Nota:

O DS é o domínio mais operacional do COBIT, assegurando a continuidade e qualidade dos serviços prestados pela TI.

Domínio 4 – Monitorar e Avaliar (ME) I

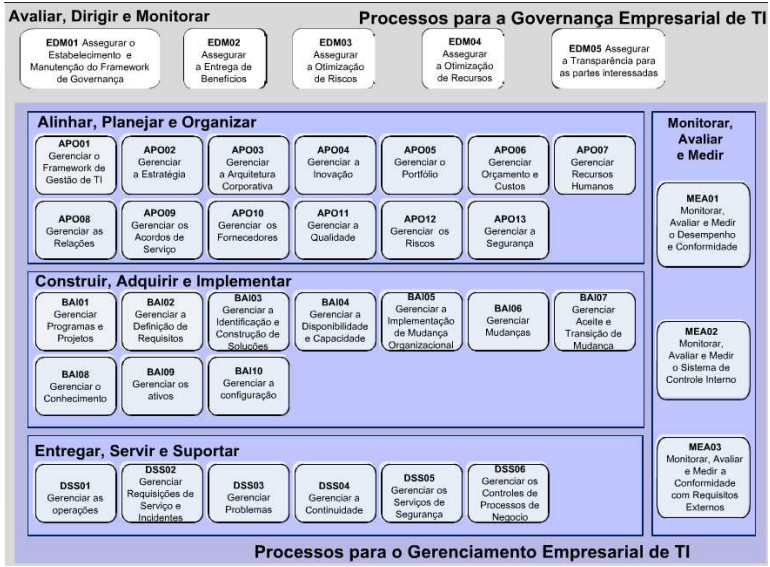
O domínio **Monitorar e Avaliar** estabelece mecanismos para mensuração e conformidade.

- Monitorar desempenho e controles internos;
- Assegurar conformidade com requisitos externos (leis, normas e políticas);
- Avaliar governança e promover auditorias de TI;
- Fornecer relatórios de acompanhamento e melhoria contínua.

Nota:

O ME garante que toda a operação de TI seja mensurável, auditável e em conformidade com padrões internos e externos.

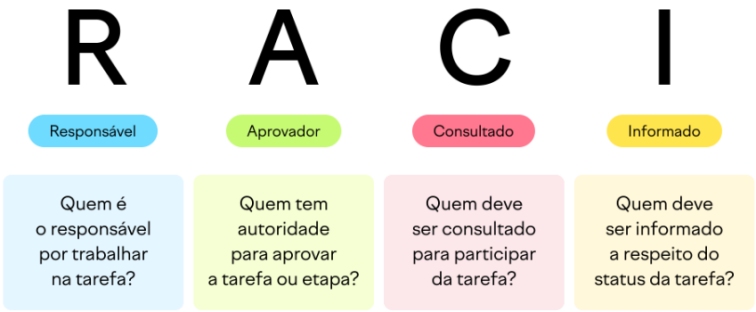
Resumo I


Avaliar, Dirigir e Monitorar
Processos para a Governança Empresarial de TI
EDM01 Assegurar o Estabelecimento e Manutenção do Framework de Governança
EDM02 Assegurar a Entrega de Benefícios
EDM03 Assegurar a Otimização de Riscos
EDM04 Assegurar a Otimização de Recursos
EDM05 Assegurar a Transparência para as partes interessadas
Alinhar, Planejar e Organizar
APO01 Gerenciar o Framework de Gestão de TI
APO02 Gerenciar a Estratégia
APO03 Gerenciar a Arquitetura Corporativa
APO04 Gerenciar a Inovação
APO05 Gerenciar o Portfólio
APO06 Gerenciar Orçamento e Custos
APO07 Gerenciar Recursos Humanos
APO08 Gerenciar as Relações
APO09 Gerenciar os Acordos de Serviço
APO10 Gerenciar os Fornecedores
APO11 Gerenciar a Qualidade
APO12 Gerenciar os Riscos
APO13 Gerenciar a Segurança
Construir, Adquirir e Implementar
BAI01 Gerenciar Programas e Projetos
BAI02 Gerenciar a Definição de Requisitos
BAI03 Gerenciar a Identificação e Construção de Soluções
BAI04 Gerenciar a Disponibilidade e Capacidade
BAI05 Gerenciar a Implementação de Mudança Organizacional
BAI06 Gerenciar Mudanças
BAI07 Gerenciar Aceite e Transição de Mudança
BAI08 Gerenciar o Conhecimento
BAI09 Gerenciar os ativos
BAI10 Gerenciar a configuração
Entregar, Servir e Suportar
DSS01 Gerenciar as operações
DSS02 Gerenciar Requisições de Serviço e Incidentes
DSS03 Gerenciar Problemas
DSS04 Gerenciar a Continuidade
DSS05 Gerenciar os Serviços de Segurança
DSS06 Gerenciar os Controles de Processos de Negocio
Monitorar, Avaliar e Medir
MEA01 Monitorar, Avaliar e Medir o Desempenho e Conformidade
MEA02 Monitorar, Avaliar e Medir o Sistema de Controle Interno
MEA03 Monitorar, Avaliar e Medir a Conformidade com Requisitos Externos
Processos para o Gerenciamento Empresarial de TI

Modelo de Maturidade e Matriz RACI I

O COBIT define instrumentos para mensuração e responsabilidade:

- **Modelo de Maturidade** – mede o grau de eficiência da organização em cada domínio;
- **Matriz RACI** – define papéis: Responsável, Aprovador, Consultado e Informado.



AIHR RACI Matrix

Task / Stakeholders	Project Lead Anne	Internal Recruiter John	Hiring Manager Natasha	Stakeholder 4: Steven	Stakeholder 5: Sarah	Stakeholder 8: Allison
Task 1: Defining the job role	A	A	R	I	R	A
Task 2: Creating a requisition	A	R	I	C	I	A
Task 3: Writing the job ad	C	A	C	A	C	C
Task 4: Posting the job ad	C	R	I	R	I	C
Task 5: Promote the position on the company channels	C	A	I	R	I	C
Task 6: Advertise the position internally	I	A	R	C	R	I
Task 7: Review applications	A	I	R	I	R	A
Task 8: Candidate screening	C	I	C	I	C	C

RACI

R - Responsible
The people who take action to get the task done. They are responsible for the work or making the decision. You can have more than one person responsible for a task, but to make the decision-making process effective, try having one person responsible for a single task.

A - Accountable
The person who owns the task or deliverable. They might not get the work done themselves, but they are responsible for making sure it is finalized. To avoid confusion and the diffusion of responsibility, it's better to have one accountable person per project task.

C - Consulted
The person, role, or group who will help complete the task. They will have two-way communication with the people responsible for the task by providing input and feedback over the task completion.

I - Informed
The people, roles, or groups that need to be up to date on the task's progress. They will not have two-way communication, but it's essential to keep them informed since they will be affected by the final outcome of the task/project.

Figure: Exemplo de Matriz RACI.

Modelo de Maturidade e Matriz RACI III

Atividades	Diretor	Gerente	Analista 1	Analista 2	Técnico 1	Técnico 2
Tarefa 1	Autoridade	Aprovador	Consultor	Responsável	Responsável	Responsável
Tarefa 2	Autoridade	Aprovador	Responsável	-	Responsável	Responsável
Tarefa 3	Consultor	Aprovador	Responsável	Responsável	Responsável	Responsável
Tarefa 4	Aprovador	Responsável	-	Consultor	Responsável	Responsável

CMM – Modelo de Maturidade I

- O CMM (*Capability Maturity Model*) avalia a **maturidade dos processos** de uma organização.
- Cada nível representa um estágio de evolução e melhoria contínua:
  1. **Nível 1 – Inicial:** Processos ad hoc e caóticos, dependentes de esforço individual.
  2. **Nível 2 – Repetível:** Processos básicos documentados, projetos semelhantes podem ser repetidos.
  3. **Nível 3 – Definido:** Processos padronizados e documentados em toda a organização.
  4. **Nível 4 – Gerenciado:** Processos medidos e controlados, com métricas de desempenho.
  5. **Nível 5 – Otimização:** Processos em melhoria contínua, com foco em inovação e eficiência.

CMM – Modelo de Maturidade II

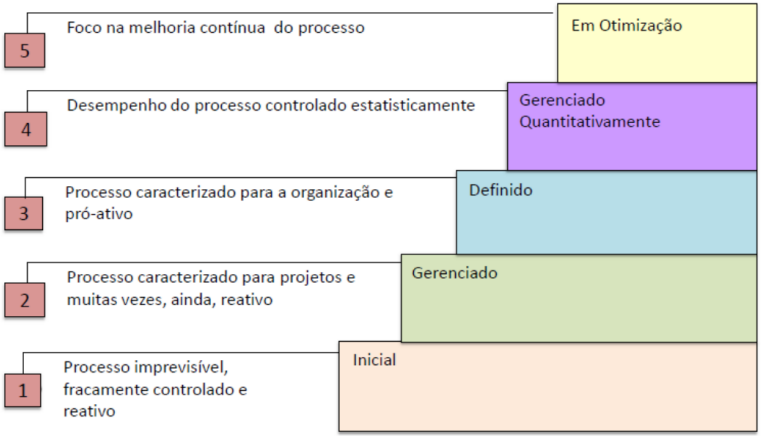


Figure: Exemplo de Matriz RACI no COBIT.

COBIT vs ISO 27000

- **COBIT:** Ajuda a organizar e monitorar os controles de TI, incluindo segurança, dentro de uma estrutura de governança.
- **ISO 27000:** Fornece normas detalhadas de segurança da informação, que podem ser implementadas dentro dos processos do COBIT.
- Portanto,
  - COBIT diz: como gerenciar TI de forma segura e eficiente.
  - ISO 27000 diz: como proteger a informação.

Bibliografia

Bibliografia Básica I

ISACA. **COBIT 4.1: Control Objectives for Information and Related Technology**. Rolling Meadows, IL, USA: Information Systems Audit and Control Association, 2007. Framework for IT governance and management. ISBN 978-1-60420-002-1. Available from: `https://www.isaca.org/resources/cobit`.

ISACA. **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT**. Rolling Meadows, IL, USA: Information Systems Audit and Control Association, 2012. Framework integrating IT governance, management and business alignment. ISBN 978-1-60420-237-7. Available from: `https://www.isaca.org/resources/cobit`.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary**. [*S. l.: s. n.*], 2018. Norma ISO, fornece visão geral e vocabulário de SGSI.

Bibliografia Básica II

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements**. [*S. l.: s. n.*], 2022. Norma certificável, define requisitos para implementar SGSI.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls**. [*S. l.: s. n.*], 2022. Diretrizes práticas para implementação de controles de segurança.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27003: Information technology – Security techniques – Information security management system implementation guidance**. [*S. l.: s. n.*], 2017. Guia de implementação do SGSI.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27004: Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation**. [*S. l.: s. n.*], 2020. Métricas e monitoramento da eficácia do SGSI.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27005: Information technology – Security techniques – Information security risk management**. [*S. l.: s. n.*], 2018. Gestão de riscos de segurança da informação.

Estes slides estão protegidos por uma licença Creative Commons

Figure: *

Este modelo foi adaptado de Maxime Chupin.

Marisangila Alves, MSc
marisangila.alves@gmail.com

UDESC
Universidade do Estado de Santa Catarina

Segurança da Informação
Normas