Disciplina: Governança em Tecnologia da Informação

Aula 3: Governança de TI

Apresentação

Com a velocidade do desenvolvimento de novas tecnologias, da globalização, de novos hábitos tecnológicos, pessoais e organizacionais, da necessidade de vantagem competitiva e da sustentabilidade das organizações, a TI ganha destaque e vira ferramenta fundamental para alavancar os negócios das organizações.

Nesse contexto, devemos considerar que os investimentos realizados pelas organizações com a área de tecnologia podem representar uma proporção significativa dos recursos financeiros e humanos, e, para isso, as empresas necessitam de métodos e ferramentas que possam orientar suas decisões e o caminho a ser seguido em consonância com as necessidades de negócio.

Nesta aula, analisaremos duas ferramentas importantes para a implementação da boa governança: A ISO 38500 e o COBIT. Compreenderemos os modelos de governança de TI apresentado e suas principais diferenças.

Bons estudos!

Objetivos

- Explicar o modelo de governança de TI da ISO 38500;
- Analisar o modelo de governança de TI do COBIT.

Norma ISO/IEC 38500

O objetivo da norma ISO 38500 é estabelecer um vocabulário comum, definições e princípios para a Governança de TI, além de oferecer um modelo de estrutura de governança para que as organizações possam avaliar, direcionar e monitorar o uso da tecnologia da informação.

Como as organizações devem proceder?

Cada organização deverá identificar as ações necessárias para a implementação desses princípios considerando a sua natureza, os riscos e as oportunidades para a utilização da TI. Assim, a norma ISO 38500 pode ser aplicada a qualquer organização e de qualquer porte: pública, privada ou organizações sem fins lucrativos.

Como já falamos nas aulas anteriores, atualmente, a TI é uma ferramenta fundamental para alavancar os negócios da organização e, nesse sentido, as despesas com a TI podem representar uma proporção significativa dos recursos financeiros e humanos da empresa. Desse modo, será essencial que a organização utilize um método para orientar suas decisões e o caminho a seguir.

O modelo de governança de TI

A norma 31800 propõe um modelo de Governança de TI em que as organizações sejam governadas por meio de três principais tarefas:

Garantia do uso eficaz da TI e do atendimento aos objetivos de negócio da organização, por meio da implementação de **estratégias e políticas**.

Monitoramento da **conformidade** das **políticas estabelecidas** e do **desempenho** em relação as **estratégias implementadas**.

Avaliação do uso atual e futuro da TI.

Um ponto destacado pela norma é quanto à delegação de responsabilidades. Ela deixa claro que a responsabilidade pelo uso efetivo, eficiente e aceitável da TI é da estrutura de governança e não pode ser delegada. No entanto, a responsabilidade pelos aspectos específicos de TI pode ser delegada aos gerentes da organização.

O modelo proposto está baseado em três pilares:

Vamos conhecê-los com mais detalhe:

Clique nos botões para ver as informações.

Avaliar

As organizações devem continuamente examinar e avaliar o uso atual e futuro da Tecnologia da Informação, considerando as pressões internas e externas que atuam sobre a empresa, como mudanças tecnológicas, tendências econômicas e sociais, obrigações regulatórias, de forma a atender os objetivos atuais e futuros da organização, assim como a manutenção da vantagem competitiva.

Dirigir

Trata do estabelecimento de responsabilidades e da implementação de estratégias e políticas de TI, e de uma cultura de governança. As estratégias devem estabelecer a direção a ser seguida e a as políticas devem orientar quanto aos investimentos, objetivos e comportamentos para utilização da TI.

Monitorar

Trata da medição do desempenho da TI, que deve estar de acordo com as estratégias estabelecidas, em atendimento aos objetivos de negócio e em conformidade com as obrigações externas (regulatórias, legislativas e contratuais) e as práticas internas da organização.

Atividade

1 - A norma ISO 31800 propõe um modelo de governança de TI baseado em três pilares: avaliar, dirigir e monitorar. Analise as questões a seguir e correlacione as colunas com as definições de cada um dos pilares:

Avaliar 1 | Dirigir 2 | Monitorar 3

a) Trata da medição do desempenho da TI e que esteja de acordo com as estratégias estabelecidas, os objetivos de negócio e em conformidade com as obrigações externas e internas da organização.

1 2 3

b) As organizações devem continuamente examinar e avaliar o uso atual e futuro da Tecnologia da Informação, considerando as pressões internas e externas que atuam sobre a organização.

1 2 3

c) Trata do estabelecimento de responsabilidades e implementação de estratégias e políticas de TI e ainda de uma cultura de governança.

1 2 3

Gabarito

Princípios da governança de TI

Na implementação da boa governança, a norma ISO 38500 define seis princípios para o uso efetivo, eficiente e aceitável de TI e que devem ser seguidos pelas organizações:

1

Responsabilidade

2

Estratégia

3

Aquisição

1

Desempenho

2

Conformidade

3

Comportamento Humano

Cada princípio trata de uma área específica e tem uma relação direta com os pilares do modelo de governança proposto pela norma:

Princípio da **responsabilidade**

Trata do conhecimento e da conscientização por parte dos indivíduos e grupos da organização de suas responsabilidades em relação ao fornecimento e demanda de TI.

Nas relações com os pilares:

Avaliar

A estrutura de governança deve avaliar a competência dos responsáveis pelas tomadas de decisões de TI e as atribuições das responsabilidades em relação ao uso atual e futuro da TI.

Dirigir

A estrutura de governança deve orientar que a área de TI preste contas e siga as estratégias já pela organização.

Monitorar

A estrutura de governança deve monitorar o desempenho das pessoas responsáveis pela governança de TI e também se os mecanismos apropriados de governança estão estabelecidos.

Princípio da **Estratégia**

Trata de como a estratégia da organização considera as capacidades de TI atuais e futuras da organização.

Nas relações com os pilares:

Avaliar

As organizações devem avaliar e garantir que o uso da TI e das atividades de TI estejam alinhadas com os objetivos organizacionais e baseados em boas práticas. Devem, ainda, avaliar a evolução dos processos de TI e de negócios de forma a garantir que atendam as necessidades futuras da organização.

Dirigir

As organizações devem garantir a definição de estratégias e políticas de forma que as organizações se beneficiem com a utilização da TI, além de fomentar a prospecção e inovação da utilização da tecnologia de forma a melhorar seus processos ou atender a novos desafios.

Monitorar

As organizações devem monitorar a implementação das propostas e o uso da TI, de forma a garantir que atendam aos objetivos propostos.

Princípio da **Aquisição**

Trata das aquisições de TI e do equilíbrio adequado entre benefícios, oportunidades, custos e riscos, em curto e longo prazo. As aquisições devem ser realizadas baseadas em análise apropriadas.

Nas relações com os pilares:

Avaliar

A estrutura de governança deve avaliar as opções tecnológicas, considerando a relação custo-benefício, de forma a atender as propostas já aprovadas.

Dirigir

A estrutura de governança da organização deve garantir que os ativos de TI sejam adquiridos dentro da capacidade necessária aos negócios das organizações.

Monitorar

A ideia é um olhar sobre os investimentos realizados em TI, de forma a garantir que forneçam as capacidades necessárias.

Princípio do **Desempenho**

Trata da adequação dos serviços fornecidos pela TI, os níveis de serviço e a qualidade destes serviços de forma a atender aos requisitos atuais e futuros da organização.

Nas relações com os pilares:

Avaliar

A estrutura de governança deve avaliar os planos de TI de forma a garantir que os processos de negócio sejam realmente apoiados pela TI, considerando a continuidade de negócio e os riscos de TI envolvidos.

Dirigir

As estruturas de governança da organização devem garantir que os recursos de TI sejam suficientes para garantir que a necessidade da organização seja atendida.

Monitorar

A estrutura de governança deve monitorar se os recursos e orçamentos utilizados pela área de TI são suficientes e foram priorizados de acordo com os objetivos de negócio da organização e se as políticas de TI são seguidas adequadamente.

Princípio da **Conformidade**

Trata do atendimento do uso da TI às leis e aos regulamentos obrigatórios.

Nas relações com os pilares:

Avaliar

A estrutura de governança deve avaliar se a TI está atendendo as regulamentações (legislativas e contratuais), políticas e normas internas.

Dirigir

Deve garantir que sejam estabelecidos mecanismos regulares para garantir que a utilização da TI atenda as regulamentações externas e norma internas da organização, assim como deve ter preocupação com o comportamento e desenvolvimento profissional dos profissionais da TI e seu comportamento ético.

Monitorar

Deve garantir a satisfação da organização em relação a TI e sua conformidade através da relatórios e práticas de auditorias.

Princípio do **Comportamento humano**

Trata de como as políticas, práticas e decisões de TI demonstram respeito pelo comportamento humano.

Nas relações com os pilares:

Avaliar

A estrutura de governança deve garantir que os comportamentos humanos das atividades de TI sejam identificados e considerados.

Dirigir

Deve garantir que os riscos, oportunidades e problemas possam ser identificados e relatados por qualquer pessoa e tratados a qualquer momento pelos decisores responsáveis.

Monitorar

Deve monitorar as práticas de trabalho da TI de forma a garantir que sejam condizentes com o seu uso adequado.

Atenção! Aqui existe uma videoaula, acesso pelo conteúdo online

Atividade

2 - Na implementação da boa governança, a norma ISO 38500 define seis princípios para o uso efetivo, eficiente e aceitável de TI e que devem ser seguidos pelas organizações. Cada princípio trata de uma área específica e tem uma relação direta com os pilares do modelo de governança proposto pela norma.

Avalie o pilar a seguir e marque o princípio a que ele corresponde: “Com o pilar avaliar, a estrutura de governança deve avaliar se a TI está atendendo as regulamentações (legislativas e contratuais), políticas e normas internas.”

a) Responsabilidade
b) Estratégia
c) Aquisição
d) Desempenho
e) Conformidade

Cobit

O Cobit (Control Objectives for Information and related Technology) fornece um modelo que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI.

As organizações criam valor por meio da TI, considerando os benefícios, os riscos e os recursos utilizados. Pela norma ISO 38500, o Cobit pode ser aplicado a qualquer organização, de qualquer porte, pública, privada ou organizações sem fins lucrativos.

Ele foi criado em 1994, pela ISACF28[1] , a partir do seu conjunto inicial de objetivos de controle e vem, desde então, evoluindo com a incorporação de padrões internacionais técnicos, profissionais, regulatórios e específicos para processos de TI.

Princípios do Cobit

O Cobit baseia-se em cinco princípios para a implementação da boa governança e gestão de TI nas organizações:

Vamos conhecer cada princípio com mais detalhe a seguir.

1º Princípio: Atender a necessidades das partes interessadas

Consiste no atendimento das partes interessadas, por meio da criação de valor como um objetivo de governança, considerando a otimização do risco e avaliando a relação de custo-benefício.

Esse princípio baseia-se no processo:

Objetivos da Governança: Criação de Valor

Nesse processo, a governança negocia sobre a avaliação dos recursos, benefícios e riscos, e decide entre interesses de valor das diferentes partes interessadas. Desse modo, as necessidades das partes interessadas devem ser transformadas em uma estratégia exequível pela organização.

Em relação às necessidades das partes interessadas, temos:

Saiba mais

Para saber mais sobre esse assunto, leia o texto "Necessidades das partes interessadas <galeria/aula3/docs/necessidades.pdf> ".

2º Princípio: Cobrir a organização de ponta a ponta

No modelo ofertado pelo Cobit, a governança de TI é integrada à governança corporativa, e a governança e a gestão da informação e da tecnologia são abordadas sob a ótica de toda a organização. Desse modo, ele abrange todas as funções e processos necessários para regular e controlar as informações da organização e tecnologias de TI onde quer que essas informações possam ser processadas.

Esse princípio baseia-se no processo:

Objetivos da Governança: Criação de Valor

Nesse processo, as organizações podem definir diferentes visões para a aplicação da governança. Lá, poderá ser aplicada a toda a organização, uma entidade, um ativo tangível ou intangível. Por isso, será essencial que a organização defina bem o **escopo de governança**.

É importante também a definição de quem está envolvido na governança, como estão envolvidos, o que fazem e como interagem dentro do escopo de governança definido. Desse modo, é essencial a definição clara de **funções, atividades e relacionamento**:

3º princípio: Aplicar um modelo único integrado

O Cobit pode ser utilizado como o principal integrador do modelo de governança e gestão, considerando que ele consegue se alinhar com eficiência a outros padrões, modelos e práticas, permitindo a construção de uma arquitetura robusta de governança com uma linguagem comum, não técnica, agnóstico-tecnológica.

No desenvolvimento do Cobit foi considerada uma série de padrões e modelos de referência, amplamente utilizados e amadurecidos.

Saiba mais

Leia o artigo “As vantagens de um negócio agnóstico <//blogs.pme.estadao.com.br/blog-do-empreendedor/as-vantagens-de-um-negocio-agnostico/> ”.

4º Princípio: Permitir uma abordagem holística

O COBIT descreve sete categorias de habilitadores que podem influenciar se algo irá funcionar ou não dentro do modelo proposto:

Para que possam ter sucesso na implementação da boa governança e atingir os principais objetivos corporativos, é importante que esses habilitadores trabalhem de forma interligada, pois:

1

Os **princípios**, as **políticas** e os **modelos** orientam de forma prática o comportamento desejado na gestão diária.

2

Os **processos** descrevem de forma organizada as práticas e atividades para que a organização possa atingir o objetivo desejado.

3

As **estruturas organizacionais** permitem a tomada de decisão na organização.

Alguns desses habilitadores também são recursos da organização e, desse modo, devem ser gerenciados:

A **informação**, que perpassa por toda a organização.

Os **serviços de infraestrutura e aplicativos**.

As **pessoas, habilidades e competências**.

Cada habilitador descrito é desdobrado em quatro dimensões:

Vamos conhecer cada dimensão com mais detalhe:

Clique nos botões para ver as informações.

Ciclo de vida

Cada habilitador tem um ciclo de vida que apresenta as seguintes fases:

- Planejar
- Projetar
- Desenvolver
- Usar/operar
- Avaliar/monitorar
- Atualizar/descartar

Boas práticas

As boas práticas apoiam o atingimento das metas de cada habilitador. Elas sugerem formas de como implementar o habilitador da melhor forma possível, seus possíveis produtos, entradas e saídas.

Partes interessadas

Cada habilitador tem partes interessadas que podem ser internas à organização ou externas e todas possuem seus próprios interesses e necessidades.

Metas

Cada habilitador tem diversas metas e, ao atingir suas metas, criam valor para a organização. Estas metas podem ser: **resultados esperados** ou **aplicativo** ou **operação do próprio habilitador**.

Como sabemos se nossos resultados são positivos ou não?

Segundo o Cobit, as seguintes perguntas devem ser respondidas para que possamos controlar o desempenho dos habilitadores:

As necessidades das partes interessadas foram consideradas?

As metas do habilitador foram atingidas?

O ciclo da vida do habilitador é controlado?

Boas práticas foram aplicadas?

5º Princípio: Distinguir a governança da gestão

O Cobit faz distinção entre a governança e gestão, já que essas disciplinas possuem atividades diferentes e requerem estruturas organizacionais distintas:

Governança

Garante que as necessidades das partes interessadas sejam desdobradas em objetivos corporativos acordados e priorizados, monitorando o desempenho e a conformidade com os objetivos estabelecidos.

Gestão

Responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com os objetivos corporativos já definidos.

No Cobit não existe uma forma rígida para a implementação dos dois conceitos. As organizações podem decidir e organizar seus processos de governança e gestão da forma que julgarem melhor, de modo que todos os objetivos de governança e gestão sejam cobertos.

Para auxiliar as organizações na implementação, o Cobit apresenta um modelo de referência dividido em dois domínios de processos principais, governança e gestão. O domínio de **governança** possui cinco processos e o domínio de **gestão** é dividido em quatro domínios e subdivididos em 32 processos:

Atenção! Aqui existe uma videoaula, acesso pelo conteúdo online

Observe que:

Clique nos botões para ver as informações.

Alinhar, Planejar e Organizar (APO)

Tem abrangência estratégica e tática. Envolve planejamento, comunicação e gerenciamento. Identifica como a TI pode melhorar os objetivos de negócio.

Construir, Adquirir e Implementar (BAI)

Trata do desenvolvimento e/ou aquisição de soluções de TI para executar a estratégia de TI estabelecida, assim como a implementação e integração junto aos processos de negócio.

Entregar, Reparar e Suportar (DSS)

Trata da entrega propriamente dita dos serviços requeridos, incluindo gerenciamento de segurança e continuidade, reparo de equipamentos e demais itens relacionados, suporte aos serviços para os usuários, gestão dos dados e da infraestrutura operacional.

Monitorar, Avaliar e Medir (MEA)

Trata da qualidade dos processos de TI e sua governança e também da conformidade com os objetivos de controle internos ou externos à organização.

Saiba mais

Para saber mais sobre esse assunto, leia o texto “Processos de TI <galeria/aula3/docs/processos.pdf> ”.

Modelo de capacidade de processo

Atenção! Aqui existe uma videoaula, acesso pelo conteúdo online

O Cobit, em sua versão 5, apresenta um modelo de capacidade de processo baseado na ISO 15504 e reconhecido internacionalmente. Ele oferece às organizações meios de medir o desempenho de qualquer um dos processos de governança ou gestão e, desse modo, permitirá identificar as áreas que precisam sem melhoradas. Neste modelo, um processo pode atingir até seis níveis de capacidade:

Nível 0

O processo não foi implementado ou não atingiu seu objetivo. Não existem evidências.

Nível 1

O processo atinge seu objetivo, pelo menos um atributo do processo.

Nível 2

O processo é implementado de forma administrativa, isto é, planejado, monitorado e ajustado.

Nível 3

O processo é implementado utilizando um processo definido capaz de atingir resultados.

Nível 4

O processo é implementado utilizando um processo definido capaz de atingir resultados dentro dos limites definidos.

Nível 5

O processo é continuamente melhorado com o objetivo de atingir os objetivos corporativos atuais ou previstos.

Atividade

3 - O Cobit apresenta um modelo de referência dividido em dois domínios de processos principais, governança e gestão. O domínio de **gestão** possui quatro domínios, listados a seguir. Faça a correlação entre as colunas:

Alinhar, Planejar e Organizar (APO) 1

Construir, Adquirir e Implementar (BAI) 2

Entregar, Reparar e Suportar (DSS) 3

Monitorar, Avaliar e Medir (MEA) 4

a) Trata do desenvolvimento e/ou aquisição de soluções de TI para executar a estratégia de TI estabelecida, assim como a implementação e integração junto aos processos de negócio.

1 2 3 4

b) Trata da qualidade dos processos de TI e sua governança e também da conformidade com os objetivos de controle sejam internos ou externos à organização.

1 2 3 4

c) Tem abrangência estratégica e tática. Envolve planejamento, comunicação e gerenciamento. Identifica como a TI pode melhorar os objetivos de negócio.

1 2 3 4

d) Trata da entrega propriamente dita dos serviços requeridos, incluindo gerenciamento de segurança e continuidade, reparo de equipamentos e demais itens relacionados, suporte aos serviços para os usuários, gestão dos dados e da infraestrutura operacional.

1 2 3 4

Gabarito

4 - O Cobit, em sua versão 5, apresenta um modelo de capacidade de processo, de modo a permitir que as organizações possam medir o desempenho de qualquer um dos processos de governança ou gestão. Qual o nível de capacidade em que o processo é implementado utilizando um processo definido capaz de atingir resultados dentro dos limites definidos?

a) Nível 1 - Processo executado
b) Nível 2 – Processo gerenciado
c) Nível 3 – Processo estabelecido
d) Nível 4 – Processo previsível
e) Nível 5 – Processo otimizado

Notas

ISACF28 [1]

Information Systems Audit and Control Foundation, ligado à ISACA — Information Systems Audit and Control Association.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 38500:2018. São Paulo: ABNT, 2018.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI:** da Estratégia à Gestão dos Processos e Serviços. 4. ed. Rio de Janeiro: Brasport, 2014.

ISACA. Cobit 5 - Modelo Corporativo para a Governança e gestão de TI da Organização. Ilinois, Estados Unidos: ISACA, 2012.

Próxima aula

- Conceitos e princípios do TOGAF;
- Visão geral de análise de negócios a partir do Guia para o Corpo de Conhecimento de Análise de Negócios (BABOK);
- Visão geral do gerenciamento de processos de negócio a partir do Guia para o Gerenciamento de Processos de Negócio - Corpo Comum de Conhecimento (BPM CBOK).

Explore mais

Assista ao vídeo:

- Balanced Score Card (BSC) <https://www.youtube.com/watch?v=R9Y3R4tuKzc> ;