
Governança em TI

SUMÁRIO

INTRODUÇÃO

A governança em TI é um conjunto de práticas, políticas e processos que visam garantir que a TI seja usada de forma eficaz e eficiente para apoiar os objetivos estratégicos do negócio. Ela é responsável por garantir a segurança, a eficiência e a eficácia da TI, além de aumentar a sua contribuição para o sucesso da empresa. Governança em TI é importante para empresas de todos os tamanhos e setores. Ela ajuda a garantir que a TI seja usada de forma responsável e ética, e que esteja alinhada com as leis e regulamentos aplicáveis. Além disso, a governança em TI pode ajudar a empresa a reduzir custos, melhorar a produtividade e aumentar a satisfação dos clientes.

Família ISO/IEC 27000

Definições e conceitos: ISO / IEC 27000 é uma norma interessante sobretudo para iniciantes na gestão da segurança da informação. Inclui um glossário de termos que ajuda, inclusive, a quem está se preparando para uma certificação profissional Fundação ISO 27002. Esta norma, define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI). O SGSI é descrito como parte do sistema de gestão global da organização, com base em uma abordagem de risco do negócio, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. O SGSI inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos. A publicação é muito conhecida entre estudantes de concursos de TI.

Como obter a certificação ISO 27000 ?

A certificação ISO 27000 comprova que a empresa segue os padrões internacionais de segurança da informação. Ela é emitida por uma empresa auditora externa, que precisa seguir as regras da ISO 27006. Esta norma trata especificamente dos auditores que certificam as organizações que implementaram um SGSI. A certificação é feita em dois estágios: A auditoria faz uma análise preliminar e informal do SGSI da empresa. É verificado se existe a documentação chave, como a Política de Segurança da Informação, a Declaração de Aplicabilidade e o Plano de Tratamento de Risco. A auditoria faz uma análise aprofundada sobre a efetividade do controle ISMS, conforme os documentos chave apresentados pela organização. A certificação ISO 27000 precisa ser renovada após a primeira emissão, por meio de revisões periódicas e novas declarações da organização que comprovem o respeito às normas e boas práticas no SGSI.

Dominios e componentes da governança em TI

A Governança de TI compreende vários mecanismos e componentes que, logicamente integrados, permitem o desdobramento da estratégia de TI até a operação dos produtos e serviços correlatados.Dentre esses componentes, temos: etapa de alinhamento estratégico e compliance; etapa de decisão, compromisso, priorização e alocação de recursos; etapa de processo, operação e gestão; etapa de medição de desempenho.

A Lei Sarbanes-Oxley (SOX) é uma lei federal dos Estados Unidos aprovada em 2002 em resposta a escândalos financeiros, como o caso Enron.
A lei visa aumentar a transparência e a responsabilização das empresas públicas e dos seus auditores.

Importância
A Lei SOX é importante porque visa proteger os investidores e o público em geral contra fraudes financeiras. A lei exige que as empresas públicas tenham controles internos robustos para proteger seus ativos e dados financeiros. A lei também exige que as empresas publiquem relatórios financeiros auditados e que os auditores sejam independentes e imparciais.

Exemplos Alguns exemplos de controles internos exigidos pela Lei SOX incluem:
Controles de acesso a dados: para proteger os dados financeiros contra acesso não autorizado.
Separação de funções: para evitar que uma única pessoa tenha controle sobre todas as etapas de um processo financeiro.

Revisão independente: para verificar a eficácia dos controles internos.

Conceitos Alguns conceitos importantes relacionados à Lei SOX incluem:

Auditoria interna: é a função independente responsável por avaliar a eficácia dos controles internos da empresa.

Auditoria externa: é a função responsável por auditar os relatórios financeiros da empresa. **Comissões de auditoria:** são responsáveis por supervisionar o processo de auditoria da empresa.

Modelos práticos Existem vários modelos práticos para implementação da Lei SOX.

Um modelo comum é o modelo COSO, que define cinco componentes essenciais de um sistema de controle interno eficaz:

Ambiente de controle: define a cultura e os valores da organização.

Avaliação de riscos: identifica e avalia os riscos aos quais a organização está exposta.

Atividades de controle: são as políticas e procedimentos que são implementados para mitigar

os riscos identificados.

Informação e comunicação: garante que as informações relevantes estejam disponíveis para as pessoas certas na hora certa.

Monitoramento: avalia a eficácia dos controles internos.

A implementação da Lei SOX pode ser um processo complexo e desafiador. No entanto, é importante para as empresas públicas cumprirem a lei para proteger seus investidores e o público em geral.

Gestão de Portfólio de Projetos em TI

A gestão de portfólio de projetos é responsável por identificar, priorizar e gerenciar um conjunto de projetos de TI. Ela ajuda a organização a garantir que os projetos estejam alinhados com os objetivos estratégicos e que sejam executados de forma coordenada. A gestão de projetos é responsável por planejar, executar, monitorar e controlar um único projeto de TI. Ela ajuda a garantir que o projeto seja concluído no prazo, dentro do orçamento e com a qualidade esperada.

A gestão de portfólio e projetos desempenha um papel fundamental na governança de TI. Ela ajuda a organização a:

Alinhar os projetos de TI com os objetivos estratégicos da organização.

Garantir que os projetos de TI sejam executados de forma eficiente e eficaz.

Reduzir o risco de projetos de TI falharem.

Melhorar o retorno sobre o investimento em TI.

A gestão de portfólio e projetos pode ser realizada por uma equipe de profissionais de TI ou por uma empresa de consultoria especial

Alguns benefícios específicos da gestão de portfólio e projetos para a governança de TI:

Melhoria do alinhamento estratégico: a gestão de portfólio ajuda a garantir que os projetos de TI estejam alinhados com os objetivos estratégicos da organização. Isso pode ajudar a organização a alcançar seus objetivos de negócios mais rapidamente e com mais eficiência.

Redução de riscos: a gestão de portfólio ajuda a identificar e mitigar os riscos associados aos projetos de TI. Isso pode ajudar a organização a evitar perdas financeiras e danos à sua reputação.

Melhoria da eficiência: a gestão de portfólio ajuda a organizar e coordenar os projetos de TI. Isso pode ajudar a organização a economizar tempo e dinheiro.

Melhoria da transparência: a gestão de portfólio ajuda a melhorar a visibilidade dos projetos de TI. Isso pode ajudar a organização a tomar decisões mais informadas sobre seus investimentos em TI.

PMBOK

O Guia PMBOK é um padrão global para gerenciamento de projetos. Ele fornece um conjunto de conhecimentos, práticas e terminologia comuns para o gerenciamento de projetos. O Guia PMBOK é desenvolvido e mantido pelo Project Management Institute (PMI), uma organização profissional que representa profissionais de gerenciamento de projetos.

O Guia PMBOK® é dividido em cinco grupos de processos:

Iniciação: define o escopo do projeto e obtém a aprovação para iniciar.

Planejamento: desenvolve um plano para o projeto que inclui objetivos, cronograma, orçamento e recursos.

Execução: realiza o plano do projeto e acompanha o progresso.

Monitoramento e controle: garante que o projeto esteja no caminho certo e identifica quaisquer problemas que possam surgir.

Encerramento: finaliza o projeto e entrega os resultados.

Aqui estão alguns conceitos e modelos práticos do Guia PMBOK®:

Escopo do projeto: o escopo do projeto é o trabalho que deve ser realizado para entregar os resultados do projeto. É importante definir o escopo do projeto com precisão para garantir que o projeto esteja no caminho certo.

Cronograma do projeto: o cronograma do projeto é um plano que descreve quando as atividades do projeto serão realizadas. É importante desenvolver um cronograma realista que seja possível de cumprir.

Orçamento do projeto: o orçamento do projeto é um plano que descreve quanto custará realizar o projeto. É importante desenvolver um orçamento preciso que reflita os custos reais do projeto.

Riscos do projeto: os riscos do projeto são eventos ou condições que podem afetar o sucesso do projeto. É importante identificar e gerenciar os riscos do projeto para reduzir a probabilidade de problemas.

Stakeholders do projeto: os stakeholders do projeto são pessoas ou organizações que têm interesse no sucesso do projeto. É importante identificar e gerenciar as expectativas dos stakeholders para garantir que o projeto atenda às suas necessidades.

Gerenciamento de serviços de TI

O gerenciamento de serviços de TI (GSTI) é um conjunto de processos e atividades que visam garantir que os serviços de TI atendam às necessidades dos negócios. O GSTI é importante para as organizações porque:

Garante que os serviços de TI sejam entregues de forma eficiente e eficaz.
Melhora a qualidade e a disponibilidade dos serviços de TI.
Reduz os custos de TI.
Aumenta a satisfação dos usuários.

O GSTI é baseado em um conjunto de conceitos e modelos práticos, incluindo:

Modelo de ciclo de vida de serviços: descreve as fases do ciclo de vida de um serviço de TI, desde o seu planejamento até a sua descontinuação.
Funções de gerenciamento de serviços: define as responsabilidades e autoridades das pessoas envolvidas no GSTI.

Processos de gerenciamento de serviços: descreve as atividades que devem ser realizadas para gerenciar os serviços de TI.

Modelos práticos do GSTI incluem:

ITIL: um framework de referência para o GSTI que fornece uma descrição detalhada dos processos e atividades envolvidos no gerenciamento de serviços de TI.

COBIT: um framework de governança de TI que fornece orientações para o gerenciamento de todos os aspectos da TI, incluindo o GSTI.

ISO 20000: uma norma internacional que fornece requisitos para o sistema de gerenciamento de serviços de TI.

Formulário de verificação sobre o entendimento e importância da governança em TI e governança corporativa.

Nome:
Cargo:
Organização:

1. Qual é a definição de governança em TI?

- A governança em TI é o processo de estabelecer diretrizes, estruturas e mecanismos para garantir que a TI seja alinhada com as estratégias e objetivos da organização.
- A governança em TI é o conjunto de processos, estruturas e responsabilidades que definem como a TI é gerenciada e controlada na organização.
- A governança em TI é o processo de garantir que a TI seja usada de forma eficiente, eficaz e segura para apoiar os negócios.

2. Qual é a importância da governança em TI?

- A governança em TI é importante para garantir que a TI atenda às necessidades dos negócios.
- A governança em TI é importante para reduzir os riscos relacionados à TI.
- A governança em TI é importante para melhorar a eficiência e a eficácia da TI.

3. Qual é a diferença entre governança em TI e governança corporativa?

- A governança em TI é um componente da governança corporativa.
- A governança em TI é responsável por garantir que a TI seja alinhada com as estratégias e objetivos da organização.
- A governança corporativa é responsável por garantir que a organização seja administrada de forma eficiente, eficaz e responsável.

4. Quais são os principais objetivos da governança em TI?

- Alinhar a TI com as estratégias e objetivos da organização.
- Reduzir os riscos relacionados à TI.
- Melhorar a eficiência e a eficácia da TI.
- Proteger os ativos de TI.
- Assegurar o cumprimento das leis e regulamentos.

5. Quais são as principais atividades da governança em TI?

- Estabelecer políticas e diretrizes de TI.
- Desenvolver e implementar processos de TI.
- Avaliar e monitorar o desempenho da TI.
- Alocar recursos de TI.
- Gerenciar os riscos de TI.

Quais são os principais benefícios da governança em TI?

- Aumento da eficiência e eficácia dos negócios.
- Redução dos custos de TI.
- Melhoria da segurança da TI.
- Melhoria da conformidade com as leis e regulamentos.
- Aumento da satisfação dos clientes.

Quais são os principais desafios da governança em TI?

- Obter o apoio da alta administração.
- Integrar a governança em TI com a governança corporativa.
- Gerenciar a complexidade da TI.
- Alinhar a governança em TI com as mudanças nos negócios.

Quais são os principais marcos da governança em TI?

- Estabelecimento de um conselho de TI.
- Desenvolvimento de um plano estratégico de TI.
- Implementação de um sistema de gerenciamento de riscos de TI.
- Implementação de um programa de segurança da informação.
- Implementação de um sistema de gerenciamento de serviços de TI.

Este formulário é uma ferramenta que pode ser usada para verificar o entendimento e a importância da governança em TI e governança corporativa. O formulário pode ser adaptado para atender às necessidades específicas da organização.

REFERÊNCIAS

https://nova.escolalinux.com.br/blog/seguranca-da-informcao-familia-iso-27000

https://www.ibgc.org.br/wp-content/uploads/2023/07/Guia-SOX-versao-2.0.pdf

https://www.ibgc.org.br/uploads/2023/07/Guia-Governanca-de-TI-versao-2.0.pdf