Governança em TI

SUMÁRIO

Familia ISO/IEC27000

A ISO 27000 é um conjunto de certificações de segurança da informação e proteção de dados para empresas e órgãos públicos. Elas servem como base para a criação de um Sistema de Gestão de Segurança da Informação (SGSI) em organizações de pequeno, médio e grande porte. O SGSI reúne políticas, procedimentos, diretrizes e recursos de proteção de informação de uma organização. O sistema deve estar alinhado aos objetivos de negócio e ser gerenciado de forma conjunta pela empresa.

- **Importância da ISO 27000:**

A importância da família ISO/IEC 27000 reside na proteção de informações sensíveis e confidenciais, garantindo a continuidade das operações e preservando a reputação da organização. Além disso, a conformidade com esses padrões é frequentemente uma exigência contratual ou regulatória.

Uma organização com as certificações da família ISO 27000 sinaliza para o mercado e para os clientes o comprometimento com a segurança da informação. Esse grupo de normas também traz diretrizes que ajudam empresas e órgãos públicos a se adequarem à LGPD e a padrões internacionais de governança de TI.

- **Exemplos:**

ISO/IEC 27001 - Este é o ponto de partida. Descreve os requisitos para estabelecer, implementar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Por exemplo, uma empresa pode usar o ISO/IEC 27001 para definir políticas e procedimentos de segurança.
ISO/IEC 27002 - Este documento fornece diretrizes detalhadas para a implementação dos controles de segurança da informação. Ele ajuda as organizações a escolher medidas práticas para proteger seus ativos de informação.
ISO/IEC 27003, 27004 e 27005 - Essas normas se concentram em orientações para implementar,

medir e gerenciar a segurança da informação. Por exemplo, o ISO/IEC 27005 ajuda as organizações a identificar e avaliar riscos de segurança.
ISO/IEC 27006 - Essa norma fornece orientações sobre como auditar e certificar um SGSI de acordo com o ISO/IEC 27001. É útil para garantir que as práticas de segurança estejam em conformidade.

- **Atualizações:**

A família ISO/IEC 27000 é periodicamente revisada e atualizada para se manter relevante e eficaz em um ambiente em constante evolução de ameaças cibernéticas. É importante manter-se atualizado com as versões mais recentes desses padrões.

- **Conceitos:**

Alguns conceitos-chave na família ISO/IEC 27000 incluem confidencialidade, integridade, disponibilidade, autenticidade, responsabilidade e conformidade. Esses conceitos servem como base para a implementação de medidas de segurança.

- **Modelos Práticos:**

Para implementar os padrões da família ISO/IEC 27000, as organizações geralmente seguem um processo que envolve avaliar os riscos de segurança, estabelecer políticas e procedimentos, implementar controles de segurança, monitorar e revisar continuamente o sistema de gerenciamento de segurança da informação.

Domínios e componentes da governança de TI

Domínios e componentes da governança de TI se referem à forma como as organizações gerenciam e supervisionam sua tecnologia da informação (TI).

- **Importância:**

A governança de TI é vital para garantir que uma organização use eficazmente sua tecnologia para atingir seus objetivos, ao mesmo tempo em que mantém a segurança e o controle. É importante porque a TI é uma parte fundamental de quase todos os negócios e, se não for gerenciada corretamente, pode levar a problemas graves.

- **Exemplos:**

Estratégia de TI: Decidir como a tecnologia será usada para atingir metas organizacionais. Gerenciamento de Riscos: Identificar e reduzir riscos relacionados à TI, como segurança cibernética.

Medição de Desempenho: Acompanhar o desempenho da TI para garantir que ela esteja atendendo às necessidades da organização. Conformidade com Regulamentações: Garantir que a TI esteja em conformidade com leis e regulamentações aplicáveis.

- **Atualizações:**

A governança de TI evolui para se adaptar a novas tecnologias e desafios. Por exemplo, a crescente importância da segurança cibernética levou a atualizações nas práticas de governança para abordar essas ameaças.

- **Conceitos:**

Responsabilidade: este princípio diz que os indivíduos e os grupos dentro da organização compreendem e aceitam as suas responsabilidades.
Estratégia: este princípio diz que a estratégia de negócio da organização deve levar em consideração as capacidades atuais e futuras da TI.

Aquisição: este princípio diz que as aquisições da TI são realizadas por razões válidas, com base em análise apropriada e de forma contínua, com decisões claras e transparentes equilibrando os benefícios, oportunidades, custos e riscos, de curto e longo prazo.

Desempenho: este princípio diz que a TI deve apoiar a organização oferecendo serviços, níveis de serviço e qualidade de serviço que sejam necessários para atender aos requisitos atuais e futuros de negócio.

Conformidade: este princípio diz que a TI cumpre a legislação e os regulamentos obrigatórios. Todas as políticas e as práticas são claramente definidas, implantadas e fiscalizadas.

Comportamento Humano: este princípio diz que todas as políticas, práticas e decisões da TI demonstram respeito pelo comportamento humano, incluindo as necessidades atuais e futuras das pessoas envolvidas no processo.

- **Modelos Práticos:**

COBIT (Control Objectives for Information and Related Technologies):
Um modelo de governança de TI amplamente usado que fornece um conjunto de práticas e estruturas. O Cobit é um modelo genérico que representa todos os processos normalmente encontrados nas funções da TI sendo compreensível tanto para a operação quanto para os gerentes. Além disso, o Cobit é representado por cinco áreas que sustentam o seu núcleo: o alinhamento estratégico que é a ligação entre o negócio e a TI, agregação de valor que se restringe em executar aquilo que entregue benefícios de acordo com a estratégia, gerenciamento de recursos em que se procura otimizar os investimentos, gerenciamento de riscos em que a alta direção conhece e entende os riscos, e a medição de desempenho em que acompanha-se e monitora-se a implantação e o andamento dos projetos e recursos associados.

ITIL (Information Technology Infrastructure Library): Um conjunto de práticas para o gerenciamento de serviços de TI. É um conjunto de práticas e diretrizes para o gerenciamento de serviços de TI. Ele fornece um conjunto de melhores práticas para ajudar as organizações a melhorar a eficiência, qualidade e alinhamento de seus serviços de TI com as necessidades do negócio. Em resumo, o ITIL ajuda as organizações a gerenciar seus serviços de TI de forma mais eficaz, garantindo que eles atendam às expectativas dos usuários e sejam alinhados com os objetivos organizacionais. Ele abrange áreas como o gerenciamento de incidentes, problemas, mudanças, capacidade, continuidade e muito mais.

ISO/IEC 38500: A norma ISO/IEC 38500 tem como objetivo fornecer uma estrutura de princípios para os dirigentes utilizarem na avaliação, gerenciamento e no monitoramento do uso da tecnologia da informação nas suas organizações. Um padrão internacional para governança de TI.

A Lei Sarbanes-Oxley (Lei SOX)

É uma regulamentação dos Estados Unidos que foi criada em resposta a escândalos financeiros e contábeis que abalaram grandes empresas no início dos anos 2000, como o caso Enron.

- **Importância:**

A Lei SOX é importante porque visa aumentar a transparência e a responsabilidade nas empresas públicas dos EUA. Ela ajuda a garantir que as informações financeiras e contábeis sejam precisas e confiáveis, protegendo os investidores e o público em geral.

- **Exemplos:**

Requer que os diretores e executivos de empresas públicas certifiquem pessoalmente a precisão das demonstrações financeiras.
Estabelece padrões rigorosos para auditorias e responsabiliza auditores por práticas inadequadas.

Exige que as empresas implementem controles internos eficazes para proteger seus ativos e garantir a precisão das informações financeiras.

- **Atualizações:**

A Lei SOX tem sido amplamente mantida e algumas de suas regras têm sido esclarecidas e aprimoradas ao longo dos anos, à medida que são identificadas melhorias necessárias.

- **Conceitos:**

Controles internos: Procedimentos e políticas que as empresas devem ter em vigor para proteger ativos e garantir informações financeiras precisas.
Responsabilidade executiva: Os executivos são pessoalmente responsáveis pela precisão das informações financeiras divulgadas pela empresa.

- **Modelos Práticos:**

A Lei SOX em si é uma regulamentação, mas empresas geralmente implementam frameworks, como o COBIT (Control Objectives for Information and Related Technologies), para auxiliar na conformidade com seus requisitos.

Gestão de portfólio e projetos para governança de TI

A gestão de portfólio e projetos para governança de TI é um processo que ajuda as organizações a tomar decisões estratégicas e gerenciar eficazmente seus projetos de tecnologia da informação.

- **Importância:**

A gestão de portfólio e projetos de TI é importante porque ajuda as organizações a investir em projetos que estejam alinhados com seus objetivos estratégicos. Isso evita o desperdício de recursos em projetos desnecessários e assegura que a TI contribua para o sucesso do negócio.

- **Exemplos:**

Imagine uma empresa que deseja expandir seu alcance online. Ela pode usar a gestão de portfólio para avaliar e priorizar projetos, como um novo site, aplicativo móvel ou estratégias de marketing digital, para atingir esse objetivo de forma eficaz.

Um exemplo prático é a criação de um escritório de gestão de projetos (PMO) que ajuda a supervisionar e priorizar os projetos de TI da empresa.

- **Atualizações:**

A gestão de portfólio e projetos de TI está em constante evolução devido a mudanças tecnológicas e necessidades de negócios. Atualizações podem incluir a adoção de novas metodologias de gerenciamento de projetos ou a implementação de ferramentas de análise de portfólio mais avançadas.

- **Conceitos:**

Portfólio de Projetos: É o conjunto de todos os projetos de TI em andamento ou planejados em uma organização.
Priorização: Decidir quais projetos são mais importantes com base em critérios estratégicos, orçamentários e de risco.
Gestão de Projetos: O planejamento, execução e monitoramento de projetos de TI para atingir seus objetivos.

- **Modelos Práticos:**

PMI (Project Management Institute): Oferece o conjunto de boas práticas do PMBOK (Guia de Conhecimento em Gerenciamento de Projetos) para gestão de projetos.
Metodologias Ágeis: Como o Scrum e o Kanban, que se concentram em entregas iterativas e colaborativas.
Ferramentas de Portfólio e Projetos: Como o Microsoft Project, JIRA, e outras, que auxiliam na gestão e monitoramento de projetos.

PMBOK

O PMBOK, ou Guia PMBOK (Project Management Body of Knowledge), é um guia que fornece boas práticas e diretrizes para o gerenciamento de projetos.

- **Importância:**

O PMBOK é importante porque ajuda as organizações a gerenciar projetos de forma mais eficiente e eficaz. Ele fornece um conjunto de padrões e práticas que podem ser aplicados a uma ampla variedade de projetos, ajudando a garantir que eles sejam concluídos com sucesso.

- **Atualizações:**

O PMBOK é atualizado periodicamente para refletir as melhores práticas atuais em gerenciamento de projetos. As atualizações garantem que o guia esteja alinhado com as tendências e necessidades em constante evolução no campo do gerenciamento de projetos.

- **Exemplos:**

Imagine que você está liderando um projeto de construção de uma casa. O PMBOK forneceria orientações sobre como planejar o projeto, definir as etapas, gerenciar recursos, controlar o progresso e garantir que a casa seja construída no prazo e dentro do orçamento.

- **Conceitos:**

Áreas de Conhecimento: São as diferentes áreas em que o gerenciamento de projetos é dividido, incluindo gerenciamento de escopo, tempo, custo, qualidade, recursos, comunicações, riscos e partes interessadas.
]
Processos: São as ações específicas a serem realizadas em cada uma das áreas de conhecimento para garantir a execução bem-sucedida de um projeto.

- **Modelos Práticos:**

Ciclo de Vida do Projeto: O PMBOK descreve diferentes fases do ciclo de vida de um projeto, desde a concepção até a conclusão. Estrutura Analítica do **Projeto (EAP):** Uma ferramenta usada para desdobrar o escopo do projeto em partes menores e mais gerenciáveis.
Rede de Diagrama de Precedência (PDM): Uma técnica usada para representar as dependências entre as atividades do projeto.

O Gerenciamento de Serviços de TI (IT Service Management - ITSM)

É um conjunto de práticas e processos para gerenciar eficazmente os serviços de tecnologia da informação em uma organização.

- **Importância:**

O ITSM é importante porque ajuda as organizações a fornecer serviços de TI confiáveis e eficientes que atendam às necessidades de seus usuários e clientes. Ele contribui para a satisfação dos clientes, melhora a produtividade e reduz os riscos de interrupções nos serviços de TI.

- **Exemplos:**

Quando você liga para o suporte técnico de uma empresa para resolver um problema com seu computador, o ITSM entra em ação para garantir que seu problema seja resolvido de maneira eficaz e que você receba um bom atendimento.

O ITSM também é aplicado quando uma organização lança um novo serviço de TI, garantindo que ele seja planejado, testado e implantado de maneira adequada.

- **Atualizações:**

O ITSM evolui constantemente para se adaptar às mudanças tecnológicas e às necessidades das empresas. À medida que novas tecnologias e abordagens surgem, as práticas de ITSM são atualizadas para acomodá-las.

- **Conceitos:**

Catálogo de Serviços: Uma lista de todos os serviços de TI oferecidos pela organização, com detalhes sobre como acessá-los e os níveis de serviço associados.
Gestão de Incidentes: O processo de lidar com eventos não planejados, como interrupções de serviço, para restaurar o serviço normal o mais rápido possível.

Gestão de Mudanças: Planejar e implementar alterações nos serviços de TI de forma controlada e eficaz, minimizando riscos.

- **Modelos Práticos:**

ITIL (Information Technology Infrastructure Library):
Um conjunto de boas práticas amplamente utilizado para o ITSM, fornecendo orientações detalhadas sobre como gerenciar serviços de TI.
COBIT (Control Objectives for Information and Related Technologies):
Um framework que aborda o alinhamento de TI com as necessidades de negócios e o gerenciamento de riscos.