Especialização em
Auditoria e Controle Interno

Auditoria de Sistema de Informação

Derlange Maia Oliveira
Samuel Leite Castelo

Especialização em Auditoria e Controle Interno

Especialização em Contabilidade Pública

Especialização em Controladoria Pública

Especialização em Gestão Pública

Especialização em Gestão Pública Municipal

Especialização em Alfabetização e Multiletramento

Especialização em Tecnologias Digitais na Educação Básica

Especialização em EaD

Especialização em Gestão Pedagógica

Especialização em Lingua Inglesa

Especialização em Educação Física na Educação Básica

Especialização em Audiodescrição

Especialização em Legendagem

Especialização em Artes

Especialização em
Auditoria e Controle Interno

Auditoria de Sistema de Informação

Derlange Maia Oliveira
Samuel Leite Castelo

Fortaleza
EdUECE
2024

Especialização em Auditoria e Controle Interno
Especialização em Contabilidade Pública
Especialização em Controladoria Pública
Especialização em Gestão Pública
Especialização em Gestão Pública Municipal
Especialização em Alfabetização e Multiletramento
Especialização em Tecnologias Digitais na Educação Básica
Especialização em EaD
Especialização em Gestão Pedagógica
Especialização em Lingua Inglesa
Especialização em Educação Física na Educação Básica
Especialização em Audiodescrição
Especialização em Legendagem
Especialização em Artes

Auditoria de Sistema de Informação

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Oliveira, Derlane Maia
Auditoria de sistema de informação [livro eletrônico] / Derlane Maia Oliveira, Samuel Leite Castelo. -- Fortaleza, CE : Editora da UECE, 2024.
PDF

Bibliografia.
ISBN 978-85-7826-945-6

1. Auditoria - Processamento de dados 2. Sistemas de recuperação da informação - Contabilidade 3. Tecnologia da informação I. Castelo, Samuel Leite. II. Título.

24-230496 CDD-657.450285

Índices para catálogo sistemático:

1. Auditoria : Finanças públicas 657.450285

Eliete Marques da Silva - Bibliotecária - CRB-8/9380

Editora da Universidade Estadual do Ceará – EdUECE
Todos os direitos reservados
Editora da Universidade Estadual do Ceará – EdUECE
Av. Dr. Silas Munguba, 1700 – Campus Itaperi – Reitoria – Fortaleza – Ceará
CEP: 60714-903 – Tel: (085) 3101-9893
www.uece.br/eduece – E-mail: eduece@uece.br

Editora filiada à
ABEU
ASSOCIAÇÃO BRASILEIRA DAS EDITORAS UNIVERSITÁRIAS

Sumário

Apresentação

Caro(a) leitor(a),

Este livro oferece uma apresentação jornada abrangente do universo da auditoria de sistemas de informação, enfocando a interseção crucial entre tecnologia e inovação. Ao longo dos capítulos, os autores exploram princípios, conceitos e processos fundamentais da Auditoria, proporcionando uma aprendizagem, de base sólida para que o público leitor compreenda o escopo e a importância da auditoria de sistemas de informação nos diversos exercícios profissionais que necessitam de sua utilização.

Para o melhor proveito de sua leitura e de seus estudos, o livro está assim dividido:

- Capítulo 1: Fundamentos da Auditoria de SI – elabora-se uma compreensão abrangente dos objetivos da auditoria, do papel do auditor, das normas, da organização de trabalho e da avaliação da equipe.
- Capítulo 2: Metodologia de Auditoria de Sistemas Conforme Normas ISACA/COBIT – Apresentação da metodologia e da capacitação dos leitores à aplicação efetiva de suas diretrizes, visando, ao fortalecimento da governança de TI e ao aprimoramento da segurança de informação nas organizações.
- Capítulo 3: Papel do Gestor na Auditoria de Sistemas de TI – Momento em que se explicita o papel estratégico dos gestores na auditoria de sistemas de TI, apresentando uma visão abrangente das suas responsabilidades.
- Capítulo 4: Desenvolvimento e Gerenciamento de Sistemas de TI – Apresentação e discussão de fundamentos, desafios, tendências e considerações éticas acerca do desenvolvimento e de gerenciamento de sistemas e programas de TI.
- Capítulo 5: Auditoria de Plano de Contingência em TI – Aprofundamento da compreensão do papel da auditoria de plano de contingência em Tecnologia da Informação, visando à preparação dos gestores e auditores para eventos adversos.

Os autores

Capítulo 1

Visão geral da Auditoria de Sistemas de Informação

Objetivo

- Fornecer uma introdução abrangente e esclarecedora sobre os principais conceitos e processos relacionados à Auditoria de Sistemas de Informação (SI).
- Preparar para compreensão do contexto, dos princípios e das práticas que orientam a auditoria de sistemas de informação dentro das organizações, servindo como base para capítulos subsequentes e aprofundamentos em tópicos específicos.

Introdução

A auditoria de SI é uma atividade que visa avaliar a eficácia dos sistemas de tecnologia da informação em uma organização. Isso inclui a verificação dos controles, do desenvolvimento de sistemas, dos procedimentos de tecnologia da informação (TI), da infraestrutura, da operação, do desempenho e da segurança da informação.

Como podemos observar na citação abaixo, ela pode ser definida como:

> Conjunto de procedimentos adotados para avaliar o grau de confiança e de qualidade dos controles existentes, verificar a correta aplicação dos sistemas e procedimentos, e detectar as falhas que estejam ocorrendo (Maria de Lourdes Deroza).
>
> Processo que busca evidências para certificar-se de que os recursos de Tecnologia da Informação: a) possibilitem alcançar os objetivos do negócio; b) sejam usados com eficiência e em conformidade com as leis e normas aplicáveis; e c) sejam adequadamente protegidos para prover informação confiável sempre que requerida às pessoas autorizadas (PACHECO, 2011).

O Guia para Auditoria de TI da Organização Internacional das Entidades de Fiscalização Superiores (INTOSAI, 2013), por sua vez, define auditoria de TI como "um exame e revisão de sistemas de TI e controles relacionados para obter garantia ou identificar violações dos princípios de legalidade, eficiência, economia e eficácia do sistema de TI e controles relacionados".

O objetivo é garantir que a tecnologia e os sistemas de informação atendam às necessidades do negócio, mantenham a integridade dos dados, melhorem os processos, usem recursos eficientemente e cumpram regulamentos e leis. É fundamental para garantir integridade, disponibilidade, confidencialidade e conformidade com normas, além de controles internos, processamento de dados, efetividade, satisfação dos usuários e usabilidade dos sistemas de computador. Segundo Lyra (2008, p. XX) "uma Auditoria de TI busca adequar, revisar, avaliar e recomendar alterações positivas nos processos internos, bem como avaliar a utilização de recursos humanos, materiais e tecnológicos envolvidos".

Portanto, a auditoria de SI visa melhorar os processos internos, avaliar a utilização dos diferentes tipos de recursos e, ainda, é essencial às organizações tendo em vista o aumento do investimento em sistemas de informação

> Os consideráveis gastos investidos no processamento eletrônico de dados demandam por auditorias apropriadas. Tais auditorias devem ser baseadas em sistemas e abranger aspectos, tais como: planejamento; uso econômico dos equipamentos de processamento de dados; alocação de pessoal com habilidades apropriadas, preferencialmente dentro da administração da organização auditada; prevenção ao mau uso; e utilidade da informação produzida (Intosai, Declaração de Lima que contém os princípios da Auditoria, 1977, p. XX)

A auditoria de SI pode se fazer presente em todos os sistemas informatizados da organização, seja em nível estratégico, seja em nível operacional. Para tanto, pode-se organizar a atuação da auditoria em sistemas que estão em produção ou em desenvolvimento, no ambiente de tecnologia da informação, em equipamentos de processamento de dados ou procedimentos específicos, alcançando entradas, processos, controles, arquivos, segurança e extratores de informações. Assim, vê-se que é necessário que a auditoria avalie todo o ambiente envolvido desde equipamentos, centro de processamento de dados até softwares.

Segundo Auditor-General's Office Singapore (2009) a importância das Auditorias de TI pode ser resumida nos seguintes benefícios:

- Aumento da quantidade, extensão e complexidade dos mecanismos de controle organizacionais.
- Aumento do impacto da TI na forma como os entes fiscalizadores exercem suas competências.
- Jurisdicionados cada vez mais automatizados, por consequência, sujeitos a maiores riscos relacionados à complexidade da TI.

- Novos conceitos e metodologias de trabalho.
- Controles Internos cada vez mais implementados em sistemas da informação.

A avaliação das funcionalidades de um sistema é um aspecto importante que pode ser abordado em uma auditoria de SI, mas contudo pode levar a uma diversidade de situações, uma vez que cada sistema apresenta funcionalidades específicas do negócio para o qual foi desenvolvido. É necessário, portanto, um conhecimento mais abrangente e específico que contemple as regras do negócio implementadas no sistema e, ainda, a legislação aplicável.

A auditoria de sistemas se materializa por meio da emissão de um parecer técnico que verse sobre:

- O controle da área de tecnologia.
- A análise da eficiência dos sistemas de informação.
- A verificação do cumprimento das legislações e normativos a qual estão sujeitos.
- A gestão eficaz dos recursos de TI.

Importa dizer que deve ser sempre realizada por profissionais capacitados, visando aferir a efetividade dos sistemas de informação, sob todos os níveis, bem como processar e tratar informações de maneira confiável, preservando a integridade dos dados para entregar informações que mantenham correspondência com a realidade.

1. Objetivos da Auditoria de Sistemas de Informação

A auditoria de sistemas consiste em reunir, agrupar e avaliar evidências para determinar se um sistema de informação atende à necessidade do negócio, mantendo a integridade dos dados, a realização dos objetivos esperados, a utilização eficiente dos recursos e, ainda, verificar a conformidade com os normativos do negócio, contemplando todo o ciclo de vida do tratamento da informação: entrada, processamento, saída e armazenamento dos dados.

A auditoria de SI contribui para identificar necessidades, processos ineficazes, custos e barreiras que afetam a eficiência dos fluxos de informação e, assim, melhora o negócio apoiado pela tecnologia.

Dentre os objetivos da auditoria de SI, tem-se:

- Avaliar o desempenho dos sistemas;
- Verificar a conformidade com regulamentos e normas;
- Garantir a segurança da informação;
- Assegurar a integridade dos dados;
- Manter a disponibilidade dos sistemas;

- Preservar a confidencialidade das informações;
- Proteger a privacidade.

Assim, a auditoria de SI visa verificar se os sistemas e aplicativos são apropriados, eficientes e controlados adequadamente, de modo a garantir que a entrada, o processamento e a saída de dados são válidos, confiáveis, oportunos e seguros, em todos os níveis de atividade de um sistema. Desse modo, são garantias da auditoria de SI:

- Garantia de Conformidade: quando assegura que os sistemas e processos de TI estão em conformidade com regulamentações internas e externas, políticas e padrões.
- Garantia de Segurança: ocorre quando a auditoria avalia a eficácia dos controles de segurança de TI, identificando e mitigando vulnerabilidades e ameaças.
- Garantia de Integridade: ao verificar a integridade dos dados, assegurando que as informações são precisas, confiáveis e não foram adulteradas.
- Garantia de Disponibilidade: assegura que os sistemas e recursos de TI estejam disponíveis quando necessários, minimizando tempo de inatividade e de interrupções.

Assim, vê-se que, para a auditoria de SI atingir seus objetivos, é necessário validar e avaliar os controles internos de SI; confirmar a eficácia do sistema; reunir, agrupar e validar evidências; garantir a segurança (física e lógica) da informação e do sistema.

2. Papel do Auditor de Sistemas de Informação

O sucesso da auditoria depende das habilidades e das competências do auditor, que deve ser ético, independente, imparcial, ter conhecimento técnico em sistemas de TI, segurança da informação e regulamentações, além de planejar e executar a auditoria de acordo com padrões aceitos. Assim, são elementos fundamentais para a credibilidade em um processo de auditoria adequado:

- Conduta ética e confiável de modo a proteger a confidencialidade das informações às quais tem acesso durante a auditoria;
- Independência e imparcialidade no trabalho, evitando conflitos de interesse e influências externas, por isso não devem ser subordinados ou dependentes do auditado;
- Integridade das descobertas, não distorcendo ou ocultando informações relevantes;
- Conhecimento técnico sólido em sistemas de TI, segurança da informação e regulamentações relevantes;

- Planejamento e execução de acordo com os padrões e as normas aceitas, garantindo uma abordagem sistemática;
- Comunicação justa, clara e eficaz do que foi constatado durante a auditoria com informações íntegras e confiáveis, incluindo recomendações para melhorias.

O auditor de sistemas verifica a eficácia dos controles e procedimentos de segurança, a eficiência dos processos, a utilização correta dos recursos e fornece recomendações para melhorias, assessorando a administração na elaboração de planos e na definição de metas, colaborando para o aperfeiçoamento dos controles internos, apontando deficiências e irregularidades que possam comprometer a segurança e o desempenho organizacional.

> O papel do auditor é auditar as políticas, práticas e procedimentos de controle interno de uma organização, a fim de assegurar que os controles são adequados para se alcançar a missão institucional (Intosai, Controle Interno: estabelecendo uma base para prestação de contas no governo, 2001, p. XX)

Com a larga utilização da tecnologia para o armazenamento das informações contábeis, financeiras e operacionais, o auditor de sistemas precisa se aprimorar no campo de atuação (processos) da organização para extrair informações, analisar banco de dados envolvidos e suportar decisões das demais áreas de auditoria.

> O auditor, para determinar a extensão e o alcance da fiscalização, deve examinar e avaliar o grau de confiabilidade dos controles internos (Normas de Auditoria da INTOSAI).

O auditor é essencial para proteger a segurança e o desempenho da organização.

2.1. Normas e Padrões de Auditoria de Sistemas de Informação

Em termos gerais, pode-se dizer que auditar é a situação fática comparada com o(s) critério(s) de auditoria, que podem ser normas, políticas, procedimentos ou, mesmo, requisitos. Contudo, a escolha desse critério deve ser feita de acordo com o objetivo da auditoria, que tem como principais referenciais:

- Constituição da República Federativa do Brasil de 1988, art. 37, *caput* (princípio da eficiência);
- COSO: framework do Comitê de Organizações Patrocinadoras da Comissão Treadway (COSO) que define um modelo amplamente aceito para controle interno e gestão de riscos;

- ISO 27001: norma internacional de segurança da informação.
- COBIT: Control Objectives for Information and Related Technologies (COBIT) é um conjunto de melhores práticas (modelo corporativo) para governança e gestão de TI;
- ABNT NBR ISO/IEC 38500:2018 – Governança da TI para a organização.

A necessidade global de referências nesse assunto estabeleceu a criação e o desenvolvimento de melhores práticas como COBIT, COSO, ISO 27001 e ITIL. Além disso, as normas e as regulamentações específicas do negócio auditado são levadas em consideração. Cada tipo de auditoria pode ter processos, critérios e metodologias específicos.

2.2. Organização de Trabalho da Auditoria de Sistemas de Informação

Uma auditoria de SI com o intuito de avaliar o controle de um determinado sistema informatizado, para fins didáticos, dever apresentar a seguinte estrutura:

- Planejamento;
- Escolha da equipe;
- Programação;
- Execução de trabalhos e supervisão;
- Revisão dos papéis de trabalho, conclusão e emissão de relatórios;
- Atualização do conhecimento permanente;
- Avaliação da equipe.

a) Planejamento

Esta etapa consiste em definir os objetivos da auditoria, o escopo (enfoque, abrangência e delimitação do sistema a ser auditado) dos procedimentos a serem avaliados, os recursos (humanos, tecnológicos, materiais e financeiros), o cronograma e as abordagens que devem ser adotadas pela equipe de auditoria.

É nessa etapa que a equipe de auditoria deve:

- Identificar as áreas de maior risco na organização.
- Entender a dependência de tecnologia da informação nos processos mais relevantes.
- Resgatar as recomendações das auditorias anteriores.
- Obter informações sobre fluxos, políticas, normas e procedimentos.
- Visualizar pontos de controle às vulnerabilidades identificadas.
- Estabelecer um cronograma de atuação, conforme prazo estipulado.

- Obter referências de boas práticas para a confecção de testes.
- Estabelecer planos de testes.
- Definir responsáveis pelas frentes de trabalho.

O planejamento da auditoria abrange vários passos importantes. A obtenção de conhecimento em relação ao negócio e à organização, representa a etapa crítica desse processo, pois forma a base para a realização de outros procedimentos de auditoria. É preciso conhecer o ambiente computacional do cliente, com informações sobre hardware, sistemas operacionais, arquitetura computacional, metodologia usada no desenvolvimento de software e os sistemas que são ou não críticos.

Ao planejar o seu trabalho, o auditor toma importantes decisões sobre a relevância e o risco de auditoria. Um produto importante do planejamento envolve a tomada de decisões preliminares sobre a estratégia a ser adotada.

b) Escolha da equipe

Um planejamento correto possibilita a identificação adequada dos perfis necessários para a composição da equipe de auditoria de TI. Devem ser levadas em consideração, no mínimo, as seguintes informações sobre os membros da equipe:

- Perfil e histórico profissional;
- Experiência acumulada por tipo de atividade;
- Conhecimentos específicos;
- Formação acadêmica;
- Línguas estrangeiras;
- Disponibilidade para viajar.

c) Programação

O responsável pela auditoria deve, nesta etapa, programar a equipe para executar os trabalhos necessários com vistas a minimizar os riscos de auditoria. Assim deve-se observar as habilidades para:

- Gerar programas de trabalho que extraiam dados corretos para testes;
- Selecionar procedimentos apropriados;
- Incluir novos procedimentos;
- Classificar os trabalhos;
- Evidenciar corretamente;
- Gerar relatórios adequados.

As tarefas devem ser distribuídas entre os membros da equipe de auditoria considerando as formações, experiências e treinamentos específicos de modo a distribuir conforme as vivências profissionais

d) Execução de trabalhos e supervisão

Após a escolha do sistema a ser auditado, é na execução que se inicia a etapa de levantamento das informações por parte da equipe de auditoria, ou seja, a coleta de evidências, que consiste na realização de testes, revisões e análises que sustentem as conclusões da auditoria de modo que sejam confiáveis e reproduzíveis.

Nesse momento deve-se buscar uma compreensão abrangente das características do sistema. Para tanto, pode-se utilizar técnicas de entrevistas, análise documental e observação direta, sendo necessário descrever as informações obtidas. Outras técnicas comumente utilizadas são os testes de sistema e análises de código-fonte (programas).

Aqui é importante identificar os pontos de integração com outros sistemas, é possível delimitar a abrangência da auditoria e não extrapolar o que foi definido no escopo do trabalho, bem como, identificar os pontos de controle que podem ser validados, seus objetivos e as funções que exercem no sistema como um todo. Diversos elementos que compõem o sistema podem ser considerados pontos de controle: telas, rotinas, documentos de entrada, integrações, relatórios de saída, dentre outros.

A supervisão visa assegurar a qualidade do cumprimento das tarefas e, ainda, mitigar prováveis riscos identificados.

e) Revisão dos papéis de trabalho, conclusão e emissão de relatórios

As responsabilidades do auditor no fechamento dos trabalhos podem ser divididas em três partes: conclusão do trabalho de campo, avaliação das descobertas e comunicação com o auditado. Uma maneira de assegurar a qualidade dos trabalhos é a revisão dos papéis de trabalho e a validação dos procedimentos aplicados, que podem ser feitas pelo líder da auditoria ou por um supervisor não envolvido com a execução dos trabalhos.

Eventualmente falhas ou descumprimentos do auditado podem ocorrer e é possível que limitem a conclusão do auditor, sendo permitido ao revisor a solicitação de novas visitas para a complementação do trabalho. Contudo, deve-se levar em consideração os impactos no escopo e no cronograma do trabalho.

É nessa etapa que se deve avaliar e analisar as descobertas por meio da comparação das evidências coletadas com os critérios estabelecidos e a identificação de não conformidades.

Aplicados os procedimentos e coletadas as evidências que permitam as conclusões sobre as questões de auditoria, deve-se produzir o relatório de auditoria, que é o documento que materializa os resultados obtidos, com as constatações, as conclusões, as recomendações e os demais encaminhamentos.

Na conclusão do trabalho de campo, o auditor precisa ter certeza de que já realizou todas as entrevistas e coletou todos os dados necessários para analisar as evidências e, assim, desenvolver um parecer correto, que auxilie o cliente a melhorar o seu ambiente de TI aumentando a sua disponibilidade, o seu caráter confidencial e a sua integridade de dados.

Para o encerramento da auditoria, é necessário que todas as constatações sejam resumidas e avaliadas. Deve-se, para tanto:

- Discutir os achados e os possíveis planos de ação com o auditado;
- Definir conjuntamente um cronograma para a resolução dos problemas ou implantação das melhorias, de acordo com o risco e o impacto envolvidos;
- Encaminhar relatório final ao supervisor ou dirigente da área, observadas eventuais confidencialidades pertinentes;
- Estabelecer estratégia de acompanhamento da implantação dos encaminhamentos e arquivar relatório.

A comunicação da equipe com o auditado pode ocorrer em qualquer momento da auditoria e deve ser feita por meio de um canal escolhido. Assim, evitam distorções de fatos e atos e dá celeridade aos trabalhos.

O relatório final deve ser cuidadosamente elaborado, bem-organizado e escrito em linguagem simples e acessível.

f) Atualização do conhecimento permanente

O conhecimento em determinado período na auditoria é sempre útil para o período subsequente. Os registros eletrônicos, a avalição dos controles e a manutenção da documentação auxiliam as tarefas subsequentes minimizando retrabalhos e otimizando o tempo. São exemplos de informações relevantes:

- Descrição do processo de negócio;
- Avaliação do ambiente de controle;
- Documentação dos controles dos processos relevantes;
- Matriz de risco;
- Execuções dos testes;
- Falhas ou fraquezas nos testes;
- Programas de trabalho.

g) Avaliação da equipe

A organização de Trabalho da Auditoria de Sistemas de Informação vai desde o planejamento até a avaliação da equipe, passando pela programação, a execução, a revisão dos trabalhos até a emissão de relatórios; a estrutura da auditoria é crucial. Destaca-se a importância da atualização do conhecimento e a avaliação da equipe.

Visando aprimorar o crescimento dos integrantes da equipe de auditoria, esta etapa se propõe a avaliar o desempenho individual, enaltecendo os pontos fortes e reconhecendo as fraquezas com o intuito de estabelecer um plano de ação para o desenvolvido do profissional ainda mais qualificado.

Síntese do Capítulo

Neste capítulo nos propusemos a, juntos com você, compreender os princípios, os conceitos e os processos fundamentais associados à prática de auditoria de sistemas de informação. Esta síntese destaca os principais pontos abordados.

- Apresentação do papel crucial da auditoria de sistemas de informação no contexto organizacional, elucidando as razões e os motivos para a realização dessas auditorias.
- Apresentação das fases típicas do ciclo de vida da auditoria de sistemas de informação, desde o planejamento até a emissão do relatório final.
- Destaque para normas e os padrões internacionalmente reconhecidos que orientam a prática da auditoria de sistemas de informação, ressaltando a importância da conformidade.
- Exploração das responsabilidades e das competências necessárias para os profissionais que atuam na área de auditoria de sistemas de informação.

Essa síntese serve como uma base sólida para que os participantes compreendam o escopo e a importância da auditoria de sistemas de informação, preparando-os para aprofundamentos subsequentes em tópicos específicos.

A auditoria de SI avalia a eficácia dos sistemas de tecnologia da informação em organizações, abrangendo controles, desenvolvimento de sistemas, procedimentos de TI, infraestrutura, operação, desempenho e segurança da informação. Os objetivos da Auditoria de Sistemas de Informação incluem avaliar desempenho, verificar conformidade com regulamentos, garantir segurança e integridade dos dados, manter disponibilidade dos sistemas e preservar a confidencialidade das informações. O auditor desempenha um papel

crucial, exigindo ética, conhecimento técnico, independência, imparcialidade, planejamento e execução conforme padrões. Avalia controles, eficiência de processos e fornece recomendações.

São abordadas normas como COSO, ISO 27001, COBIT, entre outras, que servem como critérios para auditoria, cada uma com metodologias específicas alinhadas aos objetivos e as regulamentações aplicáveis. A etapa de avaliação da equipe visa avaliar o desempenho individual da equipe de auditoria, reconhecendo pontos fortes e identificando áreas para desenvolvimento, contribuindo para o crescimento e a qualificação dos profissionais. O capítulo abrange objetivos, papel do auditor, normas, organização de trabalho e avaliação da equipe, proporcionando uma visão abrangente da auditoria de SI.

Atividades de avaliação

1. Considerando a complexidade crescente dos ambientes de tecnologia da informação, como a auditoria de sistemas de informação pode garantir não apenas a conformidade das organizações com regulamentos, mas também a efetividade real na proteção dos ativos de informação e na melhoria dos processos organizacionais?
2. Dada a importância da conduta ética e da independência do auditor, como lidar com situações em que a pressão por resultados pode entrar em conflito com a necessidade de relatar objetivamente as fragilidades nos controles de segurança de TI? Como garantir a integridade e a imparcialidade em ambientes em que as pressões para atingir metas organizacionais são intensas?

Capítulo 2

Metodologia de Auditoria de Sistemas conforme Normas Internacionais ISACA/COBIT

Objetivos

- Compreender as metodologias e as diretrizes estabelecidas pelas normas internacionais desenvolvidas pela ISACA (*Information Systems Audit and Control Association*) e, em particular, pelo COBIT (*Control Objectives for Information and Related Technologies*).

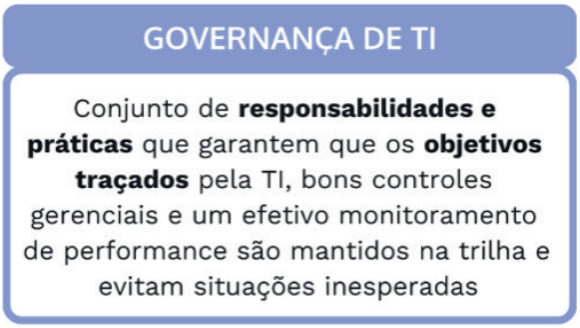
Introdução à metodologia de Auditoria COBIT

COBIT (Control Objectives for Information and Related Technologies) é uma estrutura usada para governança e administração dos ativos de TI, criada pela Associação de Auditoria e Controle de Sistemas de Informação, que adota a sigla ISACA (Information Systems Audit and Control Association). Uma das principais características do modelo COBIT é estar de acordo com os parâmetros do Commite of Sponsoring Organizations of the Treadway Commission's Internal Control – Integrated Framework (COSO).

A aplicação da metodologia COBIT na auditoria de sistemas de informação destaca-se por ser utilizada para avaliação de controles e cumprimento de processos de TI. Assim, pode-se dizer que COBIT é um conjunto de diretrizes baseadas em auditoria de processos, práticas e controles de TI, sendo uma referência mundial utilizada na avaliação de controles e cumprimento dos processos de TI.

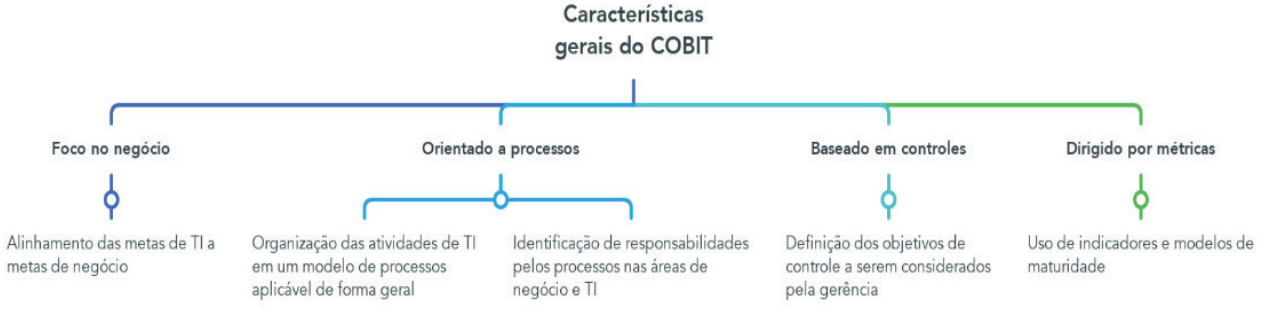
O COBIT fornece um conjunto de boas práticas para o processo de governança e de controle de sistemas de informação e tecnologia com o propósito de alinhar a TI com o negócio. Vale dizer que o COBIT não determina como os processos de TI devem ser estruturados, porém orienta sobre os controles que eles devem ter para que a TI cumpra seus objetivos em termos de governança.

Figura 01



A base principiológica do COBIT é constituída por objetivos de negócios que requerem informações produzidas por recursos de TI (dados, aplicações, infraestrutura e pessoas) que sejam gerenciados por processos controlados por seus objetivos de controle, indicadores de desempenho e indicadores de resultados com definição de responsabilidades e metas e que atendam aos critérios de qualidade, segurança e confiabilidade. O foco no negócio, a gestão de processos e uma análise precisa dos resultados proporcionados pela TI estão entre as principais características do COBIT.

Figura 02 - Características gerais do COBIT



Fonte: Adaptado pelos autores, 2024

A aplicação da metodologia COBIT foi projetado para utilização por três distintos públicos:

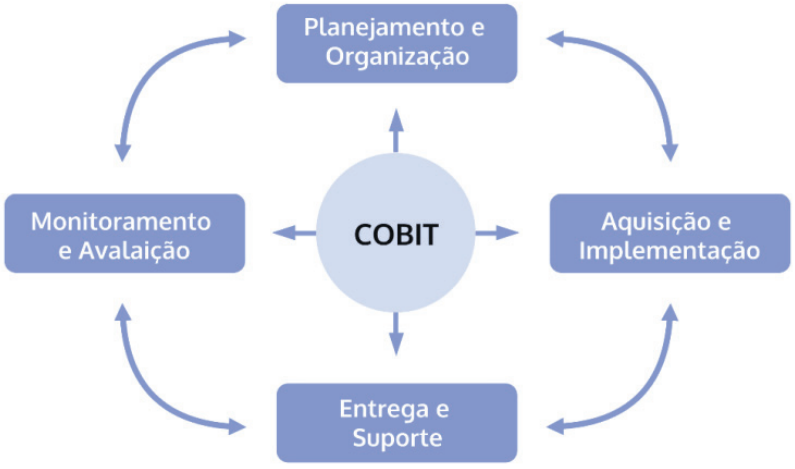
- Administradores: como instrumento de avaliação entre risco e investimento e controle do ambiente de TI;
- Usuários: certificação de segurança dos serviços fornecidos por TI (internos ou externos);
- Auditores de Sistemas: permitir uma avaliação padronizada para fundamentar a sua opinião sobre o TI da organização e permitir apresentar recomendações à administração sobre melhoria dos controles internos.

Em geral, esse modelo de gestão é empregado para aperfeiçoar os investimentos em Tecnologia da Informação, criando um ambiente mais favorável para os colaboradores usarem recursos tecnológicos avançados e eficientes. Dessa forma, o COBIT tem como uma das principais metas e vantagens fazer com que o *Return on Investments* ou Retorno sobre o Investimento (ROI) seja atingido em curto prazo, o que contribui para uma organização ter vantagem competitiva.

Vale destacar que o COBIT tem sido bastante útil para a tecnologia ser aplicada em todas as áreas de uma empresa, seguindo princípios como qualidade e segurança. Em razão disso, é necessário implementar estruturas, mecanismos e processos para que boas práticas de governança de TI estejam em uma corporação.

Esses procedimentos englobam iniciativas como o planejamento, passando pela execução e pela avaliação do desempenho. No total, o COBIT tem 34 processos e 210 pontos de controle que estão relacionados a iniciativas, como:

Figura 03



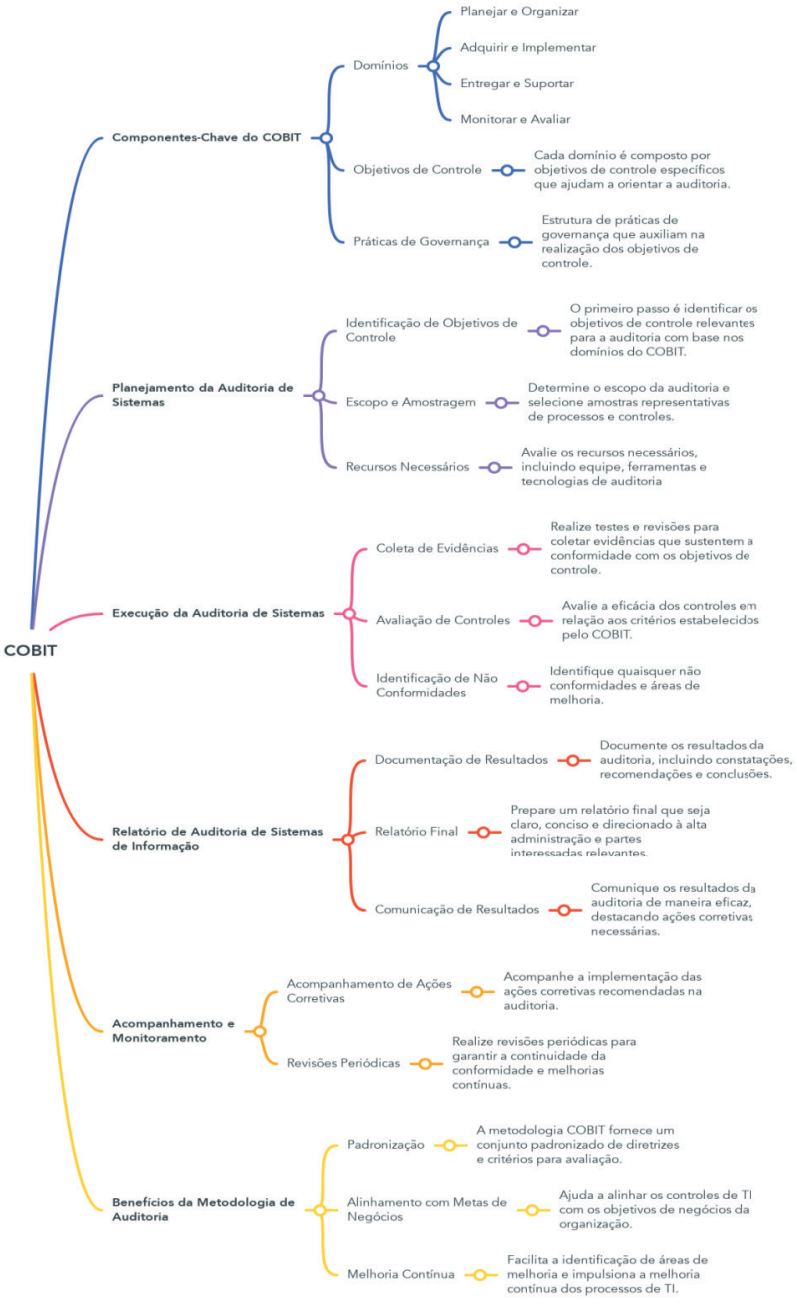
Com base nessas ações, essa metodologia de gestão passa a ser adotada para os processos de TI serem devidamente planejados, executados e monitorados com foco na redução de falhas e na melhoria contínua dos resultados.

Vale destacar que as metas de controle do COBIT estão diretamente relacionadas com as demandas de cada organização. Esse aspecto proporciona uma certa flexibilidade, mas isso não significa desconsiderar os parâmetros de qualidade ideais para uma governança de TI forte e eficiente.

Outro ponto importante é que o COBIT tem um foco no negócio da companhia. Isso não acontece com os outros modelos de gestão de TI que priorizam

apenas as atividades de Tecnologia da Informação. Esse aspecto faz com que os requisitos desse *framework* contribuam para a governança de TI estar adequada aos objetivos empresariais. Isso é muito importante para que os recursos tecnológicos estejam mais alinhados com os serviços e as demandas ligadas ao aumento da eficiência e à redução do tempo para finalizar as entregas.

Figura 04



1. A evolução do COBIT ao longo do tempo

O COBIT surgiu, em 1996, como um *framework* para auditoria e controles de TI. A ISACA lançou o COBIT em 1996, originalmente um conjunto de objetivos de controle para ajudar a comunidade de auditoria financeira a lidar melhor com ambientes relacionados à TI. Era inicialmente denominado "Control Objectives for Information and Related Technologies", embora, antes do lançamento, as pessoas o chamassem de "CobiT" como "Control Objectives for IT" ou "Control Objectives for Information and Related Technology."

No ano 2000, foi lançada a terceira versão com a inclusão de orientações para a gestão de TI. Em 2005 (COBIT 4.0) se tornou o *framework* de governança de TI, com a inclusão de processos de governança e conformidade (*compliance*). Percebendo valor na expansão do *framework* além do domínio de auditoria, a ISACA lançou uma versão mais ampla, a 2, em 1998 e a expandiu ainda mais, adicionando diretrizes de gerenciamento na versão 3 na década de 2000. O desenvolvimento de ambos os padrões [AS 8015]: Australian Standard for Corporate Governance of Information and Communication Technology, em janeiro de 2005, e o padrão mais internacional ISO/IEC DIS 29382 (que logo se tornou ISO/IEC 38500 em janeiro de 2007) aumentaram a conscientização sobre a necessidade de mais componentes de governança, tecnologias de informação e comunicação (TIC).

Em 2013, o COBIT 5 foi construído e integrado com base em seus vinte anos de desenvolvimento centrado na comunidade de auditoria de TI, tornou-se um *framework* integrador de governança e gestão corporativa de TI mais abrangente, compreensivo e aceito mundialmente.

Os principais fatores para o desenvolvimento do COBIT 5 incluem as necessidades de:

- Permitir que mais partes interessadas falem sobre o que eles esperam da tecnologia da informação e das tecnologias relacionadas (que benefícios e em qual nível de risco aceitável e a qual custo) e quais são suas prioridades para garantir que o valor esperado seja efetivamente obtido;
- Abordar a questão da dependência cada vez maior para o sucesso da organização em parceiros externos de TI e de negócios tais como terceirizadas, fornecedores, consultores, clientes, provedores de serviços na nuvem e demais serviços;
- Tratar a quantidade de informação, que tem aumentado significativamente;
- Administrar TI cada vez mais uma parte integrante do negócio;
- Cobrir o negócio de ponta a ponta e todas as áreas responsáveis pelas funções de TI.

Está alinhado com os mais atuais e relevantes padrões e *frameworks* utilizados, permitindo à organização utilizar o COBIT 5 como um integrador dos *frameworks* de governança e de gestão:

- De gestão corporativa: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000;
- Relacionados à TI: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI etc.

O COBIT 5 faz a integração do conteúdo dos principais *frameworks* publicados pelo ISACA, a saber:

- COBIT 4.1;
- Val IT - Usado para criar valor para o negócio por meio de investimentos de TI. Constituído por um conjunto de princípios orientadores e conjunto de processos e melhores práticas de negócios para apoiar a gestão executiva junto à TI na criação de valor;
- Risk IT - Dedicado a auxiliar no gerenciamento de riscos relacionados a TI;
- Business Model for Information Security (BMIS) - abordagem holística e orientada ao negócio para a gestão de segurança da informação;
- IT Assurance Framework (ITAF) - Modelo que fornece orientações sobre a concepção, realização e relatório de auditoria de TI, definindo termos e conceitos específicos para garantia de TI;
- Taking Governance Forward (TGF);
- Board Briefing on IT Governance 2nd Edition - Apresenta uma descrição abrangente dos conceitos de governança de TI como um livreto de referência ou como uma ferramenta para educar o board e a gerência executiva.

Além disso, ele se alinha a outros padrões de mercado como a Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO), Body Project Management of Knowledge (PMBOK), PRINCE2 e The Open Group Architecture Framework (TOGAF).

Assim, o COBIT 5 tornou-se uma estrutura corporativa alinhada e interoperável com outros *frameworks* e padrões anteriormente dispersos em diferentes *frameworks* da ISACA, tais como o COBIT 4.1, Val IT (valor de TI para o negócio), Risk IT (risco relacionado ao uso de TI), BMIS (segurança), integrou, também, outros conjuntos de boas práticas e metodologias, como padrões ISO, ITIL.

Figura 05

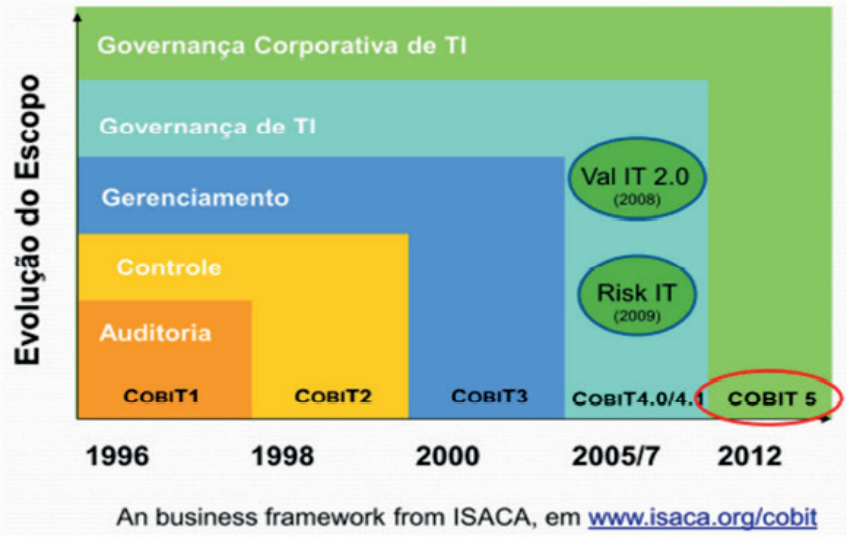


Figura 2 - Evolução do COBIT

O *framework* auxilia as organizações na criação de valor para TI, mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos. Desse modo, são objetivos do COBIT 5:

- Oferecer um framework abrangente que auxilia as organizações a otimizar o valor gerado pela TI;
- Permitir que a TI seja governada e gerenciada de forma holística para toda a organização;
- Criar uma linguagem comum entre TI e negócios para a governança e gestão de TI corporativa.

O COBIT 5, focado em governança corporativa de TI, buscou esclarecer a distinção entre governança e gestão fundamentando-se em cinco princípios:

Figura 06

Fonte: COBIT 5, p. 15, ISACA 2012

Em abril de 2019, foi lançada a versão atual do COBIT, com a denominação COBIT 2019, em que uma das principais atualizações são as orientações que permitem a personalização da governança de TI, ou seja, as diretrizes estão mais livres, alinhadas de acordo com as demandas de cada organização.

Uma das principais características da mais nova versão do COBIT abrange a preocupação com o gerenciamento de riscos, a governança e a segurança dos dados. Inegavelmente, esses aspectos necessitam de um olhar mais atento dos gestores. Afinal, os roubos e os vazamentos de dados causam prejuízos financeiros e de reputação para as marcas que podem ser irreversíveis.

O COBIT 2019 é dividido em quatro módulos:

1. Introdução e metodologia: traz os princípios básicos.
2. Objetivos de governança e gerenciamento: um guia complementar para auxiliar negócios a ter uma rotina de uso de dados com menos riscos.
3. Guia de design: um guia complementar, que facilita o desenvolvimento de um sistema de governança alinhado aos princípios da empresa.
4. Guia de implementação: um guia que orienta os times a integrar uma estratégia de governança focada nos padrões do COBIT à sua cadeia de trabalho.

Outro ponto importante é que as diretrizes do COBIT 2019 também levam em consideração a Lei Geral de Proteção de Dados (LGPD), que entrou plenamente em vigor em 2021, e a GDPR, que norteia os cuidados que as organizações precisam ter com os dados na União Europeia. Essa versão foi projetada para evoluir de maneira contínua, com atualizações mais fluidas e flexíveis. As orientações estão preparadas para o ambiente da transformação digital, em que as tendências mudam em alta velocidade. Em um cenário em que rotinas que envolvem a tecnologia são orientadas pela proteção dos dados pessoais, esse direcionamento é fundamental.

Com os ciberataques sendo cada vez mais sofisticados, é indispensável adotar boas práticas que minimizem consideravelmente os riscos. No Brasil, é cada vez mais comum ver companhias e órgãos públicos enfrentando paralisações dos serviços em virtude de ações cibercriminosas. Esse cenário, sem dúvida, mostra como a adoção correta do COBIT 2019 torna-se necessária.

O COBIT 2019 tem como um diferencial marcante em relação ao COBIT 5 a capacidade de descrever o papel das áreas com mais clareza, priorizando a manutenção de um sistema de governança sólido e mais seguro.

A versão mais nova também se mostra mais alinhada com os padrões internacionais de administração e governança de informações. Além disso, procura ser mais didática sobre as ferramentas que as organizações podem adotar para implementar um sistema de governança que atenda às mudanças provocadas pela transformação digital.

A inclusão de novos recursos on-line para a tomada de decisões e o uso de mecanismos mais inteligentes para medir a performance dos ativos e da equipe de TI são outros aspectos que diferenciam o COBIT 2019 do COBIT 5.

Ao implementar, de forma exemplar, o COBIT, uma instituição estará caminhando para alcançar um desempenho mais expressivo e eficiente por meio da Tecnologia da Informação. Afinal, terá mais condições de investir corretamente em ativos de TI e de seguir boas práticas para manter os serviços mais protegidos e disponíveis para o público-alvo.

Síntese do Capítulo

Neste capítulo, apresentamos uma introdução abrangente à estrutura COBIT, destacando seus princípios, seus objetivos e a relevância para a governança e a gestão de TI; uma metodologia específica de auditoria alinhada com os princípios do COBIT, abrangendo desde o planejamento até a emissão do relatório final. Foi também abordada a exploração do COBIT como

padrão para avaliação de conformidade, proporcionando insights sobre como medir a conformidade com seus requisitos e diretrizes e orientações para elaboração de planos de auditoria alinhados com as estruturas e requisitos do COBIT, incluindo estratégias para identificação de áreas críticas e de maior risco. O capítulo visa capacitar os participantes a aplicar efetivamente as metodologias de auditoria de sistemas de acordo com as normas internacionais da ISACA/COBIT. Ao compreender essas diretrizes, os profissionais estarão aptos a fortalecer a governança de TI e aprimorar a segurança da informação em ambientes organizacionais.

Atividades de avaliação

1. Considerando a constante evolução tecnológica e as mudanças nos ambientes de TI, como os profissionais de auditoria podem enfrentar os desafios de manter a relevância e a eficácia do COBIT ao longo do tempo? Quais são as estratégias para adaptar essa metodologia a cenários organizacionais dinâmicos?
2. O COBIT fornece um conjunto padronizado de controles e de diretrizes, mas as organizações podem ter necessidades e contextos diferentes. Como os auditores podem equilibrar a aplicação rigorosa do COBIT com a flexibilidade necessária para atender às particularidades de cada organização? Qual é o papel da personalização na eficácia da auditoria?

Capítulo 3

Papel do gestor, natureza das funções desempenhadas e sua importância

Objetivos

- Desenvolver uma compreensão abrangente das responsabilidades, das atribuições e do impacto dos gestores na área de auditoria de sistemas de TI;
- Discutir sobre o papel do gestor no contexto da auditoria de sistemas de TI;
- Descrever as responsabilidades específicas que os gestores têm no âmbito da auditoria de sistemas, desde a supervisão até a liderança estratégica;
- Descrever as diversas funções que eles desempenham incluindo a coordenação de equipes, a definição de estratégias, a gestão de riscos e a garantia da conformidade).

Introdução

No universo em constante transformação da auditoria de sistemas de informação (SI), os gestores assumem uma posição central, desempenhando um papel que evoluiu significativamente ao longo do tempo. Inicialmente, sua responsabilidade era principalmente supervisionar e coordenar atividades operacionais. No entanto, diante da crescente complexidade e interconexão dos sistemas de informação, os gestores de auditoria de TI passaram a desempenhar um papel estratégico e proativo.

No cenário atual, o gestor de auditoria de TI não apenas supervisiona, mas desempenha um papel vital na garantia da integridade, da confidencialidade e da disponibilidade dos dados. Ele se tornou um estrategista-chave na identificação de riscos e na determinação dos controles essenciais que precisam ser avaliados.

O sucesso de uma auditoria não apenas depende da expertise técnica, mas também da liderança eficaz dos gestores. Eles se inserem em uma posição relevante para contribuir/garantir a condução de auditorias bem-sucedidas, permitindo acesso às informações, motivando sua equipe acerca da importância das auditorias e, posteriormente, implementando as ações corretivas ou de aprimoramento.

Enfrentar a complexidade da auditoria de sistemas de informação exige mais do que habilidades técnicas. Requer uma liderança estratégica capaz de antecipar desafios, adaptar-se a mudanças rápidas e inspirar uma cultura organizacional centrada na segurança da informação.

Em resumo, o gestor de auditoria de TI é mais do que um supervisor. Sua função evoluiu de forma crucial para enfrentar os desafios dinâmicos da auditoria de sistemas de informação, proporcionando não apenas conformidade, mas também uma visão estratégica que impulsiona o sucesso organizacional.

1. Funções do Gestor em Auditoria de Sistemas de Informação

O gestor desempenha um papel vital na garantia de que as práticas de auditoria estejam alinhadas às regulamentações governamentais, aos padrões do setor e às políticas organizacionais, assegurando a conformidade e a integridade das ações. A integridade dos processos de auditoria é crucial para assegurar a confiança das partes interessadas e a credibilidade dos resultados.

É uma função central e estratégica na preparação, na execução e no acompanhamento das auditorias, contribuindo para a eficácia dos processos de auditoria e para a melhoria contínua da segurança e governança de TI. Abrange o planejamento inicial até o acompanhamento pós-auditoria, garantindo que cada fase seja executada eficientemente e que os objetivos se alinhem às metas organizacionais. São responsabilidades e características deste gestor:

1.1. Planejamento e Preparação

Os gestores são responsáveis por definir os objetivos da auditoria, o escopo, a equipe de auditoria e os recursos necessários. O planejamento da auditoria deve conter a formulação de estratégias para a auditoria de sistemas de TI, alinhadas aos objetivos organizacionais e a definição de metas mensuráveis e indicadores-chave de desempenho.

Os gestores devem assegurar que a auditoria de SI esteja alinhada com os objetivos estratégicos da organização, garantindo que os recursos sejam alocados de forma eficaz e considerando tanto as regulamentações externas quanto as necessidades específicas da organização.

Ao formular estratégias alinhadas aos objetivos organizacionais, o gestor assegura que a auditoria não seja apenas uma verificação de conformidade, mas um impulsionador estratégico para melhorias contínuas.

1.2. Apoio à Equipe de Auditoria

Os gestores fornecem suporte à equipe de auditoria, garantindo que ela tenha acesso às informações e recursos necessários para realizar seu trabalho de forma eficaz.

> Auditores são parte do modelo governamental de controle interno, mas eles não são responsáveis pela implementação dos procedimentos de controle numa organização. Este trabalho é específico do gestor." (INTOSAI, Padrões de Controle Interno)

Investir no desenvolvimento da equipe e na educação continuada deve ser uma prioridade para o gestor de auditoria de sistemas de TI. Isso inclui o fornecimento de treinamento contínuo, oportunidades de certificação e a promoção de um ambiente de aprendizado.

O gestor também desempenha um papel fundamental na construção de uma cultura organizacional que valoriza a segurança da informação e a proteção dos dados pessoais.

1.3. Coordenação e Supervisão

A coordenação de recursos humanos, tecnológicos e temporais é uma das tarefas primordiais do gestor. Ele alocará eficazmente a equipe de auditoria, garantindo que cada membro desempenhe um papel relevante. Essa coordenação abrange desde a definição de responsabilidades até o suporte à equipe, garantindo que todos os recursos necessários estejam disponíveis para o sucesso da auditoria.

O acompanhamento de tendências tecnológicas e a avaliação de seu impacto na auditoria de sistemas de TI, bem como a integração de ferramentas avançadas visam aprimorar a eficiência e a eficácia da auditoria.

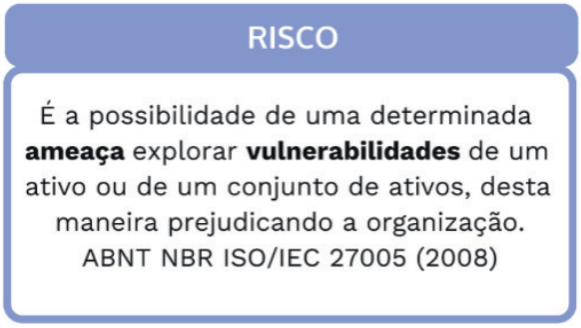
Durante a auditoria, o gestor é responsável pela supervisão contínua das atividades de auditoria, assegurando conformidade com os padrões e as normas estabelecidas. Ele fornece orientação à equipe, resolve problemas à medida que surgem e assegura que a auditoria esteja seguindo conforme o planejado. Essa vigilância contínua é essencial para garantir que todos os requisitos sejam atendidos e que a auditoria permaneça no caminho certo.

1.4. Gestão de Riscos e Controles

Identificar e avaliar riscos relacionados à segurança da informação é uma competência essencial do gestor. Ele trabalha para garantir que a equipe esteja ciente dos riscos potenciais e que os controles necessários estejam

implementados para mitigar esses riscos. Essa abordagem proativa contribui para a eficácia da auditoria e a segurança dos sistemas de TI.

Figura 07 - Significado de risco



Fonte: Autores, 2024

1.5. Comunicação e Relacionamento Intersetorial

A habilidade de comunicação é uma competência-chave do gestor. Ele deve ser capaz de se comunicar eficientemente com a equipe de auditoria, partes interessadas internas e externas e liderança sênior. A comunicação clara e transparente é vital para garantir que todos compreendam os objetivos da auditoria, os progressos realizados e os resultados esperados.

A comunicação dos resultados da auditoria à alta administração se propõe a apresentar as constatações da auditoria e o impacto nos objetivos de negócios. Assim, os gestores fornecem informações críticas à alta administração, permitindo que tomem decisões informadas com base nos resultados da auditoria.

A colaboração com setores de TI, de segurança da informação e outros correlatos é base para uma melhoria contínua. Ao apoiar a implementação de ações corretivas, os gestores contribuem para o aprimoramento dos processos de TI e para a mitigação de riscos.

1.6. Avaliação Pós-Auditoria

Após a conclusão da auditoria, o gestor desempenha um papel crítico na avaliação pós-auditoria. Ele revisa os resultados, garante que as ações corretivas sejam implementadas e identifica oportunidades para melhorias futuras. Esta fase é crucial para garantir que os aprendizados sejam incorporados e que a organização continue aprimorando seus processos de TI.

A ética é um elemento central na função do gestor de auditorias, uma vez que as decisões relacionadas à auditoria devem ser guiadas por princí-

pios éticos, assegurando a confidencialidade das informações e a imparcialidade na avaliação de controles e de riscos.

Em resumo, o gestor desempenha um papel multifacetado e estratégico na auditoria de sistemas de TI. Sua capacidade de liderar, inovar e manter altos padrões éticos contribui diretamente para o sucesso e a eficácia das atividades de auditoria, promovendo a segurança e a confiança nos sistemas de informação organizacionais.

> Neste contexto a auditoria surge como peça fundamental, que através dos seus procedimentos e técnicas, cria um cenário de confiança e segurança nos processos operacionais e na consolidação e tradução desses processos em dados e informações inseridos nestes sistemas de informática integrados. Os gestores não podem e não devem dividir seu tempo entre tomar decisões de criação e inovação dos produtos, serviços e estratégias de atuação das empresas no mercado, com a preocupação se as informações oferecidas a eles são ou não confiáveis e se estão ou não corretas, esta qualidade da informação deve ser algo implícito no negócio. (Rondinélio Ferreira Rodrigues)

Ele é o maestro que lidera a sinfonia da auditoria de sistemas de TI. Sua capacidade de planejar estrategicamente, coordenar eficientemente, gerenciar riscos, comunicar-se eficazmente e avaliar os resultados pós-auditoria é vital para o sucesso do processo. Em última análise, o gestor de coordenação não apenas lidera uma auditoria, mas facilita a busca contínua pela excelência nos sistemas de informação organizacionais.

Síntese do Capítulo

O capítulo busca apresentar uma visão abrangente das responsabilidades dos gestores na auditoria de sistemas de TI. A síntese deste capítulo destaca a contextualização da transformação do papel do gestor ao longo do tempo, passando de supervisão operacional para uma função estratégica; a identificação e exploração das responsabilidades específicas dos gestores, abrangendo supervisão, liderança estratégica e gestão de riscos e a descrição das diversas funções desempenhadas pelos gestores, incluindo coordenação de equipes, definição de estratégias e garantia da conformidade.

Destaca o papel estratégico dos gestores na gestão de riscos, determinação de controles e garantia da eficácia dos processos de auditoria e reconhece a importância da liderança dos gestores para o sucesso das auditorias, motivação da equipe e implementação eficaz de ações corretivas. Dá ênfase

na contribuição dos gestores para assegurar que a auditoria de sistemas de TI esteja alinhada com os objetivos estratégicos da organização. Descreve também o suporte oferecido pelos gestores à equipe de auditoria, incluindo acesso a recursos, investimento no desenvolvimento da equipe e adoção de tecnologias emergentes e destaca a coordenação eficaz de recursos e a supervisão contínua das atividades de auditoria, assegurando conformidade com padrões estabelecidos, reconhecendo a importância da comunicação eficiente com as partes interessadas e da colaboração com outros departamentos para o sucesso das auditorias.

Atividades de avaliação

1. Considerando a ênfase na liderança eficaz dos gestores na auditoria de sistemas, como encontrar o equilíbrio entre habilidades técnicas e habilidades de liderança? Em que medida a liderança influencia a eficácia das atividades de auditoria?
2. Diante do papel central dos gestores na definição de estratégias e na garantia da conformidade, como eles podem enfrentar desafios éticos, especialmente em situações em que a confidencialidade e a imparcialidade são cruciais? Qual é o papel dos princípios éticos na orientação das decisões dos gestores na auditoria de sistemas de TI?

Capítulo 4

Visão geral sobre desenvolvimento e gerenciamento de sistemas e programas

Objetivo

- Compreender de forma abrangente e atualizada os fundamentos, os desafios, as tendências e as considerações éticas no desenvolvimento e no gerenciamento de sistemas e programas de Tecnologia da Informação (TI);
- Apresentar conhecimentos sólidos sobre o ambiente dinâmico em que as organizações operam.

Introdução

No ambiente dinâmico da Tecnologia da Informação (TI), o desenvolvimento e o gerenciamento de sistemas e de programas são áreas essenciais que moldam a eficácia e a inovação nas organizações. À medida que as organizações buscam inovação e eficiência, o ciclo de desenvolvimento de sistemas emerge como um componente essencial, moldando a paisagem tecnológica e impulsionando a entrega de soluções alinhadas aos objetivos estratégicos. Desde a concepção de ideias até a implementação e a manutenção contínua, entender o ciclo de vida do desenvolvimento é fundamental para alcançar resultados eficazes.

Importante consolidar uma visão abrangente sobre o desenvolvimento e gerenciamento de sistemas e programas de TI, destacando suas interconexões e impactos na auditoria. Compreender os princípios e as práticas relacionados a esses aspectos é essencial para auditores de sistemas de informação, pois permite avaliar com precisão os controles e os processos de TI em uma organização. Na era da transformação digital, o papel desempenhado pelo desenvolvimento e o gerenciamento de sistemas e de programas tornou-se vital para a sustentabilidade e competitividade das organizações, bem como, nesse cenário complexo do desenvolvimento, o gerenciamento eficaz de projetos e programas de TI surge como um elemento-chave. Gerir escopo, tempo, custo e riscos, enquanto mantém a qualidade, exige abordagens pragmáticas e estratégias ágeis.

Metodologias ágeis, conhecidas por sua flexibilidade e resposta rápida às mudanças, contrastam com abordagens tradicionais, revelando a necessi-

dade de escolhas estratégicas adaptadas às demandas específicas de cada projeto. A governança de TI, por sua vez, proporciona a estrutura necessária para alinhar o desenvolvimento de sistemas aos objetivos organizacionais, assegurando decisões informadas e promovendo a conformidade. A segurança da informação, ética e responsabilidade social emergem como pilares críticos. A integração de práticas de segurança desde as fases iniciais do desenvolvimento, aliada a considerações éticas, torna-se imperativa na construção de soluções tecnológicas sustentáveis. Por fim, vê-se que a auditoria de sistemas de TI desempenha um papel essencial na garantia de conformidade, eficiência e segurança ao longo do ciclo de desenvolvimento.

1. Ciclo de vida do desenvolvimento de sistemas

O ciclo de vida do desenvolvimento de sistemas é um processo estruturado que abrange desde a concepção até a implementação e a manutenção de sistemas de informação. Importante apresentar as principais fases, como análise de requisitos, desenvolvimento, implementação, testes e manutenção. Muito mais que uma sequência linear de fases, o ciclo de vida do desenvolvimento de sistemas é um processo contínuo de adaptação e inovação.

Portanto, compreender cada fase é essencial para o sucesso da auditoria de sistemas de TI, garantindo que cada etapa seja executada com eficiência, segurança e alinhamento aos objetivos organizacionais. Esse ciclo é a espinha dorsal que sustenta a jornada da inovação tecnológica nas organizações modernas.

Da ideia à possibilidade: Identificar necessidades organizacionais, oportunidades de inovação e desafios a serem superados. Abrange a definição clara dos objetivos do sistema e a avaliação preliminar dos recursos necessários.

Análise de requisitos (entendendo as necessidades do usuário): compreender as necessidades dos usuários e do negócio. Documentar requisitos funcionais e não funcionais, identificar restrições e estabelecer critérios de sucesso.

Design do sistema: arquitetando a solução: Definir a estrutura, os componentes e as interfaces estratégicas para gerenciar dados, segurança e usabilidade.

Implementação (transformando conceitos em realidade): codificação do *design* previamente estabelecido. Programadores e desenvolvedores colaboram para transformar conceitos em códigos executáveis. Envolve a eficiência, a qualidade do código e a aderência aos padrões.

Validando a eficiência e a confiabilidade: Testes de unidade, integração e sistema para identificar falhas, garantir que o sistema atenda aos requisitos e assegurar a consistência entre as diversas partes. Correções e ajustes são implementados conforme necessário.

Implantação (colocando em produção): lançar o sistema em produção. Isso envolve a instalação de hardware, software e a migração de dados, garantindo uma transição suave do ambiente de desenvolvimento/teste para o ambiente de produção. Treinamento dos usuários e suporte inicial são aspectos críticos nessa etapa.

Manutenção e atualização (garantindo a longevidade do sistema): Correções de bugs, melhorias de desempenho e atualizações para atender a novas necessidades.

2. Metodologias Ágeis *versus* Metodologias Tradicionais

O cenário do desenvolvimento de sistemas é permeado por duas abordagens distintas, cada uma com sua filosofia, suas práticas e seus benefícios. As metodologias ágeis, representadas por estruturas como Scrum e Kanban, contrastam com as abordagens tradicionais, predominantemente exemplificadas pelo Modelo em Cascata. Assim, compreender as vantagens e as desvantagens de cada metodologia, destacando as características distintas e os contextos em que cada metodologia se destaca, é relevante para adaptar os processos de desenvolvimento às necessidades específicas da organização.

2.1. Metodologias Ágeis: adaptabilidade e colaboração em foco

As metodologias ágeis têm sua base na adaptabilidade, na flexibilidade e na colaboração contínua. O método Scrum, por exemplo, divide o desenvolvimento em iterações curtas chamadas de "sprints", proporcionando entregas incrementais e oportunidades regulares de revisão e ajuste. O foco está na entrega rápida de valor ao cliente, promovendo respostas ágeis às mudanças nos requisitos e nas condições do projeto.

Principais características

- Iterativo e Incremental: desenvolvimento por meio de ciclos curtos e entregas incrementais;
- Colaboração Contínua: interação constante entre desenvolvedores, clientes e demais partes interessadas;
- Adaptabilidade: capacidade de responder rapidamente a mudanças nos requisitos e nas condições do projeto;
- Feedback Regular: revisões frequentes para avaliação e ajuste contínuo.

Quando optar por Metodologias Ágeis

- Projetos dinâmicos e suscetíveis a mudanças frequentes nos requisitos;
- Necessidade de entregas rápidas e incrementais;
- Envolvimento ativo e colaboração contínua com os *stakeholders*.

2.2. Metodologias Tradicionais: estrutura e sequencialidade

Contrastando com a abordagem ágil, as metodologias tradicionais, representadas pelo Modelo em Cascata, seguem uma abordagem mais sequencial e estruturada. Cada fase do desenvolvimento é realizada de forma linear, com uma fase sendo concluída antes que a próxima comece. Isso implica ênfase na documentação detalhada e na compreensão completa dos requisitos antes do início do desenvolvimento.

Principais características:

- Sequencial: fases do projeto ocorrem em uma sequência linear;
- Documentação extensiva: ênfase na documentação detalhada antes do desenvolvimento;
- Menos flexibilidade: dificuldade em se adaptar a mudanças após o início do desenvolvimento;
- Entrega final: o produto é entregue ao final do ciclo de desenvolvimento.

Quando optar por metodologias tradicionais:

- Projetos com requisitos bem definidos e estáveis;
- Necessidade de documentação extensiva;
- Estruturação e controle rigorosos são prioritários.

Na prática, muitas organizações adotam abordagens híbridas, combinando elementos de metodologias ágeis e tradicionais com a expectativa de unir o melhor dos dois mundos. Essa flexibilidade permite que as equipes adaptem seu processo às necessidades específicas de cada projeto. A chave está em compreender as características únicas de cada metodologia e aplicá-las de maneira pragmática para otimizar o desenvolvimento de sistemas.

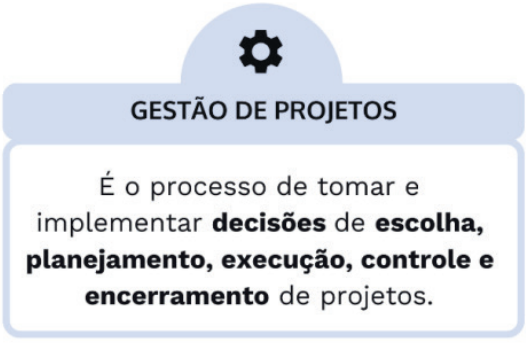
A escolha entre metodologias ágeis e tradicionais não é uma decisão única, mas uma consideração cuidadosa do contexto e dos requisitos do projeto. Ambas as abordagens oferecem vantagens distintas, e a decisão final deve refletir as dinâmicas do projeto, a cultura organizacional e a natureza dos requisitos. Ao compreender as nuances de cada metodologia, as equipes podem preparar um caminho de desenvolvimento que otimize a entrega de valor, mantendo a flexibilidade necessária para enfrentar os desafios em constante evolução.

3. Gerenciamento de projetos de TI

O gerenciamento de projetos de TI visa garantir a entrega bem-sucedida de soluções tecnológicas alinhadas aos objetivos estratégicos de uma organização. Em um ambiente dinâmico, em que a inovação é a chave para

a vantagem competitiva, o gerenciamento eficaz de projetos se torna um diferencial relevante.

Figura 08 - O que significa Gestão de projetos



Fonte: Autores, 2024

3.1. Elementos fundamentais

- Escopo do projeto: definição clara dos objetivos, das entregas e dos limites do projeto.
- Cronograma e prazos: estabelecimento de um cronograma realista com marcos e prazos definidos;
- Orçamento e recursos: alocação eficiente de recursos financeiros, humanos e tecnológicos;
- Comunicação efetiva: estabelecimento de canais claros de comunicação entre a equipe, *stakeholders* e liderança;
- Riscos e mitigações: identificação proativa de potenciais riscos, seguida por estratégias de mitigação.

3.2. Etapas da gestão de projeto

- Planejamento: elaboração de um plano detalhado com justificativas e objetivos, definição do escopo e estimativa de cronograma, custos e recursos;
- Organização: definição da equipe, infraestrutura e serviços necessários;
- Execução: implementação efetiva do plano, gerenciamento de equipe e resolução de problemas, avaliação do desempenho e controle da qualidade;
- Encerramento: entrega do resultado, documentação de lições aprendidas e transição de entregas.

3.3. Metodologias de gerenciamento de projetos

Método ou metodologia de gestão de projetos é um conjunto de princípios e de ferramentas para gerenciar o ciclo de vida do projeto, em outras palavras, uma linha de conduta para levar o projeto do começo ao fim.

Existem vários métodos de gestão, mas neste capítulo abordaremos os seguintes:

- **Métodos preditivos ou tradicionais**: planejamento de todo o projeto antes mesmo de iniciar;
- **Métodos ágeis:** foco na gestão do ciclo de vida do desenvolvimento do produto com entregas incrementais, permitindo adaptação contínua a mudanças nos requisitos
- **Kanban:** ênfase na visualização do trabalho com sinalização do progresso na execução das atividades. Não chega a ser um método,mas pode servir como ferramenta de apoio para qualquer método.

4. Referenciais de Gestão de Projetos

Um referencial ou guia para gerenciamento de projetos é um manual de instruções que orienta o processo de planejar, executar, controlar e encerrar o ciclo de vida de um projeto. Pode-se, então, dizer que o método é a doutrina e o referencial é o roteiro para aplicação do método. Os principais guias são:

- **PMBOK© (*Project Management Body of Knowledge*):** principal guia do método preditivo desenvolvido pela Project Management Institute (PMI). Ele abrange áreas-chave, como escopo, tempo, custo, qualidade, comunicação, riscos e aquisições.
- **PMD Pro© (*Project Management for Development*):** é uma adaptação do PMBOK e de outras metodologias para a realidade do setor social, é o manual para quem trabalha com organizações não governamentais (ONGs) e projetos sociais.
- ***The Scrum Guide*:** é o mais popular dentre as metodologias ágeis. No *Scrum*, os projetos são divididos em ciclos conhecidos como *sprints* (corrida). Para seus idealizadores, Ken Schwaber e Jeff Sutherland, não se trata de um método, mas sim de um *framework* (estrutura) que pode ser utilizado por todo e qualquer projeto de desenvolvimento de produto

O gerenciamento de projetos de TI é uma jornada dinâmica que exige equilíbrio entre metodologias eficazes, comunicação clara, adaptação contínua e uma compreensão profunda dos requisitos e dos riscos envolvidos. Ao abraçar as melhores práticas, ferramentas adequadas e uma abordagem estratégica, as organizações podem não apenas superar os desafios inerentes,

mas também alcançar a inovação sustentável e o sucesso em seus empreendimentos tecnológicos.

Figura 09 - Ferramentas para as diversas atapas de um projeto

Fonte: Autores, 2024

5. Gerente de Projetos

O sucesso de um projeto depende do desempenho eficaz da equipe. O gerente de projetos deve atuar como o maestro que coordena todos os seus elementos para alcançar os objetivos desejados. Em qualquer projeto, ele é a pessoa mais importante, uma vez que organiza a equipe e interage com todos os *stakeholders* a fim de viabilizar o projeto. São papéis gerenciais necessários:

Definir metas e objetivos: colaborar com os *stakeholders* para entender e definir claramente as metas e os objetivos do projeto. Inclui a identificação de requisitos específicos, expectativas de qualidade e critérios de sucesso. A habilidade de traduzir essas metas em tarefas tangíveis é essencial para guiar a equipe na direção certa.

Organizar e controlar: estabelecer um orçamento realista que abranja todas as necessidades do projeto, desde recursos humanos até tecnológicos. O controle financeiro é uma tarefa contínua, envolvendo a monitorização dos custos, a identificação de desvios e a implementação de medidas corretivas quando necessário. A gestão eficaz do orçamento assegura a viabilidade financeira do projeto.

Elaborar e gerir o cronograma: desenvolver um cronograma detalhado é uma das responsabilidades-chave do gerente de projetos. Isso envolve a identificação de marcos importantes, a sequência lógica das tarefas e a es-

timativa realista do tempo necessário para cada atividade. Durante a execução, o gerente de projetos monitora o progresso em relação ao cronograma, ajustando-o conforme mudanças e desafios surgem.

Administrar pessoas: a equipe é um ativo fundamental em qualquer projeto. O gerente de projetos é encarregado de construir e liderar uma equipe coesa, atribuindo tarefas de acordo com as habilidades individuais e motivando o grupo para alcançar os objetivos. A gestão de conflitos, o desenvolvimento de talentos e a manutenção de um ambiente de trabalho produtivo são partes integrantes desta responsabilidade. Saber trabalhar eficazmente com pessoas em equipes é uma competência fundamental para o gerente de projetos. A habilidade de equilibrar liderança, habilidades técnicas e o suporte de *framework*s é a fórmula para um gerenciamento de projetos de TI eficaz e bem-sucedido. Nesse papel o gestor trabalha com a dimensão humana e comportamental, ou seja, com as pessoas como pessoas, e não como recursos do projeto.

Implementar: é aqui que o gestor "faz o projeto acontecer", onde predominam as tarefas de executar e corrigir os planejamentos, administrar os recursos disponíveis, fornecer informações, avaliar o desempenho e cobrar providências. Embora seja inerente aos trabalhos da fase de execução, também é cabível nas fases iniciais, em que o gestor deve buscar assegurar os recursos e os consensos necessários para a eficácia do projeto.

Formular métodos: o gerente de projetos desempenha um papel crítico na orquestração de iniciativas de TI, garantindo que metas sejam atingidas, recursos sejam otimizados e que o projeto seja entregue dentro do escopo, do tempo e do orçamento previstos. Ao incorporar *framework*s estabelecidos, como PMBOK e SCRUM, os gerentes de projetos têm à disposição ferramentas robustas para navegar pelos desafios complexos e assegurar o sucesso do empreendimento.

6. Governança de TI e Gestão de Programas

A governança de TI refere-se ao conjunto de políticas, processos e estruturas que garantem que os investimentos em tecnologia da informação suportem e impulsionem os objetivos organizacionais. Ela visa assegurar transparência, responsabilidade, equidade, conformidade e entrega de valor em todos os aspectos relacionados à tecnologia.

A governança corporativa de TI, de acordo com o COBIT 5 (Control Objectives for Information and Related Technologies – referencial de boas práticas criado pela ISACA para a governança de tecnologia de informação):

> é uma visão da governança que garante que a informação e a tecnologia relacionada apoiem e possibilitem a estratégia da organização e a consecução dos objetivos corporativos. Também inclui a governança funcional de TI, ou seja, garantindo que as capacidades de TI sejam fornecidas com eficiência e eficácia.

O alinhamento estratégico na governança de TI implica garantir que as decisões relacionadas à tecnologia estejam integradas aos objetivos mais amplos da organização. Isso significa que cada iniciativa tecnológica, incluindo o desenvolvimento de sistemas, deve ser concebida e implementada com uma compreensão clara de como ela contribuirá para os objetivos estratégicos da empresa.

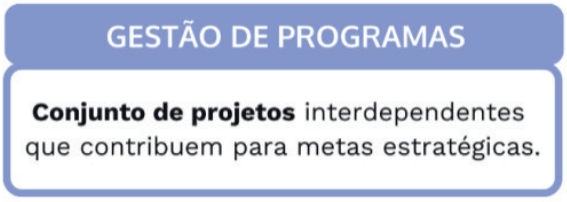
Ao iniciar um projeto de desenvolvimento de sistemas, é essencial compreender como esse sistema contribuirá para os objetivos estratégicos da organização. Isso envolve análise cuidadosa das necessidades do negócio, identificação de oportunidades de inovação e asseguração que a solução proposta esteja alinhada com a visão e as metas organizacionais.

São benefícios do alinhamento estratégico:

- A **maximização do valor de negócios;** que ocorre quando cada projeto de desenvolvimento de sistemas é concebido para agregar valor direto aos processos de negócios e, por conseguinte, aos objetivos estratégicos;
- A **priorização eficiente;** que acontece quando o alinhamento estratégico facilita a priorização de projetos, garantindo que aqueles mais críticos para os objetivos organizacionais recebam atenção prioritária;
- A **melhoria da eficiência operacional** em sistemas alinhados estrategicamente e projetados para otimizar e aprimorar os processos internos, melhorando a eficiência operacional.

O alinhamento estratégico entre a governança de TI e o desenvolvimento de sistemas é essencial para maximizar o impacto positivo da tecnologia na organização. Garantir que cada iniciativa tecnológica esteja alinhada com os objetivos estratégicos assegura que os recursos sejam direcionados eficientemente, proporcionando inovação e valor real para o negócio. O alinhamento estratégico é uma abordagem que transcende a implementação técnica, destacando a importância de cada projeto no contexto mais amplo da visão organizacional.

Figura 10 - Gestão de programas



Fonte: Autores, 2024

Segundo a norma NBR ISO/IEC 38500/2009, a Governança de Tecnologia da Informação compreende avaliar e direcionar o uso da TI para o suporte à organização e o monitoramento de seu uso com vistas à realização dos planos traçados. Essa norma define princípios da boa governança de TI que são:

Responsabilidade: Os indivíduos e grupos na organização devem compreender e aceitar as suas responsabilidades no fornecimento e na demanda de TI para, assim, garantir que a conduta ética da gestão para com o mercado, seus colaboradores, seus parceiros, na gestão financeira e fiscal.

Estratégia: A estratégia de negócio da organização tem em conta as capacidades de TI atuais e futuras. Esta estratégia diz respeito ao como será realizada a abordagem da organização para o contexto de Governança.

Aquisições: As aquisições de TI são feitas por razões válidas, com base e análise apropriada e continuada, com decisões claras e transparentes. Há um equilíbrio adequado entre os benefícios, oportunidades, custos e riscos, tanto no curto como no longo prazo.

Desempenho: A TI é adequada à finalidade de suporte da organização, à disponibilização de serviços e quanto aos níveis e qualidade dos serviços necessários para responder aos requisitos do negócio. O desempenho precisa ser medido e monitorado através de metas e métricas que viabilizem a gestão avaliar os resultados que estão sendo obtidos e a tomada de ações corretivas necessárias a eficácia do processo de governança.

Conformidade: A TI encontra-se em conformidade com a legislação e regulamentos aplicáveis, buscando uma postura transparente e adequada para com o mercado, a sociedade e a sustentabilidade.

Comportamento Humano: As políticas, práticas e decisões na TI revela respeito pelo Comportamento Humano, incluindo as necessidades atuais e a evolução das necessidades de todas as "pessoas no processo. Enfatizando a importância das pessoas para que as mudanças necessárias adoção da Governança de TI sejam alcançadas.

7. Qualidade e segurança no desenvolvimento de Sistemas e Programas

Garantir a qualidade e a segurança no desenvolvimento de sistemas e de programas é imperativo em um cenário em que a dependência da tecnologia é cada vez mais prevalente. Importante compreender as práticas, as metodologias e os princípios fundamentais que orientam a busca pela excelência em qualidade e segurança durante o ciclo de vida do desenvolvimento de software.

A integração de controles de segurança, desde o início do ciclo de vida do desenvolvimento de sistemas, é uma consideração central para a segurança do desenvolvimento destes. A garantia da qualidade no desenvolvimento de sistemas começa com **testes abrangentes** que abordam diferentes aspectos, como funcionalidade, desempenho e usabilidade. Os testes automatizados e manuais também devem ser aplicados ao longo do ciclo de vida do desenvolvimento.

As **revisões de código** por pares são práticas essenciais para identificar e corrigir problemas precocemente. Elas promovem a consistência no código, reduzindo erros e melhorando a qualidade geral, bem como, estabelecer e seguir **padrões de codificação** ajuda a manter a consistência e a facilitar a manutenção. Adotar padrões bem definidos contribuem para a garantia da qualidade do código produzido.

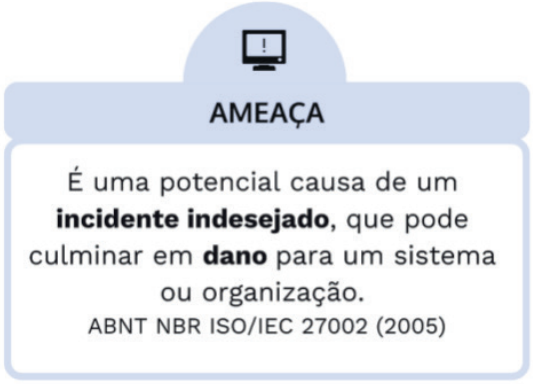
São **princípios de segurança** no desenvolvimento de sistemas:

- **Modelagem de ameaças:** identificar possíveis ameaças e vulnerabilidades desde o início do desenvolvimento é fundamental. A modelagem de ameaças ajuda a criar sistemas mais seguros ao antecipar e mitigar riscos.
- **Princípio do menor privilégio:** limitar o acesso e as permissões apenas ao necessário reduz a superfície de ataque. Isso significa que usuários e sistemas têm apenas os privilégios mínimos necessários para realizar suas funções.
- **Validação de entradas:** garantir que todas as entradas de dados sejam validadas antes de serem processadas evita vulnerabilidades comuns, como injeções de SQL e ataques de script.

7.1. O que são ameaças?

As ameaças podem ser definidas como sendo agentes ou condições incidentes que comprometem as informações e seus ativos, por meio da exploração de vulnerabilidades.

Figura 11 - Significado de ameaça

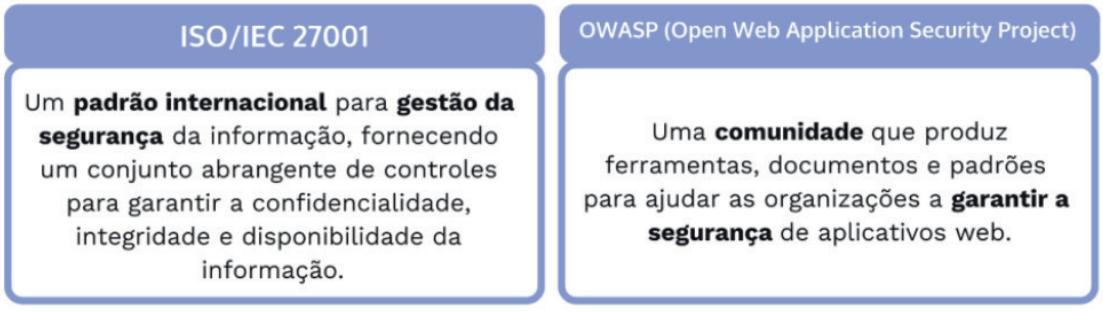


Fonte: Autores, 2024

7.2. O que são vulnerabilidades?

As vulnerabilidades podem ser definidas como fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações, que podem ser exploradas por ameaças e deixam que a ocorrência de um incidente de segurança aconteça, comprometendo negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

Figura 12 - Regras para gestão da segurança



Fonte: Autores, 2024

As vulnerabilidades, por si sós, não provocam acidentes de segurança, uma vez que são elementos passivos. Porém, quando possuem um agente causador, como ameaças, essa condição favorável provoca danos ao ambiente. São exemplos de vulnerabilidades:

Físicas

- Instalações prediais fora do padrão;
- Salas de equipamentos mal planejadas;

- A falta de extintores, detectores de fumaça e outros para combate a incêndio em sala com armários e fichários estratégicos;
- Risco de explosões, vazamentos ou incêndio.

Naturais

- Os computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades;
- Outros, como falta de energia, o acúmulo de poeira, o aumento de umidade e de temperatura etc.

Hardware

- Falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.

Software

- Erros na aquisição de softwares sem proteção ou na configuração podem ter como consequência uma maior quantidade de acessos indevidos, vazamentos de informações, perda de dados ou indisponibilidade do recurso quando necessário.

Mídias

- Discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.

Comunicação

- Acessos de intrusos ou perda de comunicação.

Humanas

- Rotatividade de pessoal;
- Falta de treinamento;
- Compartilhamento de informações confidenciais na execução de rotinas de segurança;
- Erros ou omissões;
- Ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismos, roubos, destruição da propriedade ou dados, invasões ou guerras.

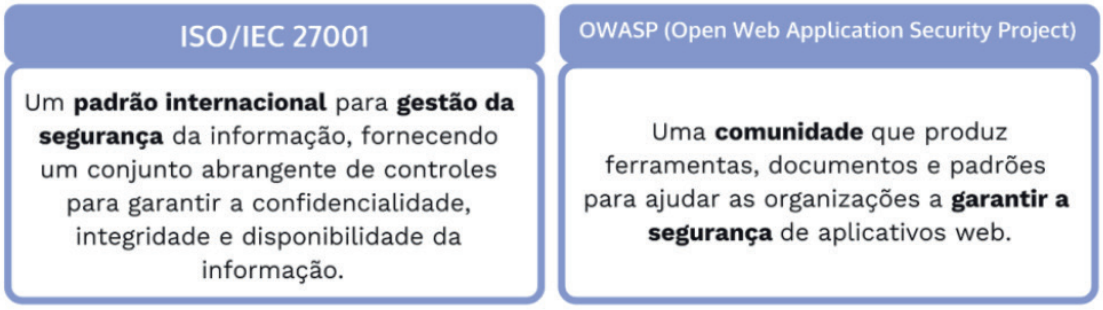
Boas práticas de qualidade e segurança

- **Feedback:** incorporar feedback contínuo dos usuários, testadores e revisores de código ajuda a identificar áreas de melhoria. Essa abordagem iterativa contribui para a evolução constante da qualidade e segurança.
- **Aprendizado com incidentes:** caso ocorram incidentes de segurança, é vital aprender com eles. Realizar análises pós-incidentes ajuda a identificar as causas raízes e implementar medidas preventivas.

A qualidade e a segurança no desenvolvimento de sistemas são alicerces essenciais para a construção de soluções tecnológicas resilientes e confiáveis. Adotar práticas de teste abrangentes, incorporar a segurança desde as fases iniciais do desenvolvimento e seguir padrões e normas estabelecidos são passos críticos para assegurar que os sistemas atendam não apenas às expectativas funcionais, mas também aos requisitos essenciais de segurança.

A busca contínua pela excelência nessas áreas é um compromisso vital para enfrentar os desafios em constante evolução no cenário de segurança cibernética e para fornecer sistemas robustos e confiáveis aos usuários finais.

Figura 13 - Regras para gestão de seguraça



Fonte: Autores, 2024

8. Desafios e Tendências em Desenvolvimento e Gerenciamento de Sistemas e Programas

O cenário do desenvolvimento e do gerenciamento de sistemas e de programas de TI está em constante evolução, apresentando uma série de desafios e tendências que impactam profundamente as organizações.

Os principais desafios em desenvolvimento e gerenciamento de sistemas são:

- **Complexidade tecnológica:** o aumento exponencial na complexidade das tecnologias, como inteligência artificial, computação em nuvem e internet das coisas, apresenta desafios significativos na integração e no desenvolvimento de sistemas robustos.
- **Ciclos de vida mais curtos:** a demanda por inovação rápida resulta em ciclos de vida de desenvolvimento mais curtos. Gerenciar essa velocidade acelerada sem comprometer a qualidade e a segurança tornou-se um desafio central.
- **Segurança cibernética:** a crescente sofisticação dos ataques cibernéticos exige uma abordagem proativa e contínua para garantir a se-

gurança dos sistemas. A proteção contra ameaças emergentes é uma preocupação constante.

- **Gerenciamento de dados massivos:** o volume crescente de dados requer estratégias eficazes de gerenciamento, desde a coleta até o armazenamento e a análise. A garantia da integridade e de confidencialidade dos dados é uma prioridade crítica.
- **Diversidade de plataformas:** a multiplicidade de plataformas, dispositivos e sistemas operacionais impõe desafios na criação de soluções que sejam interoperáveis e ofereçam uma experiência consistente ao usuário.
- **Segurança e privacidade dos dados:** a segurança dos dados armazenados é um desafio crítico, exigindo práticas rigorosas de proteção e conformidade com regulamentações.
- **Segurança da IoT:** a expansão da IoT aumenta os desafios de segurança, exigindo proteção contra vulnerabilidades e ataques em dispositivos conectados.

A seguir, apresentam-se tendências emergentes em desenvolvimento e gerenciamento de sistemas. O constante avanço tecnológico traz consigo a integração de tecnologias emergentes, como Inteligência Artificial (IA), Internet das Coisas (IoT) e Computação em Nuvem, que desempenham um papel significativo nos desafios e tendências do desenvolvimento e gerenciamento de sistemas.

- **Desenvolvimento ágil evoluído:** o desenvolvimento ágil continua a ser uma abordagem dominante, mas está evoluindo para incorporar práticas como DevOps e DevSecOps. A integração contínua e a entrega contínua (CI/CD) estão se tornando norma.
- **Computação quântica:** embora ainda em estágios iniciais, a computação quântica promete revolucionar a capacidade de processamento. A integração bem-sucedida dessa tecnologia representa uma tendência futura impactante.
- **Inteligência artificial e aprendizado de máquina:** a IA e o aprendizado de máquina estão moldando a automação, análise de dados e tomada de decisões.
- **Ética e transparência:** o uso responsável da IA envolve enfrentar questões éticas, garantindo transparência nas decisões algorítmicas e evitando viés em modelos.
- **Aprendizado contínuo:** a IA demanda aprendizado contínuo para se manter relevante. Isso requer atualização constante dos algoritmos para lidar com mudanças nas condições e nos dados.
- **IA explicável:** o desenvolvimento de modelos de IA mais compreensíveis e explicáveis é uma tendência crescente para aumentar a confiança e a aceitação.

- **Integração com processos de negócios:** a integração da IA nos processos de negócios para automatizar tarefas rotineiras e melhorar a tomada de decisões é uma tendência em ascensão.
- **Experiência do usuário aprimorada:** a combinação de IA, IoT e nuvem pode resultar em experiências do usuário mais personalizadas, eficientes e adaptáveis.
- **Edge computing:** com o aumento da Internet das Coisas (IoT), a computação de borda é uma tendência que complementa a IoT, permitindo o processamento local de dados para reduzir a latência e melhorar a eficiência.
- **Integração vertical:** a integração vertical da IoT em diversos setores, como saúde, agricultura e manufatura, é uma tendência que impulsiona a transformação digital.
- **Computação em nuvem híbrida:** a combinação de nuvens públicas e privadas para atender a diferentes requisitos de carga de trabalho é uma tendência em crescimento.
- **Habilidades multidisciplinares:** profissionais de TI precisam adquirir habilidades multidisciplinares que vão além da programação, incluindo compreensão de negócios, segurança cibernética e inteligência emocional para liderar equipes.
- **Cultura de inovação:** fomentar uma cultura organizacional que valoriza a inovação, o aprendizado contínuo e a adaptação rápida é fundamental para enfrentar os desafios e aproveitar as tendências emergentes.
- **Ênfase na segurança desde o início:** integrar a segurança desde as fases iniciais do desenvolvimento é crucial. Abordagens como DevSecOps promovem a segurança como parte integrante do ciclo de vida do software.
- **Parcerias estratégicas:** colaborações estratégicas com fornecedores, comunidade de desenvolvedores e especialistas em segurança são essenciais para enfrentar desafios complexos e manter-se atualizado com as tendências.
- **Governança eficaz:** implementar práticas de governança de TI que garantam alinhamento estratégico, conformidade e transparência é vital. Uma governança sólida orienta o desenvolvimento e o gerenciamento de sistemas para o sucesso.
- **Interoperabilidade:** garantir que diferentes tecnologias emergentes possam interagir e interoperar de maneira eficiente é um desafio crucial.
- **Gestão de dados integrada:** a integração de grandes volumes de dados provenientes de diferentes fontes exige estratégias integradas de gerenciamento para extrair valor.

8.1. Aspectos éticos no desenvolvimento de sistemas: responsabilidade e sustentabilidade

O desenvolvimento de sistemas de TI está intrinsecamente ligado a responsabilidades éticas e à busca pela sustentabilidade, refletindo o impacto significativo que essas tecnologias têm na sociedade, nos negócios e no meio ambiente. Importa reforçar os aspectos éticos no ciclo de vida do desenvolvimento de sistemas, destacando a necessidade de responsabilidade e práticas sustentáveis.

Desafios a serem destacados:

- **Viés algorítmico:** algoritmos podem refletir e perpetuar viés social. Garantir que sistemas não perpetuem discriminações é um desafio ético central.
- **Privacidade e proteção de dados:** a coleta e o uso de dados pessoais exigem responsabilidade ética para proteger a privacidade e garantir conformidade com regulamentações.
- **Consumo de recursos:** o desenvolvimento e a operação de sistemas podem resultar em grande consumo de energia e de recursos, impactando negativamente a sustentabilidade.
- **Descarte de equipamentos:** o descarte inadequado de equipamentos eletrônicos contribui para a poluição e os resíduos. O ciclo de vida sustentável dos sistemas é um desafio a ser enfrentado.
- **Tomada de decisão ética:** integrar considerações éticas nas decisões de desenvolvimento, garantindo que impactos sociais e ambientais sejam considerados.
- **Alinhamento com valores organizacionais:** assegurar que as práticas éticas e sustentáveis estejam alinhadas com os valores e a cultura da organização.
- **Conscientização da equipe:** garantir que todos os membros da equipe tenham uma compreensão sólida dos princípios éticos e sustentáveis.
- **Educação continuada:** a rápida evolução da tecnologia exige educação continuada para manter os profissionais de TI atualizados sobre questões éticas e sustentáveis.

Tendências importantes:

- **Sustentabilidade e responsabilidade social:** a conscientização ambiental e social está moldando o desenvolvimento e gerenciamento de sistemas. A busca por soluções sustentáveis e socialmente responsáveis é uma tendência crescente.

- **Ética na inteligência artificial:** a implementação de diretrizes éticas na IA, como transparência e justiça, está se tornando uma tendência, visando mitigar riscos e impactos negativos.
- **Desenvolvimento responsável:** as práticas de desenvolvimento responsável consideram o impacto social e ético desde as fases iniciais, promovendo a construção de sistemas éticos por design.
- **Eficiência energética:** a busca por eficiência energética na infraestrutura de TI e o uso de energias renováveis são tendências que visam reduzir o impacto ambiental.
- **Economia circular:** a adoção de princípios de economia circular, como reciclagem e reutilização de componentes eletrônicos, está ganhando destaque.
- **Comitês de ética em tecnologia:** a criação de comitês dedicados à ética em tecnologia, responsáveis por orientar e supervisionar práticas éticas, é uma tendência emergente.
- **Relatórios de impacto ético:** a transparência sobre as práticas éticas e sustentáveis, através de relatórios dedicados, está se tornando uma prática adotada por organizações comprometidas.
- **Treinamento em ética digital:** programas de treinamento específicos para ética digital estão sendo desenvolvidos para capacitar os profissionais a enfrentar dilemas éticos no trabalho.
- **Inclusão de ética em currículos de TI:** a inclusão de ética e sustentabilidade nos currículos de cursos de TI é uma tendência que visa preparar futuros profissionais para desafios éticos.
- **Inovação sustentável:** a integração eficaz de tecnologias emergentes oferece oportunidades para inovação sustentável, melhorando a eficiência operacional e reduzindo impactos ambientais.

O desenvolvimento e o gerenciamento de sistemas e programas de TI enfrentam desafios dinâmicos, mas também são impulsionados por tendências empolgantes que moldam o futuro da tecnologia. Ao enfrentar os desafios com inovação, resiliência e uma mentalidade de aprendizado contínuo, as organizações podem posicionar-se para tirar proveito das tendências emergentes e prosperar em um ambiente tecnológico em constante transformação.

A integração de tecnologias emergentes, como IA, IoT e computação em nuvem, traz desafios significativos, mas também abre novas fronteiras de oportunidades para o desenvolvimento e gerenciamento de sistemas e programas de TI. Navegar nessas complexidades requer uma abordagem estratégica, centrada na ética, na segurança e na inovação contínua. Ao enfrentar os desafios

com resiliência e abraçar as tendências emergentes, as organizações podem posicionar-se para liderar no cenário dinâmico da tecnologia da informação.

O reconhecimento da responsabilidade ética e a busca pela sustentabilidade no desenvolvimento de sistemas são essenciais para construir um futuro tecnológico que beneficie a sociedade como um todo.

9. Auditoria em Projetos de Desenvolvimento e Programas de TI

A auditoria em projetos de desenvolvimento e programas de TI desempenha um papel crucial na garantia de conformidade, eficiência operacional e entrega bem-sucedida de soluções tecnológicas.

9.1. Objetivos

- **Assegurar conformidade:** verificar se as práticas adotadas no projeto estão em conformidade com padrões internos, regulamentações externas e melhores práticas de governança.
- **Avaliar eficiência operacional:** analisar a eficácia dos processos de desenvolvimento e gestão, identificando áreas de melhoria e oportunidades para otimização.
- **Mitigar riscos:** identificar e avaliar proativamente os riscos associados ao projeto, contribuindo para a implementação de medidas preventivas e corretivas.

9.2. Métodos e Abordagens de Auditoria em TI

- **Auditorias internas e externas:** auditorias internas são conduzidas pela própria organização, enquanto as externas podem ser realizadas por terceiros independentes. Ambas são essenciais para garantir uma avaliação imparcial.
- **Auditorias contínuas:** realizar auditorias ao longo do ciclo de vida do projeto, desde a fase de concepção até a implementação e a manutenção contínua. Isso permite uma intervenção precoce em caso de desvios.
- **Auditorias especializadas:** em certos projetos críticos, pode ser benéfico envolver auditores especializados em segurança, conformidade ou áreas específicas de tecnologia.

9.3. Benefícios

- **Garantia de qualidade:** a auditoria contribui para a garantia da qualidade, identificando práticas inadequadas e promovendo melhorias contínuas nos processos de desenvolvimento.

- **Redução de riscos:** a avaliação regular dos riscos ajuda a mitigar potenciais problemas antes que impactem significativamente o projeto, resultando em maior probabilidade de sucesso.
- **Transparência e responsabilidade:** a auditoria promove a transparência nos processos e responsabilidade pelas ações, estabelecendo uma cultura organizacional centrada na conformidade e na eficácia.

9.4. Fases da Auditoria em Projetos de TI

- **Planejamento:** definir os objetivos da auditoria, bem como o escopo, os recursos necessários e o cronograma. Identificar áreas críticas a serem avaliadas.
- **Execução:** conduzir a auditoria de acordo com o plano estabelecido, coletando evidências, entrevistando envolvidos e analisando documentos relevantes.
- **Relatório e comunicação:** documentar os resultados da auditoria, destacando áreas de conformidade e não conformidade, além de fornecer recomendações para melhorias. Comunicar esses resultados às partes interessadas.
- **Acompanhamento:** monitorar a implementação das recomendações e a eficácia das ações corretivas, garantindo a resolução de problemas identificados.

9.5. Auditoria em Projetos Ágeis: Considerações Específicas

- **Flexibilidade no escopo:** em projetos ágeis, o escopo da auditoria pode ser mais flexível, adaptando-se às iterações e as mudanças frequentes.
- **Envolvimento contínuo:** auditorias contínuas são particularmente úteis em ambientes ágeis, proporcionando feedback regular e oportunidades para ajustes.

9.6. Ferramentas e Tecnologias de Apoio à Auditoria:

- **Software de auditoria:** ferramentas específicas de auditoria podem automatizar processos, facilitar a análise de dados e melhorar a eficiência da equipe de auditoria.
- **Monitoramento em tempo real:** utilizar ferramentas que permitam o monitoramento contínuo de indicadores-chave, promovendo uma abordagem proativa.

A auditoria em projetos de desenvolvimento e programas de TI é um pilar essencial da governança, proporcionando uma avaliação imparcial e objetiva da conformidade, da eficiência e dos riscos. Ao incorporar práticas de auditoria ao longo do ciclo de vida do projeto, as organizações podem garantir

a entrega bem-sucedida de soluções tecnológicas, alinhadas aos objetivos estratégicos e em conformidade com as normas regulatórias. A busca contínua pela excelência por meio da auditoria reflete o compromisso com a transparência, responsabilidade e aprimoramento contínuo no ambiente dinâmico da tecnologia da informação.

Síntese do Capítulo

Este capítulo oferece uma visão holística e atualizada sobre o panorama do desenvolvimento e do gerenciamento de sistemas e de programas de Tecnologia da Informação (TI). Ao abordar fundamentos, desafios, tendências e considerações éticas, busca-se preparar os alunos para enfrentar os complexos desafios e aproveitar as oportunidades nesse ambiente dinâmico. Assuntos abordados neste capítulo:

- Exploração do ciclo de vida do desenvolvimento, desde a concepção até a manutenção, enfatizando práticas eficazes de gerenciamento de programas e projetos.
- Análise dos desafios atuais, incluindo questões éticas, segurança cibernética e a integração de tecnologias emergentes, como inteligência artificial e internet das coisas.
- Exame das tendências tecnológicas que estão moldando o cenário de TI, incluindo desenvolvimento ágil, computação em nuvem e o impacto da inteligência artificial nos sistemas.
- Integração de uma abordagem ética desde as fases iniciais do desenvolvimento, destacando a importância da transparência, privacidade e responsabilidade social.
- Preparação dos estudantes para entender o contexto tecnológico em que as auditorias de sistemas ocorrem, enfatizando a interseção entre desenvolvimento de sistemas e práticas de auditoria.

Ao sintetizar esses elementos, o capítulo visa oferecer uma base abrangente que prepara os estudantes para atuar de forma eficaz em um ambiente tecnológico em constante evolução, equilibrando inovação, ética e sustentabilidade.

Atividades de avaliação

1. Considerando a rápida evolução das tecnologias de desenvolvimento de sistemas e programas, bem como a crescente importância da sustentabilidade e ética nesse contexto, reflita sobre como as organizações podem equilibrar inovação, eficiência e responsabilidade social em seus processos de desenvolvimento e gerenciamento de TI.
2. Considerando o papel fundamental do auditor de TI no contexto do desenvolvimento e do gerenciamento de sistemas, reflita sobre os desafios e as oportunidades que esse profissional enfrenta no cenário atual de rápidas transformações tecnológicas.

Capítulo 5

Controles e Segurança em Sistemas - Planos de Contingência em TI

Objetivos

- Compreender de forma abrangente, o papel vital da auditoria na garantia da prontidão e da eficácia dos planos de contingência em TI, contribuindo para a segurança e a estabilidade operacional da organização.
- Entender como a auditoria do plano de contingência contribui diretamente para fortalecer a resiliência organizacional, garantindo a capacidade de resposta a eventos imprevistos e protegendo a continuidade dos negócios.
- Reforçar a ideia de que a preparação para contingências é uma responsabilidade coletiva, envolvendo não apenas a equipe de TI, mas toda a organização, incluindo a alta administração e demais partes interessadas.

Introdução

A segurança da informação é um pilar fundamental para garantir a integridade, confidencialidade e disponibilidade dos sistemas de Tecnologia da Informação (TI). Os planos de contingência em TI são projetados para ajudar as organizações a se prepararem para interrupções imprevistas e a minimizar o impacto dessas interrupções nos processos de negócios.

Sem segurança da informação, a organização terá de lidar com riscos e possíveis ameaças para sua operação e para o alcance dos objetivos gerais, o que afetará sua credibilidade.

Enquanto cresce a complexidade e o papel da tecnologia da informação, a segurança se torna um tópico cada vez mais importante em Auditorias de TI sendo um fator crítico nas atividades organizacionais podendo acarretar danos em áreas como (INTOSAI, 2013):

- Lei – Violação de requisitos legais e regulatórios.
- Reputação – Danos à reputação organizacional, quebra na confiabilidade perante outras organizações ou até dano à imagem do governo ou unidade da federação.
- Finanças – Multas, desperdício de recursos.
- Produtividade – Redução da efetividade e eficiência em um projeto ou um serviço ofertado pela organização.

- Vulnerabilidade – Dados e sistemas acessados de maneira não autorizada propiciam o ingresso de softwares maliciosos que podem abrir caminho para invasões.

Esses danos podem ser causados por:

- Falhas de segurança;
- Acesso não autorizado a sites externos;
- Exposição da informação – Divulgação de bens organizacionais, dados pessoais e informações sensíveis.

O plano de contingência é abordado no domínio de "Gestão de Incidentes e Resposta a Incidentes" na ISO/IEC 27002:2005. Especificamente, o ponto de controle relacionado ao plano de contingência está dentro do controle 16.1.5, que trata da prontidão para incidentes e emergências cujo objetivo é assegurar a prontidão e a eficácia da resposta a incidentes e emergências.

Pondera-se a necessidade de planos de contingência em TI como parte integral da estratégia de segurança. Ao compreender os fundamentos, desenvolver e implementar planos eficazes e integrá-los com outros controles de segurança, as organizações estarão mais bem preparadas para enfrentar os desafios dinâmicos do cenário de TI contemporâneo. A auditoria constante e o comprometimento com a melhoria contínua garantem que esses planos evoluam junto com as ameaças e os desafios em constante mutação.

1. Controles e a segurança de informação

A segurança de informações visa garantir a integridade, a confidencialidade, a autenticidade e a disponibilidade das informações processadas pela instituição. A integridade, a confidencialidade e a autenticidade de informações estão intimamente relacionadas aos controles de acesso.

1.1. O que é integridade de informações?

Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação a inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

1.2. O que é confidencialidade de informações?

Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.

1.3. O que é autenticidade de informações?

Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

As fontes de informação típicas em TI durante uma Auditoria podem ser (INTOSAI, 2016):

- Diagramas de fluxos de sistema, fluxo de dados, fluxos de processo etc;
- Documentos de desenvolvimento de sistemas como Especificação de Requisitos de Usuário;
- Dados eletrônicos;
- Outras informações disponíveis na organização relacionadas às suas funções, ao controle e aos sistemas de monitoramento etc., como formulários, informações orçamentárias, relatórios diversos incluindo de auditorias anteriores e de controles internos etc;
- Políticas, procedimentos e outras orientações;
- Os usuários do sistema.

1.4. O que é disponibilidade de informações?

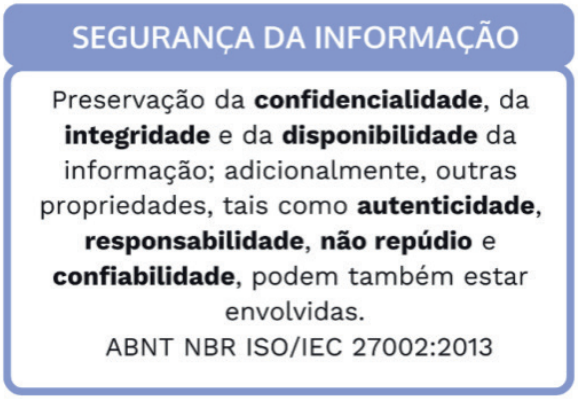
Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

2. A importância de zelar pela segurança de informações

A informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou

de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações.

Figura 14 - Segurança da informação



Fonte: Autores, 2024

Segundo a ABNT NBR ISO/IEC 27002:2013, "a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware".

2.1. Segurança física

A segurança física refere-se às medidas e às práticas destinadas a proteger os ativos físicos relacionados aos sistemas de informação de uma organização. Em relação a tal elemento, a ISO/IEC 27002:2005 oferece orientações específicas que as organizações podem adotar para proteger seus ativos físicos relacionados à informação. Aqui estão alguns pontos relevantes:

- A norma destaca a importância de identificar e proteger as áreas que contêm informações confidenciais, sensíveis ou críticas para a organização. Isso inclui a implementação de controles de acesso físico.
- Recomenda a implementação de controles de acesso físico, como fechaduras, cartões magnéticos, biometria ou outros meios, para restringir o acesso não autorizado a instalações e a áreas que abrigam ativos de informação.
- Sugere a utilização de sistemas de monitoramento por câmeras de vigilância para a detecção e o registro de atividades suspeitas em áreas críticas. Isso contribui para a prevenção de incidentes e fornece registros visuais para investigações.

- Aborda a necessidade de garantir a segurança do ambiente físico onde os ativos de informação estão localizados. Isso inclui a proteção contra ameaças como incêndios, inundações, terremotos e outros desastres naturais.
- Recomenda a implementação de medidas de segurança física para proteger os equipamentos de TI contra roubo, danos ou manipulação indevida. Isso pode incluir salas cofre e gabinetes com fechaduras.
- Aborda a segurança física relacionada ao armazenamento seguro de mídias de backup e outros meios que contenham informações sensíveis. Isso visa garantir a confidencialidade e integridade dos dados.
- Destaca a necessidade de implementar medidas de proteção física contra ameaças externas, como intrusões físicas, vandalismo e outros ataques que possam comprometer a segurança dos ativos de informação.
- Sugere a garantia de iluminação adequada em áreas críticas para facilitar a vigilância e desencorajar atividades suspeitas durante períodos não operacionais.
- Recomenda a proteção física de cabos e de conexões para evitar danos acidentais ou intencionais que possam resultar em interrupções nos serviços de TI.
- Aborda a necessidade de práticas seguras para o descarte de equipamentos eletrônicos obsoletos, garantindo a eliminação adequada de dados e a conformidade com regulamentações ambientais.

Essas diretrizes contribuem para a criação de uma abordagem holística à segurança física, complementando outras medidas de segurança da informação previstas na norma.

2.2. Segurança lógica

A segurança lógica consiste em avaliar o nível de segurança e de controle empregados com recursos tecnológicos nos processos de um determinado sistema de informação. Tais processos correspondem aos programas de computador, bem como aos procedimentos mecanizados ou aos manuais que compõem as rotinas operacionais e dos controles do sistema de informação. Em uma auditoria de sistemas, representa revisar e avaliar todos os procedimentos operacionais e de controle para transformação dos dados e das informações.

A norma ISO/IEC 27002:2005 aborda diretrizes específicas para segurança lógica. A seguir estão alguns dos pontos destacados pela norma em relação à segurança lógica:

- A norma orienta a implementação de controles de acesso lógico para garantir que apenas usuários autorizados tenham acesso a sistemas, apli-

cativos e dados específicos. Isso inclui autenticação forte, autorização e revisões regulares dos direitos de acesso.

- Sugere práticas para o gerenciamento seguro de senhas, incluindo políticas de complexidade, armazenamento seguro, expiração regular e orientações para os usuários sobre boas práticas de senha.
- Recomenda o uso de criptografia para proteger dados em trânsito e armazenados. Isso abrange comunicações seguras, criptografia de dados sensíveis e gestão adequada de chaves criptográficas.
- Aborda o gerenciamento seguro de sistemas operacionais, aplicativos e outros ativos lógicos. Isso inclui a aplicação de *patches* de segurança, configurações adequadas e a implementação de políticas de segurança.
- Destaca a importância do monitoramento contínuo de atividades de sistemas, detecção de eventos de segurança e resposta a incidentes. Isso inclui a implementação de ferramentas de monitoramento e a definição de procedimentos de resposta a incidentes.
- Recomenda práticas para a identificação e gestão de vulnerabilidades nos sistemas. Isso envolve avaliações regulares de segurança, análise de riscos e a aplicação de correções de segurança.
- Aborda a importância da geração, proteção e análise de logs de eventos. Isso contribui para a auditoria eficaz, o monitoramento de conformidade e a investigação de incidentes de segurança.
- Recomenda diretrizes para o desenvolvimento seguro de software, incluindo práticas de codificação segura, revisões de código e testes de segurança durante o ciclo de vida do desenvolvimento.
- Aborda medidas para garantir a segurança de redes e comunicações, incluindo a proteção contra ameaças como ataques de negação de serviço (DDoS) e monitoramento de tráfego de rede.
- Destaca a importância de controlar e proteger dispositivos móveis que acessam os recursos da organização. Isso inclui a implementação de políticas de uso, criptografia e controle remoto.
- Orienta sobre a implementação de práticas seguras para backup de dados e recuperação de sistemas em caso de incidentes. Isso contribui para a continuidade operacional e a proteção contra perda de dados.

Segundo a norma, a segurança da informação é adquirida a partir da implantação de um conjunto de controles apropriados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implantados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atingidos.

3. Pontos de Controle

A ISO/IEC 27002:2005, apresenta um conjunto de pontos de controle que são diretrizes e boas práticas para a implementação de controles de segurança da informação. Esses pontos de controle são agrupados em diversas categorias, cobrindo diferentes aspectos da segurança da informação. Aqui estão algumas das categorias e exemplos de pontos de controle descritos na norma.

1. Política de Segurança da Informação
2. Organização da Segurança da Informação
3. Gestão de Ativos
4. Segurança em Recursos Humanos
5. Acesso a Sistemas e Ativos
6. Criptografia
7. Segurança Física e do Ambiente
8. Operações de Sistemas
9. Controle de Acesso
10. Desenvolvimento e Manutenção de Sistemas
11. Relacionamento com Fornecedores
12. Conformidade
13. Gestão de Incidentes e Resposta a Incidentes

Esses são apenas alguns exemplos de pontos de controle presentes na ISO/IEC 27002:2005. Cada controle fornece orientações específicas e práticas recomendadas para ajudar as organizações a estabelecerem um ambiente seguro de gestão da informação.

O controle 16.1.5 inclui a necessidade de estabelecer e manter procedimentos para a resposta a incidentes e emergências, bem como planos de contingência que considerem a continuidade do negócio. Dentro desse ponto de controle, é esperado que a organização desenvolva e mantenha um plano de contingência para lidar com incidentes de segurança da informação e outras emergências relacionadas à continuidade do negócio. Esse plano de contingência deve ser elaborado considerando os riscos identificados e as necessidades específicas da organização.

A elaboração de um plano de contingência eficaz é vital para garantir que a organização esteja preparada para responder de maneira adequada a incidentes de segurança da informação, minimizando impactos e garantindo a continuidade das operações críticas.

4. Definição e Objetivos dos Planos de Contingência em TI

Um Plano de Contingência em Tecnologia da Informação (TI) é um conjunto de procedimentos e estratégias elaborados para lidar com eventos inesperados que possam interromper, comprometer ou ameaçar a operação normal dos sistemas de informação de uma organização. Esses eventos, conhecidos como contingências, podem incluir desde falhas de hardware, ataques cibernéticos, desastres naturais até interrupções de serviços críticos.

4.1. Plano de Segurança, Plano de Contingência e Plano de Continuidade

A segurança de TI contempla, como medida que possibilita a proteção dos recursos computacionais, o plano de segurança (normas e procedimentos de segurança preventiva e detectiva), o plano de contingência (instruções de segurança corretiva e restauração do ambiente de TI) e o plano de continuidade (conjunto de medidas que combinam ações preventivas e de recuperação).

Em uma perspectiva de auditoria de TI, deve-se observar os seguintes aspectos:

1. Plano de segurança:
   a. Objetividade e clareza na prevenção e detecção de sinistros;
   b. Controle e obediência às normas de segurança por parte dos usuários envolvidos;
   c. Existência de esquemas de manutenções preventivas com respaldo contratual para os equipamentos de TI;
   d. Cópias de programas e arquivos vitais de sistemas de informação guardados em locais independentes da área de computação;
   e. Teste regular e periódico da adequação do plano de segurança.
2. Plano de contingência:
   a. Identificação do pessoal responsável para a aplicação do plano de contingência
   b. Comunicação aos responsáveis pelo plano de contingência com referência a alterações que comprometam a utilização do site alternativo;
   c. Existência de provisões de reserva de TI com outros usuários em caso de quebra ou instabilidade de equipamentos;
   d. Compatibilidade de sistemas operacionais ou softwares com as instalações de outros usuários;
   e. Clareza nas prioridades de ativação das funções dos sistemas de informação em caso de sinistro;

f. Verificação de adequação de rotinas para reconstrução de arquivos;

g. Explicação detalhada para a correção e restauração do ambiente de TI, em termos de hardware e software;

h. Revisão e teste regular e periódico do plano de contingência.

3. Plano de Continuidade:

a. Riscos a que está exposta a instituição, probabilidade de ocorrência e os impactos decorrentes (tanto aqueles relativos à escala do dano como ao tempo de recuperação);

b. Consequências que poderão advir da interrupção de cada sistema computacional;

c. Identificação e priorização de recursos, sistemas, processos críticos;

d. Tempo-limite para recuperação de recursos, sistemas, processos;

e. Alternativas para recuperação dos recursos, sistemas, e processos, mensurando custos e benefícios de cada alternativa.

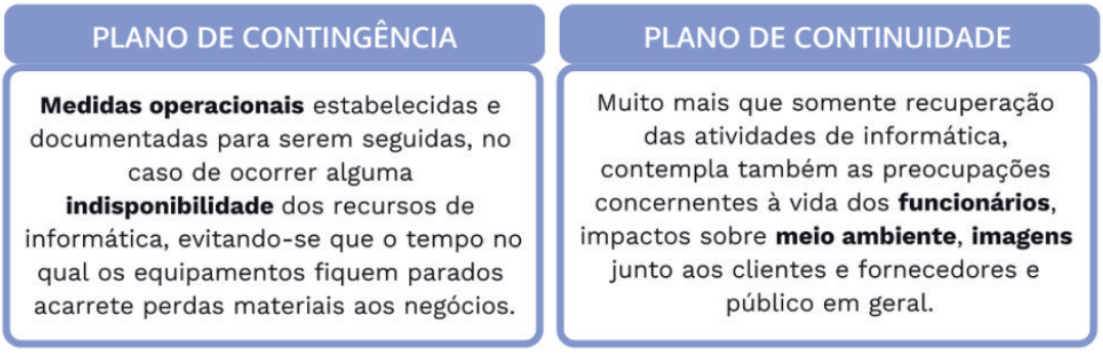
Um Plano de Continuidade do Negócio consiste em um conjunto de estratégias e de procedimentos que devem ser adotados quando a instituição ou uma área se depara com problemas que comprometem o andamento normal dos processos e a consequente prestação dos serviços.

Já o Plano de Contingência em TI é elaborado com o propósito de garantir a continuidade operacional, minimizar impactos adversos e acelerar a recuperação em situações de eventos inesperados que possam comprometer a infraestrutura de TI. Os objetivos específicos incluem os seguintes:

- Garantir que as operações críticas da organização possam continuar ou ser restauradas rapidamente após a ocorrência de uma contingência, reduzindo o tempo de inatividade.
- Minimizar perdas e proteger a integridade dos dados, sistemas e outros ativos de TI durante eventos adversos, como falhas de hardware, ataques cibernéticos ou desastres naturais.
- Reduzir os custos associados a interrupção operacional, perda de dados e recuperação, contribuindo para a estabilidade financeira da organização.
- Evitar danos à reputação da organização ao garantir uma resposta eficaz a eventos que possam comprometer a segurança ou a disponibilidade dos serviços.
- Garantir que a organização cumpra regulamentações e padrões específicos que exigem a implementação de planos de contingência em setores regulamentados, como saúde, finanças e governo.

- Estabelecer procedimentos claros para uma resposta imediata e coordenada à contingência, envolvendo equipes designadas e partes interessadas relevantes.
- Minimizar o tempo necessário para recuperar sistemas críticos, dados e operações normais, otimizando a eficiência e a eficácia do processo de recuperação.
- Promover a conscientização e preparação contínuas da equipe para situações de contingência, garantindo uma resposta rápida e eficiente.
- Realizar testes e exercícios regulares para avaliar a eficácia do plano, identificar áreas de melhoria e garantir que a equipe esteja familiarizada com os procedimentos.
- Manter o plano atualizado para refletir as mudanças na infraestrutura de TI, na tecnologia, nos riscos emergentes e nas melhores práticas do setor.

Figura 15 - Planos de contingência e de continuidade



Fonte: Autores, 2024

Ao alcançar esses objetivos, um Plano de Contingência em TI se torna uma ferramenta essencial para fortalecer a resiliência organizacional diante de eventos inesperados e garantir a sustentabilidade das operações críticas de TI.

5. Fases do Planejamento de Contingência em TI

O planejamento de contingência em TI envolve várias fases essenciais para garantir a eficácia do plano e a capacidade de resposta diante de eventos adversos. As fases típicas são listados a seguir:

5.1. Análise de Riscos

Nesta fase, são identificados e avaliados os riscos potenciais e as vulnerabilidades que podem afetar a operação dos sistemas de TI. Isso inclui

ameaças como falhas de hardware, ataques cibernéticos, desastres naturais e outros eventos que podem interromper as operações normais. Deve-se avaliar as ameaças internas e externas que podem afetar a disponibilidade, integridade e confidencialidade dos dados, ameaçando, assim, a **continuidade dos negócios**.

O processo de avaliação de riscos inclui a identificação e a análise de:

- Processos e ativos relacionados a sistemas;
- Potenciais ameaças que podem afetar a confidencialidade, integridade ou disponibilidade de sistemas;
- Vulnerabilidades de sistema e ameaças associadas;
- Potenciais impactos e riscos oriundos de ameaças;
- Exigências de proteção para a efetiva mitigação de riscos;
- Seleção de medidas de segurança apropriadas e análise de relações de risco.

A categorização dos riscos por impacto e probabilidade é uma prática valiosa. Segundo a norma ABNT NBR ISO/IEC 27002:2013, risco é a "combinação da probabilidade de um evento e de suas consequências" (ABNT NBR ISO/IEC 27002:2013).

Figura 16 - Continuidade do negócio

Fonte: Autores, 2024

5.2. Definição de Objetivos e Escopo

Estabelecimento claro dos objetivos do plano de contingência, estabelecendo metas mensuráveis para a recuperação e continuidade dos sistemas. O escopo determina quais sistemas, processos e recursos estão cobertos pelo plano, evitando ambiguidades durante a execução.

A definição do escopo da auditoria de TI se dá basicamente na delimitação da abrangência de sua avaliação, que, segundo Bergami, (2013) pode abarcar:

- Processos de negócio apoiados em TI;
- Governança e Gestão de TI;
- Aquisições de TI;
- Contratos de prestação de serviços de TI;
- Sistemas da Informação;
- Bancos de dados;
- Segurança da Informação;
- Infraestrutura física.

Para analisar esses vários segmentos de tecnologia a Auditoria de TI deve avaliar:

- A confiabilidade de informações processadas por sistemas;
- A segurança física do ambiente de processamento de TI de uma organização;
- A conformidade do funcionamento de um sistema em relação a normas, padrões e resultados esperados.
- A adequação da infraestrutura da área de TI para o processamento dos sistemas e das informações;
- A qualidade dos produtos, dos sistemas e dos serviços oferecidos pela área de TI ao negócio;
- A legalidade e eficiência da contratação de bens e serviços de TI por parte da organização.

Desenvolvimento de procedimentos de resposta: nesta fase, são elaborados procedimentos detalhados que devem ser seguidos em diferentes cenários de contingência. Isso inclui ações imediatas para mitigar impactos, a mobilização de equipes responsáveis e a comunicação eficaz durante a resposta.

Desenvolvimento de estratégias de recuperação: define estratégias para a recuperação rápida e eficiente dos sistemas, aplicativos e dados essenciais. Inclui planos de backup, procedimentos de restauração e testes de integridade dos dados.

Desenvolvimento de planos de comunicação: estabelece protocolos claros de comunicação, tanto internamente entre as equipes quanto externamente com partes interessadas. Define quem deve ser informado, como e quando.

Treinamento e conscientização: foca em programas de treinamento para garantir que as equipes estejam familiarizadas com os procedimentos do plano. A conscientização sobre a importância da preparação para contingências é reforçada regularmente.

Testes e exercícios simulados: realiza testes regulares para avaliar a eficácia do plano por meio de simulações de contingências. Esses exercícios envolvem a equipe na prática de procedimentos e identificam áreas de melhoria.

Atualização e manutenção: um plano de contingência é uma ferramenta dinâmica que deve ser atualizada regularmente para refletir as mudanças na infraestrutura de TI, nas ameaças potenciais e nas melhores práticas. Ajustes após cada simulação ou contingência real são incorporados.

Revisão e auditoria: realiza revisões periódicas do plano para garantir sua relevância e eficácia contínua. Auditorias regulares ajudam a validar a conformidade do plano com padrões regulatórios e normativos.

Documentação detalhada: todo o plano é documentado de forma detalhada, incluindo procedimentos passo a passo, responsabilidades, contatos de emergência, detalhes de backup e recuperação, e qualquer outra informação essencial.

Essas fases são interdependentes e garantem que o plano de contingência seja abrangente, prático e capaz de lidar efetivamente com diversas situações de contingência em TI.

6. Componentes de um Plano de Contingência em TI

1. **Resumo Executivo:** uma visão geral concisa do plano, destacando objetivos, escopo, responsabilidades-chave e principais procedimentos.
2. **Introdução:** contextualização do plano, explicando sua importância, seu propósito e suas relação com a estratégia de gestão de riscos da organização.
3. **Declaração de Política:** uma declaração formal que delineia a postura da organização em relação à contingência em TI, estabelecendo princípios e diretrizes gerais.
4. **Objetivos do Plano:** definição clara dos objetivos que o plano visa alcançar, como a garantia da continuidade operacional e a proteção dos ativos de TI.
5. **Estrutura Organizacional:** descrição das funções e das responsabilidades de cada membro da equipe durante uma situação de contingência, incluindo líderes de equipe, comunicadores, técnicos, entre outros.
6. **Análise de Riscos e Avaliação de Impacto:** documentação detalhada dos riscos identificados, sua probabilidade de ocorrência e impacto potencial nas operações de TI.
7. **Procedimentos de Resposta:** instruções passo a passo para responder a diferentes cenários de contingência, incluindo ações imediatas, mobilização de recursos e comunicação.

8. **Recuperação de Sistemas e Dados:** estratégias para a recuperação rápida e eficiente de sistemas, aplicativos e dados essenciais, abrangendo procedimentos de backup, restauração e testes de integridade dos dados.
9. **Planos de Comunicação:** detalhamento dos protocolos de comunicação, incluindo listas de contatos, métodos de notificação, mensagens pré-definidas e canais de comunicação internos e externos.
10. **Treinamento e Conscientização:** programas de treinamento contínuo para garantir que a equipe esteja familiarizada com os procedimentos do plano e conscientização sobre a importância da preparação.
11. **Testes e Exercícios Simulados:** procedimentos para a realização regular de testes e exercícios simulados para avaliar a eficácia do plano, identificar áreas de melhoria e garantir a prontidão da equipe.
12. **Atualização e Manutenção:** protocolos para a revisão e atualização periódica do plano para refletir mudanças na infraestrutura de TI, riscos emergentes e melhores práticas do setor.
13. **Documentação Detalhada:** documentação abrangente de todos os aspectos do plano, proporcionando um recurso fácil de seguir durante situações de contingência.
14. **Registro de Eventos e Lições Aprendidas:** um componente que registra eventos passados, contingências reais ou simuladas, e as lições aprendidas para aprimoramento contínuo do plano.
15. **Revisão e Auditoria:** procedimentos para revisões regulares do plano, garantindo sua conformidade com padrões regulatórios e normativos, além da realização de auditorias.
16. **Anexos e Recursos:** inclusão de qualquer documento adicional, ferramentas ou recursos que possam ser necessários durante uma contingência.

Ao integrar esses componentes de maneira eficaz, um plano de contingência em TI torna-se uma ferramenta completa para garantir a resiliência operacional em face de desafios imprevistos.

7. Estratégias para responder a eventos de interrupção, incluindo recuperação de desastres e planos de continuidade.

São procedimentos específicos em diversos cenários de contingência, incluindo as ações imediatas para mitigar impactos, a mobilização de equipes responsáveis, a notificação de partes interessadas e a coordenação de esforços. A descrição detalhada (documentação) dos procedimentos a serem seguidos em diferentes situações de contingência deve ser capaz de restaurar sistemas e processos críticos, garantindo uma resposta organizada e eficiente.

Todo o plano é documentado de forma detalhada, incluindo procedimentos passo a passo, responsabilidades, contatos de emergência, detalhes de backup e recuperação, e qualquer outra informação essencial. A documentação serve como guia que descreve os métodos e as ferramentas para a recuperação rápida e eficiente de sistemas, aplicativos e dados essenciais. Inclui estratégias de backup, periodicidade de backup, procedimentos de restauração e testes de integridade dos dados, bem como:

- **Backup e Recuperação de Dados:** estratégias para fazer backup e recuperar dados de maneira eficaz.
- **Equipes de Resposta a Incidentes:** formação de uma equipe de resposta a incidentes e definição de papéis e responsabilidades, destacando a importância da coordenação e comunicação eficazes.
- **Treinamento e Conscientização:** detalha programas de treinamento para garantir que as equipes estejam familiarizadas com os procedimentos do plano. A conscientização contínua sobre a importância da preparação para contingências é enfatizada
- **Comunicação e Notificação:** estabelece protocolos claros de comunicação, tanto internamente entre as equipes quanto externamente com partes interessadas, como clientes, fornecedores e autoridades regulatórias. Isso inclui listas de contatos, métodos de notificação e mensagens de comunicação pré-definidas.
- **Testes e Exercícios:** inclui estratégias para testar a eficácia do plano por meio de simulações regulares de contingências. Esses exercícios envolvem a equipe na prática de procedimentos e identificam áreas de melhoria. Os resultados dos testes são documentados para avaliação posterior.
- **Revisão, atualização e Manutenção:** um plano de contingência é uma ferramenta dinâmica que deve ser atualizada regularmente para refletir as mudanças na infraestrutura de TI, nas ameaças potenciais e nas melhores práticas. Além disso, ajustes após cada simulação ou contingência real são incorporados para otimizar a eficácia do plano.

A integração eficaz desses componentes em um plano de contingência não apenas fortalece a resiliência da organização, mas também contribui significativamente para uma estratégia de gestão de riscos abrangente. A capacidade de antecipar, responder e se recuperar de contingências em TI é essencial para garantir a continuidade operacional, a segurança dos dados e a confiança das partes interessadas.

Assim, um plano de contingência deve estar intrinsecamente ligado à estratégia de gestão de riscos, agindo como uma ferramenta proativa para mitigar impactos negativos. Ele contribui para:

- Identificação Antecipada de Riscos: ao antecipar possíveis cenários de contingência, que podem impactar a operação dos sistemas de TI, desde falhas de hardware até ameaças cibernéticas, o plano permite que a organização esteja preparada para enfrentar desafios antes mesmo de ocorrerem.
- Resposta Rápida e Eficaz: ao definir procedimentos claros, o plano facilita uma resposta rápida e coordenada diante de situações adversas, minimizando danos e interrupções.
- Minimização de Impactos Financeiros e Reputacionais: uma resposta eficiente a contingências ajuda a reduzir os custos associados a interrupções operacionais e preserva a reputação da organização.
- Conformidade Regulatória: em muitos setores, a existência de planos de contingência é um requisito regulatório. Sua implementação contribui para a conformidade com normas e padrões específicos.

Em resumo, um Plano de Contingência em TI é uma peça fundamental na gestão de riscos, capacitando as organizações a enfrentarem incertezas com resiliência e agilidade, garantindo a continuidade operacional e a segurança dos sistemas de informação.

8. Auditoria de Planos de Contingência

Na visão da ISACA (2010), a auditoria de TI é responsável por fazer uma revisão e avaliação dos riscos do ambiente de trabalho dos sistemas de informação que suportam os processos de negócio. A atividade da auditoria de TI tem como intuito ajudar a organização por meio da identificação e avaliação de exposições ao risco que sejam significativas, bem como contribuir para o avanço dos mecanismos de gestão de risco e de controle dos sistemas de informação.

No ponto de vista do IIA (2005), a auditoria de TI tem que aferir a capacidade dos controles dos sistemas de informação para resguardar a organização contra as ameaças mais relevantes e deve fornecer evidência de que os riscos residuais são pouco prováveis de causar danos significativos à organização e às suas partes interessadas, os *stakeholders*.

Uma auditoria de um plano de contingência em TI é um processo sistemático e independente que avalia a eficácia, a adequação e a prontidão do plano para lidar com eventos adversos. Aqui está uma descrição geral de como essa auditoria pode ser conduzida:

1. **Preparação:** antes de iniciar a auditoria, os auditores devem revisar documentos relevantes, como o plano de contingência, registros de eventos passados, e quaisquer relatórios de testes ou simulações anteriores. Eles também podem realizar entrevistas com as partes envolvidas para entender o contexto operacional.

2. **Avaliação da Documentação:** os auditores examinam minuciosamente o plano de contingência em TI, verificando se todos os componentes essenciais estão presentes. Isso inclui a revisão da declaração de política, objetivos do plano, procedimentos de resposta, estrutura organizacional, análise de riscos, entre outros.
3. **Verificação da Atualização do Plano:** os auditores confirmam se o plano está atualizado, refletindo as mudanças na infraestrutura de TI, na tecnologia, nos riscos emergentes e nas melhores práticas do setor. Qualquer desatualização pode representar uma vulnerabilidade.
4. **Entrevistas e Comunicação:** os auditores entrevistam membros-chave da equipe responsável pelo plano de contingência. Isso inclui líderes de equipe, gerentes de TI, coordenadores de comunicação e outros envolvidos na execução do plano. A comunicação entre as partes interessadas é avaliada.
5. **Avaliação de Treinamento e Conscientização:** os programas de treinamento são revisados para garantir que a equipe esteja bem preparada para lidar com situações de contingência. A conscientização sobre a importância da preparação é avaliada, assim como a participação em exercícios simulados.
6. **Testes e Exercícios:** os resultados de testes e exercícios simulados anteriores são revisados. Os auditores avaliam se os procedimentos de resposta foram seguidos adequadamente, identificam áreas de melhoria e verificam se as lições aprendidas foram incorporadas.
7. **Avaliação da Eficácia da Recuperação:** os procedimentos de recuperação são analisados para garantir a eficácia na restauração de sistemas, dados e operações críticas. Isso inclui a revisão dos métodos de backup, processos de restauração e a integridade dos dados após a recuperação.
8. **Revisão de Comunicação e Notificação:** a eficácia dos protocolos de comunicação é avaliada, incluindo a rapidez e precisão na notificação de partes interessadas durante uma situação de contingência. O alcance e a clareza das mensagens são verificados.
9. **Registro de Eventos e Lições Aprendidas:** os registros de eventos passados e as lições aprendidas são analisados. Os auditores verificam se as melhorias recomendadas foram implementadas e se a organização aprendeu com experiências anteriores.
10. **Relatório de Auditoria:** ao concluir a auditoria, os auditores preparam um relatório detalhado, destacando as descobertas, as recomendações de melhorias e os observações. Esse relatório é compartilhado com a equipe responsável pelo plano de contingência e a alta administração.

Ao final, a auditoria deve ser capaz de certificar que:

- Há planos desenvolvidos que contemplem todas as necessidades de contingências;
- Esses planos são suficientemente abrangentes para cobrir aspectos físicos, lógicos, de redes, de propriedades intelectuais, de pessoas, transacionais, entre outros;
- A equipe de contingência está preparada para as eventualidades;
- Esses planos são testados periodicamente;
- Os backups são atualizados;
- Os mesmos backups podem ser recuperados com pouca ou nenhuma dificuldade;
- Há relatórios gerenciais que facilitam o acompanhamento dos procedimentos;
- Os relatórios são confiáveis.

Uma auditoria de plano de contingência em TI é fundamental para garantir que a organização esteja preparada para lidar com eventos adversos, protegendo a continuidade operacional e a segurança dos ativos de TI.

9. Auditoria de segurança de informações

Esse tipo de auditoria em ambientes informatizados decide a postura ou a situação da empresa em relação à segurança das informações. Ela avalia a política de segurança da informação e, também, os controles relacionados a aspectos de segurança e controles que influenciam o bom funcionamento dos sistemas da organização.

O objetivo dos Controles Gerais de TI é assegurar o desenvolvimento e a implementação de aplicações eficientes e efetivas, assim como que a utilização destas resulte em dados relevantes que sejam armazenados em banco de dados, em arquivos ou ainda sirva como parâmetro de entrada para interações com outras aplicações (INTOSAI, 2013).

Tais controles estão descritos a seguir:

- Avaliação da política de segurança
- Controles de acesso lógico
- Controles de acesso físico
- Controles ambientais
- Plano de contingência e continuidade de serviços
- Controles organizacionais
- Controles de mudanças

- Controle de operação dos sistemas
- Controles sobre os bancos de dados
- Controles sobre computadores
- Controles sobre ambiente cliente-servidor

9.1. Gerenciamento de Manutenção, Problemas e de Mudanças

Interrupções inesperadas de serviços podem ocorrer por falhas em equipamentos ou por mudanças sem a notificação antecipada aos usuários. Para evitar essas ocorrências, um efetivo programa de manutenção é composto, principalmente, por (INTOSAI, 2013), pelos aspectos seguintes.

a) Controles preventivos e de ambiente: evitam ou mitigam danos potenciais em equipamentos e interrupções no serviço. Controles de ambiente podem diminuir as perdas causadas por algumas interrupções como incêndios ou evitar incidentes por meio da detecção antecipada de potenciais problemas, como vazamentos de água ou fumaça, de forma que eles possam ser remediados. Também, geradores de energia podem manter os equipamentos em funcionamento durante quedas ou oferecer um período para backup de dados em conjunto com procedimentos de desligamento ordenado durante longos períodos sem energia. Exemplos de controles de ambiente incluem:

I. Sistemas se supressão de fogo

II. Alarmes de incêndio

III. Detectores de fumaça

IV. Detectores de água

V. Iluminação de emergência

VI. Redundância em sistemas de refrigeração de ar

VII. Geradores de energia elétrica

VIII. Existência de válvulas de desligamento e procedimentos para linhas de encanamento que possam danificar equipamentos.

IX. Equipamentos construídos com materiais resistentes ao fogo e projetados para reduzir a sua disseminação

X. Políticas que proíbam alimentos, bebidas e cigarros em áreas com equipamentos.

b) Plano de Recuperação de Desastres: deve ser desenvolvido para a restauração de aplicações críticas. Ele inclui medidas para processamento alternativo de informações em caso de danos significativos ou inacessibilidade de equipamentos ou de sistemas. Políticas e procedimentos de

nível organizacional definem o processo e documentos de planejamento da recuperação. Além disso, um plano organizacional deve identificar os sistemas críticos, aplicações e quaisquer planos subordinados ou relacionados. É importante que esses planos sejam claramente documentados, comunicados para a equipe pertinente e atualizado para refletir as operações atuais. Devem ser documentados com a adesão dos departamentos de negócio e de segurança da informação além de comunicado à equipe afetada. O plano deve refletir as prioridades de risco e operacionais que a entidade identificou. Ele deve ser projetado de forma que os custos do planejamento de recuperação não excedam os custos associados com os riscos que o planejamento está destinado a reduzir. O plano deve ser detalhado e documentado de forma suficiente para que seu sucesso não dependa do conhecimento ou expertise de um ou dois indivíduos.

c) **Localidades Alternativas:** dependendo do grau de continuidade de serviço necessário, as escolhas de localidades alternativas vão abranger desde um estabelecimento pronto para serviço imediato de backup, conhecido como um *hot site*, a um site que tomará algum tempo em preparação das operações, chamado de *cold site*. Além disso, vários tipos de serviços podem ser pré-combinados com fornecedores. Isso inclui o acordo com fornecedores de um hardware computacional e serviços de telecomunicação, bem como um fornecedor de formulários de negócio e outros suprimentos.

d) **Testes periódicos:** testar o Plano de Continuidade é essencial para lidar com situações de emergência. Os testes podem revelar fraquezas importantes como instalações de *backup* que não repliquem operações críticas conforme antecipado. Por meio de procedimentos de teste, esses planos devem ser substancialmente melhorados. A frequência dos testes do plano de continuidade varia dependendo da criticidade das operações da organização. Normalmente os planos de continuidade para funções críticas devem ser testados integralmente ao menos uma vez a cada um ou dois anos, sempre que mudanças significativas no plano tenham sido tomadas ou quando ocorrer troca de pessoas-chave da equipe. É importante para a alta administração avaliar problemas no plano de continuidade e desenvolver uma política que abranja a frequência e a extensão desses testes. Resultados de testes de continuidades oferecem uma medida importante da viabilidade do plano de continuidade. Assim, eles devem ser reportados à alta gestão de maneira que a necessidade de modificação e de testes adicionais possam ser determinadas e que a alta administração esteja ciente dos riscos das operações de continuidade advindos de um planejamento inadequado.

e) **Segurança:** a segurança de recursos e de operações deve ser incluida nos planos de continuidade do negócio como dados críticos. Aplicações,

operações e recursos tendem a ser comprometidos facilmente durante a ocorrência de desastres ou de atividades de gerenciamento de continuidade de negócios. Por exemplo, durante um procedimento de backup de dados, a falta de segurança pode acarretar a criação de cópias e vazamentos de dados importantes.

f) **Backup e recuperação de dados em serviços terceirizados:** várias organizações terceirizam toda ou parte de suas atividades para um provedor de serviços. Sendo os controles e as operações rotineiras executados por terceiros, é essencial a garantia de que a continuidade dos negócios e o plano de recuperação de desastres esteja previsto em contrato. A organização deve também monitorar a implementação da continuidade de negócios e a prontidão do processo de recuperação de desastres oferecidos pelo provedor de serviços. Isso também inclui exigências de segurança para este, como a confidencialidade dos dados e das aplicações mantidas. Já a propriedade dos processos de negócio deve ser mantida pela organização que deve também se planejar para caso haja mudança de provedor de serviço.

Síntese do Capítulo

O capítulo destaca a importância crítica da preparação para lidar com eventos adversos que possam impactar a infraestrutura de TI de uma organização. O foco da Auditoria do Plano de Contingência é garantir que o plano de contingência em TI seja abrangente, atualizado e eficaz. Isso envolve a revisão detalhada de componentes essenciais, como procedimentos de resposta, estrutura organizacional, análise de riscos, planos de recuperação e comunicação. A eficácia da equipe em seguir os procedimentos delineados, a prontidão em situações reais e a capacidade de aprendizado contínuo são pontos chave de avaliação.

Além disso, a auditoria analisa a integração de lições aprendidas de eventos passados, identificando áreas de melhoria e ajustes nos procedimentos. A comunicação eficaz, a conscientização da equipe e a participação regular em testes e simulações são consideradas como elementos cruciais para garantir a eficácia do plano de contingência.

Atividades de avaliação

1. Como a sua organização aborda a manutenção contínua e a eficácia do plano de contingência em TI? Quais são os desafios enfrentados na implementação e na atualização regular do plano e como você percebe a importância da auditoria nesse processo para garantir a prontidão em situações de contingência?
2. Considerando as lições aprendidas de auditorias anteriores de planos de contingência em TI, como a sua equipe ajustou e melhorou os procedimentos de resposta e de recuperação? Além disso, de que maneira a comunicação e o treinamento foram aprimorados para garantir uma resposta eficaz a eventos adversos? Como essas melhorias contribuíram para a resiliência do seu ambiente de TI?

Referências

ABNT, Associação Brasileira De Normas Técnicas. **NBR ISO/IEC 17799**. Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ABNT, Associação Brasileira De Normas Técnicas. **NBR ISO/IEC 27002**, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ABNT, Associação Brasileira De Normas Técnicas. **NBR ISO/IEC 27005**. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 22301:2013 -** Sistema de gestão de continuidade de negócios - Requisitos. Rio de Janeiro - RJ: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2013** – Código de prática para controles de segurança da informação. Rio de Janeiro - RJ: ABNT, 2013.

AIKAU, Eddie. **Auditoria de sistemas de informação:** introdução, controles organizacionais e operacionais. Disponível em: https://www.jusbrasil.com.br/artigos/auditoria-de-sistemas-de-informacao-introducao-controles-organizacionais-e-operacionais/433404795

BERGAMI, P. R. **What is an IT.** *Audit*. Auditor-General's Office Singapore, 2009. Disponível em: https://www.ago.gov.sg/docs/default-source/publications/what-is-an-it-audit.pdf. Acesso em: 10 dez. 2023.

BRASIL. Tribunal de Contas da União. **Boas Práticas em Segurança da Informação.** 4. ed. Brasília: TCU, 2012. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0B226095120B

BRASIL. **Estratégia de Fiscalização do TCU em segurança da informação e segurança cibernética 2020-2023.** Disponível em:https://portal.tcu.gov.br/data/files/24/46/70/39/5D8AB710140B5BA7F18818A8/Estrategia_fiscalizacao_TCU_seguranca_informacao_seguranca_cibernetica_2020-2023.pdf

BRASIL. **Guia de Boas Práticas para Governança de Tecnologia da Informação no Setor Público.** Disponível em: https://portal.tcu.gov.br/data/files/29/C3/8D/F2/334CF610F5680BF6F18818A8/Governanca_e_tecnologia_informacao_comunicacao_setor_publico.pdf

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **COBIT 5:** modelo corporativo para governança e gestão de TI. Rolling Meadows, IL: ISACA, 2012.

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação.** Atlas

INTOSAI, ISSAI 5300: Guidelines on IT Audit. 2016. Disponível em: http://www.issai.org/en_us/site-issai/ issai- *framework* /4-auditing-guidelines.htm, Acesso em: dez/2024.

LEVANDOSKI, Robson José. **Auditoria de sistemas de informação gerencial e seus campos de aplicação.** 2014. 60 f. Monografia (Especialização) — Curso de Pós-Graduação do Departamento de Contabilidade do Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná, Curitiba, 2014. Disponível em: https://hdl.handle.net/1884/52844. Acesso em: 10 dez. 2023.

MAXIMIANO, Antonio Cesar Amaru e VERONEZE, Fernando. **Gestão de Projetos:** preditiva, ágil e estratégica / 6. Ed. Barueri: Atlas, 2022

ORGANIZAÇÃO INTERNACIONAL DAS ENTIDADES FISCALIZADORAS SUPERIORES (INTOSAI). **ISSAI 100:** Princípios Fundamentais de Auditoria do Setor Público. Brasília: TCU, 2017. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15D3169CE015D56CBA59F12A3. Acesso em: 10 dez. 2023.

PACHECO, André Luiz Furtado. **Curso de auditoria de TI.** Brasília: Escola Nacional de Governo, 2011.

RODRIGUES, Rondinélio Ferreira; CARMO, Carlos Roberto Souza; MARTINS, Vidigal Fernandes. Auditoria de sistemas de informática nas empresas modernas. **Revista Científica Linkania Master**, v. 1, n. 6, 2013.

SCHMIDT, Paulo; SANTOS, José Luiz; ARIMA, Carlos Hélio. **Fundamentos de auditoria de sistemas.** São Paulo: Atlas, 2006.

WASCHBURGER, Lucas Rafael. **Segurança da informação:** conhecimentos necessários para as empresas atuais. 2015. 39 f. Trabalho de Conclusão de Curso (Especialização) - Universidade Tecnológica Federal do Paraná, Pato Branco, 2015 http://repositorio.utfpr.edu.br/jspui/handle/1/23131.

Sobre os autores

Samuel Leite Castelo: Contador, com mestrado em Administração de Empresas pela Universidade de Fortaleza (Unifor), com Diploma de Estudos Avançados em Planejamento Territorial e Desenvolvimento Sustentável pela Universidade de Barcelona (UB). Doutorado em Gestão de Empresas pela Universidade de Coimbra (UC). Atualmente é professor adjunto do curso de Ciências Contábeis da Universidade Estadual do Ceará (Uece) e Analista de Controle Externo pelo Tribunal de Contas do Estado do Ceará TCE-CE.

Derlange Maia: Bacharel em Ciências da Computação pela Universidade Federal do Ceará (UFC) e Direito pela Universidade de Fortaleza (Unifor). É especialista em Direito da proteção e uso de dados pela PUC-Minas, em gestão pública. É analista de Controle Externo do Tribunal de Contas do Estado do Ceará, atuando na Assessoria de Qualidade e Inovação. É membro da Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD), da Associação Brasileira de Governança Pública de Dados Pessoais (govDADOS) e da Comissão sobre a Lei Geral de Proteção de Dados (LGPD - OAB/CE).

Especialização em
Auditoria e Controle interno

Fiel a sua missão de interiorizar o ensino superior no estado Ceará, a Uece, como uma instituição que participa do Sistema Universidade Aberta do Brasil, vem ampliando a oferta de cursos de graduação e pós-graduação na modalidade de educação a distância e gerando experiências e possibilidades inovadoras com uso das novas plataformas tecnológicas decorrentes da popularização da internet, do funcionamento do cinturão digital e da massificação dos computadores pessoais.

Comprometida com a formação de professores em todos os níveis e a qualificação dos servidores públicos para bem servir ao Estado, os cursos da UAB/Uece atendem aos padrões de qualidade estabelecidos pelos normativos legais do Governo Federal e se articulam com as demandas de desenvolvimento das regiões do Ceará.

UECE

UAB UNIVERSIDADE ABERTA DO BRASIL

CAPES