EAD UNISANTA

Auditoria de Sistemas

Dr. Joseffe Barroso de Oliveira

GUIA DA
DISCIPLINA

1. O QUE É AUDITORIA DE SISTEMAS DE TI

Objetivo

O objetivo deste capítulo é entender qual é a importância de auditoria de sistemas.

Introdução

A preocupação em sobreviver frente um mercado cada vez mais competitivo e a busca pela melhoria contínua é o que vem estimulando empresas a investir na auditoria de sistema da informação, ou seja, uma solução encontrada por gestores para problemas em potencial, como no caso da segurança dos dados manipulados através dos computadores na organização. Foi inevitável que as atividades realizadas manualmente se tornassem automatizadas, decorrentes principalmente do crescimento que as organizações vêm tendo, em paralelo com a evolução acelerada da tecnologia.

O ambiente empresarial foi se tornando cada vez mais complexo e os gestores precisaram adequar às áreas administrativas e produtivas com sistemas e ambientes de tecnologia da informação (TI). Embora o processamento e armazenamento das informações tenha facilitado os negócios e a tomada de decisão, muitos riscos com a segurança dos dados também passaram a existir, e é neste ponto que a Auditoria de Sistemas se torna vital, garantindo a integridade das informações e evitando eventuais erros e falhas.

1.1. O que é auditoria de sistemas de informação?

A Auditoria de Sistemas é o ramo da auditoria que se tornou um importante aliado no planejamento e tomada de decisão das organizações. Entre os objetivos estão o gerenciamento do risco operacional, a proteção dos ativos da organização, a segurança e integridade na autenticidade dos dados e o atendimento eficaz e eficiente dos objetivos da instituição. A Auditoria de Sistemas engloba a avaliação dos processos, operações, sistemas e atividades gerenciais da organização, verificando se a realização das funções rotineiras está em conformidade com os objetivos, políticas institucionais, legislação, normas e padrões exigidos.

É por meio dela que gestores podem visualizar o uso dos recursos e dos fluxos de informação, determinando quais dados são críticos para o cumprimento dos objetivos e da

missão a ser seguida, além de identificar e barrar processos repetidos, despesas e custos adicionais, valores e obstáculos que impactam diretamente o fluxo e o bom andamento de informações eficientes e necessárias.

1.2. O que é auditoria de sistemas de informação?

A realização constante de auditorias de sistemas dentro de uma organização é fundamental para a diminuição de falhas e fraudes que podem estar presentes nesses sistemas. Desse modo, esse tipo de procedimento garante a segurança, integridade das informações e mais qualidade no tocante aos serviços de TI que a empresa realiza.

Verificar se os sistemas estão seguindo as diretrizes desejadas também aumenta a confiabilidade nesses processos.

Do mesmo modo, a auditoria também confere à organização mais transparência e verifica a necessidade de adoção de ferramentas e sistemas mais adequados, garantindo uma análise mais apurada dos riscos em TI.

Por fim, a auditoria também assegura que os sistemas estejam seguindo a legislação e outras diretrizes de qualidade, mitigando riscos com problemas legais.

Além disso, a auditoria externa, em especial, também garante à organização credibilidade quanto aos seus serviços, tanto perante clientes quanto fornecedores, por exemplo.

Portanto, a auditoria de sistemas contribui para uma constante melhoria na organização. Assim, podemos considerar como os fundamentos de auditoria de sistemas:

- Diminuir falhas e fraudes nos sistemas
- Garantir a segurança e integridade das informações
- Aumentar a qualidade dos serviços de TI
- Verificar a conformidade com diretrizes, políticas e legislação
- Aumentar a confiabilidade nos processos
- Conferir transparência e credibilidade à organização

2. CONCEITOS E OBJETIVOS DA AUDITORIA DE SISTEMAS

Objetivo

O objetivo deste capítulo é entender os conceitos e objetivos da auditoria de sistemas.

Introdução

A Auditoria de Sistemas é um processo sistemático e independente que tem como objetivo avaliar a eficácia, segurança e conformidade dos sistemas de tecnologia da informação (TI) de uma organização. Seus conceitos envolvem a análise de controles internos, a detecção de vulnerabilidades e a verificação do cumprimento de normas e regulamentos. O principal objetivo é garantir que os sistemas operem de forma eficiente, protegendo dados sensíveis e suportando os objetivos estratégicos da empresa, além de mitigar riscos de segurança e fraudes.

2.1. Auditoria de sistemas e a Organização Nacional de Padronização

Uma auditoria não pode ser realizada de qualquer maneira. Para isso, existem organizações de normatização dedicadas ao estabelecimento de modelos de padronização de processos. A ISO, por exemplo, sigla para Organização Internacional de Padronização, é um desses órgãos. Sua função é promover a normatização de produtos e serviços, a fim de conferir qualidade aos mesmos.

Trata-se de um de um órgão de reconhecimento mundial que já publicou mais de 22 mil padrões internacionais. Sua representante no Brasil é a ABNT, ou Associação Brasileira de Normas Técnicas. Quando as organizações determinam estratégias para garantir qualidade e competitividade aos seus produtos e serviços, ou ainda quando é preciso estabelecer salvaguardas para o atendimento de requisitos técnicos, há a necessidade de implementar um sistema de gestão.

Isso significa seguir as normas ISO. O processo de auditoria de gestão, por exemplo, tem como referência a norma ISO 19001:2018. Nessa norma são definidos os requisitos para a implementação de um programa de auditoria, papeis, responsabilidades e o escopo do programa de auditoria.

Porém, quando falamos especificamente da auditoria de sistema de informação, devemos observar outra norma, a ISO 27000:2018. A ISO 27000 é composta por cerca de quarenta normas que versam sobre a tecnologia da informação, técnicas de segurança e sistemas de gestão.

2.2. Quais são os tipos de auditoria de sistemas?

Uma organização pode passar por diferentes tipos de auditoria de sistemas, os principais são:

- Interna
- Externa

Auditoria interna

A auditoria interna é um processo realizado pela própria organização para auditar seus sistemas e procedimentos. Com isso, a empresa visa garantir que seus parâmetros estejam sendo seguidos devidamente e que os resultados esperados sejam atingidos.

Por meio dessa auditoria, a organização toma conhecimentos dos processos que não estão em conformidade com suas diretrizes e identifica oportunidades de melhorias. No entanto, a auditoria interna não pode ser realizada por qualquer profissional. Para ser um auditor é preciso ter as competências necessárias, habilidades e experiências para executar sua função com êxito.

Para isso, o auditor interno deve ter conhecimento e ser treinado na ISO 19011, bem como no sistema ao qual será auditado. Esse tipo de auditoria é de suma importância para organizações que desejam medir, de forma eficaz, seu desempenho em relação às normas e diretrizes a serem seguidas.

Auditoria externa

A auditoria externa, como você já deve imaginar, é realizada por um auditor independente.

Por mais que a organização acredite que uma auditoria interna seja eficiente, a auditoria externa e especializada é fundamental para averiguar se os processos estão, de fato, adequados às normas e diretrizes pré-determinadas.

A importância de uma auditoria externa vem da independência em relação a empresa e, por isso, sua opinião não pode sofrer nenhum tipo de influência. Esse tipo de auditoria pode ser contratado pela própria empresa ou pode ser um processo determinado pelas leis relacionadas ao setor de atuação da empresa, tornando a auditoria externa obrigatória.

Nesse último caso, o auditor, normalmente, é um órgão regulador.

2.3. Como pode ser aplicado nas empresas?

Como você já sabe, auditoria pode ser aplicada a uma organização de duas formas: interna e externa. Nos dois casos o responsável por realizar a auditoria é o auditor.

O auditor deve ter profundo conhecimento a respeito da área auditoria. Ou seja, no caso da auditoria de sistemas, o profissional deve ter algum tipo de formação em tecnologia, como segurança da informação, por exemplo.

Mas não apenas isso, para ser um auditor é preciso ser treinado para tal. No caso dos auditores internos, é comum que a própria organização tenha um departamento de treinamento.

Uma auditoria completa pode ser resumida em quatro passos básicos:

- Planejamento
- Execução
- Relatório de resultados
- Plano de ação

O que é a LGPD?

A LGPD, ou a Lei Geral de Proteção de Dados, foi criada com o intuito de estabelecer regras para a regulamentação das práticas do uso de dados no ambiente digital, criando um cenário de segurança jurídica para proteger o direito à liberdade e privacidade dos usuários.

A necessidade da criação da LGPD surgiu da proporção que a gestão de dados tomou na economia digital. Afinal, a coleta de dados tornou-se um recurso estratégico para garantir vantagens competitivas às grandes empresas do meio.

Além disso, a era digital também trouxe consigo diversos dilemas éticos nos quais não nos preocupávamos antes. Nesse contexto, temos visto grandes empresas envolvidas em escândalos de vazamento de dados, atingindo e expondo milhares de usuários ao redor do mundo.

Diante disso, reforçar e regimentar às práticas de tratamento de dados tornou-se algo primordial.

Assim, a principal proposta da LGPD é proporcionar mais controle ao cidadão digital no tocante ao tratamento dado às suas informações pessoais. Ela baseia-se nos direitos fundamentais de liberdade e privacidade, demandando mais transparência e responsabilidade às empresas e órgãos públicos que detém e manejam esses dados.

Isso inclui, por exemplo, o consentimento explícito do usuário para a coleta e uso dos dados, além de obrigar as empresas detentoras desses dados a oferecer opções para que o usuário possa acessar, corrigir, apagar e realizar portabilidade dos dados.

Qual é a relação com a LGPD?

A criação e vigência cada vez mais próxima da Lei Geral de Proteção de Dados traz consigo uma oportunidade para que as empresas reavaliem a forma com que processam dados. Isso significa a implementação cada vez maior de uma auditoria de sistemas nas organizações.

Isso porque a LGPD prevê uma série de requisitos a serem cumpridos por essas organizações, visando a regulamentação das práticas do uso de dados. O objetivo da lei é proporcionar um cenário de segurança jurídica para proteger o direito à liberdade e privacidade dos usuários.

Junto com essas regras há, também, a determinação de sanções para as empresas que descumprirem a lei. O que obriga as empresas a adaptarem-se o mais rápido possível à nova legislação. A auditoria de sistemas é, portanto, uma consequência às mudanças previstas para o cenário da segurança da informação.

Ou seja, uma empresa que conta com uma auditoria interna de sistemas está se resguardando de possíveis sanções legais. Mas não é apenas isso. A LGPD prevê em seu art. 20 a possibilidade da realização de auditorias externas.

De acordo com a lei, a organização estará sujeita à realização de auditoria pela Autoridade Nacional de Proteção de Dados (ANPD) quando não fornecer informações requeridas pelo titular, conforme descreve o parágrafo segundo do mesmo artigo:

"Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. "

3. ORGANIZAÇÃO DE UM TRABALHO DE AUDITORIA

Objetivo

O objetivo deste capítulo é entender a organização e trabalho de auditoria de sistemas.

Introdução

O processo de organização dos trabalhos de auditoria de tecnologia de informação segue a norma de execução de trabalhos, o principal componente das normas de auditoria geralmente aceitas. Vale recapitular que essa norma contempla: planejamento de auditoria, avaliação de riscos de auditoria, supervisão e controle de qualidade, estudo e avaliação do sistema contábil e de controles internos e aplicação dos procedimentos de auditoria, documentação da auditoria, avaliação formal dos negócios da entidade, aplicação de amostragem estatística, entre outros. Para simplificar o entendimento, adotam-se as seguintes estruturas didáticas: planejamento; escolha da equipe, programação da equipe; execução e documentação de trabalho; supervisão em campo; revisão dos papeis de trabalho, conclusão e emissão (follow-up) de relatórios; atualização do conhecimento permanente e avaliação da equipe. Ressalta-se que o mesmo processo efetuado convencionalmente se adapta à auditoria de tecnologia de informações. A única diferença é que cada uma dessas etapas pode ser automatizada por meio dessas ferramentas de produtividade para o controle dos trabalhos do auditor.

Planejamento

A atividade de planejamento em auditoria de sistemas de informações é imprescindível para melhor orientar o desenvolvimento dos trabalhos. Como o trabalho de auditoria representa processo contínuo de avaliação de risco ao qual se adicionam as experiências individuais dos profissionais e a evolução da prática e metodologias, aliadas aos resultados dos trabalhos e processos de negócio anteriormente, objetos de avaliação dos auditores, o planejamento é caracterizado para evitar quaisquer surpresas que possam acontecer tanto nas atividades empresariais, objeto de auditoria, como também em relação à responsabilidade dos auditores. Desde os primeiros trabalhos deve ser desenhada uma "Matriz de Risco" que seja permanentemente atualizada a partir dos resultados obtidos nos testes e nas avaliações dos auditores, assim como do impacto das mudanças ocorridas no negócio resultantes de alterações de estratégias empresariais, evoluções tecnológicas, concorrência, mudanças estatutárias, legislações, mudanças nas leis ambientais, social e econômica ou qualquer outro fator que tenha reflexo nas demonstrações financeiras, continuidade operacional, qualidade dos controles e, sobretudo, nos processos operacionais.

Escolha da Equipe

Um planejamento detalhado e atualizado com base nas principais mudanças do negócio permite indicar o perfil básico da equipe de auditoria de TI, o qual contempla o seguinte:

- Perfil e histórico profissional;
- Experiência acumulada por ramos de atividade;
- Conhecimentos específicos;
- Apoio do grupo de especialização;
- Formação acadêmica;
- Línguas estrangeiras;
- Disponibilidade para viagens

Programar a equipe

O encarregado de auditoria deve programar a equipe para executar os trabalhos. A programação de uma equipe de auditores com o perfil adequado para a realização do

trabalho previsto não é suficiente para garantir que todos os riscos de auditoria sejam minimizados pelos testes de auditoria; no entanto, devem-se observar as habilidades que permite:

a. Gerar programas de trabalho que extraiam dados corretos para testes;
b. Selecionar procedimentos mais apropriados;
c. Incluir novos procedimentos;
d. Classificar trabalhos por visita;
e. Orçar tempo e registrar o real;
f. Evidenciar corretamente os trabalhos realizados; utilizando-se softwares de amostragens estatísticas, entre outros, para otimizar os trabalhos;
g. Gerar relatórios em consonância com os trabalhos efetuados

Execução de trabalhos e supervisão

As tarefas devem ser realizadas por auditores que tenham formação, experiência e treinamento adequados no ramo de especialização. Dependendo da complexidade do ambiente operacional, aparente risco envolvido, os trabalhos serão desenvolvidos conforme vivência profissional, ou seja, tarefas mais simples e de menor risco serão desempenhadas por membros menos experientes, e aquelas mais complexas e de maior risco responsabilidade dos membros mais experientes e de melhor formação da equipe. A questão de supervisão é inerente ao processo de auditoria para garantir a qualidade e certificar que as tarefas foram adequadamente feitas. Isto permite cobrir os riscos prováveis identificados.

Revisão dos Papeis de trabalhos

Como tarefa de atingir a qualidade exigida pelas práticas de auditoria, os papeis de trabalho são revisados pelos superiores, que têm a incumbência de assinar junto com seus subordinados o cumprimento de cada passo de auditoria concluído. Eventualmente, em decorrência dos trabalhos de auditoria, falhas ou recomendações para melhorias são identificadas e limitam a conclusão do auditor, assim como determinados procedimentos que não tenham sido concluídos por restrições do próprio cliente. No entanto, o revisor, não identificando outros passos de auditoria independentes, poderá solicitar uma nova visita para completar os trabalhos. Contudo, para as pendências de revisão, deve ser analisado o reflexo do aumento ou alteração do escopo, novos trabalhos, nova abordagem, impacto no parecer final, na carta de representação da gerência.

Ao revisar os papeis quando se adota a estratégia de Paperless Audit, a intenção das ferramentas de workflow é fundamental para garantir a integridade do processo de revisão dos papeis. A utilização de soluções de papeis eletrônicos adicionam-se recursos de automação do processo de emissão de relatórios. Isso desde a emissão das demonstrações financeiras até a carta de comentários de melhorias de controles internos. A integração com aplicativos gráficos, e-mail, formulários classificados eletronicamente é predefinida com campos que identificam responsáveis e níveis de autorização para acessos, prazos, fluxos de aprovação geralmente otimizam os trabalhos de auditoria de tecnologia de informação, evitando que o próprio auditor elimine deliberadamente as pendências de auditoria.

Atualização do conhecimento permanente

O conhecimento em determinado período de auditoria, dito como aquele que muda com pouca frequência, sempre é fundamental e server como ponto de partida para o período subsequente. A manutenção em forma eletrônica, a documentação da descrição e a avaliação do ambiente de controle interno, controles gerais e dos sistemas aplicativos e processos de negócio contribuem para a redução das horas de auditoria do período seguinte.

a. Dentre as informações relevantes destacam-se:
b. Descrição do processo de negócio;
c. Levantamento e avaliação do ambiente de controle;
d. Documentação e conclusão sobre a avaliação dos controles dos processos relevantes;
e. Matriz de risco que pontue riscos aparentes para todos os principais componentes da demonstração financeira;
f. Exceções dos testes;
g. Falhas ou fraquezas nos testes de controle internos;
h. Programas de trabalho

Avaliação da Equipe

A fim de garantir a evolução e o aprimoramento técnico dos profissionais da equipe de auditoria de TI, deve-se avaliar o desempenho, elogiando os pontos fortes do auditor, auxiliar no reconhecimento das fraquezas e na elaboração de um plano para superá-las para que se desenvolva um profissional qualificado e consciente. Como é de praxe, para

cada trabalho no qual um profissional é programado, o sistema que controla a programação emite eletronicamente uma avaliação de desempenho já preenchida pelo superior, isto é fundamental para nortear a promoção ou não do profissional.

Documentação dos papeis de trabalho

Os papeis de trabalho constituem um conjunto de formulários preenchidos logicamente no processo de auditoria de sistemas, com seus anexos que evidenciem os fatos relatados; se esses anexos forem provas documentais, podem ser escaneados para serem documentados eletronicamente. Eles contêm informações coligidas durante o teste, os procedimentos executados e as opiniões formadas sobre o objeto de auditoria.

Tais papeis, independentemente de seu enfoque ser sistêmico ou manual, deve ser autossuficiente e não devem necessitar, subsequentemente, de explicações verbais e adicionais do preparador a fim de detalhar a metodologia adotada.

Os papeis de trabalho sistêmicos são guardados em base de dados. Essas bases de papeis constituem informações de planejamento, execução, monitoramento e revisões, follow-up, controles do usuário do sistema e senhas e alguns recursos de auxílio ao usuário. Mantêm as seguintes figuras: sócios ou sócios independentes, encarregados, supervisores ou gerentes, assistentes ou seniores, cada um tendo suas telas cadastradas para exercer suas funções de administração dos serviços de auditoria, conforme segregação das funções que pode ser feita local ou remotamente por meio de notebooks ligados fora dos escritórios e em lugares distantes.

Sócio: o responsável pelos serviços de auditoria que terá acesso a todas as telas e documentos registrados sobre a auditoria cadastrados nos sistemas como revisor de qualidades do serviço como um todo. Com sua autorização, dá-se o aval sobre o encerramento dos serviços da auditoria iniciados;

Encarregados supervisor ou gerente: chefe da equipe de auditoria que geralmente deve cadastrar os dados referentes à identificação da auditoria no sistema, tais como o nome, a equipe participante e as unidades auditáveis, os programas da auditoria serem utilizados, a data de início e fim e os check-lists de monitoramento. Levanta as pendências referentes aos passos de auditoria cumpridos para serem atendidos no processo de revisão

dos trabalhos. Note-se que somente ele tem acesso para assinalar o cumprimento ou não das pendências que devem ser observadas pelos subordinados;

Preparador (assistente ou sênior de auditoria): capta informações e diretrizes da auditoria no banco de dados central, levanta informações comprobatórias para cumprir os passos de auditoria efetivando os testes, após os quais atualiza o banco.

Ressalta-se que para a implementação desta abordagem a firma de auditoria pode desenvolver seu próprio software ou adquirir softwares generalistas de automação de auditoria disponíveis no mercado.

4. TIPOS DE FERRAMENTAS DE AUDITORIA

Objetivo

O objetivo deste capítulo é apresentar os principais tipos de ferramentas de auditoria.

Introdução

As ferramentas de auditoria são essenciais para realizar auditorias internas eficazes. Elas auxiliam os auditores a coletar, analisar e reportar informações de maneira eficiente e precisa. A seguir veremos alguns dos tipos mais comuns de ferramentas de auditoria.

Monitoramento contínuo

O monitoramento contínuo é uma prática de auditoria aprimorada com a incorporação de uma solução de Gerenciamento de Processos de Negócios (BPMS).

Através do BPMS, os auditores identificam e respondem a problemas em tempo real, aumentando a eficácia operacional da organização.

A personalização dessas ferramentas de auditoria, reforçada pelo BPMS, permite sua adaptação às necessidades específicas da organização, tornando o processo mais eficaz.

Análise de dados

As ferramentas de análise de dados, amplificadas pela aplicação de Analytics, são usadas para coletar, organizar e analisar grandes volumes de dados.

As soluções de analytics fornecem uma capacidade aprimorada de identificar tendências, padrões e anomalias nos dados, transformando-os em insights acionáveis que podem fornecer uma visão valiosa sobre o desempenho e a conformidade da organização.

Além disso, a incorporação de uma solução de analytics na análise de dados pode facilitar a tomada de decisões baseada em evidências, reduzir riscos e promover a inovação, contribuindo para a competitividade e a resiliência da organização no mercado.

Entrevistas

As entrevistas são uma ferramenta valiosa para coletar informações de indivíduos dentro da organização. Elas permitem que os auditores obtenham uma compreensão em primeira mão dos processos, políticas e procedimentos da organização.

As entrevistas podem ser conduzidas pessoalmente, por telefone ou por videoconferência, e as informações coletadas podem fornecer insights valiosos que não podem ser obtidos por meio de análise de dados sozinha.

Testes de penetração

Os testes de penetração são usados para identificar vulnerabilidades nos sistemas de informação da organização. Eles envolvem a simulação de ataques cibernéticos para testar a robustez dos sistemas de segurança da organização.

Os resultados desses testes podem ajudar a organização a fortalecer suas defesas e proteger suas informações contra ameaças de segurança cibernética.

Gestão de documentos

As ferramentas de gestão de documentos, quando combinadas com uma solução de Gestão de Conteúdo Empresarial (ECM), elevam o nível de organização e gestão da documentação relacionada à auditoria.

As soluções de ECM permitem que os auditores armazenem, recuperem, compartilhem e gerenciem documentos de maneira eficiente e segura, integrando diferentes tipos de conteúdo em uma plataforma unificada.

5. SOFTWARES DE AUDITORIA DE SISTEMAS

Objetivo

O objetivo deste capítulo é apresentar os principais softwares que podem ser utilizados em uma auditoria de sistemas

Introdução

A utilização de softwares que podem ser utilizados em uma auditoria ajuda muito ao auditor e as empresas conseguirem informações valiosas e detalhadas sobre toda jornada. A seguir estão alguns dos principais softwares utilizados em auditoria de sistemas, com uma descrição detalhada de cada um e exemplos práticos de uso. Esses softwares ajudam a automatizar processos, identificar vulnerabilidades e garantir a conformidade em várias frentes, desde segurança de TI até auditoria financeira e de conformidade regulatória.

5.1. Audit Command Language (ACL)

Descrição: O ACL é uma ferramenta amplamente usada para auditoria de dados e análise, oferecendo funcionalidades avançadas para extrair, processar e analisar grandes volumes de dados. Ele ajuda a identificar padrões, outliers e irregularidades nos dados, sendo útil em auditorias financeiras e operacionais.

Exemplo prático: Em uma auditoria de conformidade fiscal, o auditor pode utilizar o ACL para analisar registros de faturamento de uma empresa. Ele pode filtrar e identificar transações suspeitas, como duplicidades de faturas, e comparar com os relatórios fiscais oficiais para verificar discrepâncias.

5.2. IDEA (Interactive Data Extraction and Analysis)

Descrição: O IDEA é uma ferramenta poderosa de análise de dados que auxilia auditores a realizar extrações, análises e amostragens em grandes volumes de dados. Ele automatiza o processo de auditoria e oferece relatórios detalhados para investigações de fraudes e conformidade.

Exemplo prático: Uma empresa de seguros pode usar o IDEA para identificar padrões fraudulentos de sinistros. Ele pode detectar sinistros com valores acima do padrão, repetição de beneficiários em curto período e outros indicadores de fraudes que, de outra forma, seriam difíceis de identificar manualmente.

5.3. TeamMate

Descrição: O TeamMate é um software de gestão de auditorias que centraliza todas as informações do processo. Ele facilita o planejamento, execução e documentação da auditoria, permitindo colaboração entre equipes e integração com ferramentas de gestão de risco.

Exemplo prático: Durante uma auditoria interna de controles de TI, uma equipe utiliza o TeamMate para acompanhar o progresso do trabalho, registrar achados e criar relatórios de conformidade. O software permite a rastreabilidade das ações corretivas recomendadas e o monitoramento de implementação de melhorias.

5.4. SAP Audit Management

Descrição: O SAP Audit Management é uma solução integrada dentro do ecossistema SAP que permite automatizar e gerenciar auditorias de sistemas de forma eficiente. Ele oferece ferramentas para planejar auditorias, executar verificações de conformidade e monitorar a eficácia dos controles.

Exemplo prático: Uma grande empresa que utiliza SAP ERP pode usar o SAP Audit Management para auditar suas operações financeiras e verificar a conformidade com o SOX (Sarbanes-Oxley Act). Ele permite a geração automática de relatórios de auditoria com base nos dados do ERP, otimizando o processo de verificação.

5.5. Pentest Tools (Nmap, Nessus, Metasploit)

Descrição: Ferramentas de teste de penetração, como Nmap, Nessus e Metasploit, são amplamente utilizadas em auditorias de segurança para identificar vulnerabilidades em redes e sistemas. O Nmap realiza varreduras de portas e mapeamento de rede, o Nessus detecta vulnerabilidades, enquanto o Metasploit executa ataques simulados para avaliar a segurança do sistema.

Exemplo prático: Em uma auditoria de segurança, a equipe pode usar o Nmap para mapear todos os dispositivos conectados à rede de uma empresa, identificar portas abertas e possíveis vulnerabilidades. Em seguida, o Nessus pode ser utilizado para identificar falhas em sistemas desatualizados ou não configurados corretamente. Por fim, o Metasploit pode

ser empregado para testar se as vulnerabilidades podem ser exploradas em um ataque real.

5.6. Wireshark

Descrição: O Wireshark é uma ferramenta de análise de tráfego de rede que permite capturar e examinar pacotes de dados. Ele é amplamente usado em auditorias de segurança e diagnóstico de rede, pois possibilita a visualização de comunicações em tempo real e a identificação de anomalias.

Exemplo prático: Durante uma auditoria de segurança de rede, um auditor pode usar o Wireshark para capturar e analisar o tráfego da rede corporativa. Se houver comunicação não autorizada ou um ataque man-in-the-middle, o Wireshark pode ajudar a identificar os pacotes suspeitos e determinar a origem da anomalia.

5.7. Splunk

Descrição: O Splunk é uma plataforma para análise de dados em tempo real, especialmente logs de sistemas e eventos de TI. Ele é útil em auditorias de segurança e conformidade, oferecendo insights detalhados sobre operações e permitindo a criação de alertas para anomalias.

Exemplo prático: Em uma auditoria de segurança cibernética, o Splunk pode ser configurado para monitorar eventos de login em sistemas críticos. Se houver um aumento incomum no número de tentativas de login com falhas ou logins de locais geográficos inesperados, o sistema pode gerar alertas para investigação imediata.

5.8. SonarQube

Descrição: O SonarQube é uma ferramenta de análise de código que verifica a qualidade e segurança do código-fonte em busca de vulnerabilidades, erros e inconsistências. Ele é especialmente útil para auditorias de software, garantindo que os sistemas estejam em conformidade com padrões de segurança e desenvolvimento.

Exemplo prático: Em uma auditoria de desenvolvimento seguro, o SonarQube pode ser utilizado para revisar o código de um aplicativo web e identificar vulnerabilidades como injeção de SQL ou Cross-Site Scripting (XSS). Ele também verifica se as melhores práticas de programação estão sendo seguidas, como manuseio adequado de exceções e uso de autenticação segura.

5.9. ControlCase

Descrição: O ControlCase é uma ferramenta voltada para auditorias de conformidade, especialmente em relação a frameworks como PCI-DSS (segurança de dados de cartões), ISO, SOC 2, e outros. Ele automatiza o processo de auditoria, permitindo o monitoramento contínuo e a geração de relatórios de conformidade.

Exemplo prático: Em uma auditoria de conformidade PCI-DSS, o ControlCase pode ser usado para garantir que uma empresa que processa pagamentos com cartão de crédito está atendendo a todos os requisitos de segurança. Ele permite a geração de relatórios automáticos para envio às autoridades reguladoras.

5.10. OpenAudit

Descrição: O OpenAudit é uma solução de código aberto para auditoria de ativos de TI. Ele permite que as empresas façam inventários detalhados de seus ativos de hardware e software, além de verificar a conformidade dos sistemas com as políticas de segurança e gestão de ativos.

Exemplo prático: Durante uma auditoria de inventário de TI, o OpenAudit pode ser utilizado para mapear todos os dispositivos conectados à rede e comparar com o inventário físico da empresa. Se forem detectados dispositivos desconhecidos ou softwares não autorizados, eles podem ser investigados para garantir que não representem uma ameaça de segurança.

6. COMPONENTES DE UMA POLÍTICA DE SEGURANÇA

Objetivo

O objetivo deste capítulo é apresentar os componentes de uma política de segurança.

Introdução

Uma Política de Segurança é um conjunto de diretrizes e práticas estabelecidas para proteger os ativos de informação de uma organização. Seus componentes essenciais incluem o controle de acesso, que define quem pode acessar sistemas e dados; a gestão de incidentes de segurança, para lidar com ameaças e violações; e as regras de uso aceitável, que estabelecem limites para o uso de recursos de TI. Além disso, contempla a proteção de dados sensíveis, a implementação de medidas de backup e recuperação e a conformidade com normas e regulamentos de segurança da informação.

6.1 O que é uma política de segurança da informação?

Para realmente entender o que é essa política, você precisa saber o que exatamente significa segurança da informação. De acordo com a definição da norma ISO 27001, que estabelece as diretrizes gerais para a gestão da informação de uma empresa, segurança da informação nada mais é que o ato de proteger os dados da empresa (especialmente aqueles confidenciais) contra diversos tipos de ameaças e riscos — espionagens, sabotagens, incidentes com vírus ou códigos maliciosos e até acidentes, como incêndio e inundação.

A segurança da informação é, então, obtida pela implantação de uma gama de controles que incluem procedimentos de rotina (como as verificações de antivírus), infraestrutura de hardware e software (como a gestão de soluções para assinatura eletrônica de documentos), além da criação de uma política devidamente documentada.

Chegamos, assim, à política de segurança da informação, definida como as regras que ditam o acesso, o controle e a transmissão da informação em uma organização. Lembrando que uma política de segurança não é um documento imutável ou inquestionável. Muito pelo contrário, requer atualização constante e participação não só da diretoria da empresa, mas também dos funcionários e da equipe de TI.

6.1.1 Quais os princípios básicos da segurança da informação?

Como se trata de uma verdadeira metodologia de proteção às informações da empresa, a PSI é implementada nas organizações por intermédio de alguns princípios básicos, os

quais garantem que cada variável importante receba a devida atenção e corrobore com o objetivo central da ação que é aumentar a integridade dos sistemas de informações.

Os princípios mencionados são: confidencialidade, integridade e disponibilidade. Cada um deles denota uma postura diferente dentro da empresa, exigindo ações pontuais para que se mantenham sempre presentes.

A seguir explicaremos de forma mais detalhada um a um:

6.1.2 Confidencialidade

O conceito de confidencialidade não foge muito à noção que o próprio termo nos passa. A confidencialidade, no contexto da segurança da informação, nada mais é do que a garantia de que determinada informação, fonte ou sistema é acessível apenas às pessoas previamente autorizadas a terem acesso.

Ou seja, sempre que uma informação confidencial é acessada por um indivíduo não autorizado, intencionalmente ou não, ocorre o que se chama de quebra da confidencialidade. A ruptura desse sigilo, a depender do teor das informações, pode ocasionar danos inestimáveis para a empresa, seus clientes e até mesmo para todo o mercado.

A exemplo, instituições financeiras, detentoras de dados pessoais e bancários de uma infinidade de usuários, não só precisam, mas devem manter a confidencialidade de todas as informações em seu domínio. A quebra desse sigilo significaria expor à riscos uma grande quantidade de pessoas, causando prejuízos incalculáveis.

6.1.3 Integridade

Quando empresas lidam com dados, um dos seus grandes deveres é mantê-los intocados, de forma a preservar a sua originalidade e confiabilidade. Caso contrário, erros podem ocorrer na interpretação dessas informações, gerando também rupturas no compliance do negócio e, no pior dos casos, sanções penais pesadas.

Nesse contexto, garantir a integridade é, pois, adotar todas as precauções necessárias para que a informação não seja modificada ou eliminada sem autorização, isto é, que mantenha a sua legitimidade e consistência, condizendo exatamente com a realidade.

Qualquer falha nesse quesito, seja por uma alteração, falsificação ou acesso irregular, gera a quebra da integridade. Da mesma forma que a quebra de confidencialidade, a ruptura na integridade das informações também pode implicar impactos negativos de grande monta em uma empresa, sobretudo de grande porte, em que os dados e informações têm um valor ainda maior.

6.1.4 Disponibilidade

A relação da segurança da informação com a disponibilidade é basicamente a garantia de acesso aos dados sempre que necessário. Ou seja, é a possibilidade de os colaboradores e membros da organização acessarem os dados de maneira fluida, segura e eficiente.

No contexto corporativo, a disponibilidade das informações é matéria de extrema importância, visto que o negócio pode depender da disponibilidade dos seus dados e sistemas para fechar contratos, vendas e atender os clientes.

Imagine como pode ser prejudicial para uma empresa que trabalha com vendas sofrer algum ataque na sua base de dados e, em razão disso, ter o sistema derrubado por um dia inteiro. Além do prejuízo à imagem, há também perdas financeiras com o não fechamento de vendas. Logo, a disponibilidade também figura como um dos pilares para a segurança da informação.

6.1.5 Que benefícios ela traz à gestão da empresa?

O bem mais importante que qualquer empresa possui é justamente a informação. E especialmente hoje, com o mercado sendo obrigado a lidar com quantidades massivas de informação em diversas camadas, é preciso se manter constantemente atento às situações que envolvem o manuseio de dados.

Ataques à integridade dos sistemas das empresas vêm crescendo tanto em número como em sofisticação. Assim, informações críticas e confidenciais correm o risco de serem

corrompidas, perdidas ou até mesmo de cair nas mãos da concorrência. De toda forma, os prejuízos são incalculáveis.

Com uma política de segurança da informação bem desenhada, é possível reduzir consideravelmente esses riscos, dando à organização a devida proteção contra ameaças internas e falhas de segurança.

Ao determinar e comunicar o time sobre as diretrizes do uso aceitável da informação, garante-se que os funcionários saibam qual é a postura esperada na hora de lidar com os diversos níveis de confidencialidade e importância, conhecimento que previne violações acidentais.

Uma vez implantada a política de segurança da informação, o aumento da transparência e a elevação da eficiência do negócio surgem como consequências naturais. Essa política deve ser mais clara possível, para que os colaboradores entendam como organizar a informação seguindo um padrão para facilitar os fluxos de processos em todas as escalas.

A execução adequada das regras de segurança da informação leva a uma evolução proporcional à drástica redução dos danos à infraestrutura de TI da empresa. Assim, a experiência do usuário também se beneficia significativamente, dando um salto de qualidade.

6.1.6 Como elaborar uma política de segurança da informação?

A segurança da informação, como dito, se desenvolve como uma metodologia, seguindo-se uma sistemática e conceitos próprios da área. Assim, é fundamental estudar e planejar essa tarefa para que possa se adaptar à empresa e, mais do que isso, cumprir o seu papel.

A elaboração de uma PSI depende de alguns cuidados básicos, algumas ações prévias que ajudarão a compor a estrutura necessária e a cultura mais indicada para que todos saibam lidar com os conceitos e ferramentas.

A seguir, listamos alguns pontos que merecem ser destacados na elaboração dessa política. Vejamos:

Definição dos contornos e ferramentas necessárias

Com já dito, uma política de informação deve atender aos requisitos da empresa. No entanto, essa etapa não pode ser feita só com profissionais do setor de TI, mas por todos os setores da organização, abrangendo diferentes equipes, visto que ela será aplicada e replicada todos os funcionários.

Nesta etapa serão definidos os processos e tarefas que poderão ser alterados para garantir a segurança. A exemplo, podemos citar:

- Definição de cronogramas de backup;
- Estabelecimento de regras para o uso de senhas e credenciais de acesso;
- Controle de acesso aos espaços físicos;
- Definição de diretrizes para o acesso à informação de diferentes profissionais e times, estabelecendo graus de acessibilidade;
- Criação de planos de contingência e de gerenciamento de riscos;
- Definição das políticas de atualização de softwares

Todas essas medidas, de alguma forma, impactam o trabalho de diferentes setores da empresa. Daí a importância de que todos participem, já que ações pontuais, realizadas por cada funcionário, quando somadas, formam um ambiente mais seguro.

Classificação das informações da empresa

Outra etapa importante para a criação de uma boa PSI é a classificação dos dados entre públicos, internos, confidenciais e secretos. Essa ação é necessária porque dependendo da empresa o mesmo tipo de dado pode receber classificações distintas.

A exemplo, para a maior parte das empresas, dados relacionados ao faturamento e balanço financeiro são tidos como confidenciais, fazendo parte da estratégia de negócio. Por outro lado, Sociedade Anônimas, de capital aberto, não tem sigilo nesse tipo de informação, dada a necessidade de os investidores conhecerem esses números.

É com base nessa classificação dos dados é que os níveis de acesso de cada colaborador às informações poderão ser estabelecidos, mantendo-se o rigor no manuseio dos dados.

6.2. Quais são suas etapas de implantação?

Agora que você já sabe o que é e por que é tão importante para sua empresa, é hora de saber que etapas deve seguir na hora de implantar uma política de segurança da informação.

Antes, porém, precisamos destacar que, para que o documento tenha aceitação na organização, deve não só ser apoiado pela cúpula estratégica da empresa, mas contar com sua participação ativa durante o processo. Dito isso, vamos aos passos:

Planejamento e levantamento do perfil da empresa

Deve ser feito um planejamento que inclua o objetivo máximo da política, determine seus responsáveis e os prazos para conclusão, analisando o que deve ser protegido, tanto em relação ao tráfego externo como ao interno.

Elaboração das normas e proibições

Etapa de criação das normas relativas ao uso de programas, internet, dispositivos móveis, acesso à rede da empresa, bloqueio de sites, uso do e-mail corporativo, de aplicativos de mensagens de texto e voz — resumindo: recursos tecnológicos em geral.

Alinhamento com as demais políticas do negócio

Esse é o momento de estudar as demais políticas da empresa, bem como sua visão, sua missão e seus valores, para que tudo esteja devidamente alinhado.

Aprovação pelo RH

Além da diretoria, o RH da empresa também deve ler o documento e aprovar suas premissas, de acordo com as leis trabalhistas e com o manual interno dos empregados da organização.

Aplicação e treinamento dos colaboradores

Trata-se de efetivamente implantar a política. Nesse momento, é preciso comunicar todos os funcionários, que devem receber uma cópia do documento, além de um treinamento prático que apresente seus pontos principais.

A política deve estar sempre acessível aos colaboradores e a assinatura de cada um deles, com uma declaração de comprometimento, deve ser recolhida após o treinamento.

Vale mencionar, ainda, a importância do desenvolvimento de planos de contingência, cujo objetivo é deixar claro para os colaboradores, gestores e profissionais de TI o que pode — e deve ser feito — em caso de ruptura na segurança. Assim, se garante respostas mais rápidas e efetivas às ameaças, reduzindo eventuais danos.

Avaliação periódica

Na verdade, essa etapa consiste em ações contínuas, já que a política deve ser revisada regularmente, a fim de atualizá-la, caso seja necessário. A segurança da informação, por ter uma íntima relação com a tecnologia, está em constante evolução.

Por esse e outros motivos, é imperioso manter uma rotina de avaliação, comparando os recursos de proteção internos da empresa à sofisticação das ameaças e, caso necessário, compatibilizando-os para que sejam suficientes e eficiente no combate às vulnerabilidades.

Atenção a novas tecnologias

O setor de TI deve estar sempre atento ao surgimento de novas tecnologias no mercado, aquelas que podem alterar as regras da política empresarial, submetendo-a às atualizações necessárias. Como exemplo aqui podemos citar a substituição das cartas registradas por soluções no e-mail corporativo.

Não se esqueça de que uma política de segurança da informação é tão eficaz quanto o grau em que é praticada dentro da organização. Portanto, uma boa política é aquela de fácil entendimento e acessível, atingindo e informando eficientemente todos os funcionários.

Também ser flexível e aberta a mudanças de requisitos e à evolução do negócio, além de constantemente atualizada para permanecer relevante. Afinal, as informações da sua organização devem ser preservadas e resguardadas de todas as formas possíveis.

Como você pôde ver, a concepção e a consequente implantação de uma política de segurança da informação é uma empreitada que, além de garantir proteção, traz maior transparência e eficiência para toda a empresa.

7. Gestão de Continuidade de Negócios

Objetivo

O objetivo deste capítulo é apresentar os conceitos da gestão de continuidade de negócios.

Introdução

A Gestão de Continuidade de Negócios (GCN) é o processo de planejamento e implementação de estratégias para garantir que uma organização possa continuar operando durante e após incidentes disruptivos, como desastres naturais, falhas de sistemas ou ciberataques. A GCN envolve a identificação de riscos críticos, o desenvolvimento de planos de recuperação e a preparação de equipes para responder de forma eficaz a crises. O objetivo é minimizar impactos, proteger ativos essenciais e assegurar a retomada rápida das operações, garantindo a resiliência do negócio em momentos de adversidade.

7.1. O que é Gestão de Continuidade de Negócios

A gestão de continuidade de negócios é caracterizada pela reunião de práticas responsáveis pela recuperação ou continuidade das operações de uma empresa, em caso de interrupções dos negócios por ameaças ou imprevisibilidades.

Portanto, é o gerenciamento efetivo que analisa e mapeia os principais riscos das empresas, incluídos os da área de TI, e cria alternativas para que a instituição siga funcionando mesmo que eles se efetivem.

Por meio de análises, treinamentos, auditorias, dentre outras atividades, a gestão de continuidade de negócios (GCN) reflete na maturidade de processos de uma empresa. A partir de sua implementação, há a compreensão por toda a empresa de que suas atividades internas e externas estão conectadas, bastando uma única falha em alguma dessas etapas para que danos sem precedentes ocorram.

Assim, a gestão de continuidade de negócios irá estabelecer uma estrutura pautada em muita estratégia para maturar a capacidade das empresas de agir em caso de riscos, criar métodos alternativos aplicados para suprir alguma ameaça, erro ou falha de um sistema ou dos bancos de dados, e para gerenciar do início ao fim uma possível interrupção de trabalho.

Para alcançar esse objetivo a gestão de continuidade de negócios é focada nos impactos de uma interrupção, mapeando quais são as ações cruciais de uma empresa e os tipos de riscos aos quais elas estão submetidas. No caso de TI a GCN objetiva encontrar esses aspectos na estrutura deste departamento.

Portanto, o escopo básico de uma gestão de continuidade de negócios é:

- **Análise de riscos:** mapear quais ameaças podem impactar a estrutura de TI da empresa e quais são as áreas mais importantes deste negócio que podem sofrer com tais práticas.

- **Análise de impacto:** quais os resultados dessas ameaças, caso concretizadas, para a estrutura de TI.

- **Planejamento estratégico:** como a empresa pode garantir a continuidade de suas atividades ou retomar a produção o quanto antes, diante desse cenário?

7.2. Quais são as etapas do plano de continuidade de negócios

Desenvolver um plano de continuidade de negócios não tem porque ser complexo, porém precisa ser abrangente. Afinal, você já conhece os processos internos da empresa e não deve ter dificuldade para definir como eles devem se adaptar em caso de desastres. É importante também confiar em um software de continuidade de negócio e contar com a participação de atores das diferentes áreas da empresa abrangidas pelo plano.

Definir o objetivo do plano

O primeiro passo na elaboração de um PCN é a definição do objetivo. Sem saber aonde se quer chegar, não se chega a lugar nenhum. Então, comece deixando claro o escopo em que ele se desenvolve e os objetivos a serem alcançados.

A finalidade do PCN é única para qualquer organização: prepará-la para manter suas atividades frente a um eventual desastre. Entretanto, a abrangência do plano varia segundo o setor e o tamanho da empresa, uma vez que esses fatores determinarão qual a amplitude da preparação necessária. Descreva o objetivo do plano no início da elaboração, mas volte para revisá-lo depois de concluídos todos os passos.

Identificar as principais áreas

Existem áreas da empresa que não precisam entrar no PCN, ou porque não são vitais ou porque já estão estruturadas de forma que uma catástrofe não afetará suas atividades. Então, cabe a você determinar quais são as áreas da empresa que precisam de um plano de continuidade.

O departamento de TI figura em praticamente todos os planos de continuidade de negócios, simplesmente porque se trata de uma área vital para o andamento dos demais setores nos dias de hoje.

O departamento de recursos humanos também integra o time principal das áreas que precisam de um plano de contingência, mas isso depende muito da estrutura da empresa e da maturidade organizacional em que ela se encontra.

A comunicação com os funcionários sobre o andamento do plano também é muito importante. Utilize os softwares de comunicação de equipe para informar os trabalhadores

sobre todos os passos. Para os que já adotam sistemas de recursos humanos, é o momento de aproveitar essas ferramentas para ter uma visibilidade total do componente humano.

Se você não tem segurança sobre todas as áreas que devem ser abrangidas pelo PCN, converse com os gestores de cada uma delas e identifique junto com eles se as atividades da respectiva área estão aptas a prosseguirem sem grande impacto em caso de catástrofe.

Identificar as atividades críticas

Uma vez definidas as áreas internas da empresa que farão parte do PCN, o passo seguinte é identificar as atividades de cada uma que são críticas para a continuidade do negócio. É sabido que há tarefas que são mais ou menos vitais dentro da organização, mas isso não significa que sejam dispensáveis.

Nessa fase, o objetivo é diferenciá-las para detectar quais operações precisam, obrigatoriamente, entrar no plano de continuidade de negócios para a atividade da empresa não ser gravemente afetada quando ocorrer um desastre.

Novamente, nessa fase é crucial contar com a participação dos gestores das áreas participantes. É importante cruzar informações para identificar atividades paralelas ou interdependentes, cujo andamento ou resultados decorrem de mais de um setor da empresa.

Determinar o tempo de inatividade aceitável para cada atividade crítica

É incontestável que a ocorrência de um desastre causará algum impacto nas atividades da organização. A proposta do plano de continuidade de negócios é minimizar esse impacto e reduzir ao máximo o tempo de reação da empresa. Para isso, você deve determinar o tempo aceitável que cada atividade crítica pode ficar comprometida.

Atividades mais vitais devem ter prioridade no restabelecimento das funções normais da empresa. Assim, além de definir os prazos de inatividade aceitáveis, é importante também estabelecer a ordem de prioridade da lista de atividades críticas.

Criar um plano de ação e recuperação de desastres

Agora que você já tem o objetivo, as principais áreas envolvidas e as atividades críticas definidos, é hora de criar o plano de ação e recuperação de desastres. Em outras palavras, você deve incluir no PCN como ele será implementado quando necessário.

O plano de ação resume o plano de continuidade de negócios em termos práticos. Nesta etapa, você deve analisar as opções de softwares de continuidade de negócio e selecionar o que melhor se adapta às definições feitas até aqui.

Para ficar completo, inclua os responsáveis e os prazos de cada ação. Ter pontos de controle também é essencial para verificar se a implementação do plano está conforme o esperado. Se possível, faça uma simulação antes da ocorrência de um caso real.

8. ETAPAS DE UMA AUDITORIA DE SISTEMAS

Objetivo

O objetivo deste capítulo é apresentar as etapas de uma auditoria de sistemas.

Introdução

Uma auditoria de sistemas segue um conjunto estruturado de etapas, desde o planejamento até a conclusão e o acompanhamento das ações corretivas. Cada etapa do processo de auditoria de sistemas é essencial para garantir que os sistemas da organização estejam protegidos, em conformidade e operando de maneira eficiente. Neste capítulo, iremos entender todas as etapas e suas atividades. Em resumo, são elas:

- **Planejamento:** Definição de escopo, objetivos, cronograma e equipe.
- **Execução:** Coleta de dados, testes de controles e análise.
- **Avaliação:** Revisão de achados e documentação de riscos.
- **Relatório:** Elaboração de relatórios e apresentação à administração.
- **Acompanhamento:** Implementação de ações corretivas e monitoramento.
- **Conclusão:** Encerramento formal da auditoria.

8.1 Planejamento da Auditoria

O planejamento é a fase inicial e crucial da auditoria, onde os objetivos, escopo e abordagem do processo são definidos.

Etapas do planejamento:

- **Definir os objetivos da auditoria:** Estabelecer o propósito da auditoria, como verificar conformidade, avaliar controles de segurança, identificar fraudes ou otimizar processos.

- **Determinar o escopo:** Identificar os sistemas, aplicações, redes e processos que serão auditados. O escopo pode ser um departamento específico, uma função de TI ou toda a infraestrutura de tecnologia.

- **Avaliação de riscos:** Realizar uma análise preliminar dos riscos para identificar áreas críticas que exigem mais atenção. Isso inclui riscos de segurança, conformidade e operacionais.

- **Recursos e equipe:** Definir a equipe de auditoria, incluindo auditores internos e, se necessário, consultores externos especializados. Também se determina as ferramentas e tecnologias a serem usadas.

- **Cronograma:** Estabelecer um calendário com prazos para cada fase da auditoria, incluindo datas para a entrega de relatórios e revisões.

Exemplo prático: Em uma auditoria de conformidade com a LGPD (Lei Geral de Proteção de Dados), o objetivo é garantir que os sistemas de TI estejam protegendo adequadamente os dados pessoais dos clientes. O escopo pode incluir sistemas de CRM, ERP e servidores de armazenamento de dados.

8.2. Execução da Auditoria

Nesta fase, os auditores realizam as atividades práticas de coleta, análise e validação de informações e sistemas com base no escopo definido.

Etapas da execução:

- **Coleta de dados:** Coletar evidências relevantes, como logs de sistemas, registros de acesso, configurações de segurança e documentos de políticas de TI. Isso pode ser feito por meio de entrevistas, revisões de documentos e análise de sistemas.

- **Testes de controles:** Realizar testes de auditoria para verificar se os controles internos estão funcionando corretamente. Isso pode incluir testes de vulnerabilidade, análise de logs, testes de integridade de dados e revisões de código.

- **Análise de dados:** Usar ferramentas de análise de dados, como ACL ou IDEA, para revisar grandes volumes de dados, identificar anomalias e avaliar o desempenho dos controles de segurança.

- **Amostragem:** Em muitos casos, a auditoria se concentra em uma amostra de dados ou transações, especialmente quando os volumes são muito grandes. Técnicas de amostragem são usadas para garantir que as conclusões sejam representativas.

- **Exemplo prático:** Em uma auditoria de segurança de rede, a equipe utiliza o Nmap para identificar portas abertas e potenciais vulnerabilidades em servidores críticos. Eles também realizam testes de penetração com o Metasploit para verificar se vulnerabilidades podem ser exploradas.

8.3. Avaliação e Documentação

Após a coleta e análise de dados, os auditores fazem a avaliação das informações e documentam suas descobertas.

Etapas da avaliação e documentação:

- **Avaliar as descobertas:** Os auditores comparam as evidências coletadas com os padrões de controle definidos no planejamento, como frameworks de conformidade (ISO, SOX, PCI-DSS). Irregularidades e vulnerabilidades são identificadas.

- **Documentar os achados**: Criar relatórios detalhados sobre os resultados da auditoria, incluindo evidências de falhas de conformidade, deficiências em controles e vulnerabilidades de segurança.

- **Classificação dos riscos:** Cada achado é classificado com base em sua severidade (crítico, alto, médio ou baixo) e impacto no negócio. Isso ajuda a priorizar ações corretivas.

- **Exemplo prático:** Em uma auditoria de segurança, os auditores documentam falhas como contas de usuário sem políticas de senha robustas ou servidores sem patch de segurança. Cada problema é classificado com base no risco que representa para a organização.

8.4. Relatório de Auditoria

Nesta etapa, os achados da auditoria são formalmente apresentados à administração e partes interessadas.

Etapas do relatório de auditoria:

- **Criação do relatório final:** O relatório é elaborado com uma visão geral do escopo da auditoria, achados principais, áreas de risco e recomendações de melhorias. Ele deve ser claro, objetivo e baseado em evidências.

- **Recomendações de ações corretivas:** O relatório inclui sugestões detalhadas de como mitigar riscos identificados, como fortalecer controles de segurança, implementar novas políticas de governança ou realizar atualizações em sistemas.

- **Discussão com a administração:** O relatório é apresentado à alta administração, que deve discutir os achados e decidir sobre as ações a serem tomadas. Feedbacks podem ser coletados para ajustes nas recomendações.

- **Exemplo prático:** Em uma auditoria de TI, o relatório aponta que 20% dos servidores estão com sistemas operacionais desatualizados, o que representa um risco de invasão. A recomendação é implementar um cronograma de atualizações regulares e monitoramento contínuo.

8.5. Acompanhamento das Ações Corretivas

Após a entrega do relatório, é importante acompanhar as ações corretivas recomendadas.

Etapas do acompanhamento:

- **Implementação das recomendações:** A organização deve tomar medidas para corrigir as deficiências identificadas durante a auditoria. Isso pode incluir mudanças em políticas de segurança, melhorias nos processos ou ajustes técnicos nos sistemas.

- **Monitoramento contínuo:** Os auditores podem realizar auditorias de acompanhamento ou monitoramento contínuo para garantir que as ações corretivas foram implementadas e estão funcionando conforme o esperado.

- **Relatórios de progresso:** Relatórios periódicos são gerados para avaliar o progresso das ações corretivas e se elas estão mitigando os riscos identificados.

- **Exemplo prático:** Se uma auditoria de conformidade detectou falhas na proteção de dados, como a ausência de criptografia em bases de dados sensíveis, a equipe de TI implementa a criptografia. Uma auditoria de acompanhamento pode ser realizada após alguns meses para garantir que a criptografia foi corretamente implementada e está em funcionamento.

8.6. Conclusão da Auditoria

Após o acompanhamento das ações corretivas, a auditoria é formalmente concluída.

Etapas da conclusão:

- **Encerramento formal:** Quando todas as ações corretivas foram implementadas ou os riscos foram aceitos pela administração, o processo de auditoria é considerado concluído.

- **Documentação final:** Um relatório final de auditoria é emitido, documentando todas as etapas, achados, ações corretivas e o encerramento do processo.

- **Exemplo prático:** Após verificar que todas as recomendações de segurança foram implementadas e que os sistemas críticos estão protegidos, a auditoria de segurança é oficialmente concluída.

9. HABILIDADES DO AUDITOR DE SISTEMAS

Objetivo

O objetivo deste capítulo é apresentar quais são as habilidades de um auditor de sistemas.

Introdução

Um auditor de sistemas precisa de um conjunto diversificado de habilidades, que vão desde conhecimentos técnicos avançados até competências comportamentais e de gestão. Esses profissionais são responsáveis por garantir que os sistemas de TI de uma organização estejam seguros, eficientes e em conformidade com regulamentos. A seguir, teremos uma visão detalhada das principais habilidades de um auditor de sistemas, bem como a sua rotina diária.

9.1. Habilidades Técnicas

Auditores de sistemas precisam dominar várias tecnologias, metodologias e ferramentas relacionadas à TI. Essas habilidades técnicas são fundamentais para identificar falhas, vulnerabilidades e problemas de conformidade.

Conhecimento em Arquitetura de TI

Entender a arquitetura de sistemas de TI, incluindo servidores, redes, banco de dados, e infraestrutura de hardware e software. Auditores de sistemas precisam compreender como os componentes de TI se interconectam e como fluxos de dados são gerenciados.

Exemplo prático: Ser capaz de auditar um sistema ERP (Enterprise Resource Planning), compreendendo como ele se integra aos sistemas financeiros, de estoque e de produção da empresa.

Segurança da Informação

Conhecimento sobre princípios de segurança da informação, como confidencialidade, integridade, disponibilidade, autenticação, criptografia e proteção contra-ataques cibernéticos.

Exemplo prático: Ser capaz de auditar a política de controle de acessos de uma empresa e identificar se há permissões excessivas, contas sem supervisão ou ausência de políticas de autenticação multifator (MFA).

Ferramentas de Auditoria e Análise

Experiência no uso de ferramentas como Audit Command Language (ACL), IDEA, Wireshark, Splunk, e ferramentas de testes de penetração como Nmap, Nessus,e Metasploit.

Exemplo prático: Usar o Wireshark para capturar pacotes de dados e identificar tráfego suspeito ou o ACL para analisar grandes volumes de transações financeiras em busca de anomalias.

Conhecimento em Normas e Padrões de TI

Compreensão das principais normas e frameworks de TI e segurança, como ISO 27001, COBIT, ITIL, PCI-DSS, GDPR (Regulamento Geral de Proteção de Dados), e SOX (Sarbanes-Oxley Act).

Exemplo prático: Realizar auditorias de conformidade com a ISO 27001, verificando se as práticas de segurança de informação da empresa estão alinhadas aos requisitos da norma.

Conhecimentos em Bancos de Dados e Linguagens de Consulta

Entendimento dos principais bancos de dados (SQL, Oracle, NoSQL) e a capacidade de usar linguagens de consulta, como SQL, para extrair dados necessários para a auditoria.

Exemplo prático: Utilizar queries SQL para acessar registros em um banco de dados financeiro e garantir a integridade das transações processadas.

Conhecimentos em Desenvolvimento de Software

Familiaridade com o ciclo de vida do desenvolvimento de software (SDLC), práticas de desenvolvimento seguro e auditoria de código-fonte.

Exemplo prático: Revisar o código-fonte de uma aplicação para identificar vulnerabilidades como injeção de SQL ou Cross-Site Scripting (XSS).

9.2. Habilidades Comportamentais

Além das competências técnicas, auditores de sistemas também precisam de habilidades comportamentais, essenciais para colaborar com diferentes equipes e navegar em situações complexas e sensíveis.

Pensamento Crítico e Analítico

Habilidade de avaliar sistemas e dados com precisão, identificar anomalias e correlacionar informações para chegar a conclusões lógicas.

Exemplo prático: Detectar uma inconsistência em um conjunto de dados que, à primeira vista, parece normal, mas que pode indicar uma fraude ou falha de sistema.

Capacidade de Solução de Problemas

Capacidade de identificar problemas de TI e propor soluções viáveis e práticas. Auditores precisam entender as causas subjacentes dos problemas, não apenas os sintomas.

Exemplo prático: Em uma auditoria de rede, identificar a causa raiz de vulnerabilidades abertas em uma infraestrutura crítica e recomendar ações corretivas específicas, como a aplicação de patches ou reconfigurações de firewall.

Comunicação Eficaz

Habilidade de explicar achados técnicos complexos de forma clara e acessível a stakeholders não técnicos, como diretores e gerentes de áreas de negócio.

Exemplo prático: Apresentar um relatório de auditoria a executivos de uma empresa, traduzindo questões técnicas em termos de risco e impacto nos negócios.

Ética e Integridade

Auditores de sistemas precisam ter um forte senso de ética, pois lidam com informações confidenciais e podem descobrir falhas que podem ter consequências graves. A integridade é fundamental para garantir uma auditoria objetiva e imparcial.

Exemplo prático: Durante uma auditoria, um auditor encontra evidências de fraude interna. Ele deve manter sigilo e seguir os protocolos apropriados para notificar a administração ou órgãos reguladores, sem comprometer o processo.

Gestão de Tempo e Organização

Auditores frequentemente gerenciam várias auditorias simultaneamente, cada uma com prazos apertados. Habilidades de organização e gestão de tempo são essenciais para garantir que todas as etapas da auditoria sejam concluídas dentro do prazo.

Exemplo prático: Durante uma auditoria de conformidade em uma grande organização, o auditor precisa gerenciar o progresso de diferentes equipes, acompanhar o status das atividades e garantir a entrega dos relatórios finais conforme o cronograma.

9.3. Rotina do Dia a Dia de um Auditor de Sistemas

A rotina de um auditor de sistemas pode variar dependendo do projeto e do estágio da auditoria, mas geralmente envolve um conjunto de atividades focadas na preparação, execução, análise e comunicação.

Revisão de Documentação e Políticas

Os auditores revisam políticas de TI, manuais operacionais, regulamentos internos e padrões para garantir que estejam de acordo com as melhores práticas e normas de conformidade.

Exemplo prático: Um auditor revisa as políticas de controle de acesso da empresa para garantir que estejam de acordo com os requisitos da ISO 27001.

Coleta de Evidências

Os auditores obtêm dados de logs, acessos a sistemas, relatórios de uso de recursos e transações para validar a conformidade e identificar problemas.

Exemplo prático: Coletar logs de autenticação de usuários e logs de acesso de sistemas para verificar possíveis tentativas de acesso não autorizado.

Testes e Verificações

Realização de testes de vulnerabilidade, auditoria de configuração de rede, testes de controles de acesso e análise de segurança em sistemas.

Exemplo prático: Realizar uma varredura de vulnerabilidades usando o Nessus para identificar falhas de segurança em servidores da empresa.

Análise de Dados

Análise de grandes volumes de dados para detectar inconsistências ou padrões incomuns que possam indicar fraudes ou violações de conformidade.

Exemplo prático: Analisar transações financeiras com o ACL ou IDEA para identificar duplicidades, fraudes ou erros no sistema de faturamento.

Reuniões e Colaboração

Auditores participam de reuniões com equipes de TI e outros departamentos para discutir os achados da auditoria, identificar causas raiz de problemas e colaborar na resolução.

Exemplo prático: Reunião com a equipe de segurança de TI para discutir recomendações de segurança após identificar brechas em políticas de firewall e VPN.

Elaboração de Relatórios

Preparação de relatórios detalhados que descrevem os achados da auditoria, explicam os riscos e oferecem recomendações de melhorias.

Exemplo prático: Criar um relatório detalhado para a alta administração, destacando as áreas de risco de conformidade e as ações corretivas necessárias.

9.4. Certificações Relevantes

Para complementar suas habilidades, auditores de sistemas podem buscar certificações que são amplamente reconhecidas e valorizadas no mercado:

- CISA (Certified Information Systems Auditor): Focada em auditoria de sistemas e controle de TI.
- CISM (Certified Information Security Manager): Focada em gestão de segurança da informação.
- CISSP (Certified Information Systems Security Professional): Focada em segurança da informação.
- ISO 27001 Lead Auditor: Focada em auditorias de sistemas de gestão de segurança da informação.