Auditoria De Sistemas

Estar por dentro de tudo o que acontece na sua empresa é um desafio complementar, no contexto da transformação digital.

Afinal de contas, além de monitorar e assegurar a conformidade de aspectos contábeis, organizacionais e de processos, cabe a aplicação da auditoria de sistemas de informação.

E você já aplica algo similar na sua empresa? O tema é fundamental, hoje em dia, porque expõe a pluralidade da nossa relação com dados, atualmente.

Inclusive, para as empresas isso significa mais atenção com relação à sua segurança cibernética e também com o uso ético dos dados de usuários externos.

O que é auditoria de sistemas de informação?

Por meio de um processo multidisciplinar, a auditoria de sistemas de informação tem o objetivo de avaliar a conformidade do ambiente informatizado da empresa.

Assim, estabelece-se um meio íntegro de compilação, uso e manipulação de dados em cada computador e nos sistemas.

Tudo isso, de acordo com a legislação vigente, as melhores práticas e checagem dos protocolos de segurança e qualidade.

É, assim, uma metodologia similar aplicada em auditorias convencionais. A grande diferença está na sua aplicação dedicada ao ambiente digital.

Qual é o objetivo da auditoria em sistemas de informação?

Ainda não sabe qual é o objetivo da auditoria em sistemas de informação? Basicamente, estamos falando de uma série de procedimentos que visa identificar falhas e alinhar protocolos e processos em conformidade com as melhores práticas do setor de ti.

Com isso, é possível identificar oportunidades de melhoria, correção e implementação para promover a segurança e a qualidade geral dos sistemas corporativos.

Para tanto, a auditoria em sistemas de informação tende a passar por etapas bem definidas, que são:

Planejamento;

Execução;

Relatório com resultados;

Plano de ação.

Auditores usam, para isso, parâmetros para estabelecer um controle específico de metas e, assim, avaliar quais delas a empresa alcança — ou não.

Quais os tipos de auditoria de sistemas?

No geral, estamos falando de dois tipos de auditoria de sistemas: interna e externa.

A primeira é realizada dentro da própria empresa, por meio de auditores que realizam os procedimentos estipulados para avaliar seus sistemas e procedimentos.

Lembrando, apenas, que existem competências, habilidades e experiências específicas (como capacitação em iso 9001) para a realização da auditoria.

Não é qualquer pessoa que tem o conhecimento necessário para realizá-la — não sendo, portanto, um mero meio de testar os sistemas.

Auditoria não é um pentest, por exemplo — que é de grande importância para a empresa, mas não carrega as competências de uma auditoria.

E a auditoria externa não ocorre por profissionais da empresa, mas por um auditor independente. Um meio de ter visões e perspectivas de fora (literalmente) da empresa e averiguar se os processos estão de acordo com normas, diretrizes e leis em vigor.

Ambas têm seus valores e aspectos a serem considerados, por isso é importante analisar detalhadamente conforme os seus objetivos.

Agora, no que tange às auditorias em ti mais aplicadas, podemos destrinchar o assunto em mais variáveis. Por exemplo:

Legal ou regulatória

Integridade de dados

Segurança cibernética e segurança da informação;

Segurança física;

Desenvolvimento de sistemas.

É importante analisar o que você e a sua equipe pretendem, por meio da auditoria de sistemas de informação. Assim, os resultados são melhor direcionados, assim como toda a jornada de planejamento e execução do trabalho.

Quais as etapas da auditoria de sistemas?

Antes de aprender como se preparar para uma auditoria, vale a pena entender como ela é conduzida, passo a passo.

E, para isso, abaixo detalhamos as etapas da auditoria de sistemas. Confira, e entenda o papel relevante de cada uma delas!

Planejamento

O planejamento é, literalmente, a fase de análise e avaliação do processo em si.

Por exemplo: os objetivos da auditoria, os riscos observados em todos os processos e as expectativas desse trabalho extenso e recheado de procedimentos e detalhes.

Execução

Hora de colocar sob análise tudo aquilo que foi discutido e apontado como relevante para a condução da auditoria de sistemas de informação.

Aqui, o auditor (independente ou interno) realiza suas atividades dentro do seu escopo de atuação e em alinhamento com o que foi proposto ao longo de todo o planejamento.

Relatório de resultados

O relatório de resultados é mais uma parte significativa das etapas de uma auditoria de sistemas de informação. Afinal, é por meio dele que se obtém as análises e impressões do trabalho do auditor.

Algumas orientações que podem vir à tona a partir dessa fase da auditoria:

Redução ou erradicação de falhas no processo;

Identificação e prevenção de fraudes;

Apontamento de novas garantias de segurança e integridade dos dados e do sistema de informação em geral;

Aprimoramento dos serviços prestados pelo departamento de ti.

Tudo isso, é claro, colocando à prova a confiabilidade dos seus sistemas de informação. Isso importa não apenas com base nos valores acima citados, mas para identificar a conformidade da sua empresa com padrões estabelecidos por órgãos ou o próprio governo.

Plano de ação

Agora que já foi visto como é feita uma auditoria em uma empresa, falta apenas colocar em prática tudo aquilo apontado no relatório.

O plano de ação é, justamente, uma resposta à etapa anterior. Os resultados são analisados e planos de correção, melhoria, implementação e inovação devem ser estabelecidos para alinhar às sugestões do auditor.

Quais são as três abordagens de auditoria de sistemas de informações?

Os testes de auditoria podem ser focados de diferentes maneiras para colocar sob análise os sistemas da empresa. E, a seguir, vamos explicar melhor como eles são conduzidos de acordo com as características do seu negócio e os objetivos e necessidades da auditoria.

Abordagens ao redor do computador

Nesse tipo de auditoria, o profissional especializado avalia os níveis de anuência segundo os controles organizacionais tecnológicos do sistema.

E isso tende a se resumir às funções de entrada e de saída — e pouco (ou quase nada) nas funções de processamento em si.

Isso acontece,porque esse tipo de auditoria em ti já ocorria antes mesmo da transformação digital. Só que a aplicação de dados era igualmente limitada, como a análise de um nível de estoque.

Dessa maneira, sua aplicação atual, em auditorias de sistema de informação, é mais focada em atividades menores.

Pois o uso dos sistemas digitais, atualmente, implica ações mais complexas e que se estendem à mera digitação de dados.

Até por isso, embora tenha o seu valor em aplicações associadas de auditoria, o método é tido como incompleto e também inconsistente quando analisado individualmente.

Isso também coloca em questão a sua eficiência operacional na auditoria.

Através do computador

A abordagem desse tipo de auditoria de sistemas de informação empreende uma atividade de análise completa através e no interior do computador. É, inclusive, um excelente complemento à técnica que citamos acima.

Afinal, é possível avaliar o sistema de múltiplas maneiras, assim, agregando mais valor e confiabilidade aos resultados obtidos.

Confira, a seguir, algumas das vantagens mais evidentes desse tipo de auditoria:

Traz mais habilidades de análise e processamento ao auditor;

Abrange as áreas de análise e testes realizados pelo profissional.

Mas é importante analisar, sempre, os pontos de atenção desse método. Principalmente, no que diz respeito à checagem de informações.

Isso porque, muitas vezes os resultados devem ser confrontados e, para isso, passam por revisões manuais.

Com o computador

Pois entre os diferentes tipos de auditoria de sistemas de informação, falamos sobre a abordagem ao redor do computador, que perdeu sua eficiência ao longo dos anos.

Também destacamos que a abordagem através do computador — embora superior à anterior — produz registros incompletos. Isso porque, ela pode ignorar procedimentos manuais, o que minimiza a abrangência de resultados obtidos.

Daí, a solução por meio da abordagem com o computador. Por meio dela, é possível auditar as tecnologias com mais amplitude, e sem perder as características detalhistas.

O que, consequentemente, agrega mais valor, precisão e assertividade ao trabalho.

E por meio desse tipo de abordagem em auditoria de sistemas de informação se configura em algumas ações-chave, como:

Análises mais complexas de dados lógicos e aritméticos (como o cálculo de depreciações e taxas e impostos, entre outros);

Capacidade de cálculos estatísticos gerais e específicos;

Capacidade de edição e classificação do sistema (o que favorece o auditor para computar diversas bases de dados e analisar informações com mais precisão e detalhes);

Obter listas de amostras de auditoria.

Qual a importância de se realizar uma auditoria de sistemas de informação?

Até aqui, exploramos algumas das características da auditoria de sistemas de informação. E, a partir delas, deve ter dado para compreender a importância desse processo nas empresas.

Inclusive, a auditoria de ti é determinante para melhorar a relação das organizações e seus gestores com as novas tecnologias. E, é claro, também com relação ao papel do auditor nisso tudo.

Trata-se de uma evolução natural da profissão e da forma com a qual nós recebemos, computamos, registramos e manipulamos a informação digital.

E isso tende a se traduzir em benefícios internos e externos. Afinal, passamos a compreender melhor como promover a segurança da empresa contra invasões e também contra a violação de dados.

Sem falar que usamos com ética e responsabilidade os dados obtidos de usuários na internet.

Algo que agrega mais qualidade aos processos aplicados, na empresa, e confere uma reputação mais positiva, em geral.

Mas veja o que isso tudo significa e o que mais a auditoria de sistemas de informação pode trazer para o seu empreendimento:

Eficiência operacional;

Redução de custos;

Redução de riscos associados à auditoria;

Alinhamento com as tendências e as futuras necessidades e características do mercado tecnológico.

Como se preparar para uma auditoria?

Anteriormente, destacamos que a auditoria de sistemas de informação passa por quatro etapas bem definidas. A primeira é o planejamento, seguido da execução, do relatório de resultados e do plano de ação.

Independentemente de realizar uma auditoria interna ou externa, sua empresa pode se preparar para uma auditoria da mesma forma.

E, abaixo, vamos explorar o passo a passo para garantir um processo menos envolto em riscos e imprevistos. Confira:

Elabore um plano com periodicidade definida

Não deixe para conferir todos os processos às vésperas da auditoria. Além de falho, o processo é recheado de erros e imprevistos que podem prejudicar o resultado final.

Por sua vez, entenda o que a auditoria de sistemas de informação confere e componha um plano de periodicidade para isso. Ou seja: com auditorias anuais, você consegue reunir sua equipe para realizar checagens com certa antecedência.

E isso é importante porque reduz o trabalho após realizada a auditoria e também agrega valor ao trabalho da sua equipe.

Afinal, eles vão continuamente aprendendo a manter conformidade aos processos e ficar dentro dos parâmetros estabelecidos na auditoria.

Para tanto, vale a pena realizar duas atividades específicas: conscientizar sua equipe sobre a importância da auditoria (e dos resultados) e entender quais departamentos são auditados.

Isso torna o seu trabalho cotidiano muito mais focado e assertivo.

Padronize os processos

A padronização é fundamental para tornar a empresa mais sob controle, segura, produtiva e auditável. Questões que só têm a agregar ao longo do ano inteiro.

E é algo também elementar para garantir bom preparo para as auditorias previstas na sua empresa. Aqui vão algumas dicas para dar início a esse processo de uniformização das atividades e processos do fluxo produtivo:

Elabore um manual de boas práticas e que tenha todo o trabalho mapeado;

Descreva os procedimentos para que todos aprendam, e compreendam, seus papéis e atividades dentro da infraestrutura da empresa;

Acompanhe a execução dos processos;

Capacite os profissionais e treine-os, gradativamente, até que a prática se torne um hábito natural;

Monitore os resultados das ações.

Lembre-se que você pode ir além com a aplicação da auditoria de sistemas de informação.

Auditoria de sistemas e a organização nacional de padronização

No entanto, 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.

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 contratada pela própria empresa ou pode ser um processo determinado pela leis relacionadas ao setor de atuação da empresa, tornando a auditoria externa obrigatória.

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

Qual é a importância da auditoria de sistemas?

Mas afinal, qual é a importância da auditoria de sistemas?

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:

Desempenho;

Segurança;

Privacidade;

Confiabilidade;

Integridade;

Disponibilidade;

Confidencialidade;

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

Qual é a relação com a lgpd?

Nós já falamos nesse artigo que 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.”.