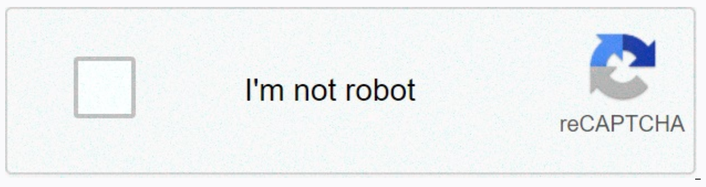

Continue

Segurança e auditoria de sistemas pdf

Este artigo ou seção contém uma lista de referência no final do texto, mas suas fontes não são claras porque não são citadas no corpo do item, o que comprometeu a confiabilidade das informações. Ajude a melhorar este artigo colocando citações no corpo do artigo. (Janeiro de 2012) A auditoria de sistemas de computador ou riscos tecnológicos é uma atividade independente envolvida como missão de gestão de riscos operacionais envolvida e avalia a desdecrtuação das tecnologias e sistemas de informação utilizados na organização da revisão e avaliação de controle, desenvolvimento de sistemas, Procedimento de TI, Infraestrutura, Operação, Desempenho e Segurança da Informação envolvendo o processo de tomada de decisão crítica das informações. A auditoria do Sistema Objetivo é um processo realizado por profissionais qualificados e consiste em reunir, agrupar e avaliar evidências para determinar se um sistema de informações adequado suporta uma vantagem empresarial, manter a integridade dos dados e alcançar as metas esperadas, utilizar eficientemente os recursos e cumprir com as normas e leis estabelecidas. Permite detectar automaticamente o uso de recursos e obter informações de fluxo em uma empresa e determinar quais informações são fundamentais para o progresso de sua missão e finalidade, identificando necessidades, processos repetidos, custos, valores e barreiras que impactam informações eficientes de fluxo. Deve compreender não apenas os equipamentos de processamento de dados ou alguns procedimentos específicos, mas sim suas visões, processamento, controles, arquivos, segurança e extração de informações, além disso, devem avaliar todo o ambiente envolvido: Equipamentos, Processamento de Data Center e Software. A auditoria consiste principalmente na avaliação de mecanismos de controle implantados em uma organização da empresa, determinando se devem se adequar e cumprir determinadas finalidades ou estratégias, estabelecem as mudanças necessárias para obtê-los. Mecanismos de controle podem prevenir, detecção, edição ou recuperação após um preocupante. Os objetivos da auditoria do

sistema são o problema de uma entrada (ou uma nota) sobre: o Controle da Área de Tecnologia; A análise da eficiência dos sistemas de informação; Verificação do cumprimento das leis e regulamentos a que estão sujeitos; A gestão efetiva dos recursos de TI. Os sistemas de auditoria contribuem para o constante aprimoramento do negócio apoiado pela tecnologia, nos seguintes aspectos: Desempenho; confiabilidade; Integridade; Disponibilidade; Segurança; Confidencialidade; Confidencialidade. Geralmente, pode ser desenvolvido em foco ou em combinação entre as seguintes áreas: Governança Corporativa; Sistema de Administração do Ciclo de Vida; Serviços de entrega e suporte; Proteção de dados e segurança da informação; O negócio continua com o plano de recuperação de desastres. Sistema auditivo O eficiência de auditoria do sistema para regular a segurança e os procedimentos existentes, a eficácia dos processos de uso, o uso correto dos recursos disponíveis, a administração da elaboração de planos e definições de finalidade, colaborando na melhoria de seus controles internos, apresentando déficits e irregularidades que possam comprometer a segurança e o desempenho organizacional. Com o amplo uso de tecnologias para armazenamento de informações contábeis, financeiras e operacionais, o auditor do sistema tem melhorado no campo de operação (processamento) da organização extraída, analisando o banco de dados envolvido e apoiando decisões de outras áreas de auditoria. A necessidade global de referência nesse tema, de exercer essa profissão, promover a criação e o desenvolvimento de melhores práticas como COBIT, COSO, ISO 27001 e ÚTIL agora a certificação CISA – Sistemas Certificados de Auditoria de Informações, Oferecido pela ISACA – Associação de Sistemas de Informação e Controle é uma das organizações mais reconhecidas e avaliadas por organizações internacionais, uma vez que o processo seletivo consiste em um extenso teste que exige conhecimento avançado, além da experiência profissional e da necessidade de se manter atualizado, por meio de uma política de educação continuada (CPE) na qual o titular do certificado deve acumular treinamento para cada período estabelecido. A formação acadêmica do computador do sistema para o final mais alto é multidiscippline: sistemas de análise, ciência da computação, administração e ênfase em TI, defesa focada em direito da computação – direito digital e correto. Os tipos de auditoria são vários tipos de Auditoria de Sistemas, estes são principais, mas não apenas: Auditoria de Planejamento e Gestão: Contração de Seus Bens e Serviços, Documentos, Orçamento, Projetos, Etc. Auditoria Legal ou Regulatória: Cumprimento de regulamentos locais e internacionais, exemplos: Lei Sarbanes-Oxley, Basileia III, Comissão de Valores Mobiliários, etc. Auditoria de Integridade de Dados: Classificação de dados, atualização, banco de dados, aplicativo, acesso, estudo de fluxo de transmissão (entrada e saída), verificação de controle de qualidade e disponibilidade de informações. Auditoria de informações de segurança: métodos de autenticação, autorização, criptografia, gerenciamento de certificados digitais, segurança de rede, gerenciamento de usuários, configuração antivírus, atualizações, políticas, padrões, manuais operacionais. Auditoria de Segurança Física: Avaliação de moradores e riscos ambientais: vida (capital intelectual), offt/roubo, acesso, umidade, temperatura, acidente, desastre, etc. com proteção: perímetro de segurança, câmera, sensores, guarda, dispositivo, proteção ambiental. Sistema de auditoria de desenvolvimento: validação de processos de gerenciamento de projetos, metodologia de conformidade e qualidade, previsão orçamentária e e avaliação de desvio. Auditoria de Infraestrutura e Operações de TI: Processos para investigar a disponibilidade e confiabilidade do ambiente de erro, acidente e fraude em operação em servidores, estações, software, hardware e canais de comunicação. Materiais, GRC e Análise de Riscos Ao planejar o calendário anual e cada auditoria do trabalho do público-chefe decide o nível de auditoria de risco (ou seja, o risco de chegar a uma conclusão irrestável com base nas evidências) que ele quer aceitar. Quanto mais eficiente e extensa for a tarefa de auditoria, o menor risco de uma fraqueza no processo será despercebido no relatório final de auditoria. A Auditoria de Risco depende da análise dos níveis de risco de cura no processo, ou seja, a possibilidade de impacto material do processo: financeiro, operacional ou de imagem, se a área de audiência é equivocada por controles efetivos ou não existentes. Esses riscos determinam quando o público realiza ou obtém a análise de risco de uma organização. Além disso, para avaliar se há uma auditoria de TI para alcançar o sucesso esperado, o auditor deve primeiro identificar o escopo e testar metas para verificar a adesão de grau aos processos e sistemas avaliados. Para cumprir a meta de auditoria e garantir que os recursos utilizados para o seu trabalho sejam utilizados de forma eficiente, o público deve definir os níveis materiais. O público deve considerar aspectos qualitativos e quantitativos para determinar os materiais. A avaliação de risco deve ser realizada para proporcionar um certo grau de conforto de que todos os itens do material relevante serão devidamente cobertos pelo trabalho de auditoria. Esta análise deve identificar áreas com alto risco de problemas que contenham material valioso no negócio. Impacto material avaliado materialmente, o Auditor do Sistema deve considerar: O nível de erros aceitáveis na gestão de processos, auditorias internas, auditorias externas, agências reguladoras e legislação. O potencial cumulativo de pequenos erros ou fraquezas torna-se material, neste caso, em marco importante. Ao mesmo tempo em que estabelecem materiais, os ouvintes podem realizar auditorias de itens não financeiros, como controle de acesso físico, lógica, sistemas de gestão de pessoas, gerenciamento de recursos, desenvolvimento, controle de qualidade, geração de senhas. Neste caso, os materiais devem ser identificados, com foco nas metas esperadas do processo de avaliação de negócios para que ele atinja suas metas de controle interno. Quando nenhuma transação financeira está envolvida, outras formas de medir o material podem ser utilizadas: O nível crítico do processo é suportado pelas operações ou sistemas avaliados. Custo ou operação do sistema (peças de computador, software, contrato de fornecedor). Custo potencial de erros ou falhas em que sistemas ou operações estão sujeitos. Número de acesso/transações / solicitações processadas por período. cumprimento de requisitos legais e contratos. Os antecedentes da sigla de Análise de Risco do GRC e do GRC vêm da união do termo governança, risco e conformidade, ou em inglês, governança, risco e conformidade. Uma tendência recente, na integração das áreas de conhecimento por meio de Gestão de Riscos, Governança Corporativa e Práticas de Controle, teve como objetivo garantir o cumprimento das leis, regulamentos, a imposição de consolidação de normas em um único modelo, inteligentemente integrado e tem como um de seus objetivos a unificação do interesse comum e a reconciliação de interesses opostos a interesses opostos de cada uma dessas funções. Nesse contexto de risco pode ser definido como o efeito da precariedade de propósito, está então relacionado à probabilidade de um evento que ocorre e aos possíveis impactos do evento sobre as metas de negócios. Por meio da Gestão de Riscos da Organização buscando antecipar perdas de falha de procedimento, causar acidentalmente ou não, externos, econômicos, ambientais, ameaças de mercado ou quaisquer eventos que possam constily interessar a organização ou impedir que oportunidades significativas para o sucesso da empresa tirem vantagem de risco é qualquer evento ou ação, produzindo internamente ou externamente, impedindo que uma organização atinja seus objetivos. O risco afeta os propósitos de controle em diversas áreas de informação: integridade, precisão, tomada de decisão temporariamente, capacidade de acesso ao sistema e confidencialidade/privacidade das informações, apenas para gerar algum impacto relacionado. A análise de risco permite que os ouvintes determinem o escopo da auditoria e avaliem o nível de auditoria de risco e risco de erro (o risco de erros ocorridos na área ser ordenada). Além disso, a análise de risco ou análise de impacto nos negócios (BIA) ajudará em decisões como: a natureza, os adversários e o cronograma do trabalho. As áreas de negócios devem ser audiências. Estão previstos tempo e recursos associados a cada tarefa de auditoria. Documentação de Análise de Risco Uma vez analisado o nível de risco, a auditoria deve documentar essa análise de seu trabalho: Descrição da Técnica de Análise de Risco Utilizada para identificar os riscos e maior significado do risco de que a auditoria abordará evidências utilizadas para apoiar a análise de risco do público. Os ouvintes do sistema lifecyle seguem os mesmos passos da auditoria tradicional, sob: Global (Anual) Planejamento para Identificar áreas de risco na organização: financeira, operacional, regulatória; Compreensão da tecnologia da informação de dependência em processos críticos; Acompanhamento da aplicação em recomendações de auditorias passadas; Estabeleça horários de desempenho. Planejamento para encontrar informações sobre o processo: fluxos, políticas, normas e procedimentos; Ver pontos de controle para identificar vulnerabilidades; Estabelecer planos de teste para cobri-los; Achar melhores práticas para preparação de testes; Define responsável pela frente de trabalho. Plano de Realização executar o exame; Encontrar evidências que tenha controle adequado ou não; Itens de validação levantados com o público; Formalizar métodos de teste e conclusões em documento de trabalho; Reúna os principais controles de incidentes para discussão. Conclusões de Melhoria Contínua Discutir planos de ação e audiências; Estabelecer prazos para resolver problemas de acordo com os riscos e impactos envolvidos; Apresentar relatório final para aprovação pela alta gestão de pós-graduação; Arquivo para rastreamento de implantação. Monitoramento acordado de fim de data; Reafirma a situação atual; Emitir um parecer sobre a nova situação nos controles anteriores requer a manutenção de níveis aceitáveis de risco. Análise de Dados e Ferramentas para a execução de testes de auditoria, utilizados pelo auditor para encontrar evidências para apoiar sua conclusão, deve-se observar geralmente aceitando normas como ISACA S6 – Desempenho do trabalho de auditoria #REDIRECT[1] Evidência: Durante o curso da auditoria, o auditor do EI deve obter provas suficientes, confiáveis e relevantes para atingir os objetivos da auditoria. Os resultados e conclusões da auditoria devem ser apoiados pela análise e interpretação adequadas dessas evidências. Auditoria de amostras um sistema de auditoria pode ser realizado de forma manual em massa: ou seja, 100% de todos os documentos e dados disponíveis ou por amostras dessa população. A amostra de auditoria é a aplicação de procedimentos para utilizar uma taxa inferior a 100% da população, a fim de permitir que os Sistemas de Auditores avaliem evidências que lhe permitam formular uma conclusão sobre essa população. Ao projetar o tamanho e a estrutura da amostra, o Auditor do Sistema deve considerar as metas de auditoria determinadas no planejamento, a natureza da população e os métodos de seleção de amostras. Selecionar a amostra de Ouvintes deve selecionar itens de amostra para representar a população. Os tipos mais comuns de amostras são: Random Sample Statistics – permite que todas as combinações de amostras da população tenham igual chance de seleção. Amostra sistemática – permite a seleção de incidentes na amostra, utilizando intervalos de seleção e intervalos para começar aleatoriamente. Amostra não amostra por escolha – o público seleciona a amostra sem uma técnica estruturada. Análise do juiz – A audiência estabelece um critério para a amostra. Por exemplo, selecione Unidades apenas acima de um determinado valor. A seleção do tamanho da amostra afetada pelo nível de risco ou esta amostra está representada no processo avaliado. O risco amostral é o risco de uma amostra erroneamente escolhida influenciar a última opinião final do público, em comparação com se o público usou toda a população. Uma vez selecionados amostras para testes, esses procedimentos devem ser adequadamente documentados nos trabalhos. Uso de técnicas de amostra Percentual considerado layout de arquivo, sistema considerado rotina, código fonte, ferramenta CAAT usam parâmetros de seleção de audiência para iniciar testes de computador via Técnicas de Auditoria de Computador (CAATS) ou TAACs, discutidos logo abaixo. Auditoria Técnica Assistida por Computador (CAATS) ou TAACS Mais Informações: Análise de dados, Linguagem de Comando de Computador, Ferramenta Técnica de Auditoria Assistida por Computador (ou Ferramenta) Ferramenta de Auditoria Assistida por Computador (CAATS) ou TAACs são técnicas especializadas ou programas de computador que geram amostras, importação de dados, importação de dados, soma e teste os monitores, condições e processos implantados nos sistemas das amostras selecionadas. Tipo CAATs incluem: Software de Auditoria Especializada (CEA) - permite que o público teste em arquivos e bancos de dados, exemplos: Analisador Arbutus, IDEA, etc. O Software de Auditoria Sob Medida (SAA) – geralmente desenvolvido pelos ouvintes para realizar tarefas específicas, é necessário quando os sistemas da empresa não estão em conformidade com o exterior, ou quando o público quer testar não é possível com o SEA, por exemplo, a rotina: Easy Trieve, SQL+, SAS, etc. Teste de dados ou operação de recálculo – o público testa os dados para verificar os controles dos funcionários do sistema por meio da validação desses dados, além disso, observa-se a precisão desses dados processados pelo sistema. Esta técnica é utilizada para validação de dados e erros de detecção de rotina, processamento de controle lógico e cálculos aritméticos, apenas para numerar algumas possibilidades. Simulação Paralela – o público utiliza informações no sistema de mapas e constrói as etapas a serem simuladas em outra ferramenta para alcançar o mesmo resultado do sistema. Integre os ouvintes de teste para enviar parâmetros de teste com dados reais, sem afetar rotinas no processamento normal do sistema. Coleta de provas através do uso do CAATS, o público poderá obter provas suficientes para apoiar os resultados finais de auditoria do sistema. As provas de auditoria devem ser suficientes, confiáveis, relevantes e capazes de auxiliar o público a formular o parecer e conclusões sobre o processo avaliado. Se o público não tem dados suficientes para fazê-lo, deve sair do campo para obter mais provas. Os procedimentos para isso variam dependendo do sistema ser ouvinte. O público escolherá o teste mais adequado para alcançar o objetivo de auditoria. Alguns listados abaixo podem ser considerados: Entrevistas e/ou Notas O monitoramento de outras evidências de reteste que a auditoria encontra deve ser documentado e organizado para apoiar os inquéritos de áudio e suas conclusões. Por fim, quando o público acredita que estes não são possíveis de encontrar qualquer razão, esse fato deve ser documentado no Relatório de Auditoria como um limite para o escopo da obra. AUDITORIA BIBLIOGRÁFICA DE REFERÊNCIA NO SISTEMA - CURSO PRATICO, Alessandro Manotti, Editora CIENCIA MODERNA, 2010, ISBN 8573939400, 9788573939408 ENTIDADE ISACA – Associação de Auditoria de Sistemas de Informação e Controle ISSA – Sistemas de Seguridade Social IIA BRASIL – Instituto de Auditores Internos no Brasil – [2] encontrada em