UNIVERSIDADE DE CAXIAS DO SUL
CENTRO DE COMPUTAÇÃO E TECNOLOGIA DA INFORMAÇÃO
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

MAURICIO MODESTO TOSCAN BRANDALISE

ROTEIRO PARA ELABORAÇÃO DE PROGRAMAS DE AUDITORIA EM SISTEMA ERP (*ENTERPRISE RESOURCE PLANNING*)

CAXIAS DO SUL
2012

MAURICIO MODESTO TOSCAN BRANDALISE

ROTEIRO PARA ELABORAÇÃO DE PROGRAMAS DE AUDITORIA EM SISTEMA ERP (*ENTERPRISE RESOURCE PLANNING*)

Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistema de Informação da Universidade de Caxias do Sul.

Orientadora Prof[a]. Iraci Cristina da Silveira De Carli

CAXIAS DO SUL
2012

RESUMO

Neste trabalho será proposto um roteiro para a elaboração de programas de auditoria, os quais estarão focados em sistema ERP (*Enterprise Resource Planning*) já em utilização. O roteiro visa ser um instrumento de apoio a equipes de auditoria. Por meio de procedimentos, normas e técnicas aplicáveis a auditorias em sistemas ERP, o roteiro terá o papel de auxiliar na estruturação de elementos que compõem um programa de auditoria. Serão avaliadas normas, técnicas e ferramentas que possam deixar o procedimento de criação de programa de auditoria mais dinâmico no ambiente da empresa.

Palavras-chave: Auditoria. Sistema ERP. Programa. Roteiro.

LISTA DE ILUSTRAÇÕES

FIGURA 1 – Estrutura típica de funcionamento de um sistema ERP 14
FIGURA 2 – Características da auditoria interna 15
FIGURA 3 – Procedimentos gerais de uma auditoria em sistemas de gestão 25
FIGURA 4 – Ciclo de vida dos pontos de controle 28
FIGURA 5 – Identificação de riscos em relação ao roteiro proposto 29
FIGURA 6 – Fluxograma de aplicação da simulação de dados 32
FIGURA 7 – As fases do roteiro e suas respectivas atividades 44
FIGURA 8 – Exemplo de atividade e demais características presentes no roteiro 45
FIGURA 9 – Fase de Iniciação e planejamento de auditoria 45
FIGURA 10 – Relação de objetivos a serem escolhidos e detalhados 46
FIGURA 11 – Relação de tipo de escopo a ser escolhido 47
FIGURA 12 – Atributos e habilidade para auditores internos 48
FIGURA 13 – Formação básica de uma equipe de auditoria interna 48
FIGURA 14 – Campos do formulário para avaliação de candidatos 49
FIGURA 15 – Modelo de questionário para conhecimento de ambiente 50
FIGURA 16 – Tópicos básicos de um plano de auditoria 51
FIGURA 17 – Ciclo de vida dos pontos de controle no roteiro 52
FIGURA 18 – A Atividade de organização, identificação e definição dos pontos de controle 53
FIGURA 19 – Pontos de auditoria a serem trabalhados 55
FIGURA 20 – O roteiro adaptado na Ferramenta Microsoft Sharepoint 60
FIGURA 21 – Ata inicial do programa de auditoria 62
FIGURA 22 – Atividade de definir equipe 62
FIGURA 23 – Parte do formulário para seleção de candidatos preenchido 63
FIGURA 24 – Ata divulgação de auditores internos definidos 64
FIGURA 25 – Recorte do artefato levantamento do ambiente 64
FIGURA 26 – Registros da atividade de revisão da primeira fase 65
FIGURA 27 – Os artefatos de saída a atividade de levantamento e organização dos pontos de controle 67
FIGURA 28 – Artefato preenchido sob o ponto de vista do usuário 67
FIGURA 29 – Modelo matriz pontos de controle auditoria 70
FIGURA 30 – E-mail enviado a comissão e gestão 71

LISTA DE TABELAS

TABELA 1 – Valores para caracterizar os pontos 54
TABELA 2 – Pontos de controle e riscos identificados 66
TABELA 3 – Pontos de controle priorizados 68
TABELA 4 – Tabela de pontos de auditoria, técnicas e ferramentas 68
TABELA 5 – Participantes da comissão de auditoria 72
TABELA 6 – Lista de gestores e usuários envolvidos no programa de auditoria 72
TABELA 7 – Descrição de resultados de auditoria 72

LISTA DE ABREVIATURAS E SIGLAS

CPD	Centro de Processamento de Dados
COBIT	*Control Objectives for Information and Related Technology*
ERP	*Enterprise Resource Planning*
ISACA	*Information Systems Audit and Control Association*
ITIL	*Information Technology Infrastructure Library*
NBR	Norma Brasileira
PED	Processamento Eletrônico de Dados
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO 8

1.1 PROBLEMA DE PESQUISA 9
1.2 OBJETIVO PRINCIPAL DO TRABALHO 10
1.3 METODOLOGIA E ORGANIZAÇÃO DO TRABALHO 11

2 AUDITORIA EM SISTEMAS ERP NAS ORGANIZAÇÕES 13

2.1 SISTEMAS ERP 13
2.2 TIPOS DE AUDITORIA EM ERP 15
2.3 OS OBJETIVOS GLOBAIS DE AUDITORIA EM ERP 16
2.4 AS FORMAS DE AUDITORIA 20
2.5 A EQUIPE DE AUDITORIA INTERNA 21
2.5.1 O auditor de sistemas 22
2.6 PROCEDIMENTOS DE AUDITORIA DE SISTEMAS 24
2.6.1 Planejamento de auditoria de um sistema ERP 26
2.6.1.1 Análises e considerações sobre ambiente a ser auditado 27
2.6.1.2 Os detalhes do planejamento 30
2.6.2 Execução de procedimentos de auditoria de um sistema ERP 31
2.6.2.1 Técnicas de auditoria aplicáveis a um sistema ERP 31
2.6.2.2 Vantagens no uso das técnicas 37
2.6.3 Conclusões de auditoria de um sistema ERP 38
2.6.4 Os produtos gerados em uma auditoria de sistemas 38
2.7 CONSIDERAÇÕES FINAIS DO CAPÍTULO 40

3 ROTEIRO PARA AUDITORIAS DE SISTEMAS 43

3.1 FASE DE INICIAÇÃO DO PLANEJAMENTO DE AUDITORIA 45
3.1.1 Definição de objetivos e escopo de auditoria 46
3.1.2 Definição de equipe de auditoria 47
3.1.3 Conhecendo o ambiente do sistema ERP 50
3.1.4 Criação do plano de auditoria 51
3.2 FASE DA ANÁLISE E DEFINIÇÃO DOS PONTOS DE CONTROLE 52
3.2.1 Organização, identificação e definição dos pontos de controle 53
3.3 FASE DE PREPARAÇÃO E EXECUÇÃO DE ATIVIDADES 56
3.4 FASE DE CONCLUSÃO E RESULTADOS DE AUDITORIA 56
3.5 CONSIDERAÇÕES FINAIS DO ROTEIRO PARA AUDITORIA DE SISTEMAS 58

4 APLICAÇÃO DO ROTEIRO DE AUDITORIA EM ERP 59

4.1 CONTEXTO DO ESTUDO DE CASO 59
4.2 O ROTEIRO IMPLEMENTADO 59
4.3 O ESTUDO DE CASO 61
4.3.1 Fase de Iniciação do Planejamento de auditoria 61
4.3.2 Fase de análise e definição dos pontos de controle 65
4.3.3 Fase de preparação e execução das atividades 69
4.3.4 Fase de conclusão de resultados de auditoria 70
4.4 CONSIDERAÇÕES FINAIS DA APLICAÇÃO DO ROTEIRO DE AUDITORIA 74

5 CONCLUSÃO 76

REFERÊNCIAS 79

ANEXOS 81

ANEXO A – Quadro normas e metodologias x objetivos globais 82

ANEXO B – Modelo definições iniciais do programa de auditoria 83

ANEXO C – Roteiro para a criação de programa de auditoria de sistemas ERP 84

ANEXO D – Modelo de plano de auditoria 85

ANEXO E – O modelo de ata de reunião 86

ANEXO F – Modelo formulário para seleção de auditores internos 87

ANEXO G – Levantamento do Ambiente de Sistema ERP 88

ANEXO H – Modelo matriz de pontos de controle identificados 89

ANEXO I – Matriz de pontos de controle definidos 90

ANEXO J – Modelo matriz dos pontos de controle auditoria 91

ANEXO K – Listagem de técnicas de auditoria para consulta 92

ANEXO L – O modelo de rascunho preliminar do relatório de auditoria 93

ANEXO M – Questionário preenchido com informações e dados do ambiente 94

ANEXO N – O artefato matriz pontos de controle identificados preenchido 95

ANEXO O – Artefato anexo da ata de reunião para levantamento de pontos 97

ANEXO P – O Plano de auditoria preenchido 98

ANEXO Q – O artefato matriz pontos de controle auditoria preenchido 100

1 INTRODUÇÃO

Sistemas informatizados são indispensáveis para a melhoria da eficácia dos processos em grandes empresas. Stair e Reynolds (2006), afirmam que os sistemas desempenham diversos papéis: coletam, processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, análises e o gerenciamento de organizações. Porém, com o passar dos anos, os sistemas e os processos acabaram tornando-se mais complexos. Isto afetou diretamente os sistemas de informação e criou necessidades de verificações e adequações por conta de customizações às regras de negócio e complexidade de alterações.

Segundo Lyra (2008), a função de auditoria de sistemas está ligada a adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos nos sistemas de informação da empresa.

A auditoria de sistemas impõe senso crítico dentro de um ambiente de sistemas de informação. Ela busca inovações, otimizações de processos empresariais, potenciais relações custo versus benefício, avaliação de riscos, maior eficiência, eficácia e segurança. É importante que uma organização possa ter um meio de medir se seus resultados estão coerentes ou se podem ser melhorados. Segundo Gil (1999), a eficácia dos resultados gerados e a eficiência dos processos concluídos necessitam ser validadas e avaliadas, e a auditoria de sistemas computadorizados pode ser o campo de ação para a certeza do alcance da qualidade de computação necessária. Em empresas onde TI (Tecnologia da Informação) é considerada parte do mapa estratégico, é importante que seus sistemas de informação estejam bem alinhados com os processos da organização.

Um sistema de informação, sob o ponto de vista de auditoria, segundo Imoniana (2005) está dividido pela gerência em diversos controles. Os controles internos são “os planos organizacionais e coordenação de um conjunto de métodos e medidas adotado numa empresa, a fim de manter o ativo, verificar a exatidão e a veracidade de registros, promover a efetividade de sistema de informação e fomentar uma grande adesão às políticas da organização”. Estes controles internos dividem-se em organizacionais, controles de segurança e privacidade, controles de preparação, controles de entrada, controles de processamento, controles de recuperação, de armazenamento de dados e de saída.

Para que uma organização, a qual deseja criar um programa de auditoria interna em sistemas, possa suprir os requisitos desejados em seus controles internos, é importante que ela conte com profissionais capacitados para a condução do programa. Estes profissionais farão

parte da equipe de auditoria, que será organizada por gestores do programa de auditoria interna. A composição da equipe deve ser feita por auditores selecionados e recrutados conforme conhecimentos e habilidades nas áreas de sistemas e de negócios.

Um auditor, tendo o conhecimento do ambiente e de seus controles internos pode ter um desempenho melhor em suas responsabilidades dentro de um programa de auditoria. Estas são etapas básicas para a aplicação do programa de auditoria, que por consequência afetarão demais atividades do roteiro. O programa de auditoria precisa ter um planejamento adequado e com os objetivos definidos, assim o auditor pode executar seus trabalhos em controles específicos, agregando técnicas de auditoria para auxílio em suas análises e constatações.

Lyra (2008) destaca os objetivos globais da auditoria de sistemas de informação: integridade, confidencialidade, privacidade, acuidade, disponibilidade, auditabilidade, versatilidade e manutenabilidade.

Para montar um roteiro de auditoria interna de sistemas, deve ser destacado o uso de referências consolidadas como normas e guias aplicáveis a sistemas de gestão. Silva (2007) cita o CobiT (*Control Objectives for Information and related Technology*) como ponto de partida para a identificação das atividades de Auditoria de Sistemas de Informação. Aborda também referenciais ITIL (*Information Technology Infrastructure Library*) e ISO 17799 para a identificação de atividades, uma vez que estes referenciais são mais específicos em alguns aspectos ligados a sistemas de gestão. A norma da ABNT, 19011 - Diretrizes para auditoria de gestão de sistemas também é um referencial para a condução de auditoria.

1.1 PROBLEMA DE PESQUISA

Empresas podem ter gastos excessivos ao não realizarem revisões periódicas nos seus sistemas de ERP. As funcionalidades de seu sistema de gestão devem ser auditadas, afim de que os processos de negócio não sejam afetados. O sistema ERP deve satisfazer o que se propõe, realizando a integração, armazenamento e apresentação das informações das diversas áreas funcionais da organização.

A dependência que existe atualmente das empresas em terem auditores externos para verificarem seus sistemas, pode acarretar nos gastos mencionados e resultados com pouca expressão. Capacitar uma equipe interna de TI pode ser uma boa solução para corte de eventuais custos e problemas. Porém Imoniana (2005), frisa que analistas de sistemas podem ainda não estarem aptos a exercerem o papel de auditor. Esta pode ser uma oportunidade de aprendizado par a organização e seus funcionários.

As diversas funcionalidades e integrações que um sistema ERP se propõe, podem apresentar complexidade, devido ao tipo de negócio e o nível de exigência de customizações e adaptações do sistema.

Devido a alta complexidade que os sistemas podem apresentar, os analistas de sistemas, segundo Imoniana (2005), podem ainda não estar preparados para atuação no ramo de auditoria. Sua capacitação depende de seus conhecimentos do sistema e de auditoria.

O risco de empresas serem auditadas é alto, principalmente as que têm de prestar contas a acionistas, investidores e *holdings*. Para estes tipos de empresas, dependendo o foco da auditoria, o sistema mais visado é o ERP (*Enterprise Resource Planning*). Este tipo de sistema é solicitado pelas auditorias, pois nele estão presentes os principais controles de registros dos processos e fonte de dados. Os sistemas ERP, assim como quaisquer outros sistemas são passíveis de serem auditados. Neles são elencados diversos pontos de auditoria, que podem ser auditados caso estejam dentro dos parâmetros definidos na auditoria. Lyra (2008) cita os seguintes pontos:

a) captação e entrada de dados;
b) transmissão de dados;
c) processamento de dados;
d) armazenamento;
e) apresentação das informações;
f) divulgação das informações.

Imoniana (2005) complementa que os principais problemas que podem prejudicar as operações da empresa estão relacionados a dados e informações contidos em um sistema ERP. Estes dados e informações podem estar: incorretos, incompletos, inoportunos, inseguros e inauditáveis.

1.2 OBJETIVO PRINCIPAL DO TRABALHO

Este trabalho tem por objetivo propor um roteiro para a elaboração de programas de auditoria de sistemas ERP. O roteiro estabelece diretrizes que podem ser seguidas por uma equipe de auditores internos, durante a estruturação de um programa de auditoria. O programa de auditoria pode seguir de acordo com o que o roteiro se propõe ou apenas ser adaptado conforme objetivos definidos pela comissão de auditoria interna.

Para fundamentar o roteiro é necessário o estudo de conceitos e diretrizes de auditorias internas e auditorias de sistemas.

Para a aplicação do trabalho será utilizado um ambiente com ferramenta para adequação do roteiro de auditoria, a ser utilizado pela comissão de auditoria e equipe de auditores para posterior criação de um programa de auditoria baseado nos estudos realizados.

A avaliação do roteiro proposto será através da aplicação e coleta de resultados ao fim de estudo de caso utilizando a ferramenta de apoio.

1.3 METODOLOGIA E ORGANIZAÇÃO DO TRABALHO

O desenvolvimento deste trabalho ocorreu através de pesquisa exploratória. Para a elaboração desta proposta foram definidas atividades que pudessem resultar na fundamentação e na estruturação do roteiro de auditoria, para posterior aplicação de estudo de caso. As atividades definidas para a execução deste trabalho foram:

a) buscar fundamentações teóricas referentes à área de conhecimento de auditoria interna, para dar início a elaboração da proposta de roteiro;
b) estudo de normas vigentes aplicáveis a sistemas de informação, focando sistemas ERP (*Enterprise Resource Planning*), para prospecção de possíveis atividades passíveis de auditoria. Elaboração de sínteses baseadas nas normas e procedimentos, para fundamentar as atividades de auditoria;
c) pesquisas sobre auditoria em sistemas de informação, além de realização de entrevistas com especialistas em auditoria de sistemas em geral, para obter depoimentos e informações relevantes ao estudo proposto;
d) análise de documentos gerados por auditorias realizadas em empresas que já possuam algum tipo de auditoria interna ou externa. Foco em documentos relevantes a sistemas ERP (*Enterprise Resource Planning*);
e) elaboração de roteiro de programa de auditoria, a ser usado por auditores em forma de documento, organizando o andamento de atividades;
f) simulação de auditoria em um sistema ERP (*Enterprise Resource Planning*) em produção, utilizando o programa criado dentro da ferramenta onde estará estruturado o roteiro, gerando documentos de *feedback* ao fim, documentando o que deve ser verificado internamente.

O trabalho está organizado em 5 capítulos e visa apoiar profissionais da área de TI, que tenha o objetivo de implantar uma metodologia de auditoria interna em Sistemas ERP, para manterem suas operações em conformidade e alinhada aos interesses e objetivos da organização.

A divisão foi feita de acordo com o estudo sobre auditorias internas relacionadas a sistemas ERP. No capítulo 1 é apresentada a introdução, onde é demonstrada a contextualização do assunto estudado, objetivo principal, problema de pesquisa e estruturação do trabalho.

O capítulo 2 descreve os conceitos e levantamentos bibliográficos, que serão utilizados como base para a elaboração e organização de um roteiro de auditoria de sistemas. Serão apresentados os objetivos de auditoria de sistemas, os tipos, as formas, os componentes e procedimentos aplicáveis à mesma.

O capítulo 3 tem por objetivo principal descrever a proposta de solução para o problema levantado, definindo a passo a passo a composição do roteiro. O roteiro é explicado conforme a sua composição, iniciando pelas suas fases. A partir das fases, serão detalhadas as atividades que as compõe, além de artefatos de entrada e saída.

No capítulo 4 é apresentado o estudo de caso em que foi aplicado o roteiro para a criação de um programa de auditoria. Neste capítulo será feita a adaptação do roteiro em uma ferramenta adequada para posterior demonstração das fases propostas no roteiro e suas conclusões.

O capítulo 5 aborda a conclusão do trabalho, em que descreve os resultados alcançados, os problemas enfrentados, assim como possíveis trabalhos futuros a serem desenvolvidos.

2 AUDITORIA EM SISTEMAS ERP NAS ORGANIZAÇÕES

Segundo Schmidt (2006, apud LYRA, 2008, p. 105): “a função da auditoria de sistemas é promover a adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos nos sistemas de informação das empresas”. Esta afirmação revela atividades que podem existir em uma auditoria, frisando também sua importância na melhoria dos sistemas de empresas.

Lima; Castro (2003, p. 31) alegam que a auditoria dispõe-se como instrumento fundamental para verificação e avaliação de determinado aspecto da organização que se deseja focar. Ainda afirmam que hoje existem diversas modalidades de auditorias tais como, na área de marketing, de sistemas informatizados, de recursos humanos, de qualidade, entre outras. Este trabalho estará focado na modalidade de sistemas informatizados, mais precisamente em sistemas ERP (*Enterprise Resource Planning*).

Este capítulo tem por objetivo apresentar o conceito e a estrutura de um sistema ERP, o qual será o foco de estudo dentro do processo de auditoria. O capítulo abordará o estudo realizado a respeito de auditorias em sistemas, contando com os objetivos globais de auditorias, as formas de auditoria, o desenvolvimento de uma equipe de auditoria procedimentos de auditoria e considerações a respeito do estudo realizado.

2.1 SISTEMAS ERP

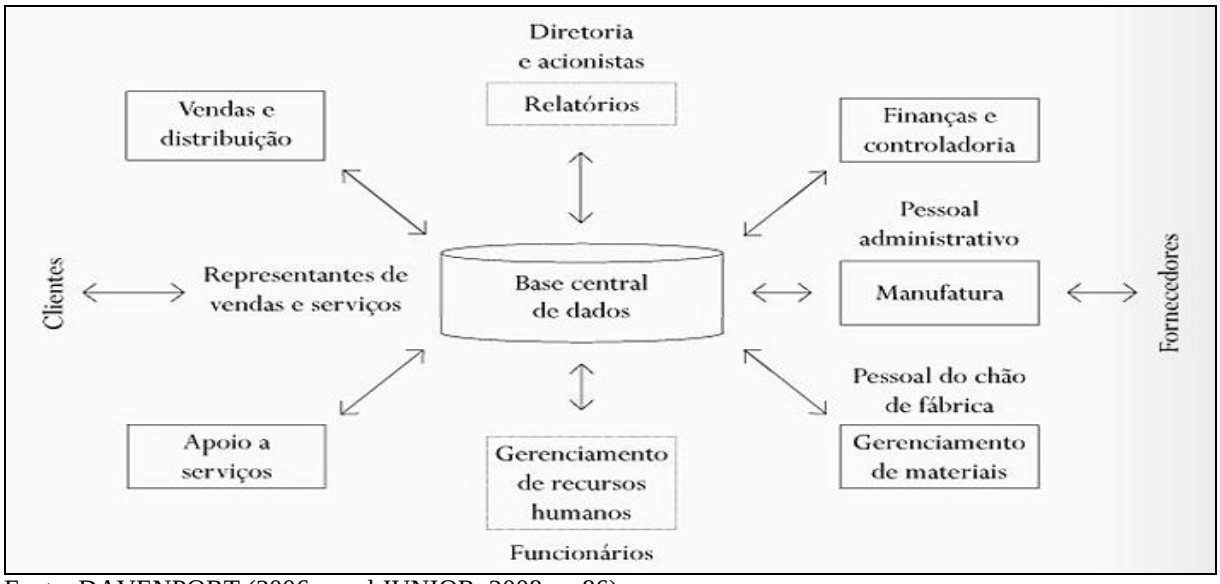
Davenport (2006, apud JUNIOR, 2008, p. 85): afirma que sistemas ERP tem a finalidade de organizar, padronizar e integralizar as informações transacionais que circulam pela organização. Esses sistemas integrados permitem acesso a informações confiáveis em uma base de dados única em tempo real.

Sistemas integrados ou Sistemas ERP (*Enterprise Resource Planning*) são divididos basicamente em módulos. Estes módulos básicos têm o objetivo de satisfazer o processo de negócio de uma organização. Para empresas que possuem processos de negócio mais complexos, fornecedores de sistemas integrados oferecem pacotes em separado, para atender demandas em que os clientes exigem customizações em produtos *standard*.

Davenport (2006, apud JUNIOR, 2008, p. 86) exemplifica através da figura 1, uma visão geral dos módulos, atividades e processos típicos de um sistema integrado ERP. A figura representa a capacidade de relacionamento entre as diversas áreas de uma empresa que

um sistema integrado pode proporcionar, gerando um repositório comum de dados e informações.

FIGURA 1 – Estrutura típica de funcionamento de um sistema ERP



Fonte: DAVENPORT (2006, apud JUNIOR, 2008, p. 86)

As empresas fornecedoras utilizam nomes diferentes para os módulos de seu sistema ERP. Junior (2008) apresenta os módulos contidos no sistema ERP da empresa SAP. São eles:

a) CO – Controladoria: envolve ferramentas de planejamento, controle e monitoramento para sistemas que gerenciam os processos da empresa. Trata-se de uma ferramenta para executivos tomarem[1] decisões;
b) FI – Finanças: módulo relativo aos dados financeiros relevantes a organização. Suporta as atividades financeiras: contas a pagar, contas a receber, tributações, impostos entre outras;
c) PP – Planejamento de Produção: módulo que permite o planejamento e controle de produção. Pode ser usado para produções normais, por encomenda, com variáveis, bem como estocar e para projetos;
d) MM – Gerenciamento de Materiais: dentro deste módulo podem ser destacados os fluxos que acionam os processos de compra de materiais, organização de fornecedores e processos de gerenciamento de estoques;
e) SD – Vendas e distribuição: aqui constam as atividades associadas à parte comercial da empresa: Relacionamento com o cliente, controle de pedidos,

[1] SAP - *SAP* é uma empresa de origem alemã, com forte presença no Brasil, criadora de *Software*s de Gestão de Empresa.

percentuais de vendas, formação de preço de produto e ainda análise de rentabilidade e de produção;

f) HR – Recursos Humanos: módulo onde constam soluções para o planejamento, administração e desenvolvimento humano de uma organização. Abrange as mais diversas funções, entre elas: recrutamento e seleção de pessoas, gerenciamento de cargos e salários, desenvolvimento de pessoal, etc.

Por ser um meio de todas as áreas da empresa se inter-relacionarem, os processos em um sistema ERP podem acabar tornando-se complexos. Esta complexidade pode estar relacionada a diversidade de transações, grande manipulação de dados, alta customização de *software* e ciclo de informações e dados em diversas áreas.

2.2 TIPOS DE AUDITORIA EM ERP

Auditorias em sistemas podem ser divididas em dois tipos de atuação: externas ou internas. As auditorias externas são caracterizadas por terem o seu grau de independência amplo e seu trabalho orientado por interesses de terceiros, tendo de seguir normas e diretrizes estabelecidas por investidores e organizações internacionais. (LIMA; CASTRO, 2003, p. 20).

A auditoria interna é uma atividade de avaliação ordenada dentro de uma organização, cujas funções incluem, entre outras, examinar, avaliar e monitorar a adequação e eficácia dos sistemas. (LIMA; CASTRO, 2003, p. 20).

Segundo a Norma da ABNT (2002), a auditoria interna também deve satisfazer estes outros pontos: requisitos de sistemas, requisitos de clientes, riscos para a organização e processos, necessidades de outras partes interessadas e as necessidades de avaliação de fornecedor.

Na figura 2 são detalhadas as características de uma auditoria interna, composta basicamente por: agentes, ações, execução de trabalhos, grau de independência, abrangência de sua aplicação e os resultados.

FIGURA 2 – Características da auditoria interna

Agente	Auditor interno (empregado da própria instituição)
Ação	Auxílio a alta administração
Atividade	Adequação do controle interno em relação à prevenção de fraudes e perdas de aderência às normas legais e às diretrizes da alta administração
Execução dos trabalhos	De acordo com as oportunidades das funções operacionais
Grau de independência	Baixo em relação à alta administração; satisfatório quanto aos demais níveis.
Áreas cobertas pelo exame	Todas da instituição
Destino dos trabalhos	Diretoria, sócios, conselhos administrativos e fiscais e auditores externos.

Fonte: LIMA; CASTRO (2003, p. 20).

Estas características existentes numa auditoria interna fazem parte das diretrizes básicas que podem ser seguidas para a elaboração de um roteiro de auditoria.

2.3 OS OBJETIVOS GLOBAIS DE AUDITORIA EM ERP

Imoniana (2005) cita que a auditoria dos sistemas aplicativos possui alguns objetivos globais. Estes identificam os controles e avaliam os riscos de confidencialidade, integridade, privacidade, acuidade, disponibilidade, auditabilidade, versatilidade e manutenabilidade dos sistemas. Além disso, a partir da auditoria, o auditor verificando pode tirar conclusões a respeito do sistema aplicativo e suas respectivas funções, se este atende às missões empresariais. A seguir, são conceituados os objetivos globais:

1) **Integridade:** dentro deste conceito, o auditor verifica se as transações são confiáveis ao serem processadas. Podem verificar se o sistema evidencia claramente a completa e correta exibição dos dados sem que os usuários tenham de se preocupar com a veracidade dos mesmos.

A ABNT (2005) cita alguns procedimentos de revisão dos controles internos. Na categoria A.12.2 - O Processamento correto de aplicações é explicada a importância da presença de controles dentro de um sistema. Os controles podem ser, por exemplo, funções que monitorem o a manutenção geral dos dados, mantendo os mesmos íntegros. A norma exemplifica que os dados sofrem este monitoramento no momento de sua entrada no sistema, processamento e suas saídas.

2) **Confidencialidade:** Beal (2005, apud JUNIOR, 2008) afirma que a confidencialidade de um sistema consiste em existir mecanismos que barrem pessoas não autorizadas, a terem acesso a informações restritas, de forma acidental ou intencional. Para maior controle, devem existir procedimentos que autorizem o acesso.

O auditor pode se basear em como a empresa se preocupa com a organização das informações dentro do sistema. Outra verificação que pode ser feita para medir a confidencialidade de um sistema ERP é através de questionários. Estes questionários devem ser bem elaborados pela equipe de TI, abrangendo as diversas formas de contornar possíveis informações falsas. Eles podem denunciar se os usuários estão com acessos indevidos a informações que não condizem às suas funções.

No COBIT, são descritos, pelo objetivo PO2.3 - Esquema de Classificação de Dados, os detalhes sobre o grau de importância que a informação pode ter (pública, confidencial,

altamente secreta). Essa diretriz pode ajudar a organização a manter um controle sobre seus dados e informações, criando mecanismos de controles de acesso a informações, arquivamentos e criptografias.

Já o item 12.4.3 Controle de acesso ao código-fonte do programa, da Norma ABNT (2005), frisa a importância restrita aos códigos fonte, evitando riscos de alterações não solicitadas.

3) **Privacidade:** o auditor deverá certificar-se de que os dados do sistema estão seguros por algum tipo de controle. Este controle visa a liberação de usuários a terem acesso a determinados programas, telas ou rotinas no sistema ERP, que realmente sejam necessários para exercer suas funções na empresa.

Procedimento para acesso ao sistema é um exemplo de controle de privacidade. O item 11.5.1 - Procedimentos Seguros para entrada no sistema da Norma ABNT (2005), foca mais precisamente o *login* no sistema. O auditor deve discutir a política de usuários do sistema ERP, se existe algum controle para as senhas e qual a periodicidade de trocas.

4) **Acuidade:** o sistema ERP deve possuir procedimentos internos de controle de entrada de dados, não permitindo a inserção de dados que invalidem as informações resultantes nos relatórios emitidos.

O item 12.2 que trata do Processamento Correto das Aplicações. Este item da Norma ABNT (2005) tem por objetivo garantir que não haja perdas, erros, modificações não autorizadas ou mal uso de informações em aplicações. Para isto o sistema deve possuir, da mesma forma que existe no objetivo global de Integridade, alguns meios de validações que são:

a) validações dos dados de entrada;
b) controle do processamento interno;
c) integridade de mensagens;
d) validação de dados de saída.

Estes meios de validação asseguram para o corpo de auditores que o processamento atual está falho ou condizendo ao que se propõe.

5) **Disponibilidade:** de alguma forma, o sistema deve estar online na maior parte do tempo para não comprometer transações. Na empresa deve existir algum modo em que seja medida a disponibilidade do sistema, para que usuários possam se precaver e para que a própria equipe de infraestrutura de TI possa ter documentado em um repositório em comum junto a analistas de sistemas e analistas de negócios.

Dentro dos domínios do COBIT, existe um processo que trata sobre continuidade de serviços. Este processo chama-se Assegurar a continuidade dos serviços – DS4, o qual tem por objetivo assegurar que as informações estejam disponíveis para usuários e processos autorizados. O ITIL, também faz referência à disponibilidade dos serviços, neste caso disponibilidade do sistema, chamando o processo de Gerenciamento de Disponibilidade.

6) **Auditabilidade:** o auditor verifica a existência de registros referentes ao sistema. O custo pode ser elevado para o armazenamento de registros, dependendo o tamanho do sistema ERP a ser verificado, e também por causa do número de transações diárias. As trilhas de auditoria podem ser aplicadas neste contexto, também chamadas de *audit trails* por alguns autores.

A auditabilidade de um sistema, segundo o COBIT, pode ser descrito pelo objetivo AI2 Adquirir e Manter *software* Aplicativo, e detalhado através do item AI2. 3 - Controle e Auditabilidade do aplicativo. Este item explica a importância em assegurar que os controles de negócio sejam expressos adequadamente nos controles dos aplicativos. Estes controles garantem que o processamento ocorra no prazo correto e seja exato, completo, autorizado e auditável. O controle de aplicação e de auditabilidade é responsável por diversos mecanismos, e para um sistema ERP podem ser citados:

a) mecanismos de autorização;
b) integridade da informação;
c) controle de acessos ao sistema;
d) esquemas de rastreamento de auditorias.

No item A.15.1 que trata de Conformidade com requisitos legais, da ABNT (2005), são destacados os objetivos de evitar violações no sistema que estejam relacionadas com crimes que afetem estatutos regulamentações ou obrigações. Alguns dos subitens deste item que são aplicáveis a sistemas ERP em produção são:

a) proteção de dados e privacidade da informação pessoal, neste caso do sistema ERP e do usuário;
b) prevenção de mau uso de recursos de processamento da informação, em que os usuários devem estar conscientes de que o uso inadequado dos dados extraídos do sistema, pode acarretar em sérios problemas.

Como foi citada pelo COBIT e pela ABNT, a auditabilidade aborda diversos controles dentro de um sistema para poder ser considerada um objetivo alcançável em uma auditoria de sistema ERP. Para um sistema ser considerado auditável existe certa complexidade devido ao alto nível de conhecimento que exigirá de auditores e sua experiência

em poder adequar ferramentas para levantamento de evidencias capazes de relacionar pontos de auditoria e serem tratados posteriormente.

7) **Versatilidade:** a versatilidade está ligada a usabilidade do sistema. Deve ser dada a atenção para disposição dos elementos que compõem o *software*. Através de questionários aplicados aos usuários podem ser levantadas possíveis melhorias. Além disso, deve ser feita uma análise se novos *workflows* operacionais de negócio da empresa podem ser adaptados ao *software* ERP. Outro importante ponto que Lyra (2008) pondera é que deve ser observada se a sincronia de aplicativos independentes é fácil de ser feita com o sistema ERP.
8) **Manutenabilidade:** durante a manutenção dos sistemas é importante a existência de documentos que descrevam os passos de como proceder em atualização do sistema. Nestes documentos é importante que sejam destacados os responsáveis pelas atualizações, testes que devem ser feitos para certificar a atualização, análise de módulos impactados, formas de restauração de dados caso ocorra algo inesperado e meio de divulgação para as áreas interessadas.

O COBIT trata dentro do domínio de Adquirir e Implementar, o objetivo AI 2.2 - Projeto Detalhado que visa a prática de revisão de se sistemas estão tendo relevantes discrepâncias técnicas e lógicas. O objetivo apresenta ações que podem ser tomadas para que sejam verificadas falhas que ocorrem em momentos de atualizações de versões de módulos, troca de procedimentos, etc.

Além disso, dentro do objetivo AI2 – Adquirir e Manter *Software* Aplicativo, no COBIT é encontrado um item que sugere às empresas uma estratégia e planos de manutenção do *software* aplicativo ou *software* ERP. Isso é importante, pois no momento em que há atualizações de estrutura do *software* e base de dados, a organização pode seguir um passo a passo de como efetuar as atualizações de forma mais organizada. Outros itens deste mesmo objetivo seriam AI6 - Gerenciar Mudanças e AI7 - Instalar e Homologar Soluções e Mudanças, onde o primeiro visa controlar as alterações em ambiente de produção de sistemas aplicativos, de forma adequada e com um gerenciamento controlado. Já o segundo processo prevê um ambiente de homologação para testes e análise de impactos.

Na questão de manutenabilidade, no item 12.5.3- Restrições em atualização de *software* da norma ABNT (2005), é explicado que mudanças em pacotes de *software* devem ser limitadas.

A partir dos objetivos citados neste capítulo o auditor deve começar a montar o escopo e o planejamento da auditoria do sistema ERP, baseado nos objetivos da auditoria e

observando critérios estabelecidos por ele e sua equipe no início dos trabalhos.

2.4 AS FORMAS DE AUDITORIA

Magalhães; Lunkes; Muller (2001, p. 21) consideram que as formas de auditoria podem ser quanto à extensão, à profundidade e à tempestividade. A seguir, é apresentado um resumo de cada uma das formas;

a) quanto à extensão:
   - geral, quando é abrange toda a organização. Geralmente há o interesse de acionistas e investidores, no cumprimento de normas legais que regulam o mercado acionário;
   - parcial, quando abrange especificamente determinadas unidades operacionais, tendo como características principais detectar desvios, erros e fraudes, investigação de existência ou prosperidade de bens econômicos, avaliação de custeios e análise de solvências;
   - por amostragem, a partir de análise do controle interno, onde são identificadas áreas de risco, centrando os exames sobre essas áreas.

b) quanto à profundidade:
   - integral, que compreende o exame minucioso de documentos (origem, autenticidade, exatificação), dos registros, do sistema de controle interno (quanto à eficiência e aderência) e das informações finais geradas pelo sistema;
   - por revisão analítica, sendo uma metodologia onde auditar é administrar o risco, operando com trilhas de auditoria mais curtas, para obter razoável certeza quanto à fidedignidade das informações.

Esta questão de profundidade é aplicável à auditoria em sistemas ERP devido a sua investigação na parte de entrada de registros e pela própria verificação na parte de resultados de saídas. No que se refere à revisão analítica, pode ser destacada a trilha de auditoria usada na avaliação de riscos, onde o sistema ERP disponibiliza registros para que aconteça esta revisão.

c) quanto à tempestividade:
   - permanente, feita habitualmente, podendo ser constante ou sazonal, porém em todos os exercícios sociais.
     a. esse processo oferece vantagens à empresa auditada e aos auditores, tais como:

  - redução dos custos com planejamento da auditoria, pois a ambientação dos auditores com a auditada torna-se menos onerosa;
  - as áreas de risco são detectadas no primeiro planejamento e o acompanhamento pelos auditores definirá as já eliminadas e as novas que possam ter surgido;
  - redução do tempo de custo.
- eventual, sem caráter habitual, por exemplo: não é feita todos os anos. Exige completa ambientação dos auditores e de planejamento sempre que será feita.

A tempestividade é uma forma de auditoria aplicável em programa de auditoria ERP. Pode ser um auxílio para responsáveis por implantação de auditoria no momento de planejamento do programa de auditoria, na definição de equipes internas e na estruturação de tarefas, devido a forma tratar da ambientação dos auditores com a empresa, que neste caso são os próprios funcionários.

Nota-se que dependendo dos objetivos de auditoria, a forma pode variar. Tanto a empresa a ser auditada como os responsáveis pela implantação da auditoria, tem de se preparar e planejar a forma ideal de programa de auditoria a ser aplicado.

2.5 A EQUIPE DE AUDITORIA INTERNA

Imoniana (2005) relata que os profissionais de auditoria e de tecnologia da informação, ao longo dos anos vinham desempenhando atividades independentes um do outro. Auditores que não possuem conhecimentos na área de tecnologia acabavam usando profissionais de informática para auxílio no momento de auditar sistemas. Atualmente este cenário vem mudando, mas ainda é grande a demanda por profissionais que possuam conhecimento em ambas as áreas. Portanto as empresas devem considerar que, antes de implantar um programa de auditoria, devem prover a capacitação de sua equipe de TI quanto a conhecimentos de auditorias internas.

As auditorias se passam com o uso dos computadores. É inevitável, segundo Imoniana (2005) que auditores de sistemas tenham de ter um conhecimento relativo a tecnologias. Para isso, o autor destaca que, na formação de equipes internas, não basta somente utilizar profissionais de informática para auditar sistemas ERP, mas sim usuários das mais diversas áreas e treiná-los para que componham uma equipe.

Algumas estratégias elaboradas por Imoniana (2005) seriam:

a) a empresa que deseja ter uma equipe interna de auditores de sistemas deve

preocupar-se em treinar os funcionários, abordando conceitos de tecnologia da informação e métodos para aplicação de auditoria em sistemas;

b) capacitar analistas de sistemas em práticas de auditoria geral e no uso das variadas técnicas e ferramentas de auditoria;

c) contratar auditores com larga experiência pode ser um caminho interessante para depois apenas capacitá-los na área de sistemas de informação.

A Norma ABNT (2002) - Diretrizes para Sistemas de Gestão relata que para a composição de uma equipe, deve ser levado em conta os aspectos a seguir:

a) competência global necessária da equipe para alcançar os objetivos da auditoria;

b) necessidade de assegurar a independência da equipe de auditoria em relação às atividades afim de evitar conflitos de interesse;

c) assegurar que os auditores consigam interagir com os auditados, para haver ações conjuntas;

d) assegurar que os membros da equipe de auditoria possuam conhecimentos e habilidades necessárias para seu desempenho.

Imoniana (2005) destaca que no mercado de trabalho existe certa dificuldade para auditores que não são da área de tecnologia capacitarem-se em auditoria de sistemas. Isso se deve aos conhecimentos exigidos para atuação na área. Enquanto isso, os analistas de sistemas, Imoniana (2005) afirma que estão aos poucos ingressando na área de auditoria. Estes profissionais estão agregando aos seus conhecimentos a capacidade de auditar, utilizando suas experiências em tecnologia de sistemas, as quais antes eram usadas apenas para auxiliar auditores de outras áreas.

Imoniana (2005) destaca também que, por auditoria de sistemas ser uma área ainda em evolução, os analistas de sistemas podem ainda não estarem preparados para atuar neste ramo. A justificativa seria de que, o profissional de sistemas ainda não possui o senso crítico e de julgamento que um auditor profissional possui, podendo levar certo tempo até ser considerado um auditor de plenas capacitações na área.

2.5.1 O auditor de sistemas

O auditor de sistemas é a pessoa encarregada de elaborar e aplicar os trabalhos de auditoria em uma organização, buscando aperfeiçoar e avaliar os resultados.

Para um auditor estar apto a exercer suas atividades é importante lembrar que existem normas aplicáveis à profissão ou a quem desempenha o papel. Estas normas dizem

respeito a qualificação técnica e postura profissional. Estes são conceitos comuns, para quem vai desempenhar um papel fundamental de analisar pontos estratégicos e informações e dados privados de empresas.

Magalhães; Lunkes; Muller (2001, p. 42) consideram algumas normas que podem ser aplicadas ao auditor:

a) o auditor deve ser independente em todos os assuntos relacionados com seu trabalho;
b) o auditor deve aplicar o máximo de cuidado e zelo na realização dos exames e na exposição de suas conclusões.

Para complementar no que diz respeito ao auditor, a ISACA (Associação de Auditores de Sistemas e Controles) estabelece o código de ética profissional, para que seus membros possam seguir ao realizarem uma auditoria. A entidade destaca que:

a) o auditor deve apoiar e conscientizar os principais envolvidos durante os trabalhos de auditoria. Isso serve para que ajudem no auxílio e compreensão dos sistemas de informação, controle e segurança;
b) o auditor seja bastante prático e tenha uma forma de comunicação adequada com os envolvidos. Deve informar sobre o resultado de seus trabalhos, expondo fatos que são relevantes aos auditados.

A importância que um auditor representa em um processo de auditoria está ligada ao desempenho em suas atividades realizadas e o que resulta delas. O auditor tem a responsabilidade de fornecer material com alta credibilidade para que os interessados no processo possam fazer o uso destes materiais sem correrem riscos de terem informações não fidedignas e mal elaboradas.

Para que o desempenho de um auditor na auditoria em sistemas seja satisfatório, ele depende de alguns conhecimentos básicos. Imoniana (2005) reitera alguns: conhecimento de auditoria, de sistemas de informação e de PED, controles internos e CPD. Gil (1999) julga que o auditor de sistemas deve se especializar em alguma área dentro de sistemas computacionais. No caso de auditor em sistemas ERP em operação, cita que o mínimo que deve conhecer é:

a) documentação de sistemas;
b) fluxogramação;
c) uma linguagem de programação, ou a lógica de programação.

Tendo em vista estas capacitações, a pessoa pode desempenhar o papel de auditor de sistemas ERP interno, pois já estará atendendo aos requisitos mínimos para iniciar os

trabalhos de auditoria. Mas é importante destacar que, como a área de TI está em constante evolução, o auditor deve estar sempre atualizado no que se refere a melhorias de programas de auditoria, podendo ser por meio de ferramentas, técnicas e artefatos.

No processo de auditoria, segundo a ABNT (2002), a escolha de um auditor líder é essencial. Ele que irá centralizar e gerenciar os pontos de verificação, a organização do plano de auditoria, dos documentos de trabalho e definição das responsabilidades dos auditores da equipe.

O auditor não deve ser visto como um sujeito que tem o objetivo de denegrir o trabalho dos outros. Deve ser visto como um parceiro da empresa para elaboração de ações estratégicas e formador de opiniões que devem ser tratadas em conjunto com os executivos da organização.

2.6 PROCEDIMENTOS DE AUDITORIA DE SISTEMAS

Os procedimentos de auditoria de sistemas devem ser entendidos como um conjunto de etapas e atividades bem distribuídas, que são planejadas, executadas e avaliadas por diversas partes interessadas, ocorrendo antes, durante e depois de uma auditoria. Imoniana (2005) explica que os procedimentos de auditoria de sistemas aplicativos referem-se àqueles executados para averiguar se os sistemas que constituem o cerne do negócio de uma empresa estão acontecendo de forma adequada, executando suas atividades rotineiras adequadamente.

A organização dos procedimentos de auditoria deve estar de forma que os trabalhos sejam feitos adequadamente dentro do processo de auditoria. Lyra (2008) afirma que é possível pensar em aplicar uma metodologia de trabalho que seja flexível e aderente a todas as modalidades da auditoria em sistemas de informação e que não se distancie de melhores práticas.

Para Lyra (2008), a metodologia pode ser composta pelas seguintes etapas:

a) planejamento e controle do projeto de auditoria de sistemas de informação;
b) levantamento do sistema de informação a ser auditado;
c) identificação e inventário dos pontos de controle;
d) priorização e seleção dos pontos de controle do sistema auditado;
e) avaliação dos pontos de controle;
f) conclusão da auditoria;
g) acompanhamento da auditoria.

Lyra (2008) considera que, o desenvolvimento de um roteiro para a auditoria de sistemas pode estar baseado na organização sugerida, onde os procedimentos ficam bem distribuídos no roteiro, assim com as atividades de revisões e avaliações dos processos e rotinas de auditoria.

Magalhães; Lunkes; Muller (2001, p. 146) afirmam que os procedimentos de auditoria devem contemplar a avaliação de:

a) dados e informações, que compõe os resultados do sistema, e

b) as rotinas de processos do sistema.

A norma da ABNT (2002) considera que os procedimentos de auditoria dentro de um programa a ser aplicado, podem ser baseados conforme apresentado na figura 3.

FIGURA 3 – Procedimentos gerais de uma auditoria em sistemas de gestão

Fonte: ABNT (2002) adaptado.

Estas etapas e atividades são aplicáveis a auditorias de sistemas ERP. Mas a sua abrangência na qual estes procedimentos podem ser aplicados, depende do escopo e complexidade da auditoria específica e o uso para as conclusões de auditoria.

A seguir serão detalhadas as principais etapas utilizadas em processos de auditoria de sistemas de gestão: o planejamento, a execução e a conclusão de auditoria. Estas etapas são resultado de variadas fontes pesquisa a respeito de auditorias e normas e procedimentos que se aplicam a sistema ERP. A partir destas etapas, haverão conclusões e definições para uma posterior aplicação em um programa de auditoria.

2.6.1 Planejamento de auditoria de um sistema ERP

Para o planejamento de uma auditoria de sistemas ERP Magalhães; Lunkes; Muller (2001, p. 146) afirmam que a principal atividade de início, é conhecer o ambiente a ser auditado. Trata-se de entender a estrutura de hardware, *software*, área de programação e análise se houverem operações de TI, estrutura da TI e produtos obtidos através do sistema.

No período de avaliação do sistema a ser auditado, existem alguns detalhes que o auditor deve observar. Para a compreensão do sistema a ser auditado, a documentação inicial de como está estruturado o ambiente de ERP deve seguir alguns pontos. Imoniana (2005) elenca os seguintes:

a) identificação dos sistemas-chaves, neste caso o sistema ERP;
b) descrição do sistema;
c) descrição do perfil do sistema;
d) documentação da visão geral do processamento;
e) descrição de riscos dos sistemas aplicativos.

Após estar esclarecido sobre a estrutura inicial do ambiente a ser auditado, o auditor exerce a atividade de análise de riscos. Segundo Imoniana (2005), sob o ponto de vista de auditoria de sistemas, trata-se de uma metodologia adotada por auditores de TI para saber, com antecedência, quais as ameaças puras ou prováveis existentes em um ambiente de TI de uma organização. Esta análise de risco, segundo Magalhães; Lunkes; Muller (2001, p. 147) é efetuada por meio de investigações nos controles internos, quando se poderão identificar as possíveis fraquezas e seu correto cumprimento.

A ABNT (2006) que trata especificamente de gestão de riscos de segurança da informação, apresenta uma série de atividades que fazem parte desta metodologia de análise de riscos. As etapas do roteiro proposto neste trabalho possuem atividades baseadas na ABNT de gestão de riscos. Porém o roteiro não segue fielmente a metodologia, apenas procura adaptá-la a realidade de algumas de suas atividades.

Para o planejamento de auditoria de sistemas ocorrer de forma mais organizada, o auditor deve ter o entendimento de como proceder nas atividades de análise e considerações no ambiente que está auditando. Além disso, ele necessita fazer o registro das informações geradas nestas atividades, para que o programa de auditoria de sistemas possa ser dinâmico e contribua em futuras tarefas.

2.6.1.1 Análises e considerações sobre ambiente a ser auditado

Para início das atividades de análise dentro do ambiente a ser auditado, é importante que o auditor de sistemas tenha pleno conhecimento do que se tratam os pontos de controle. Estes serão os principais meios de obtenção de evidências durante todo o processo de auditoria.

Gil (1999) afirma que ponto de controle é a situação do ambiente computacional caracterizada pelo auditor como de interesse para validação e avaliação. Um ponto de controle, também pode ser caracterizado como uma combinação de rotinas e informações operacionais de controle.

A auditoria de pontos de controle pode ser abordada de duas formas. Gil (1999) diz que o ponto de controle pode ser visto como controle interno seguro, o qual é composto da lógica do ponto de controle, eficiência, confidencialidade, entre outros. A outra abordagem seria a análise de fraqueza passível de ser identificada, composta de erros, omissão, falhas ou falta de procedimentos no sistema ou falta, erro e correção de dados.

Lyra (2008) relata que os pontos de controle são encontrados em documentos de entrada, relatórios de saída, telas, arquivos, banco de dados, pontos de integração e demais elementos relevantes no sistema. Gil (1999) cita as formas de se perceber os pontos de controle, além da análise de relevância de cada ponto no contexto do sistema. Para Lyra (2008) é importante identificar seus parâmetros, fraquezas e técnicas para sua validação.

Para o entendimento melhor dos pontos de controle selecionados, é importante que eles sejam decompostos. Gil (1999) exemplifica decompondo um ponto de controle chamado “Programa de Atualização” conforme a seguir:

a) rotina operacional de atualização de cadastro;
b) rotina de controle: inclusão, exclusão, alteração na base de dados;
c) informação operacional: conteúdo do registro significativo;
d) informação de controle: conteúdo dos registros de erros durante atualização.

No exemplo citado anteriormente, Gil (1999) faz uma abordagem detalhada no ponto escolhido, para que possa ficar mais claro a importância deste ponto e no que ele pode estar relacionado com outros pontos selecionados ou evidências de auditorias apontadas.

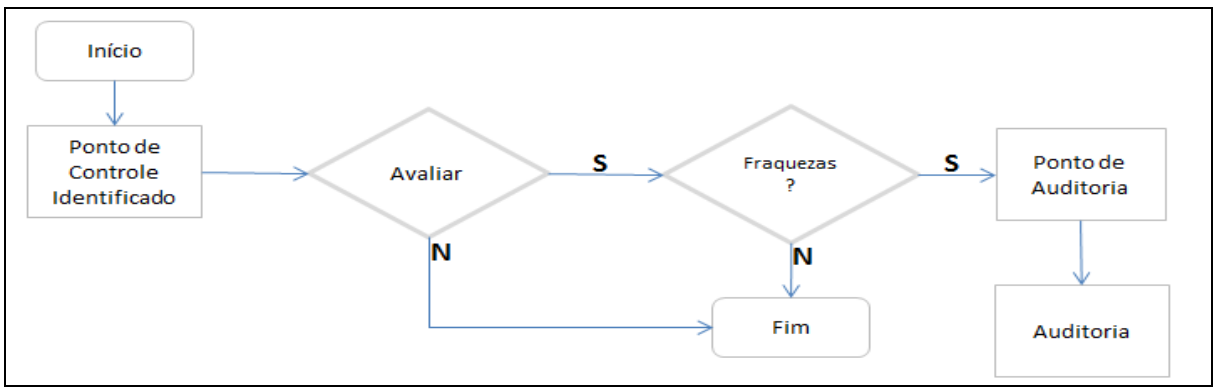
No contexto de sistema ERP, este ponto pode ser uma atualização de uma rotina no *software*.

Gil (1999) destaca que durante os processos de auditoria, o ponto de controle deve ser:

a) identificado dentro do ambiente de sistema computadorizado;
b) observado por suas características em termos de recursos que o compõe, por exemplo, seus módulos;
c) analisado em termos de risco, sob a ótica dos parâmetros de controle interno, segundo a natureza de fraqueza passível de ocorrer;
d) auditado conforme as técnicas que sejam mais apropriadas com os objetivos de risco parametrizados;
e) registrados após a aplicação das técnicas e levantados os resultados para a elaboração e apresentação de opinião que agregue ao ponto de controle validado.

Para ilustrar resumidamente como chegar aos pontos de controle, Gil (1999) apresenta o ciclo de vida do ponto de controle na figura 4. Partindo do ponto de controle já identificado, após a aplicação de análises iniciais, o ponto sofre avaliação por parte de auditores e outros responsáveis pela auditoria. Caso realmente seja importante será avaliado através de análise de artefatos preenchidos e cruzamento com informações levantadas até determinada etapa da auditoria. Após sua avaliação e detectados pontos de fraqueza, o mesmo acaba se tornado um ponto de auditoria, sendo o foco de atuação dos auditores.

FIGURA 4 – Ciclo de vida dos pontos de controle



Fonte: GIL (1999).

Durante a seleção de pontos de controle em um sistema a ser auditado, devem ser priorizados e observados alguns aspectos, baseados em análise de risco. Lyra (2008) define que esta análise consiste na verificação dos prejuízos que poderão ser acarretados pelo sistema, a curto, médio e longo prazo. Deve ser avaliado o grau de risco, mas em relação ao sistema como um todo. As existências de ameaças e os pontos que possuem maior disponibilidade de recursos.

A norma da ABNT (2006) sobre a gestão de riscos de segurança da informação é composta pelas atividades de definição de contexto, análise e avaliação de riscos, tratamento

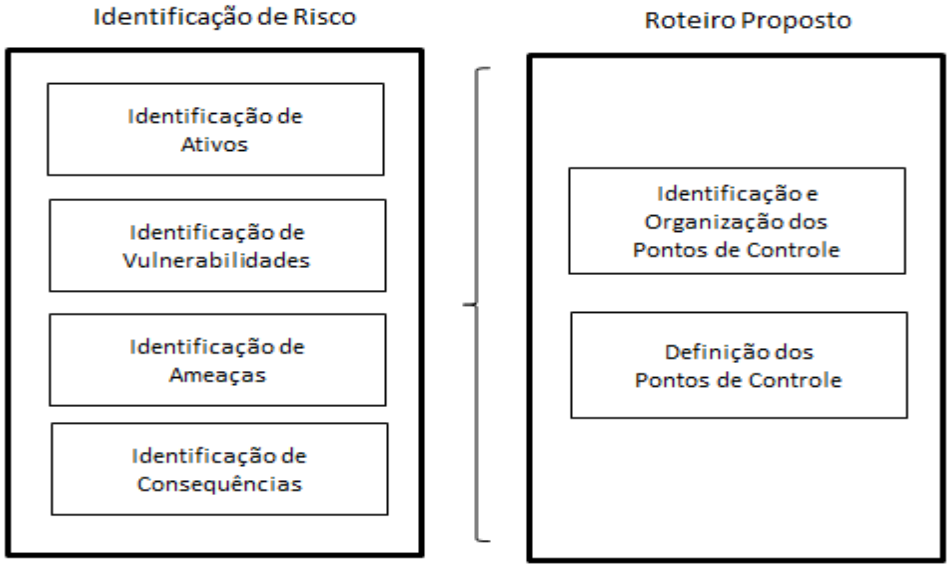
de riscos, aceitação de riscos, comunicação de risco, monitoramento e análise crítica de risco. Para esta etapa de definição dos pontos de auditoria, é possível de serem adaptadas e utilizadas duas delas, as quais seriam: definição do contexto e a análise e avaliação de riscos.

A atividade de definição de contexto, segundo a ABNT (2006) seria o levantamento de informações do ambiente a ser implementada uma gestão de risco. No caso desta proposta de trabalho, esse levantamento poderia ser aplicado no momento de entrevistas junto a usuários e gestores a respeito do ambiente a ser auditado. A definição de contexto trata também de outras ações, mas que seriam voltadas a respeito do gerenciamento de risco e que não estão no escopo deste trabalho.

A outra atividade citada e adaptável a este trabalho seria a de análise e avaliação de riscos. Esta atividade pode auxiliar no momento de seleção dos pontos de controle por ser um método completo na avaliação dos pontos e identificar os riscos. A ABNT (2006) cita que a identificação de riscos é composta de etapas que servem para coletar dados para a criação da estimativa de riscos. Estas etapas são: identificação dos ativos, a identificação das ameaças, a identificação de vulnerabilidades e de consequências.

Todas as etapas mencionadas sobre análise de risco estarão relacionadas em atividades no roteiro durante o tratamento dos pontos como: identificação, organização e definição dos pontos de controle. Para que a atividade de análise de risco aconteça de forma objetiva no roteiro de auditoria, é importante que suas etapas já estejam previamente parametrizadas com informações que sustentem a identificação do risco. A figura 5 mostra a relação do roteiro para com o que é especificado na norma sobre gerenciamento de riscos.

FIGURA 5 – Identificação de riscos em relação ao roteiro proposto



Fonte: LYRA (2008).

A priorização dos pontos a serem auditados é importante, pois o impacto em não focar primeiramente nos processos mais relevantes dentro do sistema pode influenciar no andamento da auditoria. Por isso, também deve haver uma preocupação a mais em cada ponto levantado, analisando sua pertinência para com as próximas atividades a serem realizadas. (LYRA, 2008).

2.6.1.2 Os detalhes do planejamento

A razão deste planejamento inicial é um direcionamento e coordenação para a execução da auditoria. Este planejamento agrega todos os processos de auditoria, elencados por Gil (1989, apud MAGALHAES; LUNKES; MULLER, 2001, p. 47):

a) conhecimento do ambiente;
b) estabelecimento de estratégias;
c) aplicação de técnicas;
d) análise de etapas executadas;
e) relatórios finais.

Estes procedimentos serão evidenciados em documentos, principalmente no plano de auditoria. Neste plano que podem ser retratadas as áreas de risco e pontos de controle, prioridade de execução, tarefas, tempos de execução, equipe de auditoria e recursos metodológicos.

A norma da ABNT (2002) considera que, para o início dos trabalhos é importante o desenvolvimento de um plano de auditoria que contemple o maior número de detalhes possíveis. A flexibilidade deve ser considerada, de modo que conforme evoluam as atividades de auditoria, o plano possa sofrer modificações. A seguir, são elencados alguns itens que são considerados pela norma:

a) objetivos da auditoria;
b) o escopo da auditoria;
c) as datas e lugares onde as atividades de auditoria serão realizadas;
d) definição de funções e responsabilidades dos membros da equipe de auditoria e das áreas auditadas;
e) os principais pontos do relatório de auditoria;
f) quaisquer ações de acompanhamento de auditoria.

Este plano deve passar por um fluxo de aprovação interno, para que seja validado junto aos principais envolvidos na auditoria interna. Suas revisões devem ser acordadas entre

todas as partes, para o andamento do processo.

2.6.2 Execução de procedimentos de auditoria de um sistema ERP

Lima; Castro (2003, p. 49) explicam que os procedimentos de auditoria são o conjunto de técnicas que permitem ao auditor ou equipe de auditoria obter evidências e provas para fundamentar opiniões sob os processos auditados.

Nesta etapa, cabe aos responsáveis pelos trabalhos de auditoria, definirem o grau de amplitude necessário para a utilização das técnicas que resultam na obtenção dos elementos de convicção que sustentarão sua opinião.

A aplicação dos procedimentos de auditoria realiza-se por meio de provas seletivas, testes e amostragens. As técnicas evidenciadas a seguir auxiliam na verificação dos pontos de controle selecionados durante o procedimento de planejamento de auditoria.

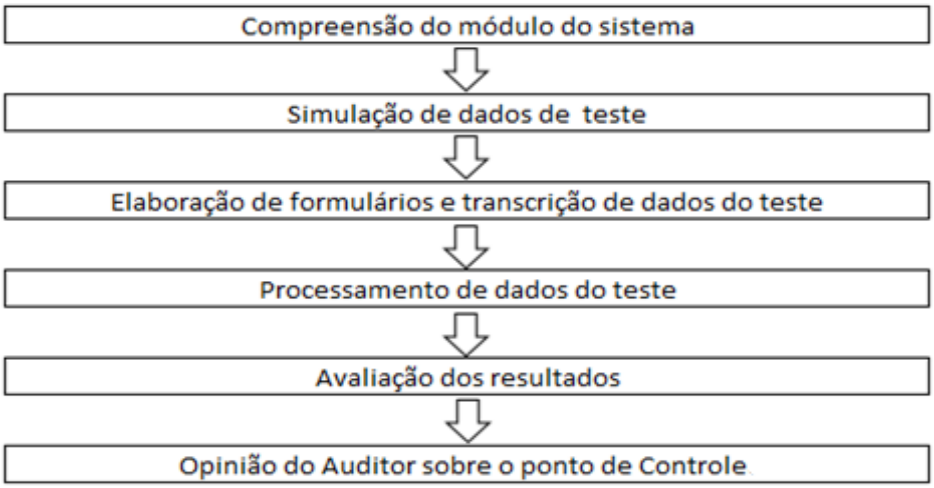
É importante salientar que os testes são iniciados pela compreensão do sistema em geral. O planejamento de testes que a equipe de auditoria decidir realizar pode ser de maneira diferente desta compreensão, como por exemplo, relacionar apenas um módulo em específico dentro de um sistema ERP.

2.6.2.1 Técnicas de auditoria aplicáveis a um sistema ERP

As técnicas de auditoria de sistemas ERP são um conjunto de métodos que devem ser aplicados durante a fase de validação dos pontos de controle. Durante esta fase de validação Gil (1999) explica que as técnicas podem variar de acordo com o nível desejado das análises. As análises podem ser de nível de registros ou até mesmo em detalhes de lógica de programação.

Segundo Imoniana (2005), o conjunto de técnicas que serão apresentadas opera-se com base principalmente no fluxo da figura 6. Trata-se de um fluxograma de ponto de partida, o qual auxilia o auditor durante uma pré-abordagem do ponto de controle. Após avaliar os resultados do ponto de controle, o auditor pode relacionar uma técnica adequada para aquele ponto de controle, de acordo com o que ele levantou em sua pré-avaliação.

FIGURA 6 – Fluxograma de aplicação da simulação de dados



Fonte: IMONIANA (2005).

As seguintes técnicas foram estruturadas conforme referências bibliográficas da área de sistemas, fazendo-se um filtro das técnicas aplicáveis a sistemas ERP.

2.6.2.1.1 Dados de teste ou test data

Imoniana (2005) explica que este tipo de teste envolve um conjunto de dados bem preparados e projetados com o objetivo de testar as funções de entrada de dados do sistema. Para o início destes testes devem ser rodadas diversas transações. Após isso o auditor compara os resultados obtidos com os predeterminados. Para que essa técnica seja efetiva, Magalhães; Lunkes; Muller (2001, p. 153) afirmam que os testes devem compreender o maior número possível de situações, incluindo dados errados, exceções, campos inválidos, duplicidade e outras situações de erro.

Imoniana (2005) destaca que para a geração de dados em massa, podem ser usados *software*s específicos. Uma desvantagem que Magalhães; Lunkes; Muller (2001, p. 153) é que o teste fica limitado ao universo que o auditor delimitou, com dados e transações dentro de parâmetros planejados, deixando de criar situações reais e que poderiam evidenciar mais resultados para análises posteriores.

2.6.2.1.2 Facilidade de teste integrado

Conhecida também por alguns autores como *Integrated test facility* (ITF). Esta técnica utiliza os ambientes reais de processamento para a introdução de dados de teste afirma Lyra (2008). Imoniana (2005) diz que esta técnica, além de usar o ambiente de produção,

envolve a aplicação de entidades fictícias, tais como funcionários que não existem na folha de pagamento ou clientes inexistentes no contas a receber. São confrontados dados do processamento de transações reais com esses dados e os resultados comparados com aqueles predeterminados. No momento de verificar os resultados, são criados arquivos em separados para não confundir dados da organização com os dados fictícios elaborados pela auditoria.

Uma vantagem deste tipo de técnica que Lyra (2008) se refere é que pode ser aplicada em ambiente de produção da empresa, sem ser necessária a criação de uma base de dados e um ambiente só para a execução. Imoniana (2005) se refere como vantajosa a possibilidade de testes dos controles programados no sistema.

As desvantagens desta técnica seriam os efeitos que estes dados inventados poderiam causar. Lyra (2008) alerta para que o auditor fique atento na quantidade de dados fictícios inseridos, e que sejam parametrizados de forma que fiquem fáceis de serem distinguidos dos dados reais. A possibilidade de contaminar dados verídicos é extrema, causando grandes transtornos em fechamentos de mês por exemplo.

2.6.2.1.3 Simulação paralela

Este tipo de técnica serve para ser aplicada em situações onde são constantes as divergências de resultados. Lyra (2008) cita que, por meio de um programa customizado, mas que tenha as mesmas regras de negócio do programa original, é possível simular as funcionalidades do programa em produção. Imoniana (2005) afirma que nesta técnica o próprio auditor pode desenvolver o programa para fazer a execução paralela e depois comparar os resultados com os programas originais.

Gil (1999) aborda que a estrutura desta técnica pode conter o levantamento e identificação das inconsistências, através de documentações do sistema, o desenvolvimento de programa com a lógica da rotina a ser auditada, o qual faz o teste para comparar as lógicas do programa a ser auditado e preparação de ambiente de testes para processamento do programa desenvolvido pelo auditor.

Algumas vantagens desta técnica seriam:

a) os testes podem ser feitos in loco;
b) o grande volume de dados que pode ser processado é enfatizado pela maioria dos autores.

Magalhães; Lunkes; Muller (2001, p. 155), aponta que a desvantagem seria quando são detectadas divergências entre os dados de saída gerados por esta técnica e pelo sistema

auditado, pode ser que o erro esteja no programa elaborado pelo auditor e não no sistema.

2.6.2.1.4 Rastreamento e mapeamento

Técnica utilizada para criar e implementar uma trilha de auditoria. Alguns autores chamam de *audit trails*, que são rotinas de acompanhamento para transações. Além disso, Imoniana (2005) aponta que o mapeamento da execução de transações em programas pode trazer alguns dados estatísticos. Alguns exemplos são:

a) funções não executadas;
b) tempo de máquinas utilizado;
c) funções executadas e o número de execução das mesmas;
d) demais registros pertinentes que devem ser documentados.

Lyra (2008) afirma que, por conter análise de registros das operações do sistema, esta técnica também é chamada de *accountability*. As vantagens deste tipo de técnica são: auxilia na avaliação dos controles internos que devem ser seguidos; permite a criação de alertas quanto à aplicação de controles operacionais e seus cumprimentos.

Imoniana (2005) lista algumas desvantagens:

a) exige do auditor habilidades avançadas em TI para que possa interpretar lógicas de programação;
b) existe um aumento no tempo das transações processarem.

2.6.2.1.5 Análise da lógica de programação

Trata-se de uma técnica de validação que avalia se as instruções dadas ao sistema aplicativo são as mesmas identificadas em suas documentações. Imoniana (2005) considera que esta técnica pode ser feita manualmente, e é aplicável nos principais programas de um sistema. Também pode ser aplicada em programas de maior risco para a empresa com a utilização de *softwares* especializados.

2.6.2.1.6 Análise do programa fonte

Este procedimento visa a análise visual do código-fonte do sistema sob auditoria. Porém, antes de tudo, o auditor deve certificar-se que a organização possui as fontes dos programas e rotinas a serem auditados.

Tendo esta premissa atendida, Gil (1999) cita que esta análise permite ao auditor verificar se o programador cumpriu normas de padronização de código (*labels*), rotinas, arquivos e programas. Também permite que seja feita a análise da qualidade de estruturação de programas e a detectar vícios de programação e o nível de atendimento às características da linguagem utilizada no desenvolvimento.

Alguns passos descritos por Gil (1999) de como executar esta técnica seriam por exemplo:

a) preencher uma ordem de serviço determinando à produção que compile o módulo-fonte, encontrado em diretório de reposição dos arquivos fonte;
b) executar um programa que compare o código-objeto gerado na primeira etapa, com o código-objeto do programa que se encontra gravado na bilblioteca-objeto da produção;
c) efetuar verificações em eventuais divergências que ocorram na segunda etapa.

2.6.2.1.7 Entrevistas no ambiente de sistemas

Gil (1999) relata que esta técnica corresponde à realização de encontros entre o auditor e os auditados, profissionais usuários e usuários de TI envolvidos no ambiente.

Elenca uma sequência de procedimentos que correspondem a:

a) análise dos pontos de controle e planejamento da reunião com os profissionais que possuem interesse, além dos envolvidos. Isso deve ser feito antecipadamente, fazendo a comunicação detalhada do que irá ser abordado na reunião;
b) elaboração de questionário para a realização de entrevistas. Questões podem ser divididas por parâmetros de controle interno, por área ou assunto de processamento eletrônico de dados. Deve ser estimado o tempo de duração da entrevista;
c) ao planejar as reuniões, devem ser dadas atenção a hierarquias dentro das áreas a serem auditadas, além de fazer uso de uma ferramenta adequada para tabulação de respostas dos questionários;
d) é importante que se faça uma ata de reunião, para posterior divulgação e consultas;
e) a análise e formação de opinião do auditor acerca do nível de controle interno do ponto de controle, finalizando o processo com a emissão de um relatório com as observações.

Esta técnica pode estar associada a outras, dependendo o contexto utilizado pelo auditor.

2.6.2.1.8 Análise de relatórios e telas

Neste método, Gil (1999) explica que devem ser analisados documentos, relatórios e telas do sistema sob auditoria. Deve ser observado o nível de utilização pelo usuário, o grau de confidencialidade do seu conteúdo, forma de utilização e integração entre relatórios, telas e documentos e as distribuições de informações segundo o leiaute vigente.

Para aplicação da técnica são abordados:

a) a relação por usuários de todos os relatórios, telas ou documentos que pertençam ao ponto de controle a ser analisado. O auditor pode classificar essas listagens.
b) obtenção de modelo ou cópia de cada relatório, documento ou tela para os papéis de trabalho.
c) elaboração de um *check-list* para a realização do levantamento acerca dos relatórios, telas ou documentos;
d) aplicação de entrevistas, utilizando parte do método de entrevistas no ambiente de sistemas;
e) análise das respostas, emitindo opinião sobre o que foi auditado;

Os resultados desta técnica podem ser:

a) relatórios, telas ou documentos não mais utilizados pelos usuários;
b) leiautes inadequados;
c) confidencialidade de dados não estabelecida ou evidenciada.

Com esta técnica vale frisar também que, com a desativação de alguns programas não mais utilizados dentro de um sistema ERP, podem ser cortados custos e direcionados estes para melhorias de programas que realmente sejam considerados críticos para a empresa.

2.6.2.1.9 Snapshots

Técnica que fornece uma listagem ou gravação do conteúdo das variáveis do programa (acumuladores, chaves, áreas de armazenamento) quando determinado registro está sendo processado. A quantidade de situações a serem extraídas é pré-determinada. (GIL, 1999).

Esta técnica pode ser usada como auxílio na depuração de programas, quando existem problemas e realmente exige um bom conhecimento de PED por parte do auditor.

Gil (1999) explica que se trata de uma listagem onde estão gravados o conteúdo das variáveis do programa.

Este tipo de trabalho pode ser feito por programas específicos, mas devem estar instalados no ambiente que roda o programa principal, neste caso do sistema ERP.

As técnicas de auditoria de sistemas são totalmente aplicáveis a sistemas em operação. Entretanto, a aplicação de algumas pode estar relacionada à tecnologia computacional existente no ambiente vigente sob auditoria. Gil (1999) enfatiza que várias destas técnicas são aplicáveis, independente do ambiente ou de que ferramentas utilitárias estão disponíveis como recurso para o uso das técnicas.

O mais importante é que o auditor de sistemas possua conhecimentos para poder suportar a indisponibilidade de recursos para a aplicação de técnicas e realmente consiga efetivar seu trabalho nos pontos de auditoria definidos.

2.6.2.2 Vantagens no uso das técnicas

A utilização de técnicas, ajuda no desenvolvimento de uma auditoria consistente e confiável para todos os envolvidos no trabalho. Imoniana (2005) elenca algumas vantagens que podem ser trazidas com o uso de técnicas pelos auditores internos:

a) produtividade: com as reduções de ciclos operacionais e aumentando o foco em serviços mais dinâmicos durante a auditoria;
b) custo: como o auditor é um funcionário interno, não haverão custos extras. Desse modo evitam-se gastos comparados com auditores de empresas terceiras, por exemplo, com deslocamentos até a empresa e hospedagens;
c) qualidade assegurada: utilizando-se de técnicas consolidadas, o auditor pode adequar seus trabalhos a padrões destacados na área de auditoria, melhorando a qualidade dos serviços prestados;
d) valor agregado: disponibiliza tempestivamente resultados para a tomada de decisões que necessitam de mudanças de rumos mais urgentes. Isso faz com que as correções sejam mais eficazes, possibilitando também reflexões sobre impactos em contexto geral;
e) benefícios para o auditor: utilizando estas técnicas, fica de forma mais fácil para o auditor executar algumas de suas atividades. Ele tem os benefícios de:

- eliminação de tarefas repetitivas, que através de técnicas podem ser automatizadas;
- reduções de risco de auditoria, uma vez que conseguindo se programar com as técnicas, as chances são menores de algo passar despercebido;
- maior tempo para sugerir e pensar no momento de formatar relatórios de verificações de auditoria.

2.6.3 Conclusões de auditoria de um sistema ERP

Gil (1999) cita que o aspecto crucial da auditoria de sistemas é a apresentação do resultado de seus trabalhos à alta administração. Vários fatores precisam ser atendidos para a perfeita comunicação entre a auditoria e a alta administração:

a) objetividade na transmissão dos resultados da auditoria;
b) esclarecimento nos debates realizados entre auditoria e os auditados;
c) clareza nas recomendações de alternativas de solução;
d) explicitação da coerência de atuação da auditoria.

Ao fim dos trabalhos realizados pela auditoria, são geradas diversas opiniões, constatações e pareceres. Nestas conclusões o auditor expressa sua opinião quanto à satisfação dos elementos avaliados, se a auditoria foi realizada dentro das normas usuais geralmente aceitas e se existem algumas ressalvas especificadas nos pontos de controle auditados.

As opiniões do auditor podem ser expressas por meio de relatórios e acompanhadas por pareceres e certificados de auditoria. Os resultados compilados apresentam-se em artefatos que são chamados também produtos gerados de uma auditoria.

2.6.4 Os produtos gerados em uma auditoria de sistemas

A auditoria pode auxiliar administradores por meio de relatórios e pareceres, mostrando através destes artefatos, possíveis evidenciações de erros, fraudes ou omissão de dados e informações.

Gil (1999) procura enfatizar que a auditoria de sistemas necessita retratar o resultado de seus trabalhos e para tal, vale-se dos seguintes relatórios:

a) relatório de fraquezas de controle interno;

Os objetivos do relatório de fraquezas de controle interno estão estruturados da seguinte forma:

- mostrar os objetivos do projeto de auditoria;
- pontos de controle auditados;
- conclusão alcançada a cada ponto de controle;
- alternativas e sugestões de solução para a correção das fraquezas.

b) certificado de controle interno;

No certificado de controle interno são apresentadas as opiniões da auditoria em termos gerais e sintéticos. Neste certificado que são colocados os achados de fraquezas de controle interno, dos pontos de controle auditados, conforme as normas de auditoria aplicadas a opinião de auditores.

Gil (1999) afirma que este certificado é o artefato que vai expressar para a alta direção da organização, os resultados em formato macro, podendo também ser mais simples e trazendo somente os pontos de controle onde a situação é mais grave.

Já Imoniana (2005) cita que existem empresas que possuem seu próprio modelo de relatório final. O autor destaca que não há problemas em cada empresa adotar um padrão, porém desde que aborde os seguintes elementos:

- a observação, onde estão os processos de auditoria;
- consequências que a empresa incorre em decorrência das fraquezas apontadas;
- recomendações, para que os auditores possam sugerir as medidas de correção;
- comentários de gestor de auditoria, havendo a concordância ou não com o ponto levantado e apontamento do prazo para a implementação das medidas.

c) relatório de redução de custos;

Redução de custos, muitas vezes podem ser os principais resultados que os administradores esperam que uma auditoria consiga desempenhar. O relatório descrito por Gil (1999) é um subconjunto do relatório de fraquezas de controle interno, onde explicita economias financeiras que podem ser feitas. Estas economias são baseadas conforme as adoções de recomendações feitas pelos auditores.

Este relatório é uma base para que a empresa possa utilizar em suas análises internas de retornos sobre investimentos.

d) manual de auditoria interna do ambiente computadorizado auditado.

Este manual é uma base para se manterem em histórico as auditorias realizadas. Nele Gil (1999) explica que é armazenado o planejamento da auditoria feita, os pontos de controle elencados, testados e flagrados. As auditorias futuras terão um aditivo para realizarem seus trabalhos se existir este manual, podendo analisar a evolução de pontos de controle.

Para detalhar um pouco mais alguns dos artefatos gerados em auditoria, Lima; Castro (2003, p. 31) citam as formas mais comuns de configurações de relatório:

- forma breve: utiliza-se quando o exame não revelar os aspectos fundamentais que devam ser divulgados a terceiros;
- forma longa: onde inclui todas as informações levantadas de auditoria. O auditor expressa o escopo que ele definiu e o grau de responsabilidade. O auditor descreve de forma sucinta ou bem explicada seus comentários;
- síntese de relatório: em auditorias muito longas, a elaboração de sínteses tem por objetivo apenas mostrar o andamento e encaminhamento das atuais tarefas.

Outras formas de relatórios mais customizadas podem ser apresentadas conforme indica Imoniana (2005). O auditor pode decidir apresentar níveis de detalhes para que os usuários ou a gestão percebam os itens:

a) os objetivos de controles que forem testados;
b) as conclusões alcançadas após os testes;
c) identificação dos pontos de controles atenuantes mitigam os riscos ou não;
d) descrição dos procedimentos de testes de controles;
e) resultados dos testes;
f) observações e constatações relevantes;
g) julgamento das constatações;
h) recomendações e sugestões;
i) concordância ou não da gerência;
j) respostas da gerência.

O nível de detalhamento pode depender dos critérios e objetivos elencados pelos interessados da auditoria interna. Este tipo de relatório é bastante pertinente devido o nível de detalhes que possui.

O objetivo da auditoria que pode delimitar os resultados obtidos e necessários para serem mostrados aos interessados. Os tipos de relatórios ficam a cargo da equipe de auditoria envolvida e também dependendo do grau de gravidade dos pontos de controle auditados.

2.7 CONSIDERAÇÕES FINAIS DO CAPÍTULO

A partir das características específicas de um sistema ERP foram estudados os conceitos de auditoria. Estes conceitos tratam das definições e procedimentos essenciais para o entendimento de uma auditoria em sistema ERP.

Um sistema ERP, como citado por Junior (2006) se caracteriza por:

a) possibilitar maior integridade das informações e dados, que por qualquer mudança neles acabam refletindo em todo o sistema;
b) conceder maior segurança sobre os processos de negócio da empresa, como por exemplo os controles baseados em *login* e senha para acesso a determinadas transações;
c) eliminar redundâncias e redigitação de dados, mantendo um controle central de informações e dados, acessível as diversas áreas da empresa.

Para um sistema ERP em produção, podem ser realizadas auditorias internas com diferentes objetivos, tais como: integridade, manutenabilidade, auditabilidade, disponibilidade, integridade, confidencialidade, privacidade, acuidade e versatilidade.

As auditorias internas podem ser classificadas pela sua forma, para que sua extensão e tempo possam ser proporcionais aos objetivos que propõem. As formas de auditoria apresentadas são: extensão, profundidade e tempestividade e contribuem para a formação da auditoria interna, pois através destas formas, são impostos limites dentro de uma auditoria.

De acordo com o que foi estudado neste capítulo, as técnicas de auditoria contribuem para o levantamento de evidências. Sua escolha e execução podem ser programadas de acordo com os pontos de auditoria a serem selecionados, para a posterior aplicação da técnica compatível. As técnicas também podem ser pré-selecionadas de acordo com os objetivos que a auditoria se propõe a atingir.

A capacitação de profissionais é importante para que sejam conduzidos os trabalhos que envolvem a criação de um programa de auditoria. Através de pré-requisitos estabelecidos por uma comissão interna, o desenvolvimento de uma equipe de auditoria acaba por selecionar os profissionais mais capacitados a exercerem a condução e delegação de atividades que compõe uma auditoria interna, registrando e extraindo resultados ao fim dos trabalhos.

Apesar de autores considerarem diferentes etapas de auditoria, elas podem ser resumidas em planejamento de auditoria, execução de procedimentos de auditoria e as conclusões de auditoria. Com base nestas etapas citadas, o roteiro de auditoria começa a ser formado. Além disso, apresenta também as atividades e os produtos gerados que podem ser os artefatos de saída e entrada, onde ficam registradas informações e dados relevantes de uma auditoria interna.

As etapas estudadas neste capítulo serão melhor entendidos em sua aplicação, durante a elaboração do roteiro de auditoria de sistemas ERP no capítulo 3. Dentro desta

elaboração do roteiro, serão abordados detalhes de como e quais as atividades devem ser exercidas para a criação e disponibilização da auditoria. Além disso, serão expostos os artefatos gerados que contemplam o roteiro de auditoria e auxiliam os auditores no andamento do programa de auditoria.

3 ROTEIRO PARA AUDITORIAS DE SISTEMAS

A sistematização de auditorias na área de Sistemas de Informação é uma atividade recente, que vem ganhando força. Uma auditoria pode ser melhor estruturada, a partir de um artefato ou instrumento que contenha as diretrizes para sua aplicação e gerenciamento.

Um roteiro para a elaboração de programas de auditoria proporciona diretrizes básicas que, segundo LYRA (2005), auxiliam às organizações na construção de um programa estruturado de auditorias.

Empresas que consideram seus sistemas informatizados como a base para sustentação de seus processos de negócio, entendem que seu ERP deve ser uma fonte de informações consistente e o mais confiável possível. Devido a alta necessidade de adequações, customizações e até pelo mau uso do software, o sistema ERP pode acabar de alguma forma se tornando instável e oneroso ao longo dos anos. A auditoria de sistemas pode ser uma ação que contribuirá na verificação deste sistema e poderá levantar quais as principais deficiências a serem analisadas e tratadas, através do uso de um roteiro para criação de programas de auditoria.

Este trabalho propõe um roteiro para elaboração de programas de auditoria em sistema ERP que pode ser seguido conforme a proposta ou adaptado pelas organizações. A adaptação será necessária conforme o objetivo e o escopo definido pela comissão de auditoria. No caso deste roteiro os objetivos propostos foram: manutenabilidade, auditabilidade, disponibilidade, integridade, confidencialidade, privacidade, acuidade e versatilidade.

Este roteiro está fundamentado em normas gerais de auditoria, como a NBR ISO 19011 instrumento de pesquisa para adequação de atividades genéricas de auditoria. O roteiro também está baseado em normas específicas e outras referências da área de TI, que apresentam diretrizes aplicáveis a sistemas ERP: NBR ISO 27005, NBR 27002, NBR 17799, ITIL e Cobit.

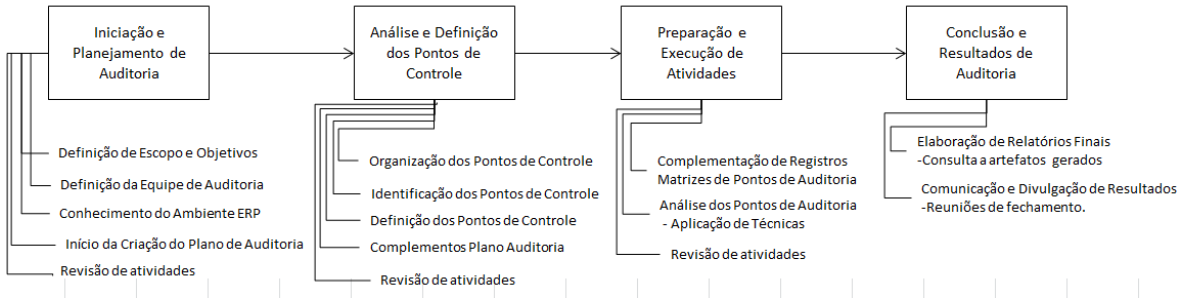
Um roteiro, segundo consta em Michaelis significa normas ou regulamentos. Estes significados estendem o conhecimento para preceito, que segundo Michaelis seria a determinação, norma ou guia para qualquer procedimento.

O roteiro propõe uma estrutura de etapas, compostas por atividades sequenciadas, que são executadas por responsáveis pré-determinados. Os responsáveis fazem o uso de artefatos para execução de suas atividades e realizam o registro de dados e informações, quer serão utilizados na sequência do programa de auditoria.

O processo de auditoria, segundo Stair e Reynolds (2006) é motivado em uma empresa a partir de vários fatores: diversidade de transações, customizações, adequações, grande volume de dados do sistema, adequações e complexidade de funcionalidades. Estes fatores podem ser trabalhados por uma empresa através da aplicação de um programa de auditoria estruturado, que ao fim ofereça propostas de ações e acompanhamento das atividades, trazendo ganhos para a empresa e utilização ideal do sistema.

O roteiro proposto contempla quatro grandes fases: A Iniciação do Planejamento de Auditoria, Análise de Definição dos Pontos de Controle, Preparação e Execução de Atividades e Conclusão e Resultados de Auditoria. As fases são executadas de forma sequencial conforme pode ser visto na figura 7. A primeira fase propõe atividades essenciais na definição de requisitos básicos que compõe o planejamento e estruturação do programa de auditoria de sistemas. Nas segunda e terceira fases são apresentadas as atividades propriamente ditas de auditoria como análises, definições de pontos de controle e execução de atividades de auditoria. Para finalizar, a quarta fase, retrata as atividades de fechamento de auditoria e apresentação de resultados obtidos.

FIGURA 7 – As fases do roteiro e suas respectivas atividades



Fonte: Elaborado pelo autor.

Além de apresentar as fases e atividades, também possui os artefatos de entrada, artefatos de saída e os responsáveis por cada uma das atividades delegadas aos participantes do programa de auditoria.

Para cada atividade do roteiro são propostos artefatos. Os artefatos de entrada servem como orientação de determinada atividade, como por exemplo, na primeira atividade de definição de objetivos, onde o artefato de entrada seria a tabela de objetivos globais relacionados com as normas, metodologias e procedimentos aplicáveis a sistemas ERP. Os artefatos de saída mantém o registro de cada atividade, como por exemplo, as atas de reuniões para registro de encontros entre a comissão de auditoria, gestores ou equipe de auditoria.

O roteiro procura relacionar as fases, com suas respectivas atividades, artefatos de

entrada, artefatos de saída e os responsáveis por cada uma das atividades. Esta relação pode ser vista na figura 8, que apresenta um recorte parcial do roteiro proposto.

FIGURA 8 – Exemplo de atividade e demais características presentes no roteiro

Fase	Atividades		Artefatos Entrada	Artefatos Saída	Responsável
Iniciação do Planejamento de Auditoria	Definição de Objetivos	a)Entrevistas com os principais interessados na aplicação de auditoria, b)Reuniões entre a comissão de auditoria e possíveis auditores.	Consulta a tabela de Objetivos GLOBAIS de Auditoria x Diretrizes de Normas, Metodologias e procedimentos aplicáveis a sistemas ERP.	Atas de reuniões para registro de Informações complementares. Documento das definições iniciais do programa de auditoria	*Comissão de Auditoria, Gestores*

Fonte: Elaborado pelo autor.

Conforme vão seguindo o roteiro, os envolvidos na auditoria vão executando as atividades e preenchendo os artefatos. O roteiro completo segue esboçado conforme no anexo C e será explicado fase por fase a partir dos próximos capítulos.

3.1 FASE DE INICIAÇÃO DO PLANEJAMENTO DE AUDITORIA

Na fase de iniciação do planejamento de auditoria são direcionados e organizados os trabalhos que envolvem o programa de auditoria. É nesta fase que são definidos os objetivos e o escopo da auditoria. Estes conceitos iniciais são fundamentais, pois eles determinarão o rumo do programa de auditoria, e darão o foco de trabalho da equipe.

Esta etapa é composta pelas atividades de definição de objetivos, definição do escopo, definição da equipe de auditoria, conhecimento do ambiente de sistemas e a criação do plano de auditoria conforme é mostrado na figura 9.

FIGURA 9 – Fase de Iniciação e planejamento de auditoria

Fase	Atividades		Artefatos Entrada	Artefatos Saída	Responsável
Iniciação do Planejamento de Auditoria	Definição de Objetivos Definição do Escopo	a)Entrevistas com os principais interessados na aplicação de auditoria, b)Reuniões entre a comissão de auditoria e possíveis auditores.	* Consulta a tabela de Objetivos GLOBAIS de Auditoria x Diretrizes de Normas, Metodologias e procedimentos aplicáveis a sistemas ERP.	* Atas de reuniões para registro de Informações complementares. * Documento das definições iniciais do programa de auditoria	*Comissão de Auditoria, Gestores*
	Definição de Equipe de Auditoria	**Recrutamento e Seleção dos auditores.** Análise de requisitos necessários: Habilidade e Conhecimentos sobre auditoria e sobre sistemas de gestão.	* Documentos e Questionários de avaliação; * Documentos de Trabalho: formulários para registros: reuniões, evidências e constatações. * Matriz de habilidades;	* Documento com informações sobre a equipe de auditoria, o líder e suas atividades.	*Comissão de Auditoria, Gestores*
		Atribuição de responsabilidades aos selecionados.	* Matriz de funções de auditores.	* Documento formalizado com as responsabilidades de cada membro da equipe.	*Líder de Auditoria*
	Conhecimento do Ambiente de Sistemas	Análise de informações existentes, entrevistas, aplicação dos questionários.	* Questionários sobre o ambiente do sistema ERP	*Questionário respondido.	*Equipe de Auditoria, Líder de Auditoria*
	Criação do Plano de Auditoria	Consultar os artefatos gerados até então para o preenchimento de campos no Plano de Auditoria		MODELO - Plano de Auditoria	*Líder de Auditoria*

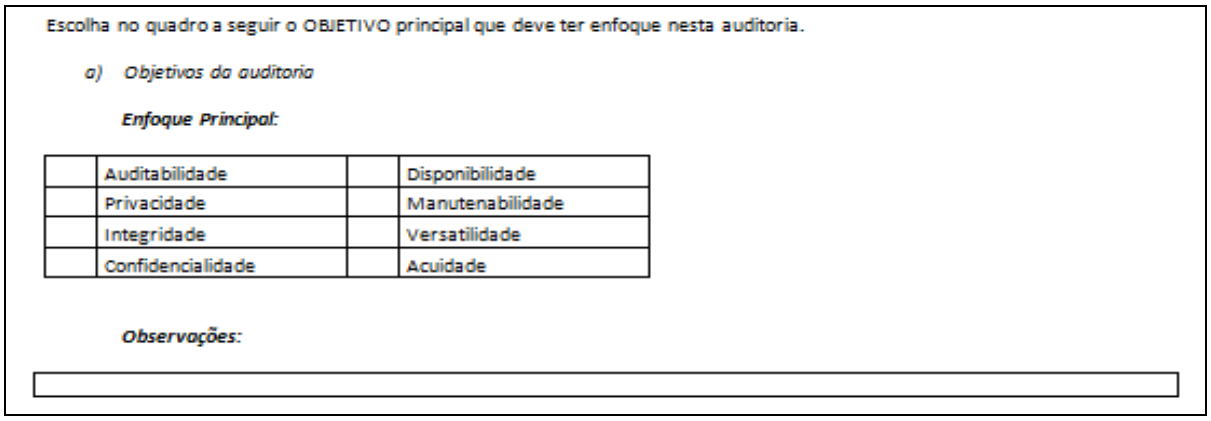
Fonte: Elaborado pelo autor.

3.1.1 Definição de objetivos e escopo de auditoria

Os objetivos de um programa de auditoria estabelecidos por Lyra (2008) no capítulo 2.3 são o alicerce para uma auditoria ser eficaz e consistente. Os responsáveis por estabelecer os objetivos são a comissão de auditoria responsável pelo programa ou até mesmo gestores envolvidos no processo de criação do programa. Esta comissão de auditoria deve ser formada por usuários chave das áreas e que possuam o conhecimento pleno do funcionamento do sistema a ser verificado , além de fatores que implicam nos processos da empresa.

Para estabelecer os objetivos de modo formal, o preenchimento deve ocorrer no artefato de Definições Iniciais do Programa de Auditoria. Na figura 10 é apresentado uma parte do artefato de Definições Iniciais do Programa de Auditoria. O artefato é preenchido por integrante da comissão de auditoria, visando os objetivos propostos e observações relevantes a cada um deles. Este artefato pode ser visto por completo no anexo D.

FIGURA 10 – Relação de objetivos a serem escolhidos e detalhados



Escolha no quadro a seguir o OBJETIVO principal que deve ter enfoque nesta auditoria.

a) Objetivos da auditoria

Enfoque Principal:

	Auditabilidade		Disponibilidade
	Privacidade		Manutenabilidade
	Integridade		Versatilidade
	Confidencialidade		Acuidade

Observações:

Fonte: Elaborado pelo autor.

Os integrantes da comissão e envolvidos no programa de auditoria podem utilizar o artefato de consulta sobre os objetivos globais para entendimento de cada um, além da sua relação com as Normas e Metodologias aplicáveis a sistemas ERP. Através desta relação, a comissão pode começar a projetar futuras atividades e escopo de auditoria.

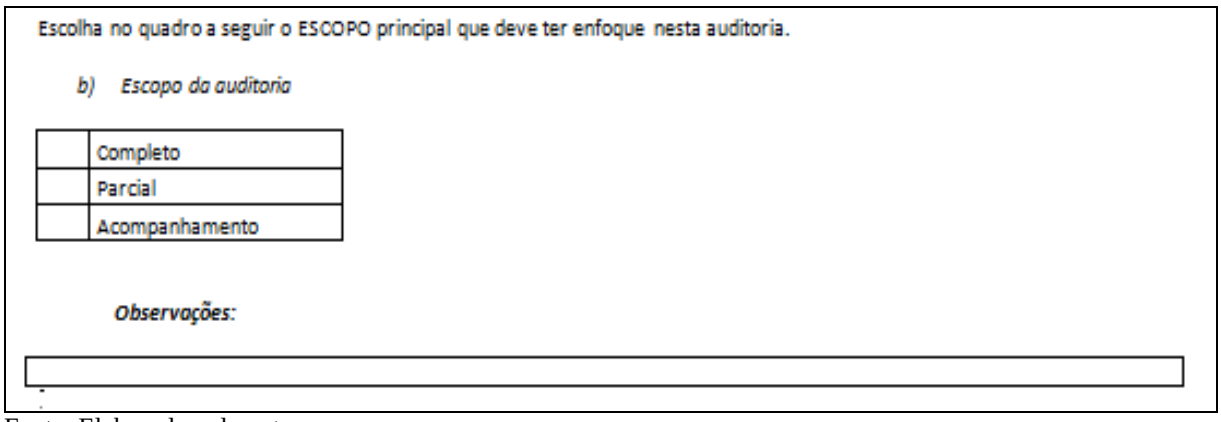
O escopo de uma auditoria deve ser definido juntamente aos objetivos. Dependendo do que a empresa está considerando relevante dentro do processo em um ERP, esta auditoria pode ser classificada por escopo. Segundo a ABNT (2002) existem alguns tipos de escopo que podem ser aplicados:

a) completa: abrange todas as funções e atividades pertinentes à organização ou unidade;

b) parcial: limita-se à determinada função, área, linha de produto ou atividade de interesse;
c) de acompanhamento (*follow-up*): realizada para verificar a implementação e eficácia de ações corretivas previamente acordadas.

Para complementar o artefato de Definições Iniciais do Programa de Auditoria, o escopo segue a mesma linha que a definição de objetivos. O preenchimento ocorre por parte de algum integrante da comissão de auditoria, em que através de reunião com demais presentes, procede selecionando o tipo de escopo que o programa de auditoria atenderá. Na figura 11 é demonstrado parte do artefato a ser preenchido e as observações a respeito do escopo da mesma forma como fora preenchido os objetivos.

FIGURA 11 – Relação de tipo de escopo a ser escolhido


Escolha no quadro a seguir o ESCOPO principal que deve ter enfoque nesta auditoria.

b) Escopo da auditoria

	Completo
	Parcial
	Acompanhamento

Observações:

Fonte: Elaborado pelo autor.

Para o auxilio no registro de reuniões, entrevistas realizadas e preenchimento do artefato de Definições Iniciais, o roteiro sugere a utilização de atas de reuniões. O preenchimento das atas pode ser feito por algum integrante da comissão de auditoria. Este integrante faz os registros de participantes, cargos, ações a serem realizadas e as datas para solução das ações. No anexo E segue uma ata de modelo sugerida no roteiro de auditoria.

3.1.2 Definição de equipe de auditoria

Gil (1999) afirma que o auditor necessita de conhecimento das áreas de auditoria de Sistemas de Informação e processamento de dados. Cada vez mais o auditor precisa estar especializado e em treinamento constante sobre tecnologias que envolvem sistemas num contexto geral.

Durante a formação de uma equipe de auditoria interna, existem requisitos básicos que devem ser seguidos para o recrutamento de um auditor interno. A comissão que está

elaborando um programa de auditoria interna em sistemas, tem de estar ciente que nem sempre encontrará funcionários com os requisitos necessários. Segundo a ABNT (2002), por conta disso, a comissão terá que assegurar treinamentos que visam a capacitação dos funcionários para que se possa ter uma equipe consistente de auditores em seu sistema ERP.

A norma da ABNT (2002) elenca atributos e habilidades pessoais que devem ser observados no momento de seleção de uma equipe interna de auditoria como é mostrado na figura 12. De acordo com a norma estes são os requisitos básicos para a seleção de um auditor.

FIGURA 12 – Atributos e habilidade para auditores internos

Competências para expressar clara e fluentemente conceitos e ideias, oralmente ou através da escrita.
Habilidades interpessoais para um desempenho eficiente da auditoria, como diplomacia e habilidade para escutar.
Habilidade para manter suficientemente independência e objetividade.
Organização pessoal necessária ao efetivo desempenho da auditoria.
Habilidade para realizar julgamentos aceitáveis, baseado em evidências objetivas.

Fonte: ABNT (2002).

Além dos atributos e habilidades pessoais, exige-se que um auditor tenha as capacidades técnicas e profissionais para poder participar do processo de seleção. O candidato deve conhecer e saber compreender os princípios e objetivos da auditoria que irá tentar ingressar. Gil (1999) complementa a importância da formação da equipe, em que se distinguem as responsabilidades e competências dos funcionários que a formarão. A hierarquia ou os cargos dentro de um programa de auditoria podem distinguir as necessidades de competência e nível de responsabilidades dos auditores.

Na figura 13 é apresentada uma formação ideal para uma equipe de auditoria interna.

FIGURA 13 – Formação básica de uma equipe de auditoria interna

Papel	Funções
Auditor Líder	Programar a Auditoria Interna
	Disponibilizar recursos para a Equipe de Auditoria Interna
	Coordenar a execução das atividades de Auditoria, reuniões
	Auxiliar na elaboração dos artefatos junto a Equipe de Auditoria
	Analisar criticamente a efetividade das ações tomadas pela organização
Equipe de Auditoria	Preparar listas de verificação, questionários, entrevistas
	Efetuar Auditoria
	Preencher registros de constatações de Não-Conformidades

Fonte: ABNT (2002) adaptado.

A primeira coluna apresenta o papel do auditor num programa de auditoria, dividido por níveis hierárquicos. Na coluna secundária, as funções que podem ser delegadas dentro do programa de auditoria.

Para o auxílio na seleção e recrutamento de pessoas, a comissão de auditoria interna pode divulgar a seleção através de murais, reuniões com gestores ou recrutar funcionários de auditorias passadas.

A seleção da equipe de auditoria pode ser feita pela comissão de implantação de auditoria através de questionários, baseados nos conhecimentos e habilidades elencados anteriormente. Para auxiliar na condução da seleção, o responsável pela atividade pode avaliar documentos internos de Recursos Humanos.

No anexo F é apresentado um modelo de formulário para seleção de auditores internos. O processo consiste no preenchimento do formulário por parte da comissão de auditoria, começando por nome e setor em que o candidato trabalha atualmente, além do cargo que deseja desempenhar no programa de auditoria. Para avaliar os candidatos serão considerados os atributos pessoais, marcos com valores de 5 a 1, sendo 5 o mais forte e o 1 o mais fraco. Na figura 14 é exemplificado através de um recorte esta etapa de preenchimento.

FIGURA 14 – Campos do formulário para avaliação de candidatos

Avaliação de Candidato

Preencha as colunas de acordo com as competências do candidato:

Atributos pessoais em Auditoria Interna	5	4	3	2	1	Observações
Competências para expressar clara e fluentemente conceitos e ideias, oralmente ou através da escrita.						
Habilidades interpessoais para um desempenho eficiente da auditoria, como diplomacia, fato e habilidade para escutar.						

Fonte: Elaborado pelo autor.

A definição dos escolhidos, parte do constatado em entrevistas e resultados do preenchimento do formulário de seleção de auditores. Esta definição de equipe fica a critério da avaliação dos artefatos desta atividade de seleção, realizada pela comissão de auditoria e responsáveis. O desempenho de cada candidato pode ser registrado nos próprios formulários de seleção de auditor, para que seja mantido em sigilo e privado a cada candidato.

O registro dos candidatos selecionados pode ser feito através das atas de reuniões, onde poderão ser colocados os nomes, cargos o programa de auditoria e principais atividades a desempenhar.

A divulgação dos selecionados pode ser feita da mesma maneira que as vagas, através de divulgações em murais ou registrados em atas.

O auditor líder pode formatar em um documento, a lista das principais atividades e seus respectivos responsáveis. Isso facilita no momento de exigir informações do ambiente e saber como está o andamento das atividades.

3.1.3 Conhecendo o ambiente do sistema ERP

Dentro do processo de criação de um programa de auditoria, é importante que os auditores conheçam o ambiente de ERP em que irão trabalhar. Magalhães; Lunkes; Muller (2001, p. 146) relatam que o escopo de uma auditoria pode ser delimitado através do conhecimento que se tem do ambiente de sistema a ser auditado. O conhecimento a ser adquirido pode ser através da compreensão do fluxo do sistema ou de técnicas citadas por Magalhães; Lunkes; Muller (2001, p. 146).

A compreensão do fluxo aborda uma série de questões que Imoniana (2005) destaca. Estas questões poderiam estar formatadas em um modelo, visando detalhamento do escopo de auditoria e podem auxiliar na tomada de decisões futuras durante o andamento dos procedimentos de auditoria. As informações geradas a partir da análise destas questões devem ser anexadas junto ao plano de auditoria. As técnicas que Imoniana (2005) cita seriam por meio de visitas ou entrevistas junto a gestores ou analistas das áreas. Na figura 15 é apresentado o modelo que contempla importantes questões, as quais podem ser discutidas internamente e que complementam demais artefatos utilizados no programa de auditoria

FIGURA 15 – Modelo de questionário para conhecimento de ambiente

	Questões	S/N	Documentos/Artefatos Referência
1	Há padrões de documentação para programas de sistema ERP que estão configurados para executar em modo *batch* ?		
2	Está sendo usado o padrão de documentação ?		
3	Há softwares de apoio à documentação do sistema ERP a ser auditado ?		
4	Existe trilha de auditoria do sistema ERP? (*logs*)		
5	Existem arquivos/relatórios/registros de controle no sistema ?		
6	As alterações de programas dos módulos do ERP, são controladas e registradas ?		
7	Existe grau de sigilo de arquivos e programas consoantes norma estabelecida ?		
8	Existe documentação referente ao sistema ERP, quanto a processos, manuntenções no sistema ?		
9	Existem procedimentos documentados descrevendo como os relatórios de saída são gerados e entregues aos usuários ? (acessos)		
10	Há monitoração via arquivos de *logs* enquanto ocorrem ciclos de processamento no sistema ?		
11	Há documentação de quem dá manutenção e suporte nas operações e funcionalidades do sistema ERP ?		

Fonte: (MAGALHAES; LUNKES; MULLER, 2001, p.146) adaptado.

No anexo G, é apresentado o artefato Levantamento do Ambiente de Sistema ERP em formato de questionário a ser aplicado, que pode ser utilizado para o levantamento destas

informações. Este formulário serve para que os auditores tenham uma noção do atual cenário do sistema ERP e para complementar as informações básicas levantadas nas entrevistas sobre o sistema.

Os resultados destas atividades servirão como base para a montagem do plano de auditoria, o relacionamento e o início da análise dos pontos de controle.

3.1.4 Criação do plano de auditoria

A partir das definições feitas nesta fase de Iniciação e Planejamento de Auditoria , é possível iniciar a elaboração do plano de auditoria.

O plano de auditoria é um artefato elaborado durante toda a auditoria e deve ser preenchido conforme o roteiro determina, sendo geralmente no fim de cada uma das fases. Seu principal objetivo é agregar informações e dados a respeito do programa de auditoria, de forma que seja simples de ser utilizado dentro de um programa de auditoria e para consultas de gestores interessados nas informações contidas. O plano de auditoria é composto basicamente pelos tópicos que aparecem na figura 16.

FIGURA 16 – Tópicos básicos de um plano de auditoria

Tópicos
Objetivos da auditoria;
Critérios de auditoria e qualquer documento de referência;
O escopo da auditoria;
Definição de funções e responsabilidades dos membros da equipe de auditoria e das áreas auditadas;
Pareceres do ambiente de sistema a ser verificado.
Os principais pontos do relatório de auditoria;
Quaisquer ações de acompanhamento de auditoria.

Fonte: ABNT (2002) adaptado.

Planos de auditoria são flexíveis, sendo modificados durante o processo de auditoria. Estas modificações podem ser a agregação de mais detalhes nos tópicos ou mudanças nos existentes. Imoniana (2005) destaca que a auditoria é um processo contínuo de avaliações de risco ao qual se adicionam experiências individuais dos profissionais e a evolução da prática e metodologias, com isso são inevitáveis que algumas mudanças mínimas acabem influenciando em pequenos ajustes no plano de auditoria.

O plano de auditoria também é importante no processo de comunicação interna durante um programa de auditoria, pois elenca diversos tópicos de comum interesse aos auditores, auditados e comissão de auditoria. Na norma da ABNT (2002) afirma-se que os

envolvidos devem estar cientes de tudo que está contemplado no plano de auditoria, sendo este válido oficialmente dentro do programa de auditoria somente após o conhecimento de todas as partes interessadas.

Com a criação do plano de auditoria, a fase atual pode ser dada como por encerrada. Algumas questões apenas são cabíveis, como pequenas revisões dos artefatos gerados, para um possível alinhamento com toda a equipe e para possíveis registros de considerações detectadas ou adequações para as próximas fases.

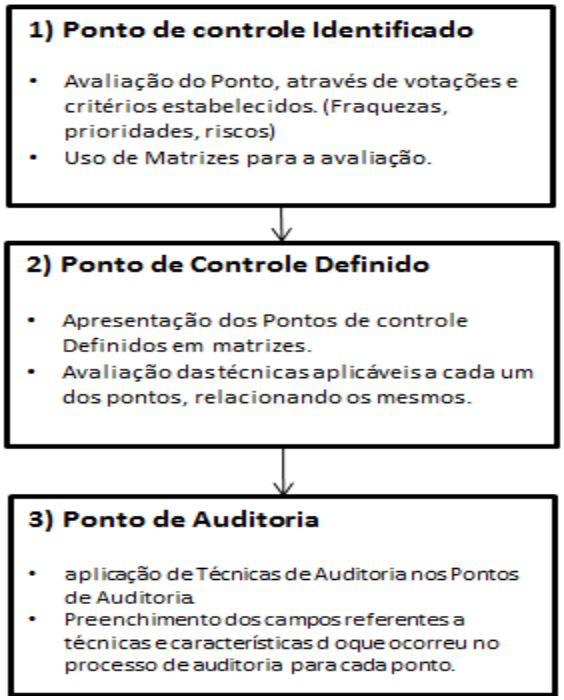
No anexo D é demonstrado um modelo de um plano de auditoria básico, que pode ser adaptado para auditorias de sistemas específicos.

3.2 FASE DA ANÁLISE E DEFINIÇÃO DOS PONTOS DE CONTROLE

Nesta fase, começam a ser trabalhados os pontos de controle do sistema. A fase está dividida em atividades que tem por objetivo tratar os pontos de controle, de modo que se tenham diversas etapas antes da definição de quais irão ser trabalhados, observando os objetivos estabelecidos no plano de auditoria, para as etapas de identificação e definição dos pontos de controle a serem utilizados no programa de auditoria.

Na figura 17 é apresentado o ciclo de definição de um Ponto de Controle, que ao fim se torna um Ponto de Auditoria e é utilizado como evidência de auditoria no processo.

FIGURA 17 – Ciclo de vida dos pontos de controle no roteiro



Fonte: Elaborado pelo autor.

Neste ciclo de vida dos Pontos de controle, são exercidas as atividades de análise e definição dos pontos. Durante estas análises e definições, são gerados alguns artefatos, onde a comissão de auditoria, auditores e demais envolvidos irão realizar os trabalhos de definições.

Os artefatos utilizados pela comissão e gestores envolvidos estão ligados às análises feitas durante as atividades exercidas sob o ambiente do sistema ERP na fase de Iniciação do Planejamento de Auditoria. Eles serão úteis na identificação de todos os pontos de controle e também auxiliarão na análise e definição de quais pontos serão utilizados durante as atividades de auditoria.

3.2.1 Organização, identificação e definição dos pontos de controle

Para tratar todo o ciclo de vida dos pontos de controle, Gil (1999) propõe a elaboração de uma série de matrizes para a avaliação conjunta da equipe envolvida no programa de auditoria. O planejamento destas matrizes pode contar com a presença de representantes das áreas de negócio, um representante da área de análise de sistemas, principais gestores e caso necessário um profissional de consultoria externa com qualificações em auditoria e sistemas.

Na figura 18, é apresentado recorte da atividade de organização, identificação e definição dos pontos de controle. Dentro desta atividade, existem artefatos de entrada que apresentam matrizes, onde serão tratados os pontos de controle envolvidos, dividido por etapas para sua seleção.

FIGURA 18 – A Atividade de organização, identificação e definição dos pontos de controle

Análise e Definição dos Pontos de Controle	Organização, Identificação e Definição de Pontos de Controle.	* Criação de arquivo que contém os pontos levantados cfe criterios estabelcidos. * Reuniões com a comissão * Análise de auditorias passadas e pontos considerados importantes.	Etapa 1 - Matriz de Ponto de Controle Identificado Etapa 2 - Matriz Ponto de Controle Identificado Etapa 3 - Matriz de Ponto de Controle Definido	* Modelo Matriz Pontos de Controle Identificados * Matriz Pontos de Controle Auditoria	*Equipe de Auditoria, Auditor Lider, Gestão*

Fonte: Elaborado pelo autor.

Esta atividade inicial da fase de análise e definição de pontos de controle contempla uma série de preenchimento de artefatos. Começa pela organização e identificação dos pontos, baseados no levantamento de informações e dados junto a gestores e usuários. Este artefato servirá para o registro do maior número de pontos de controle que a gestão e usuários chave entenderem serem importantes para o bom funcionamento do sistema ERP, já que todos podem ser passíveis de auditoria. Para que estas atividades ocorram, é necessária a formatação de um artefato que contenha as matrizes citadas por Gil (1999) e informações que complementem o artefato. O artefato inicial a ser utilizado será chamado Matriz Pontos de

Controle Identificados e será composto por pontos de controle, seus detalhes específicos e os riscos de cada ponto apontado pelos participantes da seleção, conforme anexo H.

O preenchimento do artefato Modelo Matriz Pontos de Controle Identificados ocorre durante reunião realizada entre a equipe de auditoria, gestores e principais usuários do sistema. Os gestores e usuários em conjunto com a equipe de auditoria preenchem o artefato de acordo com os pontos de controle existentes. Para cada um dos pontos de controle, os riscos são avaliados.

A avaliação de riscos será baseada nas etapas existentes na identificação de riscos, que são: identificação de pontos, identificação de ameaças, identificação de vulnerabilidades e identificação de consequências. As identificações de vulnerabilidades e consequências de risco estarão relacionados ao conhecimento de negócio que o gestor e usuários envolvidos apontarão como sendo razões para o ponto elencado, e constarão na coluna de riscos do artefato Modelo Matriz Pontos de Controle Identificados.

Após o artefato Modelo Matriz de Pontos de Controle Identificados estar preenchido, parte-se para a etapa de seleção de pontos de controle a serem trabalhados. O artefato que contempla estas informações é o de Matriz Pontos de Controle Definidos conforme anexo I. Este artefato conta basicamente com os pontos de controle a serem analisados pela comissão e gestores, os riscos já identificados e uma coluna para o grau de importância a ser preenchido.

As colunas de ponto de controle, descrição e riscos são as mesmas preenchidas devido à avaliação anterior. Na coluna de grau, os participantes das áreas irão considerar o grau de importância para o ponto de controle a ser avaliado. Gil (1999) define os valores conforme tabela 1, para caracterizar os pontos.

TABELA 1 – Valores para caracterizar os pontos

Grau	Conceito
1	Muito Fraco
2	Fraco
3	Regular
4	Forte
5	Muito Forte

Fonte: GIL (1999).

A lógica de avaliação segue a importância que representa para a empresa o ponto de controle registrado. É importante que seja avaliado com cautela e baseado nos objetivos definidos no plano de auditoria.

Os valores da coluna grau vão de 1 a 5 e representam a importância do ponto de controle, sendo 1 o grau mínimo de importância e 5 o grau máximo. O grau 5 indica um ponto

de controle considerado importante em relação as funcionalidades e atendimento ao negócio da empresa. Caso exista algum tipo de igualdade em pontos avaliados, os critérios de desempate partem da não conformidade reincidente ou da própria escolha pelos gestores envolvidos responsáveis. (GIL, 1999).

Através de reunião, o líder de equipe convoca gestores e usuários chave para o preenchimento individual do anexo e a definição dos pontos definidos.

Durante a avaliação individual, o participante avalia os campos já preenchidos. Nesta avaliação existe a atividade de análise de risco agregada, onde cada participante deve considerar o risco do ponto elencado no momento de avaliar os graus de cada um deles.

Após ter sido realizada a votação a partir do artefato Matriz Ponto de Controle Definidos, fica a critério da comissão ou dos auditores a formalização em um documento simples, sobre os pontos de controle selecionados para os trabalhos de auditoria.

Para o andamento das atividades de programa de auditoria ocorrer, quando finalizado o processo de escolha dos pontos, deve ser criado um novo artefato. Este novo artefato chamado Modelo de Matriz Pontos de Controle Auditoria, trata basicamente da listagem dos pontos de controle definidos anteriormente e será usado também na fase de preparação e execução de atividades. Neste documento o auditor líder irá delegar as responsabilidades para a equipe de auditoria interna. Ele conterá registros dos auditores responsáveis por cada ponto, uma coluna para serem citadas as técnicas a serem aplicadas nos pontos, características, referências pesquisadas, considerações sobre a aplicação das técnicas e descrição de sugestões de melhoria para cada evidência relatada no ponto. A figura 19 apresenta o recorte do artefato mencionado e explicado anteriormente. Ele também pode ser visto por completo através do anexo J.

FIGURA 19 – Pontos de auditoria a serem trabalhados

MATRIZ DE PONTOS DE CONTROLE AUDITORIA

Realize o preenchimento do artefato de acordo com as informações levantadas nas matrizes e demais artefatos de fases anteriores.

PONTOS DE CONTROLE AUDITADOS:

Ponto de Auditoria	Técnicas e Ferramentas	Descrição/ Características da Auditoria	Docs. Verificados	Responsável	Considerações a respeito	Recomendações	Não Conformidade	Conformidades	Evidências

Fonte: Elaborado pelo autor.

Para a seleção de técnicas a serem aplicadas nos pontos de controle definidos, o auditor pode consultar o documento de listagem de técnicas que será anexado junto ao roteiro

de auditoria. O anexo G traz um esboço da listagem de técnicas estudadas a partir dos referenciais teóricos do capítulo 2.

Portanto, nesta fase de Análise e Definição dos Pontos, serão preenchidos os campos de ponto de controle e responsáveis, deixando os demais para a próxima fase, que contará com as informações geradas após a aplicação das técnicas de auditoria aqui elencadas.

3.3 FASE DE PREPARAÇÃO E EXECUÇÃO DE ATIVIDADES

Nesta fase começa acontecer a auditoria propriamente dita com o exame dos pontos de controle definidos.

O artefato Modelo de Matriz Pontos de Controle Auditoria possui a listagem de pontos de controle definidos. Este documento deve vir com alguns campos preenchidos pela equipe de auditoria, como por exemplo, os próprios pontos de controle, as técnicas de auditoria e o responsável por cada ponto.

O ponto de controle passa a ser chamado de ponto de auditoria. É na atual fase que serão aplicadas as principais técnicas de auditoria elencadas na fase anterior, para o levantamento de evidências e não conformidades de auditoria. O auditor pode complementar com mais técnicas caso seja necessário, e após isso, inicia as execuções. Dependendo das técnicas utilizadas, pode ser gerado um grande número de dados e informações, havendo a necessidade do auditor filtrar esses resultados e compilá-los para posterior registro no artefato Modelo Matriz dos Pontos de Auditoria.

Os dados e informações resultantes da aplicação das técnicas devem ser utilizados para o preenchimento dos demais campos do documento Modelo Matriz Ponto de Controle Auditoria conforme ele está apresentado no anexo F.

A partir da próxima fase e com o Modelo de Matriz Ponto de Controle Auditoria preenchido é que começarão a serem formalizados os relatórios e demais artefatos onde constam parte das informações coletadas nesta fase e nas demais. A partir do trabalho de compilação e preparação dos dados gerados anteriormente, os auditores devem procurar distribuir essas informações nos artefatos finais que serão apresentados aos envolvidos na auditoria, principalmente a alta gestão.

3.4 FASE DE CONCLUSÃO E RESULTADOS DE AUDITORIA

A fase de conclusão de uma auditoria de sistemas é marcada pela compilação de todas as outras fases anteriores. Para compilar as principais informações é importante que a

equipe de auditoria interna tenha registrado a maior quantidade possível de informações a respeito dos trabalhos exercidos ao longo da auditoria. Estas informações, que serão encontradas a partir de artefatos gerados em cada fase, serão consultados para a montagem dos relatórios finais.

Imoniana (2005) cita que antes de emitir relatórios finais, é imprescindível solicitar a compreensão ou não dos auditados para dirimir as dúvidas que porventura tenham persistido durante o processo de auditoria. Os artefatos usados neste momento são a carta-comentário e o rascunho preliminar do relatório final de auditoria. A ABNT (2006) apresenta a etapa de comunicação de risco, que no âmbito da auditoria pode ser associada a comunicação de evidências de auditoria. O objetivo é semelhante, fazer com que as partes envolvidas no processo de auditoria tenham conhecimento do que foi abordado e evidenciado ao longo dos trabalhos.

Para a pré-formalização do fechamento do programa de auditoria por parte dos auditores, pode ser utilizada a carta comentário. Ela é um artefato sucessor ao rascunho preliminar de auditoria, o qual estes apenas dependem da aprovação por parte dos destinatários, que podem ser os gestores responsáveis pelas áreas envolvidas.

Para que a carta-comentário contenha uma base de informações consistente, a equipe de auditoria elabora o artefato chamado Rascunho Preliminar do Relatório de Auditoria. Este artefato, mostrado no anexo J, é um arquivo gerado e preenchido pela equipe de auditores com base na avaliação de artefatos gerados em outras fases do roteiro, principalmente dos resultados dos pontos de auditoria, e que será enviado em anexo à carta-comentário, onde constarão os tópicos que seguem:

a) objetivo do controle;
b) considerações no ponto;
c) descrição dos procedimentos executados;
d) resultados;
e) não conformidades e evidências achadas;
f) recomendações;
g) aval dos responsáveis internos.

Dentro destes tópicos, o destinatário, que provavelmente será algum responsável pelo acompanhamento de auditoria ou um gestor, terá apenas de preencher o último tópico.

Com a aprovação deste rascunho de relatório e o conhecimento de todas as partes interessadas, a próxima atividade é a criação do relatório final. Este relatório final é de responsabilidade do Líder da Equipe de Auditoria. Além de informações contidas no rascunho

inicial, devem ser citados outros elementos que compõe o processo de auditoria, são eles:

a) relação de normas, instruções, procedimentos e outros documentos utilizados como base (referência) para as avaliações;
b) relação dos membros de equipe de auditoria;
c) nomes de quaisquer outros observadores, participantes e de pessoas que foram contatadas em qualquer fase da auditoria;
d) constatações finais, dando ênfase para deficiências detectadas. Devem ser fornecidos detalhes suficientes para permitirem avaliação, ação corretiva e providências complementares pela organização/setor auditado.

O relatório pode ser distribuído aos gestores e responsáveis no momento da comunicação de encerramento do programa de auditoria, para que tenham o conhecimento dos resultados e pareceres finais extraídos do programa implantado.

Conforme citado na norma da ABNT (2002), as ações corretivas, preventivas ou de melhoria, que podem ser aplicáveis ao fim da apresentação dos resultados fica a critério do auditado e não são consideradas como parte da auditoria. A norma também enfatiza que para a verificação das ações, pode ser criado outro programa de auditoria, para que sejam verificadas as ações tomadas e a sua eficácia.

3.5 CONSIDERAÇÕES FINAIS DO ROTEIRO PARA AUDITORIA DE SISTEMAS

Neste capítulo foi apresentado o roteiro para elaboração de auditoria em sistemas ERP, baseado nos estudos realizados no capítulo 2.

No roteiro proposto foram apresentadas as fases, suas principais atividades, os responsáveis pela realização delas, os artefatos que devem ser utilizados como referência e, além disso, os artefatos gerados por cada atividade executada.

A utilização do roteiro pode ser feita por profissionais encarregados de implantar auditoria em ambientes internos de organizações. Este roteiro pode ser alterado quando necessário, sendo acrescidas mais regras para verificações, atividades e artefatos. Estes critérios de mudança ficam sob a responsabilidade da comissão ou equipe interna responsável pela elaboração de auditoria interna.

O roteiro criado neste capítulo será adaptado a uma ferramenta, em que sua estrutura possa ser bem distribuída. Isso servirá para uma posterior aplicação do roteiro na criação de um programa de auditoria de modo que fique bem dividido e com uma usabilidade melhor do que o esboçado inicialmente.

4 APLICAÇÃO DO ROTEIRO DE AUDITORIA EM ERP

Com o propósito de avaliar o roteiro proposto para a elaboração de auditorias em ERP, será realizado um estudo de caso. Este estudo de caso ocorreu em uma empresa do ramo de administração de consórcios no sistema ERP da mesma.

4.1 CONTEXTO DO ESTUDO DE CASO

A aplicação da auditoria aconteceu no principal sistema da empresa de administração de consórcios e chama-se Genesis. Este software trata-se de um sistema ERP que tem o objetivo de atender todo o processo de negócio administrado pela empresa. Atualmente o sistema conta com os seguintes módulos: comercial, adesão, financeiro, assembleia, jurídico, análise de crédito, cobrança, central de atendimento e contábil.

O Genesis é um software ERP desenvolvido em linguagem *WEB* por uma empresa terceirizada. Esta empresa realiza atendimentos na verificação de problemas, na análise e desenvolvimento de melhorias, nas adequações a procedimentos legais e no auxílio em integrações do software com outras aplicações.

Atualmente o software pode ser acessado por meio da intranet da empresa, porém também oferece algumas funcionalidades que podem ser acessadas fora da rede interna da empresa.

4.2 O ROTEIRO IMPLEMENTADO

A ferramenta utilizada para a sua implementação foi o Microsoft Sharepoint na versão 2007. Ela apresenta diversas funcionalidades que podem ser adaptadas a realidade do roteiro proposto, além da facilidade de manipulação e compreensão de sua estrutura.

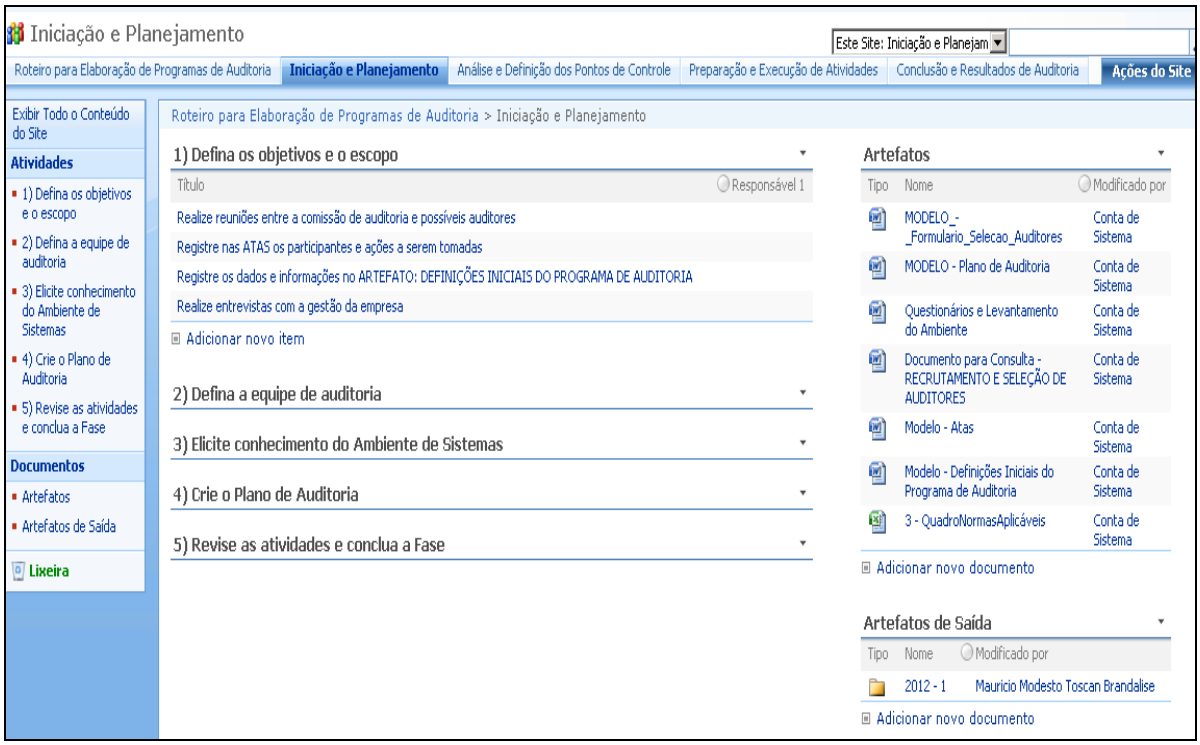
Atualmente a empresa utiliza esta ferramenta para a centralização de algumas informações e dados referentes aos mais diversos sistemas, inclusive para gestão de demandas de software, gestão de pequenos projetos, gestão de atividades e gestão de arquivos.

Por incluir funcionalidades que se caracterizam por atender ao que o roteiro procura propor, entendeu-se que o Microsoft Sharepoint poderia ser a estrutura ideal para a implementação do roteiro

O roteiro foi estruturado na ferramenta seguindo a proposta. Ele exibe as fases, atividades, artefatos de entrada e saída e responsáveis para fazerem a sua adaptação e

distribuição de atividades, conforme mostrado na figura 20. As fases estão definidas em abas, as quais se localizam na parte superior do roteiro. No centro da tela são exibidas as atividades da fase selecionada. Ao lado de cada atividade é exibido o responsável. No lado esquerdo da tela aparecem as atividades organizadas em ordem. No lado direito da tela aparecem os artefatos de entrada com os documentos logo abaixo, assim como na parte inferior onde aparecem os artefatos de saída.

FIGURA 20 – O roteiro adaptado na Ferramenta Microsoft Sharepoint



Fonte: Elaborado pelo autor.

Ao selecionar uma atividade, são exibidos os modelos dos artefatos de entrada e saída correspondente.

Se a auditoria em questão já iniciou, os artefatos podem ser acessados através dos diretórios apresentados, conforme distribuídos em suas pastas na ferramenta. Nesta consulta aos diretórios os auditores podem fazer as buscas por artefatos já preenchidos e obter informações de quais atividades já estão concluídas.

O roteiro adaptado na ferramenta obedece a mesma lógica de distribuição apresentada na planilha onde foi construída a versão inicial do roteiro.

Para um melhor entendimento por parte da comissão que irá utilizar o guia apresentado, foi desenvolvido um pequeno documento de ajuda, que pode ser acessado através da página inicial do roteiro. Este documento contém as principais informações a respeito do roteiro e do que ele é composto.

4.3 O ESTUDO DE CASO

Antes de ser realizada a criação do programa de auditoria, foi necessária a definição de uma comissão interna de auditoria, que pudesse conduzir a criação e organização do programa no período. A comissão foi definida pela gerência, partindo do princípio que este programa de auditoria estaria ligado a determinadas áreas, e de que envolvia importantes questões do sistema ERP. A área de TI contou com 3 participantes, sendo dois analistas de negócio e um gerente de projetos, responsáveis pela manutenção e suporte dos sistemas internos. Para representar as demais áreas administrativas, foi sugerido o coordenador administrativo e estratégico da empresa e um analista de sistemas da qualidade.

As atividades realizadas para a elaboração do programa de auditoria interna em sistema ERP aconteceram no período de junho e serão apresentadas conforme segue a distribuição de fases no roteiro.

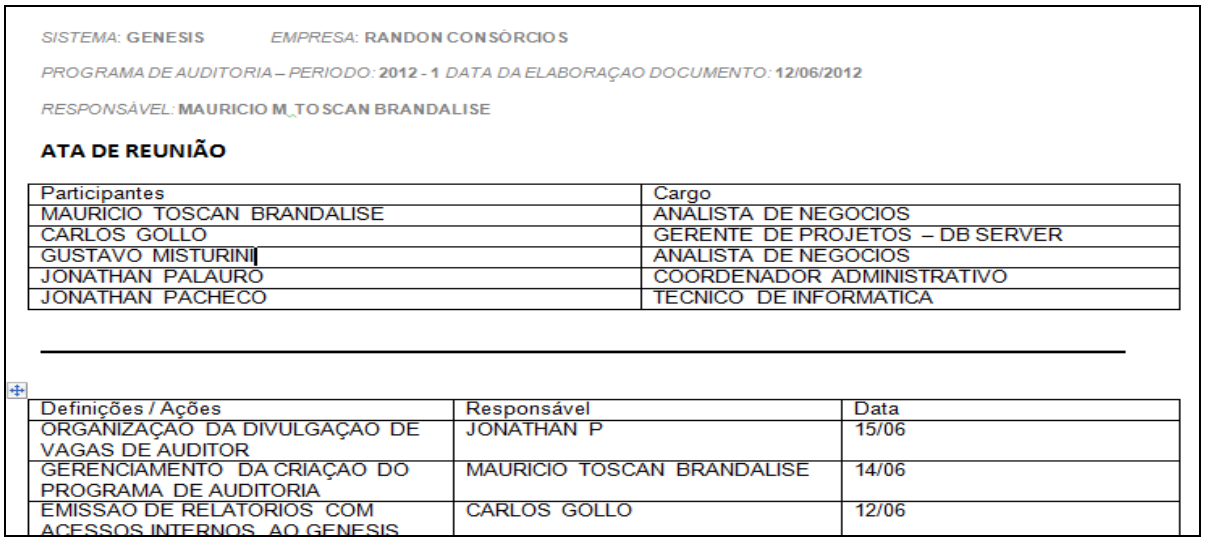
4.3.1 Fase de Iniciação do Planejamento de auditoria

O início desta fase foi marcado por importantes definições da criação do programa de auditoria. Como a comissão de auditoria já estava definida, foram realizadas reuniões de abertura para o início das atividades. Os participantes envolvidos na reunião expuseram os atuais problemas encontrados de forma que ficasse claro para a comissão que tipos de objetivos e escopo a auditoria poderia contemplar.

Por se tratar do software que contempla a maior parte dos processos e funcionalidades de negócio da empresa e também por ser um ERP, o software a ser auditado foi o Genesis. Sua escolha foi feita pela maioria e os principais fatores para isso foram a sua atual número de transações, alto número de customizações e adequações e algumas funcionalidades instáveis.

Na figura 21, é exibida a ata conforme modelo de artefato. Nela são apresentados os participantes da reunião em que foi realizado o preenchimento do documento inicial de definições do programa de auditoria e algumas ações a serem tomadas para o andamento das atividades.

FIGURA 21 – Ata inicial do programa de auditoria



SISTEMA: **GENESIS** *EMPRESA:* **RANDON CONSÓRCIOS**

PROGRAMA DE AUDITORIA – PERIODO: **2012 - 1** *DATA DA ELABORAÇAO DOCUMENTO:* **12/06/2012**

RESPONSÁVEL: **MAURICIO M_TOSCAN BRANDALISE**

ATA DE REUNIÃO

Participantes	Cargo
MAURICIO TOSCAN BRANDALISE	ANALISTA DE NEGOCIOS
CARLOS GOLLO	GERENTE DE PROJETOS – DB SERVER
GUSTAVO MISTURINI	ANALISTA DE NEGOCIOS
JONATHAN PALAURO	COORDENADOR ADMINISTRATIVO
JONATHAN PACHECO	TECNICO DE INFORMATICA

Definições / Ações	Responsável	Data
ORGANIZAÇAO DA DIVULGAÇAO DE VAGAS DE AUDITOR	JONATHAN P	15/06
GERENCIAMENTO DA CRIAÇAO DO PROGRAMA DE AUDITORIA	MAURICIO TOSCAN BRANDALISE	14/06
EMISSAO DE RELATORIOS COM ACESSOS INTERNOS AO GENESIS	CARLOS GOLLO	12/06

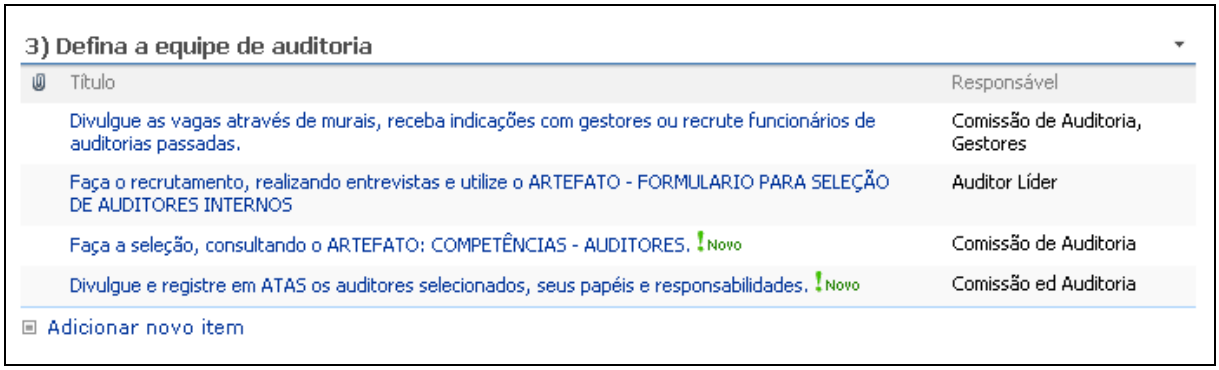
Fonte: Elaborado pelo autor.

Os objetivos da auditoria serão manutenabilidade e integridade do sistema ERP atual. Os objetivos da auditoria foram discutidos na mesma reunião do dia. Cada um dos presentes pôde através dos fatores expostos pela gestão, discutir quais seriam os objetivos que melhor se identificavam com o que o fora apresentado a todos.

Nesta primeira reunião, também foi definido o tipo de escopo de auditoria. O indicado foi o parcial, devido a limitar-se apenas a algumas funcionalidades do sistema que apresentam um grande impacto para a empresa e seus processos de negócio.

Após estarem estabelecidos os objetivos e o escopo de auditoria, a comissão de auditoria começou a focar suas atenções nas próximas atividades. De acordo com o roteiro, a próxima atividade que constava era a criação da equipe de auditoria interna. Para isso, foram necessárias algumas reuniões a fim de definir ações para o recrutamento e seleção de pessoas. Na figura 22, é apresentada a atividade de definir equipe de auditoria e como ela pode de ser conduzida.

FIGURA 22 – Atividade de definir equipe



3) Defina a equipe de auditoria

Título	Responsável
Divulgue as vagas através de murais, receba indicações com gestores ou recrute funcionários de auditorias passadas.	Comissão de Auditoria, Gestores
Faça o recrutamento, realizando entrevistas e utilize o ARTEFATO - FORMULARIO PARA SELEÇÃO DE AUDITORES INTERNOS	Auditor Líder
Faça a seleção, consultando o ARTEFATO: COMPETÊNCIAS - AUDITORES. ! Novo	Comissão de Auditoria
Divulgue e registre em ATAS os auditores selecionados, seus papéis e responsabilidades. ! Novo	Comissão ed Auditoria

Adicionar novo item

Fonte: Elaborado pelo autor.

A definição da equipe de auditoria foi conduzida de acordo com o elencado no roteiro, mas agregando uma forma interessante de divulgação inicial das vagas para seleção. Foram enviados *e-mail*s direcionados a coordenadores explicando do que se tratava o programa e qual o tipo de perfil esperado para a seleção dos auditores internos. Salientou-se que o sucesso do programa dependeria do modo com o qual as ideias seriam compartilhadas com os funcionários.

As definições de papéis e atividades a serem exercidas no âmbito da auditoria, seguiram de acordo como é apresentado no documento de relação de atividades de auditores líderes, auditores plenos e demais ocupações que serão elencados sempre em atas.

As vagas oferecidas não atraíram muitos candidatos, mas para a seleção já era o suficiente no andamento do programa de auditoria. Com os candidatos relacionados, foram feitas as primeiras entrevistas de acordo como estabelecia o roteiro. O preenchimento dos documentos de seleção de candidatos ocorreu de acordo como o previsto. Na figura 23 é apresentado parte do documento de avaliação do candidato.

FIGURA 23 – Parte do formulário para seleção de candidatos preenchido

SISTEMA: GENESIS *EMPRESA:* RANDON CONSORCIOS

PROGRAMA DE AUDITORIA – PERIODO: 2012 - 1 *DATA DA ELABORAÇAO DOCUMENTO:* 11/06/2012

RESPONSAVEL: MAURICIO M. TOSCAN BRANDALISE

Formulário para Seleção de Auditores Internos

Nome do candidato: GABRIELA RICARDO DOS REIS

Setor: QUALIDADE

Cargo pretendido:

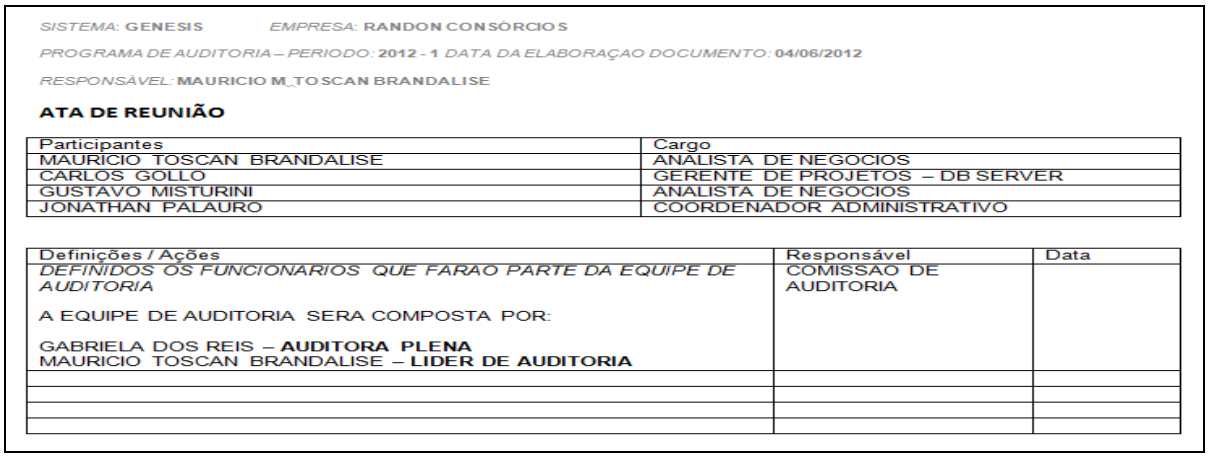
X	Auditor Líder
X	Auditor Pleno
	Auditor Trainee

Fonte: Elaborado pelo autor.

Após entrevistas junto a possíveis candidatos, é feita a seleção perante os resultados objetivos de cada envolvido.

A escolha dos candidatos ocorreu de forma simples. O candidato que apresentava a maior média nos graus em relação a concorrentes para o mesmo cargo, assumia a função desejada. O perfil e comportamento da pessoa na entrevista também contribuíam para a seleção. A divulgação interna ocorreu através de *e-mail*s para os candidatos que conseguiram atingir o nível adequado para exercer a função no programa de auditoria. Além dessa divulgação, o registro em ata, como e mostrado na figura 24, para manter histórico e divulgar para o publico maior.

FIGURA 24 – Ata divulgação de auditores internos definidos



SISTEMA: **GENESIS** *EMPRESA:* **RANDON CONSÓRCIOS**

PROGRAMA DE AUDITORIA – PERIODO: **2012 - 1** *DATA DA ELABORAÇAO DOCUMENTO:* **04/06/2012**

RESPONSÁVEL: **MAURICIO M_TOSCAN BRANDALISE**

ATA DE REUNIÃO

Participantes	Cargo
MAURICIO TOSCAN BRANDALISE	ANALISTA DE NEGOCIOS
CARLOS GOLLO	GERENTE DE PROJETOS – DB SERVER
GUSTAVO MISTURINI	ANALISTA DE NEGOCIOS
JONATHAN PALAURO	COORDENADOR ADMINISTRATIVO

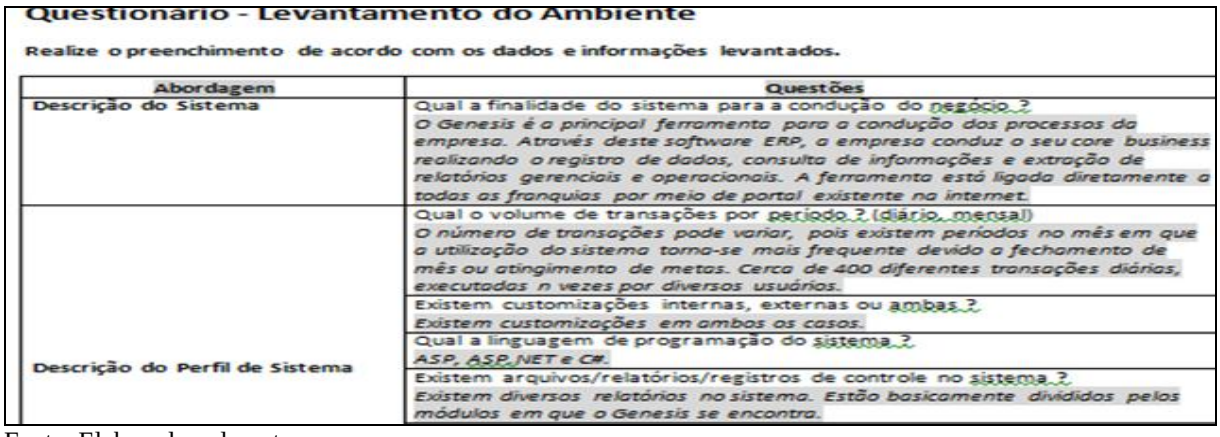
Definições / Ações	Responsável	Data
DEFINIDOS OS FUNCIONARIOS QUE FARAO PARTE DA EQUIPE DE AUDITORIA A EQUIPE DE AUDITORIA SERA COMPOSTA POR: GABRIELA DOS REIS – **AUDITORA PLENA** MAURICIO TOSCAN BRANDALISE – **LIDER DE AUDITORIA**	COMISSAO DE AUDITORIA	

Fonte: Elaborado pelo autor.

Na sequência da aplicação do roteiro de auditoria, a atividade de elicitar conhecimento do ambiente de sistemas foi conduzida pelo auditor líder, como é sugerido e mostrado no roteiro.

Esta atividade foi realizada junto à área gerencial da empresa, às áreas de negócio e à área de TI. O questionário de Levantamento do Ambiente foi um artefato simples de ser utilizado. Parte de seu preenchimento ocorreu através de pequenas reuniões informais com usuários das áreas citadas. As principais contribuições partiram das áreas gerenciais e da área de TI, que detinham o conhecimento dos processos e sua importância e do conhecimento técnico essencial para o entendimento do ambiente. Na figura 25 é apresentado o recorte do questionário aplicado nas áreas.

FIGURA 25 – Recorte do artefato levantamento do ambiente



Questionario - Levantamento do Ambiente

Realize o preenchimento de acordo com os dados e informações levantados.

Abordagem	Questões
Descrição do Sistema	Qual a finalidade do sistema para a condução do negócio ? *O Genesis é o principal ferramenta para a condução dos processos da empresa. Através deste software ERP, a empresa conduz o seu core business realizando o registro de dados, consulta de informações e extração de relatórios gerenciais e operacionais. A ferramenta está ligada diretamente a todas as franquias por meio de portal existente na internet.*
Descrição do Perfil de Sistema	Qual o volume de transações por periodo ? (diário, mensal) *O número de transações pode variar, pois existem periodos no mês em que a utilização do sistema torna-se mais frequente devido a fechamento de mês ou atingimento de metas. Cerca de 400 diferentes transações diárias, executadas n vezes por diversos usuários.*
	Existem customizações internas, externas ou ambas ? *Existem customizações em ambos os casos.*
	Qual a linguagem de programação do sistema ? *ASP, ASP.NET e C#.*
	Existem arquivos/relatórios/registros de controle no sistema ? *Existem diversos relatórios no sistema. Estão basicamente divididos pelos módulos em que o Genesis se encontra.*

Fonte: Elaborado pelo autor.

Os dados e informações referentes ao questionário aplicado junto às áreas citadas podem ser vistos por completo no anexo M. Este documento auxiliou no avanço para a próxima etapa de criação do plano de auditoria, visto o tipo de questões que possuía.

A criação do plano de auditoria depende do conhecimento e finalização de todas as atividades anteriores. Este artefato foi preenchido pelo auditor líder e distribuído à equipe de auditoria e comissão de auditoria para conhecimento. É importante lembrar que, neste momento, só são preenchidos os itens: Objetivos de auditoria, escopo de auditoria, datas e locais e sobre as funções da equipe no programa de auditoria.

A revisão é a última atividade da fase. Nesta revisão foram analisadas as atividades junto à equipe de auditoria e registrado em ata, as ações pendentes de solução. Na figura 26 é apresentado o recorte do artefato em que foram registradas as ações que estavam pendentes.

Estas definições ou ações definidas, foram importantes para que durante a realização da auditoria, não houvesse a falta de dados ou informações para o andamento da mesma. As ações ocorreram dentro do previsto e foram satisfatórias.

FIGURA 26 – Registros da atividade de revisão da primeira fase

ATA DE REUNIÃO : REUNIÃO DE ENCERRAMENTO DA FASE 1

Participantes	Cargo
JONATHAN PALAURO	COORDENADOR ADM
MAURICIO TOSCAN BRANDALISE	LIDER DE AUDITORIA
GABRIELA REIS	AUDITOR PLENO

Definições / Ações	Responsável	Data Solução
SOLICITAR APOIO A GESTORES PARA O ANDAMENTO EFETIVO DO PROGRAMA DE AUDITORIA	JONATHAN PALAURO	08/06
BUSCAR INFORMAÇOES A RESPEITO DE HORÁRIOS PARA AGENDAMENTO DE REUNIÕES	GABRIELA REIS	08/06
COMPLEMENTAR ARQUIVO DE ELICITAÇÃO DE INFORMAÇÕES SOBRE O SISTEMA ERP JUNTO AO FORNECEDOR	MAURICIO M TOSCAN BRANDALISE	09/06

Fonte: Elaborado pelo autor.

Finalizadas as ações mencionadas na figura anterior, as atividades da fase 1, iniciação e planejamento de auditoria deram-se por concluídas. Assim iniciamos a próxima fase, conforme descrito na sequência pelo roteiro.

4.3.2 Fase de análise e definição dos pontos de controle

O início desta fase foi marcado por uma reunião com os principais envolvidos na criação do programa de auditoria. Estiveram presentes o líder de auditoria e sua equipe, parte

da comissão de auditoria e gestores das áreas administrativa e de TI, convocados pela comissão interna. Esta atividade foi marcada pela citação a todos os presentes de que, a escolha dos pontos de controle deveria obedecer aos objetivos centrais do programa de auditoria corrente: atender a manutenabilidade e a privacidade.

Após estar claro como iria ser o andamento desta atividade, a reunião tratou de discutir em conjunto, quais pontos de controle deveriam ser elencados. A identificação dos pontos de controle foi registrado no artefato Matriz Pontos de Controle, conforme anexo N.

Durante o preenchimento do artefato, houve a discussão em relação aos riscos que cada um poderia apresentar. Para o preenchimento da coluna de riscos, o conteúdo foi baseado conforme as etapas de identificação de risco citadas no capítulo 3. Os pontos de controle levantados podem ser vistos na tabela 2.

TABELA 2 – Pontos de controle e riscos identificados

ID	Ponto de Controle	Riscos
1	Funcionalidades do Módulo de Gestão de Franquias	A empresa pode estar correndo o risco na prospecção de clientes, no planejamento estratégico para melhorias das unidades, no comissionamento de funcionários, etc.
2	Função geração de boletos automáticos	Possíveis riscos financeiros. Faz-se necessária a verificação da padronização da liberação de versões do *software*, detalhando ao máximo o que contempla cada uma.
3	Funcionalidade de integração financeira e contábil com outras ferramentas internas e externas	Atualmente a empresa apresenta problemas nas funcionalidades de integração do ERP.
4	Funcionalidades em tela de pagamentos	Necessidade de reavaliação na tela de pagamentos. Ocorrem erros na realização da efetivação de pagamentos e isso pode estar relacionado ao alto número de registro vinculado.

Fonte: Elaborado pelo autor.

Durante a reunião de levantamento dos pontos, a gestão apresentou um documento que entenderam ser relevante na análise e pode ser visto no anexo O. Ele trata de demandas levantadas periodicamente por um grupo de usuários interno da empresa e que serve como verificação de possíveis melhorias e ajustes no sistema ERP.

Os demais materiais verificados pela equipe de auditoria foram anexados junto aos artefatos desenvolvidos e mantidos nas pastas de artefatos de saída no roteiro, conforme figura 27.

FIGURA 27 – Os artefatos de saída a atividade de levantamento e organização dos pontos de controle

Fonte: Elaborado pelo autor.

Com os pontos candidatos a controle identificados e organizados, o auditor líder pode dar o segmento nas atividades para a avaliação definição dos mesmos.

Para definir os pontos de controle, todos os candidatos avaliaram. Cada participante avaliador votou nos pontos, atribuindo graus de 1 a 5, conforme está demonstrado na figura 28.

FIGURA 28 – Artefato preenchido sob o ponto de vista do usuário

SISTEMA: GENESIS *EMPRESA:* RANDON CONSORCIOS

PROGRAMA DE AUDITORIA – PERIODO: 2012 - 1 *DATA DA ELABORAÇAO DOCUMENTO:* 11/06/2012

RESPONSAVEL: MAURICIO M. TOSCAN BRANDALISE

Matriz de Pontos de Controle DEFINIDOS – Etapa 2

NOME AVALIADOR: MAURICIO M TOSCAN BRANDALISE
CARGO: ANALISTA DE NEGOCIOS

Valores para votação (Grau-Conceito):

5- Muito Forte	4-Forte	3-Regular	2-Fraco	1-Muito Fraco

- Realize o preenchimento da tabela de acordo com os graus acima.

Matriz do Ponto de Controle

ID	Ponto de Controle	Detalhes	Riscos	Grau
1	Funcionalidades do Módulo de Gestão de Franquias	Franquias e unidades vêm relatando algumas dificuldades em relação a utilização do módulo externo do ERP em relação a geração de relatórios homologados e em produção. Os relatórios, algumas vezes apresentam diferenciações na contabilização de determinados dados e na exibição de informações. A gestão acredita que este seja um ponto passível de ser auditado, com o objetivo de verificar a integridade dos dados e informações.	A empresa pode estar correndo o risco na prospecção de clientes, no planejamento estratégico para a melhorias das unidades, no comissionamento de funcionários, etc.	4
2	Função geração de boletos automáticos	Atualmente a funcionalidade de geração de boletos automáticos necessita de uma revisão. Existem estatísticas em relatórios, que segundo os usuários apontam o não recebimento via e-mail do boleto automático conforme solicitação do cliente. O sistema apresenta-se parametrizado e o processo de geração corretos.	Possíveis riscos financeiros. Faz-se necessária a verificação da padronização da liberação de versões do software, detalhando ao máximo o que contempla cada uma.	5
3	Ajuste de integração financeira e contábil com outras ferramentas internas e externas	Atualmente a empresa apresenta problemas nas funcionalidades de integração do ERP.	Possíveis riscos financeiros. É necessária a intervenção neste ponto, pois as ameaças e vulnerabilidades existem.	3

Fonte: Elaborado pelo autor.

Nesta atividade de definição dos pontos, o objetivo foi priorizar os pontos de controle que atendiam aos objetivos e que apresentavam maior risco.

A priorização dos ponto de controle seguiu de acordo com o grau avaliado. A atividade de consolidar os valores, foi realizada pela própria equipe de auditoria interna e divulgada apenas para a comissão de auditoria e gestores. A priorização dos pontos ficou organizada conforme tabela 3.

TABELA 3 – Pontos de controle priorizados

ID	Descrição do Ponto de Controle	GRAU
1	Funcionalidades em tela de pagamentos	9
2	Função geração de boletos automáticos	8
3	Funcionalidade de integração financeira e contábil com outras ferramentas internas e externas	8
4	Funcionalidades do Módulo de Gestão de Franquias	7

Fonte: Elaborado pelo autor.

Os pontos de controle priorizados foram organizados num terceiro artefato chamado Matriz Pontos de Controle de Auditoria que será utilizado na execução da auditoria, propriamente dita. Parte deste artefato pode ser visto na tabela 4. O artefato ficou encaminhado para o preenchimento das demais colunas, como as técnicas e ferramentas a serem utilizadas. Neste momento, são definidos, além dos pontos de controle, as técnicas e ferramentas a serem utilizadas. Para auxílio no preenchimento, ocorreram verificações no artefato Consulta de Técnicas, apresentado no anexo G e disposto no roteiro.

TABELA 4 – Tabela de pontos de auditoria, técnicas e ferramentas

Ponto de Auditoria	Técnicas e Ferramentas
Ajustes em tela de pagamentos	- Entrevistas com usuários das áreas relacionadas - *Test* data - Análise do Programa Fonte - Análise de Relatórios e Telas
Função geração de boletos automáticos	- Entrevistas com usuários das áreas relacionadas - *Test* data - Análise do Programa Fonte
Ajuste de integração financeira e contábil com outras ferramentas internas e externas	- Entrevistas com usuários das áreas relacionadas - Utilização da ferramenta Oracle para a verificação na base de dados de alguns dados. - Análise de Relatórios e Telas
Funcionalidades do Módulo de Gestão de Franquias	- Entrevistas com usuários das áreas relacionadas. - Análise de Relatórios e Telas - Análise do Programa Fonte

Fonte: Elaborado pelo autor.

O artefato de Matriz Pontos de Controle Auditoria foi utilizado brevemente nesta fase. Somente a partir das execuções de atividades de auditoria que o mesmo foi completado com as demais informações e dados referentes aos pontos de controle, o que ocorreu na Fase de Preparação e Execução de atividades.

A complementação do plano de auditoria foi realizada pelo auditor líder. Neste preechimento houveram considerações e a inserção de informações levantadas até então, sobre os pontos de controle e as áreas auditadas, conforme anexo P.

A última ação a ser realizada foi a de revisão das atividades, que serviu para avaliar todas as ações delegadas dentro do programa de auditoria. A equipe de auditoria pôde discutir, em reunião, as dificuldades em relacionar os pontos de controle e as técnicas devido a base de conhecimento que alguns dos participantes não detinham sobre algumas partes do sistema, logo não conseguia fazer a relaçao com possíveis técnicas apresentadas.

4.3.3 Fase de preparação e execução das atividades

Como citado no roteiro, esta é a fase em que ocorrem as atividades de auditoria nos pontos de controle elencados.

A utilização do roteiro e o artefato de Matriz Pontos de Controle Auditoria, serviram para que os auditores partissem a execução das atividades de auditoria, fazendo o uso de demais artefatos e técnicas elencadas.

Durante a aplicação da auditoria, o uso do roteiro para consultas a informações elencadas em outras fases, auxiliona avaliação dos pontos de controle e no cruzamento de alguns dados e informações. O roteiro contribuiu para a troca de experiências entre auditores que estavam trabalhando em diferentes pontos de controle, mas que podiam ter análises parecidas e aplicação de técnicas semelhantes.

As dificuldades começaram a surgir no momento da aplicação das técnicas, onde um dos auditores não detinha o conhecimento necessário para aplicação. O auditor líder pôde auxiliar neste caso com o conhecimento que detinha sobre a técnica e auxiliando na verificação do ponto.

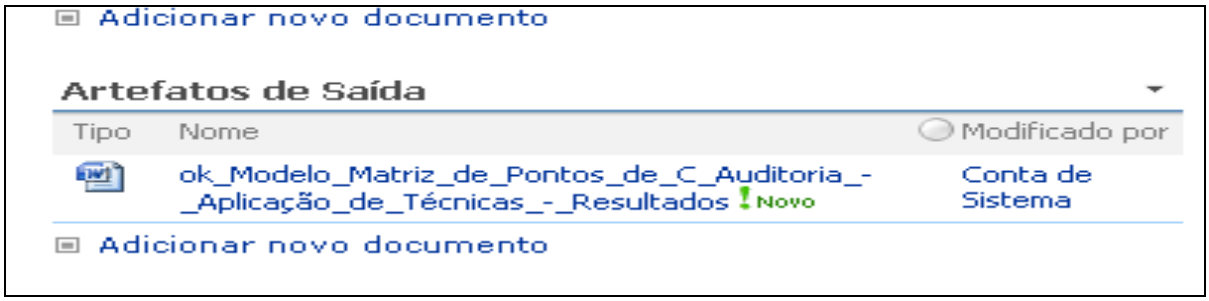
A maioria dos campos foi preenchida de forma padrão, pois o auditor líder era quem revisava o preenchimento do documento feito pela equipe e complementava com importantes observações dependendo do campo.

Com a execução da auditoria realizada, foi possível obter conteúdo necessário para que os auditores dessem suas recomendações, apontassem quais documentos verificados,

quais evidências levantadas, se o ponto estava conforme ou não e as observações em geral do trabalho executado.

O artefato preenchido e finalizado, encontra-se no anexo Q. Após sua finalização, o mesmo foi disponibilizado na área de artefatos de saída, como mostra a figura 29.

FIGURA 29 – Modelo matriz pontos de controle auditoria



Fonte: Elaborado pelo autor.

Com o trabalho de auditoria quase finalizado, a atividade de revisão foi necessária para que fosse validadas as informações e dados levantados pela equipe de auditoria. Esta revisão serviu para que o auditor líder pudesse em conjunto da equipe, analisar o status de cada ponto de auditoria e as considerações realizadas pelos auditores, a fim de estabelecer uma padronização no documento.

Os registros não aconteceram em ata nesta ocasião. Ocorreram somente mudanças realizadas pelo auditor líder no artefato de Matriz pontos de controle auditoria, com o propósito de deixar o documento o mais claro possível para a realização das atividades da fase seguinte.

4.3.4 Fase de conclusão de resultados de auditoria

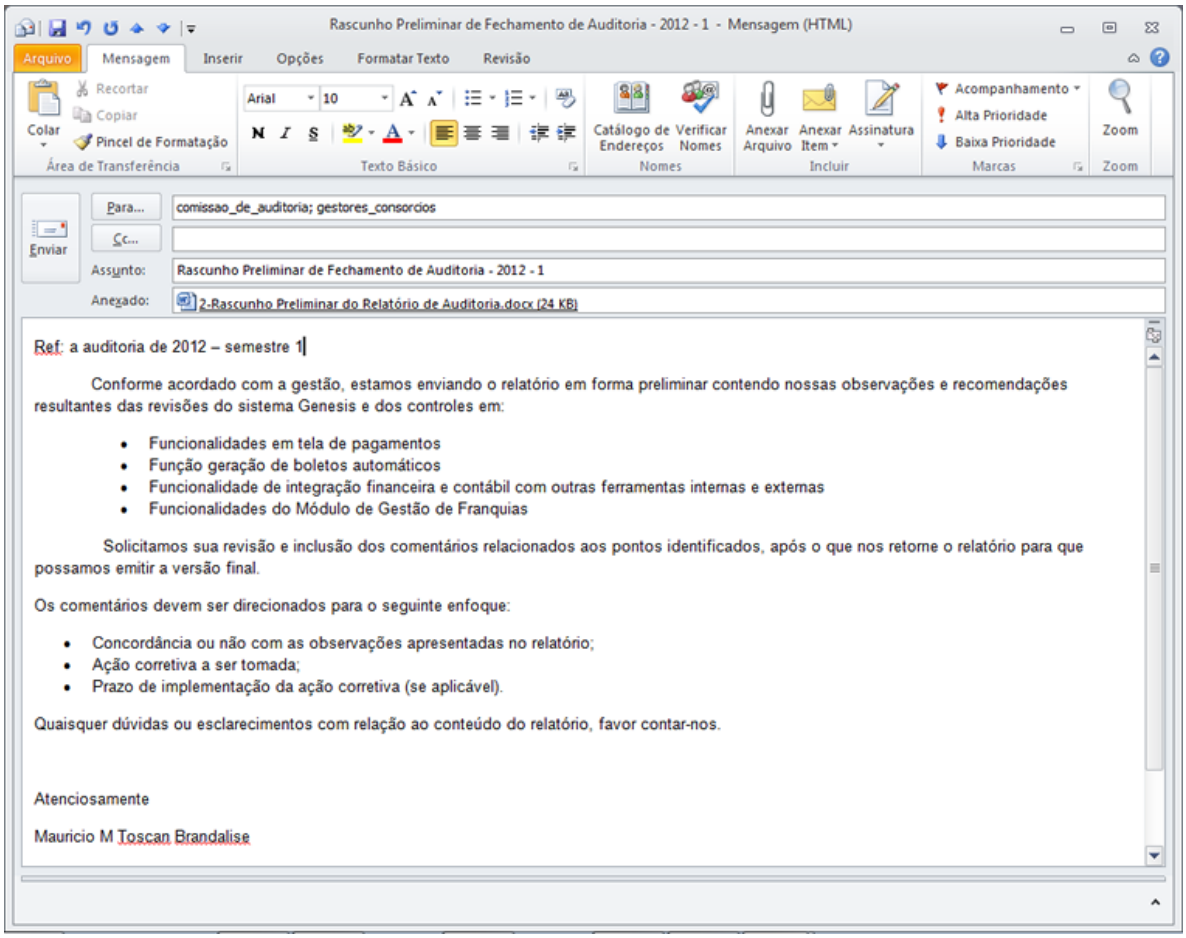
A fase de conclusão de resultados de auditoria iniciou através da atividade de elaboração de artefatos de fechamento da auditoria.

O auditor líder e a equipe de auditoria utilizaram os artefatos e procedimentos realizados até a fase de execução da auditoria, para preparar um artefato de fechamento da auditoria. O que compõe este fechamento é a carta preliminar e o rascunho preliminar.

A carta preliminar, como descrito no roteiro, serve para que a comissão de auditoria e gestores tenham o conhecimento dos trabalhos realizados no programa de auditoria. Em anexo a carta preliminar, enviou-se o rascunho preliminar, onde constavam as informações de auditoria detalhados e para que possam ser analisados criticamente pela comissão e gestores.

Com o rascunho preliminar e a carta comentário, foram enviados por *e-mail*, para que fosse feita a avaliação por parte dos destinatários, que neste programa de auditoria foram a comissão de auditoria e os gestores. A figura 30 mostra o modelo de carta enviado e em anexo o rascunho preliminar.

FIGURA 30 – E-mail enviado a comissão e gestão



Fonte: Elaborado pelo autor.

Os destinatários avaliaram o relatório preliminar e reencaminharam suas posições quanto a avaliação realizada do documento. O auditor líder recebeu estes retornos e fez uma análise prévia das considerações recebidas para posterior elaboração do preenchimento do relatório final de auditoria e para a realização dos comunicados de fechamento.

O relatório foi elaborado com os conteúdos que seguem. No primeiro campo foram citados os objetivos escolhidos no início da auditoria. No campo seguinte foram citadas as normas utilizadas: NBR 17799: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação, a NBR 27002: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da

informação e o COBIT 4.1 e o ITIL v3.

O relatório final também conta com informações necessárias sobre participantes da comissão de auditoria, conforme solicitado e preenchido na tabela 5.

TABELA 5 – Participantes da comissão de auditoria

NOME	CARGO	FUNÇÕES NA AUDITORIA
FULANA DOS REIS	Analista da Qualidade	AUDITORA PLENA
MAURICIO TOSCAN BRANDALISE	Analista de Negócios	LIDER DE AUDITORIA

Fonte: Elaborado pelo autor.

A relação de usuários e gestores que contribuíram de alguma forma na auditoria seguem conforme tabela 6. Os principais envolvidos foram membros que eram da comissão de auditoria e gestor da área administrativa da empresa.

TABELA 6 – Lista de gestores e usuários envolvidos no programa de auditoria

NOME	CARGO	Contribuições na auditoria
BELTRANO	Analista de Negócios	*Informações e dados a respeito do sistema. *Informações sobre servidores *Dados e telas de programas
JOHN P	Coordenador	*Informações e dados a respeito da empresa *Informações sobre gestão de demandas
CICLANO	Gerente de Projetos	*Informações sobre servidores. *Informações sobre regras de negocio * Informações e dados sobre arquivos fonte *Informações e dados sobre configuração de sistema
FULANA DOS REIS	Analista da Qualidade	*Evidências de telas do sistema * Contribuições em geral.

Fonte: Elaborado pelo autor.

Para finalizar o documento, era necessário informar a descrição dos resultados de auditoria. Esta descrição conta com as evidências de auditoria, considerações e recomendações, conforme segue na tabela 7.

TABELA 7 – Descrição de resultados de auditoria

Ponto de Auditoria	Considerações a respeito	Recomendações	Evidências
Funcionalidade em tela de pagamentos	* Este ponto de controle não apresenta versionamento de alterações. *Verificando o ponto de controle, haviam outras versões da tela de pagamentos, porém a mesma foi atualizada sem ter evidencias ou comunicação com o usuário. *Verificando o ponto de controle, haviam outras versões da tela de pagamentos, porém a mesma foi atualizada sem ter evidencias ou comunicação com o usuário.	*Revisar as funcionalidades da tela de pagamentos. *Revisar os procedimentos de atualização de *software*, documentando	*Tela ajuste de pagamentos com funcionalidades apresentando erros. *Arquivos fontes com diversas versões.
Função geração de boletos automáticos	Atualmente, além do envio de boletos por correio, o banco central obriga que, para usuários que possuem *e-mail* e tenham escolhido esta forma de envio, a administradora envie os mesmos por *e-mail*.	- Revisão no relatório de envios de boletos por *e-mail*. - Revisão nas funcionalidades de envio.	*Relatórios apresentam divergências no número de envios com o número de confirmações de recebimentos.
Funcionalidade de integração financeira e contábil com outras ferramentas internas e externas	*Constatou-se falha no momento da integração pelo número de registros envolvidos. *Constatou-se funcionalidade paliativa para resolução do problema.	*Buscar a melhor forma de fazer a integração dos sistemas externos com o ERP da empresa. * Revisão do programa de integração contábil junto ao fornecedor.	* Durante a integração do sistema genesis com outros sistemas (SAP) ocorreram erros de registros
Funcionalidades do Módulo de Gestão de Franquias	* Existem funcionalidades na gestão de franquias apresentando erros e diferentes números comparados a relatórios internos do Genesis. - Ocorrem erros de sistema, dependendo dos parâmetros utilizados nos relatórios e consultas.	* Revisar as funcionalidades nos relatórios da gestão de franquias, reavaliar codificação e integridade dos números apresentados.	*Telas apresentando erro ao fim da execução das transações.

Fonte: Elaborado pelo autor.

A partir do relatório final fechado, o programa de auditoria pode ser dado como concluído no período. Este relatório foi revisado pela equipe de auditoria e disponibilizado em local de acesso comum para a gestão, nos artefatos de saída da fase de conclusão e resultados de auditoria. O relatório final, será utilizado pela comissão de auditoria e principalmente os gestores na elaboração de planos de ação para a verificação de cada ponto levantado e evidenciado no programa de auditoria.

Junto a este relatório, foi disponibilizado o plano de auditoria como segue no anexo Q, e pode ser utilizado como material para futuras consultas e ações a serem tomadas.

4.4 CONSIDERAÇÕES FINAIS DA APLICAÇÃO DO ROTEIRO DE AUDITORIA

A aplicação do roteiro para a criação de programas de auditoria ocorreu de forma satisfatória, a fim de que se pudesse realizar as ações conforme o proposto no trabalho. Através de sua adaptação, do modelo inicial para a ferramenta Microsoft Sharepoint 2007, foram notáveis os ganhos em usabilidade e facilidade no uso do roteiro.

A adaptação do modelo inicial proposto para a ferramenta Microsoft Sharepoint 2007, deixou o roteiro num formato mais dinâmico e utilizável para a comissão de auditoria. A comissão de auditoria pôde, através do roteiro melhor estruturado, se guiar melhor pelas fases e atividades propostas. A localização dos artefatos facilitou no momento de poderem ser registrados dados e informações relativos ao programa de auditoria do período e consultados posteriormente devido a demais atividades que precisariam destes artefatos.

A aplicação do roteiro se mostrou produtiva conforme as atividades iam ocorrendo, tendo o envolvimento de usuários de áreas de negócio, áreas de TI e gestão da empresa. Não houveram problemas maiores na utilização da ferramenta disponibilizada. Parte da comissão de auditoria e da equipe de auditores eram usuários com experiência no Microsoft Sharepoint, portanto a sua utilização ocorreu de forma eficiente e sem que precisassem serem desenvolvidos treinamentos para a utilização.

A comissão de auditoria percebeu que o envolvimento das áreas de negócio poderia ter sido um pouco maior. As discussões a respeito dos pontos de auditoria poderiam ter rendido um pouco mais, a fim de se estabelecer uma identificação melhor para os riscos apontados nos pontos de controle. Porém isso pode estar relacionado a diversos fatores, sendo um deles a relação momento em que foi criado o programa de auditoria, onde haviam outras questões importantes sendo discutidas na empresa, causando um pouco de dispersão na participação efetiva dos usuários na auditoria proposta.

De um modo geral a gestão contribuiu para que o programa de auditoria ocorresse de forma satisfatória, envolvendo-se em reuniões ou apenas dando opiniões informais aos auditores. Estas contribuições da gestão foram muito importantes, pois sem este tipo de apoio, dificilmente teria se conseguido criar um programa de auditoria satisfatório e com informações consistentes.

A aplicação do roteiro para a criação de programas de auditoria mostrou que é viável sua utilização para futuras auditorias. Como citado no trabalho, seguir as fases requer dedicação e envolvimento de toda a comissão de auditoria na estruturação do programa de auditoria. Para isso, a premissa inicial é comissão de auditoria ter um conhecimento

satisfatório a respeito da ferramenta e ter o apoio das mais diversas áreas da empresa, para que o compromisso e responsabilidade seja de todos, tornando a auditoria interna uma atividade séria e importante para a empresa.

5 CONCLUSÃO

O desenvolvimento deste trabalho propiciou a pesquisa e aplicação dos conceitos de auditoria em sistemas ERP. Sua aplicação foi na elaboração de um roteiro para ser implantando em uma empresa que possua um sistema ERP em produção.

Inicialmente, como colocado na proposta de trabalho, foram feitas pesquisas por fundamentações teóricas referentes à área de conhecimento de auditoria interna de sistemas, encontradas principalmente na ABNT NBR 19011 que trata de diretrizes para auditorias de sistema de gestão. Esta norma contribuiu para um bom direcionamento nos estudos sobre como proceder na elaboração de um roteiro para a auditoria de um sistema ERP, além de explicar genericamente procedimentos comuns a qualquer tipo de auditoria.

Na sequência do trabalho, foram realizados estudos a partir de objetivos que Imoniana (2005) e Lyra (2008) definem como essenciais para dar enfoque na auditoria a ser realizada. Os objetivos relacionados são: manutenabilidade, auditabilidade, disponibilidade, integridade, confidencialidade, privacidade, acuidade e versatilidade.

A partir destes objetivos, foram feitas pesquisas nas principais normas e metodologias aplicáveis a sistemas ERP segundo órgãos como ISACA e bibliografias de auditoria em sistemas. As normas e metodologias estudadas foram:

a) NBR 17799: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;
b) NBR 27002: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;
c) COBIT 4.1;
d) ITIL v3.

Estes estudos foram feitos para que houvesse entendimento de suas abordagens e para que se pudesse fazer um relacionamento com os objetivos, os quais estão diretamente relacionados dentro de uma auditoria de sistema ERP. Para quando for elaborado um roteiro de auditoria de sistemas, o auditor possa ter uma base consistente e possa direcionar seus esforços com o auxilio do que a norma ou metodologia impõe em suas diretrizes.

O capítulo 2 também tratou da importância na formação da equipe interna de sistemas. Onde os responsáveis pela definição de equipe, devem ter algumas atenções voltadas na formação da equipe e nas características que um auditor deve ter para poder prestar seus serviços de maneira correta e eficaz.

Os procedimentos de auditoria foram evidenciados conforme estudos realizados em diversas bibliografias. Foram divididos pelas etapas mais significativas dentro de um processo de auditoria, que são: o Planejamento, a Execução e as Conclusões de auditoria.

O capítulo 3 foi fundamentado a partir do capítulo 2. Nele foi iniciado o processo de elaboração do roteiro de auditoria. Também foram relacionados em fases, todos os procedimentos de auditoria estudados e suas características. As fases foram compostas por atividades e artefatos gerados a partir de cada uma delas. A partir desta organização pré-definida no trabalho teórico, o roteiro sofreu ajustes finais de acordo com o plano proposto e também sua posterior validação e avaliação para adaptação em ferramenta selecionada.

Com o objetivo de avaliar a proposta apresentada foi aplicado o roteiro para a criação de programas de auditoria em ERP. O capítulo 4 foi dividido conforme as fases propostas na elaboração do roteiro através da utilização de uma ferramenta. A ferramenta utilizada foi o Microsoft Sharepoint 2007, e auxiliou nos trabalhos exercidos pela comissão de auditoria e pela equipe de auditoria interna no registro das atividades, na criação de artefatos, na consulta de documentos e na comunicação entre as áreas.

O estudo de caso permitiu que fosse criado um programa de auditoria por uma comissão de auditores. Esta comissão era formada por integrantes de áreas de negócio, TI e gestão da empresa e tinha por objetivo conduzir os trabalhos de auditoria.

Durante o estudo de caso, houve a percepção da diversidade de artefatos presentes no programa de auditoria criado. Este fato foi um ponto negativo, pois alguns dos artefatos poderiam contemplar informações e dados equivalentes em apenas um só documento. Além disso, os usuários do roteiro encontraram algumas dificuldades no preenchimento de alguns artefatos devido ao nível de detalhe exigido. Como ponto positivo, a ferramenta disponibilizada foi essencial para a condução da auditoria. A estrutura do roteiro ficou adequada e organizada, apresentando fácil usabilidade e integração entre as fases, atividades e na armazenagem dos artefatos.

O parecer final após o estudo de caso aplicado foi positivo em relação ao plano proposto inicialmente. O programa de auditoria elaborado no estudo de caso seguiu sem muitas adaptações o que o roteiro propunha de atividades, tendo apenas pequenos ajustes em alguns artefatos e atividades.

Como principais contribuições deste trabalho podem ser citados:

a) a definição de estrutura de roteiro para a criação de programas de auditoria em sistemas ERP, onde foram reunidos estudos de diferentes áreas sobre auditoria, como por exemplo, a ABNT NBR 19011, a ABNT NBR 14598 e demais normas

importantes no desenvolvimento do trabalho.

b) a adaptação dos estudos de auditoria de sistemas de informação para ERP. O roteiro pode ser adaptado em diversos sistemas com as mesmas características, porém um pouco mais direcionados, seguindo os objetivos.
c) a aplicação de roteiro para criação de programas de auditoria, estruturado através de normas e metodologias aplicáveis a sistemas ERP.
d) a auditoria em sistemas de informação é uma prática recente para os profissionais da área. O roteiro é uma contribuição muito importante, pois dá uma direção a ser seguida e pode ser aprofundado dependendo dos objetivos.

Para a melhoria e aprimoramento sobre os estudos realizados e procedimentos criados, podem ser destacados trabalhos de:

a) definição de estrutura de roteiro criação de programas de auditorias voltados a outros tipos de sistemas;
b) adequação de artefatos, de modo que fiquem mais compactos e contemplem o maior número de informações e dados.
c) desenvolvimento ou integração de ferramentas que possam ser integradas ao roteiro elaborado, oferecendo maior dinâmica entre a ferramenta onde se encontra o roteiro e as ferramentas onde se encontram evidências.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14598: **Tecnologia da Informação – Avaliação de produto de *software*: parte 1: visão geral**. Rio de Janeiro: ABNT, 2001. 14p.

_____. NBR 17799: **Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005. 132p.

_____. NBR 27002: **Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005. 140p.

_____. NBR ISO 19011: **Diretrizes para auditoria de gestão da qualidade e/ou ambiental**. Rio de Janeiro: ABNT, 2002. 25p.

_____. NBR ISO 27005: **Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação**. Rio de Janeiro: ABNT, 2006. 65p.

ATTIE, William. **Auditoria conceitos e aplicações**. São Paulo: Atlas, 2010.

GIL, A. L.. **Auditoria de computadores**. São Paulo: Atlas, 1999.

IMONIANA, Joshua O. **Auditoria de sistemas de informação**. São Paulo: Atlas, 2005.

IT GOVERNANCE INSTITUTE. COBIT 4.1 Estados Unidos, 2004. Disponível em <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>. Último acesso em: 09 set. 2011.

IT SERVICE MANAGEMENT FORUM. **An Introductory Overview of ITIL**. Version 1.0.a itSMF: United Kingdom, 2004.

JUNIOR, Cicero Caiçara. **Sistemas integrados de gestão ERP**. Curitiba: Editora Ibpex, 2008.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Metodologia do científico**. 6. ed. São Paulo: Atlas, 2006.

LAUDON, Kenneth C.. **Sistemas de informação gerenciais**: administrando a empresa digital. São Paulo: Pearson, 2004.

LIMA, Diana Vaz; CASTRO, Robinson G.. **Fundamentos da auditoria governamental e empresarial**. São Paulo: Atlas, 2003.

LYRA, Maurício R.. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Editora Ciência Moderna, 2008.

MAGALHAES, Antonio de Deus F.; LUNKES, Irtes Cristina; MULLER, Aderbal Nicolas. **Auditoria das organizações metodologias alternativas ao planejamento e á operacionalização dos métodos e técnicas**. São Paulo: Atlas, 2001.

MICHAELIS. **Dicionário *online***. Disponível em: <http://michaelis.uol.com.br>. Acesso em: 19 nov. 2011.

SEMOLA, Marcos. **Gestão da segurança da informação**. São Paulo: Editora Campus, 2003.

SILVA, P. M.. **A função auditoria de sistemas de informação**: modelo funcional e de competências. Braga: Universidade do Minho - Escola de Engenharia, 2007.

STAIR, Ralph M.; REYNOLDS, George W.. **Princípios de sistemas de informação: uma abordagem gerencial**. São Paulo: Thomson, 2006.

ANEXOS

ANEXO A – Quadro normas e metodologias x objetivos globais

Normas, Metodologias	Manutenabilidade	Auditabilidade	Disponibilidade	Integridade	Confidencialidade	Privacidade	Acuidade	Versatilidade
COBIT	**AI2.** Manter Software Aplicativo; **AI2.2** Projeto Detalhado; **AI6** Gerenciar Mudanças; **AI7** Instalar e Homologar Soluções e Mudanças **AI2.5** Configuração e Implementação de Software Aplicativo Adquirido: Customizar e implementar as funcionalidades automatizadas adquiridas para alcançar os objetivos de negócios.	**AI2.3** - Controle e Auditabilidad e do Aplicativo	**DS4** - Assegurar a continuidade dos serviços.		**PO2.** Definir Arquitetura: Processo que melhora a qualidade de decisão e gerenciamento certificando-se de que informações seguras e confidenciais sejam fornecidas. **PO2.3** Esquema de classificação dos dados. Revisão de políticas de permissão e acesso dentro do ERP			**PO2.** Definir Arquitetura.
ABNT NBR ISO/IEC 17799:2005 e NBR ISO 27002	**10.3 e 10.3.2** Aceitação de sistemas, **12.5.3** Restrições em atualizações de softwares	15 Conformidade com requisitos legais		**12.2** O processamento correto das aplicações **12.2.1** Validação nos dados de entrada **12.2.2** Validação no processamento de dados **12.2.4** Validação nos dados de saída	**12.4.3** Controle de acesso ao código fonte do programa	11.5.1 Procedimentos Seguros para entrada no sistema	12.2 - O processamento correto das aplicações	10.3 - Planejamento e aceitação dos sistemas: visando diminuir o risco de acontecerem problemas nas atualizações dos sistemas ERP. **10.3.2** Aceitação de sistemas. **10.8.5** Sistemas de
ITIL	Gerenciamento de Configuração: Config. Do software, Verificação da existência de documentação.		Gerenciamento de Continuidade, Gerenciamento de Disponibilidade,					

ANEXO B – Modelo definições iniciais do programa de auditoria

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO:____/____/____

RESPONSÁVEL:_____

Definições Iniciais do Programa de Auditoria

Escolha no quadro a seguir o OBJETIVO principal que deve ter enfoque nesta auditoria.

a) Objetivos da auditoria

Enfoque Principal:

	Auditabilidade		Disponibilidade
	Privacidade		Manutenabilidade
	Integridade		Versatilidade
	Confidencialidade		Acuidade

Observações:

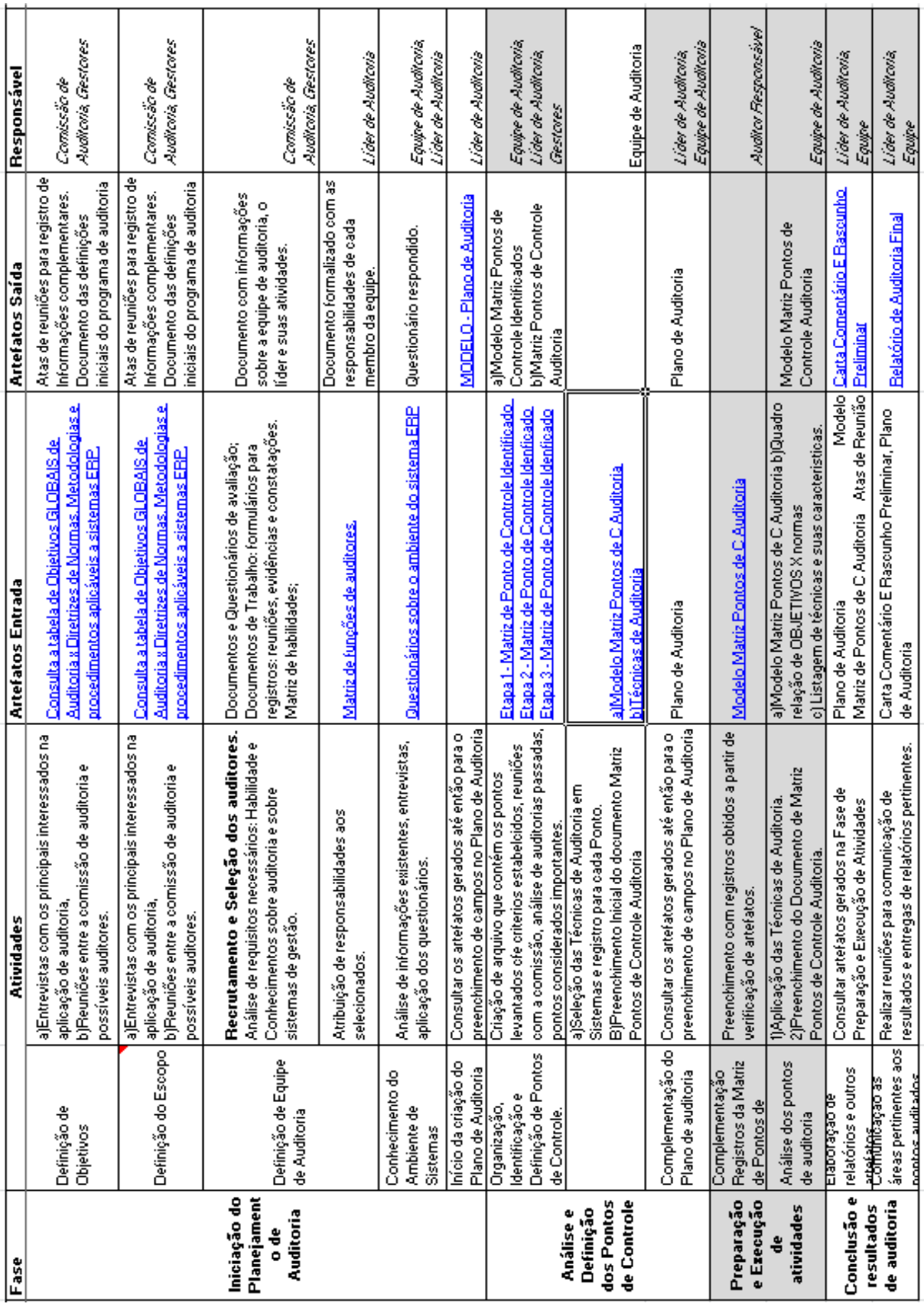
Escolha no quadro a seguir o ESCOPO principal que deve ter enfoque nesta auditoria.

b) Escopo da auditoria

	Completo
	Parcial
	Acompanhamento

Observações:

ANEXO C – Roteiro para a criação de programa de auditoria de sistemas ERP



Fase	Atividades		Artefatos Entrada	Artefatos Saída	Responsável
Iniciação do Planejamento de Auditoria	Definição de Objetivos	a)Entrevistas com os principais interessados na aplicação de auditoria, b)Reuniões entre a comissão de auditoria e possíveis auditores.	Consulta a tabela de Objetivos GLOBAIS de Auditoria x Diretrizes de Normas, Metodologias e procedimentos aplicáveis a sistemas ERP	Atas de reuniões para registro de Informações complementares. Documento das definições iniciais do programa de auditoria	*Comissão de Auditoria, Gestores*
	Definição do Escopo	a)Entrevistas com os principais interessados na aplicação de auditoria, b)Reuniões entre a comissão de auditoria e possíveis auditores.	Consulta a tabela de Objetivos GLOBAIS de Auditoria x Diretrizes de Normas, Metodologias e procedimentos aplicáveis a sistemas ERP	Atas de reuniões para registro de Informações complementares. Documento das definições iniciais do programa de auditoria	*Comissão de Auditoria, Gestores*
	Definição de Equipe de Auditoria	**Recrutamento e Seleção dos auditores.** Análise de requisitos necessários: Habilidade e Conhecimentos sobre auditoria e sobre sistemas de gestão.	Documentos e Questionários de avaliação; Documentos de Trabalho: formulários para registros: reuniões, evidências e constatações. Matriz de habilidades;	Documento com informações sobre a equipe de auditoria, o líder e suas atividades.	*Comissão de Auditoria, Gestores*
		Atribuição de responsabilidades aos selecionados.	Matriz de funções de auditores.	Documento formalizado com as responsabilidades de cada membro da equipe.	*Líder de Auditoria*
	Conhecimento do Ambiente de Sistemas	Análise de informações existentes, entrevistas, aplicação dos questionários.	Questionários sobre o ambiente do sistema ERP	Questionário respondido.	*Equipe de Auditoria, Líder de Auditoria*
	Início da criação do Plano de Auditoria	Consultar os artefatos gerados até então para o preenchimento de campos no Plano de Auditoria		MODELO - Plano de Auditoria	*Líder de Auditoria*
Análise e Definição dos Pontos de Controle	Organização, Identificação e Definição de Pontos de Controle.	Criação de arquivo que contém os pontos levantados ofe criterios estabelcidos, reuniões com a comissão, análise de auditorias passadas, pontos considerados importantes.	Etapa 1 - Matriz de Ponto de Controle Identificado. Etapa 2 - Matriz de Ponto de Controle Identificado. Etapa 3 - Matriz de Ponto de Controle Identificado	a)Modelo Matriz Pontos de Controle Identificados b)Matriz Pontos de Controle Auditoria	*Equipe de Auditoria, Líder de Auditoria, Gestores*
		a)Seleção das Técnicas de Auditoria em Sistemas e registro para cada Ponto. B)Preenchimento Inicial do documento Matriz Pontos de Controle Auditoria	a)Modelo Matriz Pontos de C Auditoria. b)Técnicas de Auditoria		Equipe de Auditoria
	Complementação do Plano de auditoria	Consultar os artefatos gerados até então para o preenchimento de campos no Plano de Auditoria	Plano de Auditoria	Plano de Auditoria	*Líder de Auditoria, Equipe de Auditoria*
Preparação e Execução de atividades	Complementação Registros da Matriz de Pontos de	Preenchimento com registros obtidos a partir de verificação de artefatos.	Modelo Matriz Pontos de C Auditoria		*Auditor Responsável*
	Análise dos pontos de auditoria	1)Aplicação das Técnicas de Auditoria. 2)Preenchimento do Documento de Matriz Pontos de Controle Auditoria.	a)Modelo Matriz Pontos de C Auditoria b)Quadro relação de OBJETIVOS X normas c) Listagem de técnicas e suas caracteristicas.	Modelo Matriz Pontos de Controle Auditoria	*Equipe de Auditoria*
Conclusão e resultados de auditoria	Elaboração de relatórios e outros artefatos	Consultar artefatos gerados na Fase de Preparação e Execução de Atividades	Plano de Auditoria Modelo Matriz de Pontos de C Auditoria Atas de Reunião	Carta Comentário E Rascunho Preliminar	*Líder de Auditoria, Equipe*
	Comunicação as áreas pertinentes aos pontos auditados	Realizar reuniões para comunicação de resultados e entregas de relatórios pertinentes.	Carta Comentário E Rascunho Preliminar, Plano de Auditoria	Relatório de Auditoria Final	*Líder de Auditoria, Equipe*

ANEXO D – Modelo de plano de auditoria

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO:____/____/____

RESPONSAVEL:_____

Definições Iniciais do Programa de Auditoria

Escolha no quadro a seguir o OBJETIVOprincipal que deve ter enfoque nesta auditoria.

a) Objetivos da auditoria

Enfoque Principal:

	Auditabilidade		Disponibilidade
	Privacidade		Manutenabilidade
	Integridade		Versatilidade
	Confidencialidade		Acuidade

Observações:

Escolha no quadro a seguir o ESCOPO principal que deve ter enfoque nesta auditoria.

b) Escopo da auditoria

	Completo
	Parcial
	Acompanhamento

ANEXO E – O modelo de ata de reunião

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERIODO: _____ DATA DA ELABORAÇAO DOCUMENTO:____/____/____

RESPONSÁVEL:_____

ATA DE REUNIÃO

Participantes	Cargo

Definições / Ações	Responsável	Data para solução

ANEXO F – Modelo formulário para seleção de auditores internos

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO___/___/___

RESPONSÁVEL:_____

Formulário para Seleção de Auditores Internos

Nome do Candidato:
Setor:

Cargo pretendido:

	Auditor Líder
	Auditor Pleno
	Auditor Trainee

Avaliação de Candidato

Preencha as colunas de acordo com as competências do candidato(preenchido pela comissão auditoria):

Atributos pessoais em Auditoria Interna	5	4	3	2	1	Observações
Competências para expressar clara e fluentemente conceitos e ideias, oralmente ou através da escrita.						
Habilidades interpessoais para um desempenho eficiente da auditoria, como diplomacia, fato e habilidade para escutar.						
Habilidade para manter suficientemente independência e objetividade.						
Organização pessoal necessária ao efetivo desempenho da auditoria.						
Habilidade para realizar julgamentos aceitáveis, baseado em evidências objetivas.						

ANEXO G – Levantamento do Ambiente de Sistema ERP

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO:____/____/____

RESPONSÁVEL:_____

Questionário - Levantamento do Ambiente

Realize o preenchimento de acordo com os dados e informações levantados.

Abordagem	Questões
Descrição do Sistema	Qual a finalidade do sistema para a condução do negócio ?
Descrição do Perfil de Sistema	Qual o volume de transações por período ? (diário, mensal)
	Existem customizações internas, externas ou ambas ?
	Qual a linguagem de programação do sistema ?
	Existem arquivos/relatórios/registros de controle no sistema ?
	Existe trilha de auditoria do sistema ERP? (logs)
	Os processamentos ocorrem por lote, *on line* ou ambos ? Há monitoração via arquivos de logs enquanto ocorrem ciclos de processamento no sistema ?
Documentação da Visão Geral do Processamento	Relacionar os *workflows* das funções-chaves no processamento das informações significativas e frequência de uso.
	Há padrões de documentação para programas de sistema ERP que estão configurados para executar em modo batch ?
	Existem procedimentos documentados descrevendo como os relatórios de saída são gerados e entregues aos usuários ? (acessos)
	Está sendo usado o padrão de documentação ? Existe documentação referente ao sistema ERP, quanto a processos, manutenções no sistema ?
	As alterações de programas dos módulos do ERP, são controladas e registradas ?
	Há softwares de apoio à documentação do sistema ERP a ser auditado ?
	Relacionar os fluxos das principais transações consideradas enfatizando as entradas-chave(fontes das principais entradas), lógicas dos processamentos e saídas-chaves(relatórios, arquivos, terminais e a utilização de algumas destas saídas, mencionando os arquivos-mestre e tabelas importantes, inclusive integrações com outros sistemas).

ANEXO H – Modelo matriz de pontos de controle identificados

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERIODO: _____ DATA DA ELABORAÇAO DOCUMENTO:____/____/____

RESPONSAVEL:_____

Matriz de Pontos de Controle IDENTIFICADOS – Etapa 1

- Realize o preenchimento da tabela abaixo de acordo com os pontos de controle definidos em reunião.

Matriz do Ponto de Controle

ID	Ponto de Controle	Detalhes	Riscos

Participantes na Seleção dos Pontos de Controle

NOME	CARGO

Anotações Gerais:

ANEXO I – Matriz de pontos de controle definidos

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO:____/____/____

RESPONSÁVEL:_____

Matriz de Pontos de Controle DEFINIDOS – Etapa 2

NOME AVALIADOR:
CARGO:

Valores para votação (Grau-Conceito):

5- Muito Forte	4-Forte	3-Regular	2-Fraco	1-Muito Fraco

- Realize o preenchimento da coluna de GRAU, de acordo com os graus acima.

Matriz do Ponto de Controle

ID	Ponto de Controle	Detalhes	Riscos	Grau

Anotações Gerais:

ANEXO J – Modelo matriz dos pontos de controle auditoria

SISTEMA: _____ EMPRESA: _____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO: ___/___/___

RESPONSAVEL: _____

MATRIZ DE PONTOS DE CONTROLE AUDITORIA

Realize o preenchimento do artefato de acordo com as informações levantadas nas matrizes e demais artefatos de fases anteriores.

PONTOS DE CONTROLE AUDITADOS:

Ponto de Auditoria	Técnicas e Ferramentas	Descrição/ Características da Auditoria	Docs. Verificados	Responsável	Considerações a respeito	Recomendações	N. C.*	C.	Evidências

OBSERVAÇÕES:

ANEXO K – Listagem de técnicas de auditoria para consulta

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO:____/____/____

RESPONSÁVEL:_____

TÉCNICAS DE AUDITORIA PARA CONSULTA

TÉCNICAS	
a)	Dados de teste ou Test Data
b)	Facilidade de Teste Integrado
c)	Simulação Paralela
d)	Rastreamento e Mapeamento
e)	Análise da lógica de programação
f)	Análise do Programa Fonte
g)	Entrevistas no ambiente de sistemas e aplicação de questionários
h)	Análise de Relatórios e Telas
i)	Snapshots

a) Dados de teste ou Test Data

IMONIANA (2005) explica que este tipo de teste envolve um conjunto de dados bem preparados e projetados com o objetivo de testar as funções de entrada de dados do sistema. Para o inicio destes testes devem ser rodadas diversas transações, após isso o auditor compara os resultados com os predeterminados. Mas para que essa técnica seja efetiva, (MAGALHAES; LUNKES; MULLER, 2001, p. 153) abordam que deve ser compreendido nos testes o maior número possível de situações, incluindo dados errados, exceções, campos inválidos, duplicidade e outras situações de erro.

IMONIANA (2005) destaca uma vantagem nela que é, para geração de dados em massa, podem ser usados *softwares* específicos. Porém sua desvantagem seria na própria aplicação, onde no ambiente de negócio das empresas é complicado planejar e antecipar todas as possíveis combinações de transações. Outra desvantagem que (MAGALHAES; LUNKES; MULLER, 2001, p. 153) é que o teste fica limitado ao universo que o auditor delimitou, o que pode ser mais restrito ainda dependendo da complexidade e tamanho do sistema ERP auditado.

B) Facilidade de Teste Integrado

ANEXO L – O modelo de rascunho preliminar do relatório de auditoria

SISTEMA: _____ EMPRESA:_____

PROGRAMA DE AUDITORIA – PERÍODO: _____ DATA DA ELABORAÇÃO DOCUMENTO:____/____/____

RESPONSÁVEL:_____

Modelo Rascunho Preliminar do Relatório de Auditoria

a) Objetivos do Controle:

b) Considerações:

c) Descrição dos procedimentos executados:

d) Resultados obtidos:

e) Não Conformidades / Evidências achadas:

f) Recomendações:

g) Aval dos responsáveis internos:

ANEXO M – Questionário preenchido com informações e dados do ambiente

PROGRAMA DE AUDITORIA – PERÍODO: 2012 - 1 DATA DA ELABORAÇÃO DOCUMENTO: 11/08/2012

RESPONSÁVEL: MAURICIO M. TOSCAN BRANDALISE

Questionário - Levantamento do Ambiente

Realize o preenchimento de acordo com os dados e informações levantados.

Abordagem	Questões
Descrição do Sistema	Qual a finalidade do sistema para a condução do negócio ? *O Genesis é a principal ferramenta para a condução dos processos da empresa. Através deste software ERP, a empresa conduz o seu core business realizando o registro de dados, consulta de informações e extração de relatórios gerenciais e operacionais. A ferramenta está ligada diretamente a todas as franquias por meio de portal existente na internet.*
Descrição do Perfil de Sistema	Qual o volume de transações por período ? (diário, mensal) *O número de transações pode variar, pois existem períodos no mês em que a utilização do sistema torna-se mais frequente devido a fechamento de mês ou atingimento de metas. Cerca de 400 diferentes transações diárias, executadas n vezes por diversos usuários.*
	Existem customizações internas, externas ou ambas ? *Existem customizações em ambos os casos.*
	Qual a linguagem de programação do sistema ? *ASP, ASP.NET e C#.*
	Existem arquivos/relatórios/registros de controle no sistema ? *Existem diversos relatórios no sistema. Estão basicamente divididos pelos módulos em que o Genesis se encontra.*
	Existe trilha de auditoria do sistema ERP? (logs) *Existe uma tabela de logs, onde são registrados todos os logs de sistema.*
	Os processamentos ocorrem por lote, *on line* ou ambos ? Há monitoração via arquivos de logs enquanto ocorrem ciclos de processamento no sistema ? *Não existem monitoramentos internos, apenas as trilhas de auditoria.*
Documentação da Visão Geral do Processamento	Relacionar os *work-flows* das funções-chaves no processamento das informações significativas e frequência de uso.
	Há padrões de documentação para programas de sistema ERP que estão configurados para executar em modo batch ? *Não se aplica. Em suma, a maioria dos sistemas está programado através de JOBS nos servidores da TIVIT.*
	Existem procedimentos documentados descrevendo como os relatórios de saída são gerados e entregues aos usuários ? *Não se aplica.*
	Está sendo usado o padrão de documentação ? Existe documentação referente ao sistema ERP, quanto a processos, manutenções no sistema ? *As documentações existem a partir da modelagem do sistema, porém podem não estar atualizadas, devido a customizações recentes.*
	As alterações de programas dos módulos do ERP, são controladas e registradas ? *Todas as solicitações são abertas e gerenciadas pelo gestão de demandas. Solicitações que ficam fora deste escopo são consideradas ajustes ou apenas modificações rápidas.*
	Há softwares de apoio à documentação do sistema ERP a ser auditado ? *Através do TEAM WEB ACESS, software do DB Server, existem os fluxos do funcionamento do sistema.*

ANEXO N – O artefato matriz pontos de controle identificados preenchido

SISTEMA: GENESIS EMPRESA:

PROGRAMA DE AUDITORIA – PERÍODO: 2012 - 1 DATA DA ELABORAÇÃO DOCUMENTO: 08/06/2012

RESPONSAVEL: MAURICIO M. TOSCAN BRANDALISE

Matriz de Pontos de Controle IDENTIFICADOS – Etapa 1

- Realize o preenchimento da tabela abaixo de acordo com os pontos de controle definidos em reunião.

Matriz do Ponto de Controle

ID	Ponto de Controle	Detalhes	Riscos
1	Funcionalidades do Modulo de Gestao de Franquias	Franquias e unidades vem relatando algumas dificuldades em relação a utilização do módulo externo do ERP em relação a geração de relatórios homologados e em produção. Os relatórios, algumas vezes apresentam diferenciaçoes na contabilizaçao de determinados dados e na exibição de informações. A gestão acredita que este seja um ponto passivel de ser auditado, com o objetivo de verificar a integridade dos dados e informações. [INTEGRIDADE]	A empresa pode estar correndo o risco na prospecção de clientes, no planejamento estratégico para a melhorias das unidades, no comissionamento de funcionários, etc.
2	Funçao geraçao de boletos automaticos	Atualmente a funcionalidade de geraçao de boletos automáticos necessita de uma revisão. Existem estatisticas em relatórios, que segundo os usuários apontam o não recebimento via e-mail do boleto automático conforme solicitaçao do cliente. O sistema apresenta-se parametrizado e o processo de geração corretos. [MANUTENABILIDADE]	Possiveis riscos financeiros. Faz-se necessária a verificação da padronização da liberação de versões do software, detalhando ao máximo o que contempla cada uma.
3	Funcionalidade de integraçao financeira e contábil com outras ferramentas internas e externas	Atualmente a empresa apresenta problemas nas funcionalidades de integração do ERP. [INTEGRIDADE E MANUTENABILIDADE]	Possiveis riscos financeiros. E necessária a intervenção neste ponto, pois as ameaças e vulnerabilidades existem.
4	Funcionalidade em tela de pagamentos	Necessidade de reavaliaçao na tela de pagamentos. Ocorrem erros na realização da efetivação de pagamentos e isso pode estar relacionado ao alto número de registro vinculados. [MANUTENABILIDADE]	Possiveis riscos de insatisfaçao de fornecedores, acarretando em serviços necessários para a administradora.

Participantes na Seleção dos Pontos de Controle

NOME	CARGO
	ANALISTA DE NEGÓCIOS
	GERENTE DE PROJETOS – DB SERVER
	ANALISTA DE NEGÓCIOS
	COORDENADOR ADMINISTRATIVO
	ANALISTA DA QUALIDADE
	COORDENADOR DE TI

Anotações Gerais:

O preenchimento deste artefato ocorreu com a presença dos principais envolvidos na criação do programa de auditoria. As demandas foram organizadas de acordo com o que coordenadores e gestão puderam levantar internamente e além disso, com considerações realizadas pela equipe de auditoria ao analisar históricos de chamados e verificações de não conformidade em auditorias passadas.

ANEXO O – Artefato anexo da ata de reunião para levantamento de pontos

	ATA DE REUNIÃO	Data: 29/05/12	N.º 19/2012
ASSUNTO	Reunião do Grupo de Usuários Gestão da Demanda		
LOCAL	Sala de Reuniões Diamante		
COORDENADOR	Mauricio Brandalise		
RESPONSAVEL	Mauricio Brandalise		

Manutenção:

- **Gestão de Demandas**
  Para evitar o retrabalho e garantir melhor a qualidade do software sempre que for priorizado alguma demanda será analisado, sempre que possível, todas as demais demandas que são relativas ao mesmo processo. O objetivo será conseguir atender o processo como um todo além de, documentar todo este fluxo e migrar toda a aplicação para a nova plataforma de tecnologia já existente no sistema. Sempre que isto ocorrer será pautada e destacada no detalhamento de cada item priorizado.

Jurídico

- Ajuste de processos do Serasa
  Criar uma nova funcionalidade para incluir e excluir do Serasa que não seja pelo fluxo da operação. Isto se tornou necessário devido as críticas que são devolvidas pelo Serasa.
  Também terá que ser implementado uma nova regra para a ordenação de geração do arquivo, como estava fazendo em ordem alfabética estavam sendo criticados alguns avalistas que estavam antes dos titulares.

Cobrança – Geração de boletos e Arquivo de débito em conta

- Processo de Geração de Boletos e Arquivos de débito
  Finalizando o processo de geração de arquivo e cálculo do débito em conta.

Priorizados

Adesão

- Débito em Conta / Bancos credenciados para Débito em conta *[PRIORIZADA]*
- ID826 - Assinatura Digital – Testemunhas
- ID823 - Documentos da Cota/Bem vinculado

Análise de crédito

- 99914237 - UC 119 - Alienar Bem e UC 054 - Substituir garantia
- 99915029 - UC 054 - Substituição de Garantias (botão cancelar)

Assembléia

- Adequar participações de coordenadores, gerentes e diretores de algumas empresas do grupo, na participação de assembleias. (**questão LEGAL**)
  - Falta a definição de algumas regras. O acesso a base de dados SAP já foi garantido.

Contábil

- 4440 - [CR] Desenvolvimento de Novo Relatório - Cotas Ajuizadas
  Desenvolver relatórios para acompanhamento e controle de operações atípicas.

ANEXO P – O Plano de auditoria preenchido

SISTEMA: GENESIS EMPRESA:

PROGRAMA DE AUDITORIA – PERÍODO: 2012 - 1 DATA DA ELABORAÇÃO DOCUMENTO: 08/06/2012

RESPONSAVEL: MAURICIO M. TOSCAN BRANDALISE

Plano de Auditoria Interna

Introdução

Este documento descreve os objetivos e o escopo (abrangências) dos procedimentos a serem avaliados e as abordagens que devem ser adotadas pela equipe de auditoria de sistemas como suporte aos trabalhos de auditoria do sistema do CLIENTE para o ano findo *de 20 de junho de 2012*.

Um breve parecer do sistema verificado citando:

a) Objetivos da Auditoria

Enfoque Principal:

	Auditabilidade		Disponibilidade
	Privacidade	x	Manutenabilidade
x	Integridade		Versatilidade
	Confidencialidade		Acuidade

Descrição detalhada:

INTEGRIDADE: *a fim de assegurar se as transações atuais do genesis são confiáveis e seguras, a comissão entende que este seria um objetivo importante de ser atendido no momento de criação deste programa de auditoria. Atualmente existem ocorrências esporádicas sobre a exibição dos dados, colocando em dúvida usuários e gestores no que se refere a análises de dados de relatórios e comparativos com outras fontes.*

MANUTENABILIDADE*: a partir do mapa estratégico da empresa de manter sistemas atualizados e em pleno funcionamento, a manutenabilidade tem o objetivo de controlar as atualizações que vem ocorrendo do sistema Genesis. A partir de auditorias passadas, foram detectados possíveis evidências de não conformidade no gerenciamento destas atualizações.*

Escopo da auditoria;

	Completo
X	Parcial
	Acompanhamento

Observações: *O escopo desta auditoria prevê atender basicamente funcionalidades ligadas as manutenções do*

A) Datas e lugares onde as atividades de auditoria serão realizadas: *IN LOCO – RANDON CONSÓRCIOS no PERIODO DE 08/06 A 12/06*

B) Definição de funções e responsabilidades dos membros da equipe de auditoria e das áreas auditadas;

	Funções	Responsabilidades
Auditor Líder	*Conduzir e delegar os testes de auditoria em sistemas;* *Conduzir tarefas e delegar atividades para a equipe;*	*Conduzir o programa de auditoria de forma que sejam atendidos os objetivos propostos em conjunto a gestão.*
Auditores Auxiliares	*Auxiliar na condução do programa de auditoria* *Realizar tarefas delegadas pelo auditor líder*	*Cumprir tarefas delegadas pelo auditor líder, a fim de satisfazer as atividades e atender os resultados.*

*Fase de Planejamento / Fase de Execução

C) Principais pontos do relatório de auditoria;

ID	Descrição do Ponto de Controle	GRAU
1	*Ajustes em tela de pagamentos*	*9*
2	*Função geração de boletos automáticos*	*8*
3	*Ajuste de integração financeira e contábil com outras ferramentas internas e externas*	*8*
4	*Funcionalidades do Módulo de Gestão de Franquias*	*7*

D) Áreas de risco levantadas: *FINANCEIRO, FINANCEIRO DE GRUPOS CONTÁBIL, COMERCIAL, JURÍDICO E TI*

E) Tempos de execução das tarefas: *As tarefas ocorreram dentro do período determinado no programa (08-06 a 12-06).*

F) Normas utilizadas (NORMAS, ISOS, ETC), *As normas utilizadas são as que contemplam a estrutura do roteiro e definem os objetivos da auditoria:* NBR 17799: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação; NBR 27002: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação; COBIT 4.1;ITIL v3.

G) Quaisquer ações de acompanhamento de auditoria.

Ação	Observ.
A elaboração do relatório final de auditoria foi realizada pelo auditor líder.	*Houve a participação da gestão na elaboração deste relatório, em conjunto também com a equipe de auditoria.*
A gestão da empresa irá analisar as evidências apontadas, assim como as considerações dos auditores, a fim de realizar ações pós auditoria.	*Os planos de ação serão organizados pela área de qualidade em conjunto com a TI.*

Obs: ***O relatório final de auditoria em anexo, contém os pontos de controle com suas considerações principais.***

ANEXO Q – O artefato matriz pontos de controle auditoria preenchido

Realize o preenchimento do artefato de acordo com as informações levantadas nas matrizes e demais artefatos de fases anteriores.

Ponto de Auditoria	Técnicas e Ferramentas	Descrição/ Características da Auditoria	Docs. Verificados	Responsável	Considerações a respeito	Recomendações	N. C. *	C. I.	Evidências
Funcionalidades em tela de pagamentos	-Entrevistas com usuários das áreas relacionadas - Test data - Análise do Programa Fonte - Análise de Relatórios e Telas	- Reuniram-se os usuários da área financeira, contábil e TI. Foram solicitados prints de telas, para averiguação do registro. - Foram realizados testes com inserção de dados em base de homologação. - Feita a análise do programa fonte, a fim de levantar evidências para malhoria de codificação e layout	Plano de auditoria, consulta a intranet da Randon consórcios para verificar documentos de auditorias passadas. Análise de questionário inicial. Análise de riscos apontados em artefatos iniciais		-Este ponto de controle não apresenta versionamento de alterações. -Verificando o ponto de controle, haviam outras versões da tela de pagamentos, porém a mesma foi atualizada sem ter evidencias ou comunicação com o usuário.	-Revisar as funcionalidades da tela de pagamentos. - Revisar os procedimentos de atualização de software, documentando	x		-Tela ajuste de pagamentos com funcionalidades apresentando erros -Arquivos fontes com diversas versões.
Funcionalidades geração de boletos automáticos	-Entrevistas com usuários das áreas relacionadas - Test data - Análise do Programa Fonte	- Foram verificados os padrões de envio de boletos. Atualmente existem dois: por correios e por e-mails. A auditoria buscou investigar se por e-mail os boletos estavam sendo endereçados aos usuários finais corretamente e se havia o registro deste envio no sistema.	Plano de auditoria, consulta a intranet da Randon consórcios para verificar documentos de auditorias passadas. Análise de riscos apontados em artefatos iniciais Relatório de envios automáticos		Atualmente, além do envio de boletos por correio, o banco central obriga que, para usuários que possuem e-mail e tenham escolhido esta forma de envio, a administradora envie os mesmos por e-mail	- Revisão no relatório de envios de boletos por e-mail - Revisão nas funcionalidades de envio.	X		-Relatórios apresentam divergências no número de envios com o número de confirmações de recebimentos.
Funcionalidade de integração financeira e contábil com outras ferramentas internas e	- Entrevistas com usuários das áreas relacionadas - Utilização da ferramenta Oracle para a verificação na base de dados de alguns dados. - Análise de Relatórios e Telas	-Foram consultados usuários das áreas contábeis e financeira, afim de esclarecer melhor o processo. -Ocorreram acompanhamentos no momento da integração, analisando logs, registros em tabelas e prints de relatórios.	Plano de auditoria, consulta a intranet da Randon consórcios para verificar documentos de auditorias passadas Análise de riscos apontados em artefatos iniciais.		-Constatou-se falha no momento da integração pelo número de registros envolvidos. -Constatou-se funcionalidade paliativa para	- Buscar a melhor forma de fazer a integração dos sistemas externos com o ERP da empresa. * Revisão do programa de integração contábil junto ao fornecedor.	X		. -Durante a integração do sistema gennesis com outros sistemas (SAP) ocorreram erros de registros.

Ponto de Auditoria	Técnicas e Ferramentas	Descrição/ Caracteristicas da Auditoria	Docs. Verificados	Responsável	problema. Considerações a respeito	Recomendações	N. C. *	C.	Evidências
Funcionalidades do Módulo de Gestão de Franquias	- Entrevistas com usuários das áreas relacionadas. - Análise de Relatórios e Telas - Análise do Programa Fonte	- Ocorreram testes de inserção de dados, conforme o maior número possível de situações possíveis, incluindo dados errados, exceções, testes de duplicidade e outras situações de erro	-Consulta ao software de chamados e as atas de melhorias pendentes. - Análise de e-mails com considerações de usuários	MAURICIO TOSCAN BRANDALISE	- Existem funcionalidades na gestão de franquias apresentando erros e diferentes números comparados a relatórios internos do Genesis. - Ocorrem erros de sistema, dependendo dos parâmetros utilizados nos relatórios e consultas.	- Revisar as funcionalidades nos relatórios da gestão de franquias, reavaliar codificação e integridade dos números apresentados.	x		- Telas apresentando erro ao fim da execução das transações.

Observações: