Universidade Eduardo Mondlane
Faculdade de Ciências

Departamento de Matemática e Informática

Trabalho de Licenciatura

Modelo Conceptual de Auditoria do Sistema SAP/R3

Caso de Estudo: Auditoria do Sistema SAP/R3 nas Empresas do Grupo Petromoc

Discente: Emídio Afonso Fanequiço

Maputo, Junho de 2005

Universidade Eduardo Mondlane
Faculdade de Ciências

Departamento de Matemática e Informática

Trabalho de Licenciatura

Modelo Conceptual de Auditoria do Sistema SAP/R3

Casó de Estudo: Auditória do Sistema SAP/R3 nas Empresas do Grupo Petromoc

Discente: Emídio Áfonso Fanequiço

Supervisor: Dr. Fernando Rafael Comolo

Maputo, Junho de 2005

DEDICATÓRIA

Dedico o presente trabalho a toda minha família em especial ao meu querido pai Naftal Fanequiço e mãe Aureliana Afonso, aos meus irmãos Iolanda Afonso, Leonel Fanequiço, Eunice Naftal e Dorcass Nália, as minhas sobrinhas Cleópatra Eunice e Lariça Thausene que todos duma forma ou de outra contribuíram para a realização deste trabalho.

AGRADECIMENTOS

Agredeço à Deus Pai todo poderoso que dele quase sempre busquei inspiração em todos momentos da execução do trabalho e nunca senti abandono da sua parte.

Ao meu actual grande amigo e companheiro da "batalha", Dr João Macave, que apesar de fisicamente estar distante tem incentivado muito para a minha formação.

Aos meus grandes amigos e colegas de faculdade Bernardo Macie, Afonso Timba, Arnaldo Cumbe, que me acompanharam nas jornadas estudantís ao longo da formação.

Aos meus amigos e colegas de trabalho Rossana Carimo, Nelsa Ramson, Carlos Valente, Ernesto, Osias Owana, Alvaro Chacha, Arshad Amade pelo contributo significativo na efectivação do presente trabalho.

Aos meus amigos Catarina Camal, Arsénia, Iko Vieira , Casimiro, Serrafim Milito, Dulcídio João e Elídio Venâncio que com eles partilhamos momentos de confraternidade.

Ao Dr. Fernando Comolo pela sua dedicação, observação e crítica na intenção de elevar a qualidade deste empreendimento. A todos trabalhadores da EBS e em especial ao Dr. Luis de Jesus, Engº Brito Marcos por terem concedido um campo para investigação, pesquisa e metido a minha disposição meios suficientes para que levasse à cabo este estudo.

DECLARAÇÃO DE HONRA

"Declaro por minha honra, que o presente trabalho é resultado das minhas próprias investigações e o mesmo foi realizado apenas para ser submetido como Trabalho de Licenciatura em Informática, na Universidade Eduardo Mondlane".

Emídio A. Fanequico

Emídio Afonso Fanequisso

SÍMBOLOS E ABREVIATURAS

ABAP	Advanced Business Application Programming
BD	Base de Dados
CAD	Computer-Aided Design
CPI-C	Common Programming Interface-Communication
EBS	Eletronic Business System
EDI	Electronic Data Interchange
FI	Financial Account
HR	Human Resource
IBM	International Business Machine
IS	Industry Solutions
LAN	Local Area Network
MAPI	Messaging Application Programming Interface
MM	Material Management
MOM	Mapa de Oportunidades de Melhoramentos
ODBC	Open Data Base Connectivity
OLE	Object Linking and Embedding
PP	Production Planning
QA	Quality Assurence
RAM	Random Access Memory
R/3	Runtime System 3
SAP	System Application Product
SAPGUI.	SAP Graphical User Interface
SD	Sales & Distribution
SGBD	Sistema de Gestão de Base de Dados
SGBDR	Sistema de Gestão de Base de Dados Relacional
SI	Sistema de Informação
SNA	System Network Architecture
SQL	Strutured Query Language
TCP/IP	Transmission Control Protocol / Internet Protocol.
TI	Tecnologia de Informação
WAN	Wide Area Network

RESUMO

O presente trabalho de forma didática tem o propósito de proporcionar as empresas que usam o SAP/R3 uma garantia da devida implementação e operacionalização do sistema, por forma que, não se verifiquem constrangimentos de grande envergadura pela criação de usuários sem o devido licenciamento, má definição dos perfis, falta de medidas fiáveis de recuperação do sistema, etc.

Partindo de um estudo em auditoria de sistemas de informação, auditoria dos utilizadores, dos especialistas em tecnologias de informação, da segurança do sistema, das técnicas de auditoria de sistemas e do SAP/R3 com base bibliográfica, concebeu-se um modelo de auditoria com a ilustração das fases de pré-auditoria, com objectivos de preparar a documentação da auditoria, formar a equipa de auditoria e traçar plano de trabalho adequado a entidade a ser auditada; A fase de planeamento, com objectivos de, conhecer o ambiente do sistema, analisar o sistema instalado e verificar a satisfação dos utilizadores; A fase de execução, mostrada a abordagem de sistemas que é top down; A fase de análise em que faz se a análise das informações colhidas nas fases anteriores; A fase de conclusão, mostrando os resultados da auditoria, a discussão dos resultados e as recomendações.

Implementou-se o modelo conceptual no contexto das empresas do grupo Petromoc, usando as técnicas de auditoria como os questionários, entrevistas e visita presencial; A implementação teve como base a fase de execução do modelo conceptual em que, verificou-se a má criação dos perfis dos utilizadores, a não parametrização periódica do SAP/R3, a falta de conhecimentos de utilização do sistema nos utilizadores, inexistência de medidas fiáveis de recuperação do sistema após a perda e, são desenvolvidos programas no mandante Produtivo.

Deste modo, as conclusões e recomendações são por forma que se tenha uma devida operacionalização do sistema evitando os constrangimentos verificados.
O modelo conceptual é abrangente abarcando as partes técnica e funcional necessitando, como limitação, conhecimentos adicionais das implicações na análise da carga, exploração, base de dados e da funcionalidade do sistema.

Índice

CAPÍTULO I – INTRODUÇÃO

"*Toda e qualquer Auditoria é a actividade que consiste na emissão de uma opinião profissional sobre o objecto de análise, a fim de confirmar se cumpre adequadamente as condições que lhe são exigidas*"(Carneiro, 2001:9).

Um modelo de auditoria informática refere- se a emissão de uma norma para adopção da opinião profissional referente a auditoria às empresas que os seus Sistemas de Informação englobam as Tecnologias de Informação[1] como forma de obter elevados índices de produtividade e desempenho nas suas principais actividades.

Segundo Carneiro (2001:23), a *Auditoria de Sistemas* concentra os seus esforços na análise e avaliação, quer envolvendo-se em processos de planeamento, desenvolvimento, testes e aplicação dos sistemas, quer examinando a estrutura lógica, física, ambiental, organizacional de controlo, segurança e protecção de dados.

O elevado fluxo de informação nas organizações proporcionado pelo desenvolvimento da sociedade e organizações em geral, faz com que os sistemas de informação (SI) sejam entendidos como sendo a combinação de processos, informações, recursos (humanos e outros) e/ou tecnologias de informação, organizados para o alcance dos objectivos de uma organização. Os SI são ditos Informatizados quando usam as tecnologias de informação (TI).

O SI regista e mantém actualizada a informação relativa a valorização das transações[2]. Raramente o suporte tecnológico (suporte informático), cobre a transação do princípio ao fim, e neste caso, existe uma símbiose entre o processo manual e o processo informático.

O controlo interno deverá garantir que não só o processamento informático dá garantias de "integridade e exactidão" da transação, mas também que as funções complementares, manuais, quer a montante quer ajuzante, dão essa garantia.

É fácil concluir que se houver bons controlos internos sobre a informação processada após a sua entrada no "módulo de entradas" (ou seja do processamento informático) sem que seja garantido

[1] Tecnologias de Informação são vistas como o conjunto de todos recursos tecnológicos envolvidos no planeamento, desenvolvimento, exploração e manutenção dos SI(Santos, 1996).
[2] Transação, entende- se como sendo o conjunto de dados que identifica as alterações (actualizações) que foram feitas nos ficheiros de um arquivo(Carneiro, 2001:279).

esse rigor no processo manual a montante, o sistema pode estar a fazer um bom controlo interno informático sobre informação errada, incompleta ou insignificante.

Embora o "processo informático" seja potencialmente um óptimo veículo para o controlo de displina do controlo interno no seu todo, gostaria de decompôr a auditoria funcional de um processo de uma transação no processo de interacção manual e processo informático propriamente dito.

Para este trabalho, é vista a auditoria do processamento informático podendo ser feita a vários sistemas existentes nas empresas tais como: SAP/R3, PHC, Primavera, etc. O SAP (System Application Product) é um conjunto de sistemas (módulos) integrados, com dados que interagem e se realimentam com os diversos módulos.

Empresas nacionais como Mozal, Coca-Cola, Hidro-eléctrica de Cahora Bassa, Banco de Moçambique e a Petromoc são um exemplo de organizações que usam o sistema SAP, e a Petromoc particularmente não tem feito auditorias regulares nos seus sistemas e tecnologias de informação e comunicação.

É com base no conhecimento real das empresas proporcionado pela auditoria do SI Informatizado – SAP/R3 que a administração vai planear as suas actividades como forma estratégica de desenvolver o seu negócio.

Tendo como base a necessidade de auditoria do SI Informatizado – SAP/R3, que se pretende descrever no presente trabalho, uma auditoria de referência para que as organizações possam de forma equilibrada auditar os seus sistemas, minimizando coerentemente as possíveis falhas ou erros de utilização e aumentando significativamente a fiabilidade e segurança das informações advindas do SAP/R3.

Neste contexto, são mostrados a seguir pontos correspondentes a definição do problema, os objectivos do trabalho, materias e métodos, estrutura do trabalho.

1.1. Definição do Problema

A auditoria do SAP/R3 por ser uma das formas de criar transparência dos dados produzidos pelo sistema e todos os processos nele envolvidos, de manter o sistema operando devidamente proporcionando à administração e/ou gestores da organização informação segura para o desenvolvimento da organização, aos chefes e/ou directores decisões fiáveis e aos técnicos operacionais uma eficiência no uso do sistema; A não adopção da Auditoria do SAP/R3, pode causar os seguintes problemas para a Organização em que o sistema está inserido:

- Criação de utilizadores sem o respectivo licenciamento, o que originará custos adicionais para a empresa que usa o sistema, a quando de uma auditoria realizada pelos donos do sistema;
- Baixos níveis de produtividade por parte dos utilizadores do sistema, acesso descontrolado (autorizações) dos diversos módulos do sistema e inexistência de medidas correctivas fiáveis no caso de eventos catastróficos (inundações, violações, incêndios, etc.);
- Desconfiança nos utilizadores do SAP/R3 devido ao incumprimento de prazos nas actividades que lhes são incumbidas e/ou deficiente qualidade dos resultados produzidos pelo sistema, altos níveis de erros e dificuldade de correcção destes na introdução de dados por parte do utilizador;
- Os dados produzidos pelo SAP/R3 por mais que mostrem eficiência à organização, podem reflectir uma realidade bem distinta da que seria se todos os processos fossem transparentes e averiguados por entidades competentes;
- Investimentos exorbitantes em novas tecnologias de informação que não se adequem ao sistema SAP/R3 ou causem mau desempenho do sistema;
- Eminentes falhas no *hardware* e *software* da sala de servidores.

Estes e outros problemas aparecem principalmente pela falta de uma política de auditoria do sistema SAP/R3, ou seja, de um modelo que representaria a auditoria do SAP/R3 para as organizações em que o sistema é usado.

1.2. Objectivos

1.2.1. Geral

- Desenvolver um Modelo de Auditoria do Sistema SAP/R3, que sirva de política de auditoria do SAP/R3 para minimizar os constrangimentos que tem ocorrido no uso do sistema.

1.2.2. Especificos

- Fazer o estudo da auditoria e segurança de SI para familiarização dos aspectos que tem a ver com a auditoria de um sistema em operação;
- Fazer o estudo do sistema SAP/R3 para auxiliar a implementação do modelo proposto de auditoria;
- Criar um modelo de auditoria do sistema informático que sirva de modelo de referência na auditoria do sistema SAP/R3;
- Implementar o modelo para as empresas do grupo Petromoc.

1.3. Materiais e Métodos

Para a elaboração do presente trabalho, efectuou-se a recolha de dados usando as seguintes técnicas:

- questionários;
- entrevistas estruturadas e não estruturadas;
- visita presencial;
- pesquisa bibliográfica.

Os questionários elaborados e dirigidos aos funcionários que trabalham com o SAP/R3 nas empresas em que foi implementado o modelo, permitiram reunir informação sobre o uso do sistema.

As entrevistas permitiram colher dos inquiridos se o uso do sistema SAP/R3 atinge adequadamente as expectativas da sua aquisição pelas empresas, as diversas transações ou processamentos que supostamente o SAP deveria facultar às empresas, os critérios de autorizações se estão sendo devidamente cumpridos, problemas frequentemente verificados no uso do SAP e como são solucionados, mecanismos de segurança e protecção do sistema contra eventuais catástrofes (inundações, violações).

A visita presencial permitiu verificar o modo ineficiente do uso do sistema SAP/R3, a insatisfação e/ou desconfiança dos utilizadores do sistema SAP/R3 no que respeita aos dados produzidos pelo sistema e no processamento dos dados, a má definição dos controlos internos de utilização, o ambiente organizacional e a vulnerabilidade do SAP nas empresas do grupo Petromoc.

Fez-se a pesquisa e referência bibliografica, para a elaboração do presente trabalho, isto para o melhor entendimento do sistema SAP/R3 e da auditoria nos mais variados aspectos por analisar, com bases científicas.

O *software* usado na elaboração deste trabalho foi o Microsoft Word 2000, para o processamento do texto.

1.4. Estrutura do trabalho

O trabalho está dividido em vários capítulos onde, no capítulo I é feita uma abordagem introdutória de auditoria, da auditoria de sistemas inseridos nas organizações, os problemas encontrados nas empresas que usam o sistema SAP/R3 quando este não for auditado e os objectivos do trabalho.

No capítulo II é apresentado um breve historial da auditoria, evolução histórica, controlo interno, as funções e o relatório final do auditor do sistema, a auditoria de sistemas informáticos, auditoria dos utilizadores, especialistas em TI, do ambiente organizacional e as vantagens da auditoria.

No capítulo III são apresentadas as técnicas de auditoria de sistemas de uma forma geral, das quais destaco, o questionário, entrevistas, análise de relatórios, visita presencial e o *software*.

O capítulo IV, aborda os principais aspectos relacionados com o sistema SAP/R3 (System application Product), em especial à visão geral do sistema, arquitectura cliente/servidor, tecnologia do sistema, registos mestres do usuário e às autorizações.

No capítulo V é apresentado o modelo proposto de auditoria do sistema SAP/R3 para qualquer empresa que usa o sistema. São mostradas as diversas fases de auditoria, as respectivas actividades e objectivos de cada fase.

O capítulo VI, está composto basicamente, pelo caso de estudo, que corresponde a implementação do modelo proposto nas empresas do grupo Petromoc.

CAPÍTULO II – AUDITORIA DE SISTEMAS DE INFORMAÇÃO

O desenvolvimento espontâneo dos sistemas e tecnologias de informação, acompanhado pelo crescimento progressivo das organizações e da complexidade das actividades organizacionais, fazem com que torne-se complexa a actividade de auditar SI como forma de garantir informação segura do desempenho da organização.

Por forma que o estudo da auditoria de sistemas de informação seja abrangente, neste capítulo são mostrados: o breve historial sobre auditoria, o controlo interno, as funções e o relatório final do auditor de sistemas, a auditoria de sistema informático, auditoria dos utilizadores dos sistemas, auditoria dos especialistas em TI, auditoria de segurança de sistemas informáticos, auditoria do ambiente organizacional e por fim, as vantagens da auditoria de sistemas.

2.1. Breve historial sobre Auditoria

Segundo Costa (2000:52), a auditoria surge na Grã-Bretanha nos meados do séc. XIX devido a revolução industrial. À medida que a actividade económica se desenvolve, mais útil se torna o seu controlo, pelo que as empresas sentem necessidade de implementar procedimentos contabilísticos e medidas de controlo interno, visando a obtenção de informação exacta e credível.

Tal como acontecia no início do séc XX, a auditoria tinha como objectivo fundamental de detectar erros e fraudes. É evidente que isto pode acontecer em consequência do trabalho e auditoria. Vista ainda como um exame sistemático das demonstrações económicas e financeiras (Balanço analítico, demonstração de resultados líquidos, Anexo, etc.) de uma empresa e ainda dos registos e operações efectuadas, com a finalidade de verificar se estão de acordo com os princípios de contabilidade geralmente aceites, com as políticas estabelecidas pela direcção e com qualquer outro tipo de exigências legais ou voluntariamente aceites (Nabais, 1993:92)

A cada vez maior utilização dos computadores no processamento das diversas operações das empresas levou ao desenvolvimento da auditoria informática praticada por técnicos internos ou externos da empresa (Costa, 2000).

Hoje em dia, inegavelmente, os avanços da informática e das tecnologias especialmente informáticas têm exercido efeito significativo na vida das organizações. Com a massificação do uso da tecnologia, particularmente da TI proveniente de base de dados[3] (BD) geradas por computadores, há necessidade de que as pessoas que actuam nas organizações, e delas fazem parte, evoluam na sua forma de agir e de pensar.

A esta alta tecnologia empregue nas organizações, justificada pela intenção de melhoria dos seus sistemas faz com que exista interesse por parte das organizações em fazer com que os seus sistemas (aplicações) produzam informação com finalidade de cumprimento dos seus objectivos estratégicos e do exercício das diversas actividades.

Esta informação produzida pelos sistemas deve ser credível por forma que a empresa atinja indicadores de desempenho desejáveis mais sobretudo credíveis. Daí a necessidade de auditorias de sistemas como forma de credibilizar as informações advindas dos SI das empresas.

Nesta óptica de ideia, a auditoria da área de Informática visa o alcance dos seguintes objectivos (Carneiro, 2004:17):

a) inventariar e avaliar os meios f'isicos e as tecnologias adequadas à recolha e processamento dos dados necessários à obtenção das informações necessárias;

b) examinar a existência de controlos apropriados e avaliar a sua eficácia;

c) concluir sobre a qualidade e a utilidade da informação obtida

d) garantir a montagem e a adequação de procedimentos e sistemas de controlo que assegurem a segurança do SI na sua realizaao directa com os materiais informáticos (*hardware* e *software*).

O crescente desenvolvimento das tecnologias e o uso intensificado das tecnologias computacionais no manuseamento da informação torna complexa a área de auditoria informática.

De um modo geral, a auditoria intervém em diversos domínios organizacionais, focalizando vários alvos.

[3] Base de dados refere- se ao conjunto integrado de dados, inter-relacionados, armazenados num dispositivo de armazenamento com acesso directo (Carneiro, 2001:274).

A auditoria pode apresentar sugestões de melhoria e até planos de acção para eliminar disfunções e fraquezas, as quais são incluidas no relatório final sob o nome de recomendações.

Vista como uma das ramificações de auditoria, a auditoria de sistemas concentra os seus esforços na análise e avaliação, quer envolvendo-se em processos de planeamento, desenvolvimento, testes e aplicação dos sistemas, quer examinando a estrutura lógica, fisica, ambiental, organizacional de controlo, segurança e protecção de dados (Carneiro, 2001:23).

2.2. Controlo Interno

O Controlo é um conjunto de procedimentos e métodos, cuja finalidade é vigiar as funções e atitudes das empresas, permitindo verificar se todas as operações são realizadas conforme os programas adoptados e as directrizes e principios estabelecidos(Carneiro, 2001:76).

O propósito de revisar a adequação do sistema de controlo interno, é de constartar se o sistema estabelecido, proporciona uma razoável segurança de que os objectivos e metas da empresa se cumpram de forma eficiente e económica (Datasoft, 2000).

O Controlo Interno informático verifica diariamente se todas as actividades dos SI estão a ser realizadas cumprindo os procedimentos, os padrões e as normas definidas pela direcção informática, assim como os requisitos legais (Carneiro, 2001:76).

2.3. Funções do Auditor de sistemas

Carneiro (2001:39) afirma que, o auditor de sistemas tem de cuidar da correcta utilização de todos os recursos que a organização utiliza para poder dispor de um sistema suficientemente eficiente e eficaz. Tem como função importante emitir um juízo global ou parcial baseado em factos e situações inteiramente correctas, mas não tem o poder para modificar a situação por ele analisada.

O auditor de sistemas dever ser um profissional de grande conhecimento da área de processamento de dados e todas as suas fases. Deve ter objectividade, descrição, raciocínio lógico e principalmente um sentimento real de independência, ou seja, em seus relatórios sejam eles intermediários ou finais, devem possuir personalidade e até mesmo os factos incorrectos na administração do auditado (Lawrence, 2000).

2.4. Relatório final do Auditor

Segundo Carneiro (2001), o relatório final é um documento técnico de carácter confidencial apresentado ao orgão de gestão com resultados da análise, de avaliação de recomendações correctivas e/ou que contribuam para um melhor nível de qualidade dos SI informatizados.

O relatório deve incluir apenas os factos que constituem problemas de relevante importância para os objectivos da auditoria em causa e as informações nele apresentadas têm de explicar com segurança esses mesmos factos.

Embora haja diversos tipos de relatórios tais como, relatórios preliminares, especiais, evidenciando maior complexidade, etc., mas de modo geral, a sua estrutura básica é composta pela introdução, apresentação do âmbito e dos objectivos da auditoria, as áreas auditadas, a caracterização da situação encontrada, nomeadamente, a descrição dos problemas detectados, comentários e recomendações correctivas que contribuam para um melhor nível de qualidade dos SI informatizados, terminando pela avaliação global do ambiente auditado (Anexo 17).
O relatório de auditoria pretende ser um factor de acção. Deveria, portanto, ser apresentado de tal forma que não dê margem para exitações na tomada de decisões correctivas.

2.5. Auditoria de Sistemas Informáticos

Segundo Auditoria Sistemas(2004), a auditoria de sistemas informáticos tem como objectivo avaliar a eficácia e eficiência com que se está operando com o sistema para que se tomem decisões que permitam corrigir os erros, no caso de existência, bem como melhorar a forma de actuação.

Os objectivos gerais da auditoria de sistemas informáticos são (ibidem):

- Assegurar uma maior integridade, confidencialidade e confiabilidade das informações;
- Garantir a segurança dos utilizadores, dos dados, do *hardware*, do *software* e das instalações;
- Buscar uma maior relação custo-beneficio dos sistemas automáticos;
- Conhecer a situação actual da área de informática para integrar os objectivos;
- Apoiar à função informática nas metas e objectivos da organização;
- Garantir a utilidade, confiança, privacidade e disponibilidade do ambiente informático;
- Garantir a capacitação e educação sobre controlos nos SI;

- Incrementar a satisfação dos usuários dos sistemas informáticos.

A realização da auditoria de sistemas informáticos tem de acompanhar as diferentes linhas de evolução da empresa nos seus processos tratados, pelo sistema e das várias tecnologias que estão incluídas no domínio das operações informáticas.

No fim da auditoria do SI Informatizado na organização, o auditor deve manter os dados em sigilo ou seja, divulgar à direcção ou administração que o tenha solicitado o serviço. Isto como forma de não criar constrangimentos indesejáveis que não interessam de forma alguma o bom desempenho da organização (Fantinatti, 1998).

2.6. Auditoria dos Utilizadores dos Sistemas

Sendo o utilizador por vezes o maior inimigo do sistema, a auditoria destes tem que ser conduzida de tal forma que, se torne transparente toda a operação por estes realizada quanto ao uso do sistema.

Como não se pode parametrizar o utilizador para que funcione de forma "*standard*", tem que se incorporar controlos a nível de *input*.

Estes controlos são para reduzir o risco de serem introduzidos no sistema erros de *input*, quando se trabalha em "*Batch input*[4]" ou seja, uma gama de informação diversa mas integrada, é introduzida num só ponto, os controles de "*Batch* e *Hash Totals*[5]" são fundamentais.

Os controlos internos de *input* e *output* referem-se, segundo Carneiro (2001:88), aos procedimentos manuais tradicionais que os utilizadores devem executar sobre os documentos e transações, antes e depois do seu processamento informático por forma a verificar o adequado e contínuo funcionamento dos controlos das aplicações.
Contudo, o controle de base fundamental é garantir que o utilizador conheça perfeitamente a funcionalidade que está a executar e a relação que existe quer amontante quer ajuzante do seu posto, entre a informação recebida e executada.

[4] Batch input refere-se ao método e ferramentas para importação rápida dos dados dos ficheiros sequenciais na base de dados R/3 (Brand, 1998:532).
[5] *Batch Total* refere-se ao somatório de um conjunto lógico de dados, como por exemplo, quantidades, códigos numéricos; enquanto que, *Hash Total* refere-se ao somatório de um conjunto ilógico de dados, como por exemplo, datas.

A auditoria dos utilizadores é feita usando as técnicas normais de auditoria de sistemas como, as entrevistas, questionários e as visitas presenciais (ver Anexos 4 e 14).

2.7. Auditoria dos especialistas em TI

Equipa de especialistas em TI é a equipa de técnicos profissionais que gerem, administram e programam o sistema na empresa em que o mesmo está instalado.

Esta equipa por ser constituida por pessoas, também existe o pequeno dilema de parametrização das suas actividades e seu comportamento. A operacionalidade começaria pela avaliação prévia dos programas pela equipa configurados, as parametrizações feitas e as autorizações ou permissões configuradas para os utilizadores comuns do sistema.

É através desta auditoria (Anexo 2), que a gestão da empresa auditada teria uma informação segura do trabalho desenvolvido pela equipa de especialistas em TI, de modo que sejam alcançados os objectivos pré-definidos na aquisição do sistema em causa.

Administrar um sistema integrado requer um elevado nível de conhecimento das ferramentas existentes no sistema, no tráfego da informação nos diversos módulos, na execução dos *backups* do sistema e ao *disaster recovery*[6], etc. Por estas e outras razões, a auditoria à esta equipa é conduzida com o objectivo de assegurar:

- o devido patentiamento do sistema em termos de contratos de aquisição, manutenção e assistência;
- a correcta execução dos *backups* do sistema;
- a correcta parametrização dos módulos;
- a correcta definição dos perfis dos utilizadores do sistema;
- os planos de contigência definidos para casos de eventos catastróficos;
- a segurança do *hardware*, *software*, da rede e equipamentos que compõem o sistema;
- a definição dos planos contínuos de formação aos utilizadores.

[6] Disaster recovery é o processo de planeamento estabelecido e teste dos procedimentos de recuperação, com a finalidade de prover serviços (Fantinatti, 1998:30).

2.8. Auditoria de Segurança de sistemas Informáticos

Segundo Carneiro (2002:136), perante o crescente valor da informação, baseada na construção de sistemas de TI e tecnologias de comunicação (TC), é indispensável que sejam estabelecidas protecções adequadas que venham a ser avaliadas ou recomendadas pela auditoria de segurança.

A auditoria da segurança está atenta em verificar se o dia-a-dia de operação do ambiente de segurança está em alinhamento com a informação da política de segurança. A política de segurança deve ser a base da auditoria. Sem uma política de segurança compreensiva não se consegue medir se está se conseguindo alcançar a meta de manter um ambiente seguro (Ucpel, 2005).

Aos equipamentos informáticos que suportam o SAP/R3 e o próprio sistema, devem ser garantidas seguranças eficazes para que os mesmos não se tornem vulneráveis. É deste modo que a auditoria de segurança foca a sua atenção em:

- Avaliar a protecção do acesso aos locais em que se encontram os servidores, as BD's e os *routers* do sistema SAP/R3;
- Avaliar a segurança dos equipamentos, se os mesmos estão sendo devidamente usados, respeitando as normas de utilização de computadores ou equipamentos sensíveis;
- Avaliar o nível de conhecimento dos utilizadores no que respeita a segurança do sistema;
- Verificar se os equipamentos informáticos não estão sob incidência de raios solares;
- Verificar a existência de interferências electromagnéticas nos locais em que está o sistema;
- Avaliar as instalações dos locais em que o sistema está inserido, referindo o estado de degradação destas;
- Avaliar e validar os planos de contigência dos equipamentos, isto no concernente à segurança.

Partindo deste pressuposto, os sistemas e equipamentos podem estar vulneráveis quando os devidos cuidados de segurança não forem tomados em consideração.

2.9. Auditoria do ambiente organizacional

Uma vez visto que os factores ambientais são aspectos que podem causar grandes prejuízos às empresas quando negligenciados, independentemente da boa qualidade dos equipamentos que as empresas possuam.

O auditor de sistemas por forma a averiguar a infra-estrutura ambiental, deve levar em consideração os aspectos seguintes:

a) qualidade da rede eléctrica: as oscilações de corrente ou se a rede eléctrica dos computadores é a mesma utilizada por outros aparelhos que consomem grande quantidade de corrente, como ar condicionados, geleiras, etc.;
b) temperatura adequada aos equipamentos, fazendo com que não sofram superaquecimento. Daí a necessidade de ventilação adequada dos equipamentos;
c) ambiente sem muita interferência electromagnética;
d) os raios solares não podem incidir directamente sobre os aparelhos;
e) humidade, pois, os computadores tem apresentado falhas nos ambientes húmidos;
f) aspectos ergonométricos.

Este e outros aspectos devem ser tomados enconta no processo de auditoria da infra-estrutura ambiental da organização (Anexo 7) onde os sistemas informáticos estão inseridos.

2.10. As vantagens da Auditoria de Sistemas

O processo de *auditoria* é de vital importância pois é através dela que a administração poderá e deverá ditar os rumos da empresa, isto para o caso de um evento catastrófico (fraudes, violações, etc) ocorrer junto à mesma (Fantinatti, 1998).

É neste sentido que, a auditoria de sistemas é importante na medida que as organizações na imagem da administração ou gestão ficam com o controlo exacto do seu negócio e onde direccionar os seus investimentos para melhoria da prestação dos seus serviços.

Das inúmeras vantagens da adopção de auditoria de sistemas informatizados, destacam- se as seguintes:

- Optimização dos métodos e procedimentos no uso do sistema;
- Diminuição de erros ou falhas no sistema e das fontes de vulnerabilidade mencionadas anteriormente (Ponto 9);
- Investimento optimizado nas TI que assegurem o correcto funcionamento do sistema;
- Transparência no uso do sistema;
- Incremento no nível de confiança dos utilizadores do sistema.

CAPÍTULO III - TÉCNICAS DE AUDITORIA DE SISTEMAS

Das diversas técnicas de auditoria de sistemas existentes são apresentadas as seguintes: questionários, entrevistas, análise de relatórios, visita presencial e *software*. Passamos a descrever de forma sintéctica para o melhor conhecimento das mesmas.

3.1. Questionários

O questionário é uma das técnicas de auditoria de sistemas que visam aquisição de informação correspondente ao sistema alvo de auditoria. Devem ser elaborados respeitando certos princípios vigentes nos questionários no geral como, perguntas cujas respostas sejam "sim/não" e com possibilidade de comentários caso necessário, um número não excessivo de perguntas e objectividade nas perguntas para que se colham informações pertinentes para o estudo (Gil, 1989:81).

A técnica questionário corresponde a elaboração de um conjunto de perguntas com objectivo de verificar determinado ponto de controlo, aderência aos parâmetros de controlo interno e dados quantitativos (Audy, 2000).

A sequência básica de aplicação de questionários à distância é (Gil, 1989:82):

- Analisar o ponto de controlo e elaborar o questionário;
- Seleccionar os profissionais auditados que deverão responder ao questionário;
- Elaborar um conjunto de instruções de como responder às questões;
- Distribuir/remeter o questionário para os profissionais seleccionados;
- Controlar a recepção dos questionários respondidos;
- Analisar as respostas às questões;
- Formar uma opinião do ponto de controlo auditado em decorrência das respostas obtidas;
- Elaborar relatório de auditoria.

Outro factor para o sucesso dessa forma de aplicação do questionário é a elaboração de perguntas que imponham respostas conclusivas e, de preferência quantificáveis (Gil, 1989:83).

3.2. Entrevistas

Além de possibilitar a consulta da documentação de que o auditor necessite, as entrevistas são uma das formas que este utiliza para obter informação relevante para o seu processo de análise. Estas podem obedecer a um método preestabelecido e correponder a finalidades bem definidas ou serem conduzidas de forma aberta ou semi-dirigida para que o entrevistado forneça todos os dados que lhe pareçam ter alguma relação com o tema em causa (Carneiro, 2001:113).

Normalmente as entrevistas devem ser previamente preparadas como forma de reduzir se o tempo desta e o alcance da informação relevante para o caso em análise. É deste modo que também não terão um carácter cansativo ou aborrecido para o entrevistado e, com uma marcação também prévia da data, hora, a duração e o local.

É aconselhável agora que o auditor considere as respostas a fim de saber qual o nível de controlo interno do ponto de controlo. Posteriormente o auditor tem condições para elaborar um relatório de fraquezas de controlo interno. Regra geral, as entrevistas são formas de tomar conhecimento das características de uma dada situação, que são acompanhadas por outras formas como a visita presencial e a utilização de questionários (ibidem:114).

3.3. Análise de Relatórios

Segundo Carneiro (2001:120), a análise dos relatórios sobre o controlo interno é uma técnica muito importante para se poder avaliar a eficácia do sistema e exige que sejam considerados aspectos como o nível de utilização de cada utilizador, a forma de distribuição desses relatórios, a sua maior ou menor confidencialidade e a utilização da informação que contêm.

Dado ser conveniente o estabelecimento de prioridades no processo de análise, a utilização desta técnica deve considerar a seguinte sequência (Carneiro, 2001:120):

- Reunir diversos relatórios que digam respeito ao ponto de controlo a ser analisado, conferindo- lhes uma arrumação adequada à continuação do trabalho de auditoria;
- Redigir um questionário e/ou *check-list*[7] destinado a fazer um levantamento completo da situação;

[7] Lista de tarefas, perguntas e outros elementos que pode ser utilizada pelo auditor como um auxiliar da memória (Carneiro, 2001:275)

- Com base nas informações destes relatórios, entrevistar os utilizadores e considerar os seus comentários e/ou informações complementares;
- Por último, fazer a análise de todos dados recolhidos dos relatórios e das entrevistas e formular um parecer sobre o nível de controlo interno.

Esta técnica é primordial para a avaliação do parâmetro eficácia do sistema (Gil, 1989:92).

3.4. Visita Presencial

A visita presencial de acordo com Audy, (1989:87) corresponde à actuação pessoal do auditor junto a sistemas, procedimentos e instalações do ambiente auditado.

Normalmente, combinada com outras técnicas de auditoria, particularmente questionário, a visita presencial implica o cumprimento da seguinte sequência de procedimentos (Gil, 1989:88):

a) Marcar data e hora com a pessoa responsável que irá acompanhar as verificações, ou convocá- la no momento da verificação quando o factor surpresa se tornar necessário:
   - A participação do auditado na mecânica, visita presencial, normalmente, é importante para o sucesso da aplicação da técnica por serem necessários esclarecimentos quanto a pontos nebulosos que ocorram;

b) Anotar procedimentos e acontecimentos, colectar documentos, caracterizar graficamente a situação via elaboração de fluxo de rotinas e de *layout* de instalações.
   - A aplicação do questionário e a cópia das respostas são particularmente importantes, pois permitirão, no trabalho futuro de elaboração do relatório de auditoria, consulta e recuperação fácil de factos referentes à verificação presencial feita;

c) Anotar nomes completos das pessoas e data e hora das visitas realizadas;

d) Analisar os papéis de trabalho obtidos, avaliar respostas e a situação identificada;

e) Emitir opinião via relatório de fraquezas de controlo interno.

A presença do auditor é fundamental para a constatação física da existência de activos computacionais da empresa, bem como seu estado de conservação e qualidade dos procedimentos de utilização (Gil, 1989:88).

3.5. Software

Até há alguns anos foram empregues "*packages*" de auditoria, que põem à disposição programas adequados para auditores que têm uma reduzida qualificação técnica no domínio da informática. Posteriormente, estes *softwares* integram uma vertente estatística, possibilitando assim, o estudo das prováveis consequências da situação real de uma instalação (Carneiro, 2001:132).

O *software* usado como técnica de auditoria nos sistemas em operação correlaciona arquivos, tabula e analisa o conteúdo, usualmente gerando cópias da base real. É um provê meios para obter acesso e manipulação de dados mantidos em sistemas computacionais (Audy, 2002).

CAPÍTULO IV - SYSTEM APPLICATION PRODUCT (SAP)

O *System Application Product* (SAP) é um conjunto de sistemas (módulos) integrados, com informações que interagem e se realimentam com os diversos módulos. O SAP é uma ferramenta robusta que proporciona uma maior confiabilidade dos dados e diminuição do retrabalho, dados estes monitorados em tempo real.

Neste estudo é apresentada a visão geral sobre o sistema SAP, a arquitectura cliente/servidor do sistema, a tecnologia do sistema, registos mestres do usuário e as autorizações.

4.1. Visão Geral sobre o Sistema SAP

SAP foi fundado em 1972 na Alemanha por cinco engenheiros da IBM, sendo hoje em dia a maior empresa do seu ramo. O seu sistema R/3 foi optimizado para gerir os processos de produção e gestão, logística e recursos humanos. O SAP R/3 é uma solução do tipo cliente/servidor e já existe há aproximadamente cinco (5) anos. A versão mais recente é a 4.0. A solução já possuí mais instalações que o anterior sistema, o SAP R/2. A principal diferença entre estes dois sistemas é que o R/3 utiliza uma arquitectura cliente/servidor enquanto que o R/2 utiliza mainframes (Silva, 2000).

O sistema SAP/R3 foi desenvolvido para satisfazer uma maior diversidade de processos de negócio de forma integrada, oferecendo um serviço completo à direcção da empresa em que o sistema está instalado e, é independente do ramo de actividade o qual o sistema se destina (Miller, 1998:329).

É pois, um sistema que suporta todo o processo de negócio nas empresas pois, a título de exemplo incorpora módulos aplicativos nas seguintes áreas (ibidem:383):

- Contabilidade Financeira (FI – *Financial Accounting*);
- Contabilidade Analítica (CO - *Controlling*);
- Recursos Humanos (HR – *Human Resources*);
- Planeamento da Produção (PP – *Production Planning*);
- Vendas e Distribuição (SD – *Sales & Distribution*);
- Administração de Materiais (MM – *Material Management*);
- Sistema de Projectos (PS – *System Project*);

- Soluções Industriais (IS – *Industry Solutions*);
- Segurança de Qualidade (QA – *Quality Assurence*).

Pela integridade dos módulos, complexidade em termos de processos tratados pelo sistema, isto requer elevados cuidados no uso do sistema sejam considerados pois, dados introduzidos num módulo afectam todos módulos do sistema.

O SAP/R3 é visto como um sistema *Enterprise Resource Planning* (ERP[8]), pois, segundo Kale (2000:13), um sistema ERP é um sistema integrado de aplicações, com vários módulos cobrindo as mais diversas áreas da empresa e processando a flexibilidade para configurarar e customizando dinâmicamente a funcionalidade entregada do pacote para servir as exigências específicas da empresa.

Dos diversos exemplos de sistemas ERP, destacam- se os seguintes (Silva, 2000):

1) SAP/R3;
2) Oracle Financials;
3) Baan IV;
4) Magnus;
5) Microsiga; e
6) Etc.

Pelos inúmeros módulos nestes sistemas faz com que as empresas que usam os ERP's, por si só, tenham um domínio exacto do seu desempenho, alterando ou redefinindo os seus processos de actuação no "negócio".

Os sistemas ERP apresentam características comuns como:

- uma única BD;
- módulos integrados que, os dados uma vez introduzidos são usados por qualquer módulo do sistema;
- a arquitectura cliente-servidor;
- complexidade de processos.

[8] ERP é uma abordagem estruturada para a optimização da cadeia de valor interna de uma empresa. Norris et al. (2001:4)

O sistema SAP/R3 como um exemplo de sistema ERP, existem neste possibilidades de parametrizações ou configurações segundo as necessidades específicas de cada empresa. É sim um sistema aberto permitindo que informações vindas de outras aplicações sejam acolhidas ao sistema.

Segundo Silva (2000), o *software* SAP/R3 apresenta as seguintes potencialidades:

- Facilita a existência de um SI integrado de todas as áreas funcionais de uma empresa;
- Executa as tarefas críticas de uma empresa, aumenta a qualidade dos serviços a clientes melhorando a imagem da empresa;
- Integração de todas as esferas de produção, que permitem unir a produção, venda e controlo financeiro numa só;
- Ajuste fácil a novas inovações tecnológicas: *Electronic Data Interchange* (EDI), *Internet*, *Intranet*, *Ethernet*, Vídeo Conferência, Comércio electrónico, etc;
- Existência de relacionamento com plataformas das maiores firmas produtoras;
- Fornece ferramentas inteligentes (suporte à decisão, informação executiva, *Dataminning*, prevenção de erros), permitindo maior facilidade na tomada de decisões.

4.2. Arquitectura Cliente / Servidor do sistema SAP/R3

Para Smith (1992), do ponto de vista do *software*, as arquitecturas cliente/servidor consistem em três (3) camadas, a saber:

- Camada de apresentação
- Camada de aplicação
- Camada de base de dados

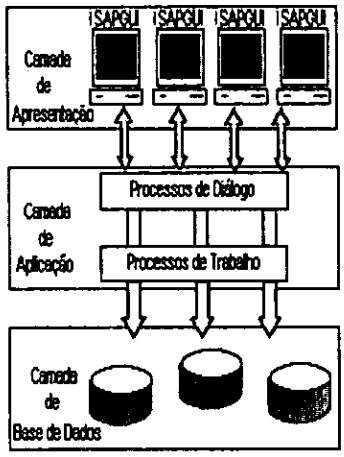


Fig1. Arquitectura cliente/servidor (Brand, 1998:57)

Do ponto de vista de *hardware*, estas três (3) camadas podem funcionar separadas em servidores diferentes ou todas juntas no mesmo servidor. O sistema R/3 também permite a distribuição dos níveis de apresentação e aplicação por múltiplos servidores (Will, 1998:2).

Por esta razão, esta configuração do exemplo do único computador é usada normalmente somente para finalidades de demonstrações ou de testes.

4.3. Tecnologia do Sistema SAP/R3

A tecnologia de rede padrão é usada entre as camadas que são distribuídas sobre múltiplos computadores, dentro das camadas, e para conectar o sistema R/3 ao mundo exterior (Will, 1998:8).

O sistema R/3 requer uma BD que tenha um sistema de gestão da BD relacional (SGBDR) como Oracle, Informix, MS SQL Server, ADABAS D e DB2 (Metzger e Roehrs, 1998:11).

Deste contexto, fala- se dos seguintes princípios dos sistemas abertos incluídos no SAP/R3:

- RPC – inclui em *Advanced Business Application Programming* (ABAP[9]/4) como RFC (chamada remota da função) constitui a relação da programação aberta de R/3 concedendo que outros sistemas estão conectados com as funções de R/3;
- CPI-C (*Common Programming Interface-Communication*) – utilizado para as comunicações programa-a-programa através de múltiplos sistemas;
- SQL – *Structured Query Language*;
- ODBC – *Open Data Base Connectivity*. São as normas utilizadas para o acesso aberto de dados aos dados comerciais de R/3 nas BD relacionais;
- OLE/DDE – *Object Linking and Embedding*. É o padrão principal para integrar as aplicações do PC com o sistema R/3;
- X.400/X.500, MAPI – *Messaging Application Programming Interface* & EDI. São as normas para as comunicações externas;
- As BD: Informix, Oracle, *Software* AG, Sybase;
- Sistemas Operativos: Unix, Open VMS, MPE/iX e Windows NT;
- *Front-end*: Windows, OSF/Motif, OS/2PM e Macintosh.

[9] ABAP É a linguagem de programação do sistema R/3 (Brand, 1998:530).

4.4. Registos Mestres do Usuário

Directamente após a instalação, um número padrão de clientes e de utilizadores estão disponíveis em R/3. Os utilizadores são sempre clientes-dependentes, isto é, são somente válidos no cliente atribuido a eles (Will, 1998:216).

Particularmente, o registo mestre do usuário deve conter o perfil desejado da autorização para o usuário específico (Brand, 1998:218).
Um usuário tem também uma senha, que deve-se introduzir quando entrar no sistema, e que pode ser alterada em qualquer altura. Ao entrar no sistema, pode ser seleccionada a lingua que preferir usar dentro das linguas disponíveis na instalação R/3. Pode-se também seleccionar uma língua no início de uma sessão quando criar um usuário (Will, 1998:217).

O nome do usuário e os atributos do usuário compreendem o registo mestre do usuário.
O registo mestre do usuário consiste nos seguintes elementos: Nome do usuário, Cliente atribuído, Senha, Endereço da companhia, Tipo de usuário, Menu de começo, Língua de início de uma sessão, Ajustes pessoais da impressora, Tempo da zona, Grupo da actividade, Autorizações, Data de expiração, Ajuste de parâmetro de defeito (ibidem:217).

4.5. Autorizações

As autorizações determinam que actividades um usuário de um tipo de usuário e de um grupo de utilizadores particulares pode executar (Will, 1998:222).

O perfil da autorização permite que se dê a um usuário as autorizações desejadas como uma unidade. Um perfil de autorização representa uma descrição do papel do trabalho em R/3. Por exemplo, se uma pessoa B tem as mesmas tarefas que a pessoa A e requer consequentemente as mesmas autorizações, pode se dar as pessoas B e A o mesmo perfil de autorização (Brand, 1998:218).

A execução apropriada das autorizações é um ingrediente crítico para a manutenção da segurança em um sistema R/3. Conformemente, exige um processo formal apropriado. Uma aproximação preferida envolve as seguintes etapas (Best, 2000):

1. Definir papél organizacional;
2. Identificação das funções R/3 (opções do menu) associadas com cada papel;
3. Identificação das autorizações requeridas para cada função;
4. Projectando autorizações e perfis;
5. Criando autorizações e perfis no sistema de desenvolvimento;
6. Autorizações e perfis testando no sistema de garantia de qualidade;
7. Transportando autorizações e perfis ao sistema de produção;
8. Atribuir perfis aos registros mestres do usuário.

CAPÍTULO V – MODELO CONCEPTUAL DE AUDITORIA DO SISTEMA SAP/R3

De um modo geral, por forma a realizar- se uma auditoria de um sistema em operação que esteja em concordância com os desenvolvimentos verificados tanto nos sistemas e/ou tecnologias de informação como na complexidade das actividades das organizações, faz com que, o auditor de sistemas tenha que inicialmente familiarizar- se com o ambiente organizacional o qual será auditado, sua infra-estrutura tecnológica, seus sistemas e aplicações de modo a adequar as normas de auditoria de sistemas à realidade da organização alvo (Gil, 1989).

É neste sentido que, o modelo de auditoria do SAP/R3 proposto com este trabalho, viria como um modelo de referência de carácter técnico e independente da entidade a ser auditada com a apresentação das fases do modelo conceptual ilustradas na figura2:

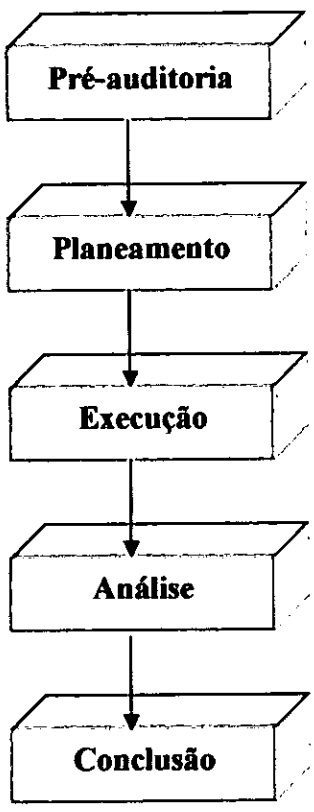


Fig.2: Fases de auditoria do sistema SAP/R3

Este modelo de auditoria apresenta cinco (5) fases, **pré-auditoria**, **planeamento**, **execução**, **análise** e **conclusão** como forma de alcance detalhado das diversas áreas de auditoria de sistemas em operação.

É importante que no final de cada fase de auditoria sejam preparados relatórios da fase, constando os objectivos da fase alcançados ou não, os constrangimentos identificados e as sugestões correctivas destes, isto para uma análise e elaboração do relatório final que seja sobre tudo fidedígno.

5.1. Fase de Pré-auditoria

Esta é considerada fase inicial da auditoria, segundo Fantinatti (1998:9), é nela que, é recebida a solicitação da equipa de auditoria, são detalhados os objectivos da auditoria, são preparadas equipas para auditoria e as datas do início e término da auditoria.

Inicialmente a entidade que será auditada prepara um documento formal solicitando uma auditoria, que no documento constam as razões para auditoria. É através deste documento formal que o sector de auditoria começa com as actividades e os seus respectivos planos de trabalho para auditoria solicitada.

O sector de auditoria solicita a entidade a ser auditada através dum documento para que sejam feitas sensibilizações a todos sectores ou departamentos, os especialistas em TI e todos utilizadores do sistema SAP/R3 em como será realizada uma auditoria. A sensibilização não é no intuíto de camuflar as informações, mas sim, para que a equipa de auditoria não seja vista como intrusa na organização e para que não se perca muito tempo na auditoria.

Ainda dentro desta fase, são feitas as primeiras reuniões da administração e o corpo de auditores, onde são revisadas as actividades, as áreas abrangidas, os funcionários da empresa que directa ou indirectamente darão auxílio a equipa de auditores e os planos de trabalho.

A figura3 ilustrada, mostra as actividades relevantes desta fase com os respectivos produtos:

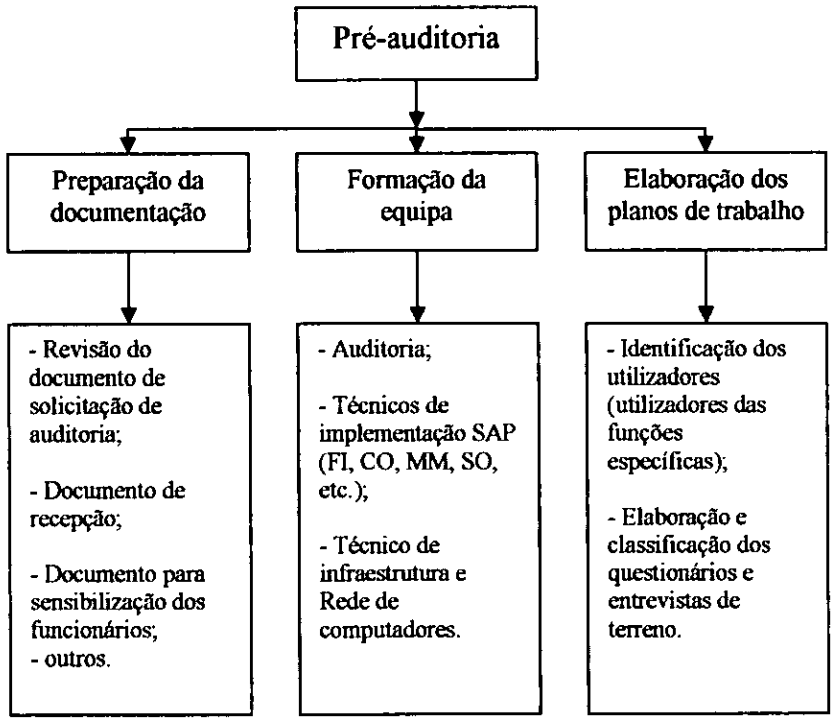


Fig.3: Actividades da fase de Pré-auditoria

A actividade da preparação da documentação tem em vista a revisão do documento formal de solicitação da auditoria por forma a que este, esteja claro quanto às razões para auditoria, as datas previstas da auditoria, documento para o envio à entidade que pretende ser auditada em gesto de confirmação ao documento formal recebido, etc.

A formação da equipa tem que ser de acordo com as razões para a auditoria do sistema SAP/R3 pois, ela pode ser para um simples conhecimento do desempenho da organização, não necessitando de uma equipa altamente composta. A formação da equipa tem que ser de modo a que seja feita uma auditoria que vá de acordo com às expetactivas da organização a auditar.

A equipa tem que ser composta por profissionais altamente competentes com conhecimentos de auditoria, técnicos de implementação do sistema R/3 nas diversos módulos (FI, MM, CO, SD, etc.), redes de computadores e conhecimentos técnicos de computadores. Assim sendo, o responsável da entidade que irá auditar o sistema deverá:

- ter conhecimentos de auditoria de sistemas e crítico nas análises das informções verificadas no processo de auditoria;
- distribuir a equipa de forma que utilize o máximo de competência técnico-funcional de cada integrante;

- focar as metas e os objectivos pertinentes ao cumprimento das actividades previamente planeadas;
- ser claro na explanação dos objectivos e áreas ou sectores com maior atenção por parte da equipa de auditoria;
- acompanhar cuidadosamente a par e passo, os trabalhos desenvolvidos pela equipa para que esta não se desvie ou perca muito tempo na realização do trabalho;
- pautar por ética e sobre tudo espírito de liderança;
- cobrar competência e produtividade dos integrantes da equipa;
- ter a habilidade de trabalho em equipa.

Os planos de trabalho devem ser tais que, a auditoria seja concretizável com os mesmos. Deste modo, o plano de trabalho deve ser cuidadosamente elaborado, muito bem definidos os tempos por cada fase ou etapa da auditoria com as respectivas actividades e pessoal da equipa de auditoria empregue por cada fase.

Os objectivos desta fase são:

1) Elaborar documento sobre a auditoria solicitada;
2) Formar a equipa de auditoria;
3) Traçar plano de trabalho adequado a entidade a ser auditada.

5.2. Fase de Planeamento de Auditoria do Sistema SAP/R3

É considerada como a segunda fase de auditoria pois, é através dela que será direccionada a auditoria, isto pelo conhecimento preliminar da organização e do sistema.

A equipa de auditoria deve estudar a organização a ser auditada quanto à estrutura de implementação do sistema, sistema de alimentação eléctrica, segurança contra eventos catastróficos, segurança das TI, segurança dos utilizadores, sala do servidor, os módulos do SAP/R3 a que os utilizadores estão permitidos a aceder, entre outros aspectos.

A fase de planeamento de auditoria do sistema SAP/R3 inclui as seguintes actividades mostradas na figura abaixo:

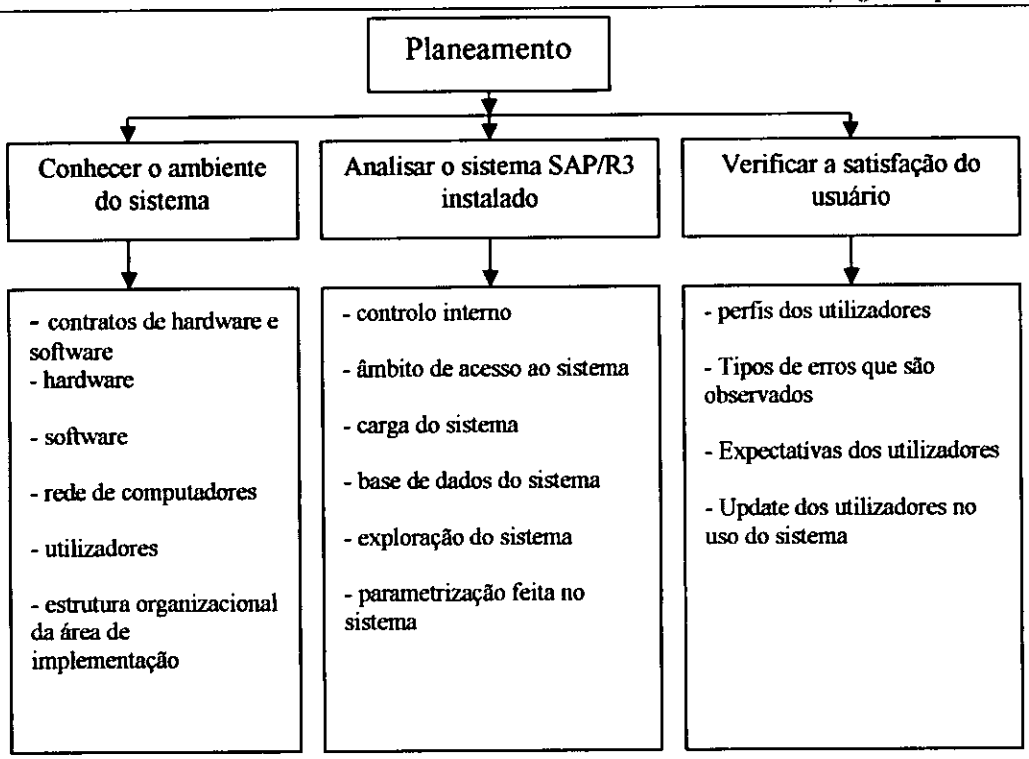


Fig.4: Actividades da fase de Planeamento

5.2.1 Conhecimento do Ambiente do Sistema SAP/R3

É uma actividade da fase de planeamento porque é nesta actividade que o auditor toma conhecimento dos contratos de *hardware*, de *software* e de aplicativos.

São também vistos os recursos computacionais ou não que lidam com o sistema SAP/R3 existente na organização e a própria organização.

No que respeita aos contratos, os objectivos definidos segundo Gil (1989:126), são os de assegurar que as transações de compra, venda, aluguer, *leasing*, seguros e manutenção dos equipamentos (*hardware*) disponíveis no ambiente computacional, bem como as transações de compra, alocação e manutenção de *software* (básico, de apoio e aplicativo) estão respaldadas pelos respectivos contratos, assim como as cláusulas componentes, no tocante a aspectos financeiros, operacionais, técnicos e administrativos, são de interesse da organização.

Uma verificação geral dos contratos inclui (ibidem):

- Aprovação pelo departamento jurídico;
- Data da celebração;

- Validade e autencidade das assinaturas;
- Vigência e situações de rescisão;
- Condições de pagamento;
- Critérios de reajustes de preços;
- Adendos e suas implicações;
- Número e tipo de utilizadores licenciados.

Quanto aos recursos computacionais, esta actividade visa o conhecimento dos seguintes recursos:

- *Hardware*;
- *Software*;
- Meio ambiente da organização;
- Rede de computadores;
- Utilizadores;
- Estrutura organizacional da área de implementação do SAP/R3;

Para o conhecimento destes recursos são recomendadas as técnicas de auditoria de sistemas em operação que, segundo Magalhães et al. (2001:146), são a prior, o contacto com especialistas em TI dos sistemas em operação por meio de visitas presenciais, entrevistas e questionários. Nesta actividade o recurso correspondente ao meio ambiente da organização será avaliado na auditoria usando a visita presencial como técnica de auditoria do sistema.

A visita presencial, a entrevista e o questionário como técnicas de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de meio ambiente organizacional visam avaliar a razoável segurança física:

- Sistema de alimentação eléctrica, pois pode- se dar o caso de estarem ligados aparelhos que consomem tanta corrente como aparelhos de ar condicionado, geleiras, fogões, etc. A existência de estabilizadores e geradores de corrente nos casos de queda de corrente, mantendo os computadores e equipamentos funcinando em condições desejadas. Neste ponto, são também vistas as blindagens dos cabos e calhas de suporte para evitar ataques de predadores e água;
- Segurança contra eventos catastróficos como inundações e incêndios;

- Segurança das tecnologias de informação contra humidade, fogo e inundações. Esta segurança é referente a existência de sistemas de detenção de fogo (extintores, mangueiras de água, etc.), e de brigadas de incêndio;
- Segurança dos utilizadores;
- Controlos de acesso ao ambiente, referente a identificação por via de leitores ópticos aos cartões dos utilizadores ou funcionários da empresa, impressões digitais, assinaturas, retina, senhas, telefones internos, etc.;
- Segurança das construções; São aqui vistos o estado de degração das instalações físicas (paredes, tecto e o piso) e, do plano de contigência para situações inesperadas.

A visita presencial como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de h*ardware* visa avaliar e validar:

- A existência de segurança física do *hardware*;
- A existência de humidade nos locais em que se encontra o *hardware*;
- A existência de raios solares directamente insidindo sobre *hardware*;
- A temperatura ambiente onde se localiza o *hardware*, isto é, a existência de ventilação onde se encontra o *hardware*;
- Interferências electromagnéticas no local em que está o *hardware* do sistema.

A visita presencial como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de *software* visa avaliar e validar:

- A configuração do sistema;
- A existência de segurança lógica do *Software*;
- A utilização do processador;
- A utilização da memória;
- *Performance* da BD;
- Arquitectura da BD;
- Os tempos de resposta por transação;
- Os tempos de resposta de programas desenvolvidos.

A visita presencial como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de rede de computadores visa avaliar e validar:

- O tipo de cablagem usada;

- Os *routers* e *hubs* usados em termos de capacidade;
- A configuração da rede.

A visita presencial como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de utilizadores visa verificar:

- O grau de conhecimento dos utilizadores no uso do sistema;
- Os factores ergonométricos, isto é, a disposição dos utilizadores com os computadores;
- Os tipos de problemas mais frequentes no uso do sistema;
- Erros ou falhas frequentemente cometidas e como são solucionadas.

A entrevista como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de h*ardware* visa verificar (ver Anexo 5):

- Se os contratos de aquisição, manutenção e aluguer do *harware* existentes na empresa são referentes aos padrões estabelecidos pela gestão do topo;
- O *hardware* usado para o suporte do sistema;
- Os problemas ou erros devido o *hardware* usado;
- Como são solucionados problemas que advém do *hardware*;
- A manutenção preventiva;
- A manutenção correctiva;
- Os planos de contigência para o *hardware* do sistema.

A entrevista como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de *software* visa (ver Anexo 6):

- Verificar se os contratos de aquisição e manutenção do *Software* se cumprem com as normas estabelecidas pela gestão do topo;
- Verificar a existência dos mecanismos de segurança lógica definidos;
- Tempos de resposta de programas desenvolvidos;
- Erros ou falhas do *software*.

A entrevista como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de rede de computadores visa verificar (ver Anexo 9):

- O tipo de rede implementada;

- Problemas comumente apresentados pelos utilizadores do sistema relacionados com a rede de computadores e por fim, avaliar o desempenho da rede.

A entrevista como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de utilizadores visa verificar (ver Anexo 4):

- O nível de fomação da área específica para a actividade que desempenha;
- O nível de conhecimento para utilização do sistema SAP/R3;
- As limitações e/ou constrangimentos de utilização do SAP/R3;

O questionário como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de *hardware* visa (ver Anexo 12):

- Verificar se os contratos de *hardware* foram aprovados pela gestão do topo;
- Os contratos de aquisição, aluguer e manutenção do *Hardware*.

O questionário como técnica de auditoria do sistema SAP/R3 na actividade de conhecimento do ambiente em termos de *software* visa (ver Anexo 13):

- Verificar a existência dos mecanismos de segurança lógica definidos;
- Os contratos de aquisição e manutenção do *software*.

5.2.2 Análise do Sistema SAP/R3

Na análise do sistema SAP/R3 serão feitas análises do controlo interno, da BD, da carga no sistema, da capacidade do *hardware*, análise da rede de computadores, exploração do sistema SAP/R3 e da parametrização.

Esta é uma actividade que tem como um dos principais objectivos a verificação das licenças dos utilizadores e do âmbito de acesso ao sistema se está equilibrado. O âmbito de acesso é referente a possibilidade de entrada de intrusos ao sistema já que aconselham-se mecanismos para manter o ambiente das empresas livre.

Deste modo, podem ser analisadas as *passwords*[10] dos utilizadores de forma que as mesmas possam ser reinicializadas periódicamente e o comprimento ou número de caractéres da *password* faça com que tentativas para a descoberta da *password* verdadeira seja quase que remota.

É nesta actividade que também são vistas as parametrizações "*standard*" do sistema SAP/R3 e dos programas específicos desenvolvidos por forma a verificar se estes adequam- se aos processos de negócio da empresa.

Nestes programas desenvolvidos, serão avaliados em termos de documentação dos mesmos, testes e se foram feitos por pessoa(s) diferente da que desenvolveu e se os mesmos fazem o que expetactivamente deveriam fazer. Deve- se ter o cuidado da verificação da documentação de qualquer alteração que seja feita ao programa desenvolvido.

A análise do sistema é efectuada usando as técnicas de auditoria de sistemas em operação como visitas presencias e entrevistas observando a análise da carga no sistema, análise da BD, análise da capacidade de *hardware*, análise da rede de computadores e a análise à exploração do sistema.

Análise do controlo interno consiste nos seguintes parâmetros:

- Fidelidade da informação em relação ao dado;
- Segurança física;
- Segurança lógica;
- Confidencialidade;
- Segurança ambiental;
- Eficiência.

Análise da carga no sistema consiste em (Roff[11], 2005):

- Distribuição por módulo;
- Distribuição por programa;
- Distribuição por transação;

[10] *Password* é um método muito usado nas aplicações de software para garantir a segurança de acesso (Coelho, 1998:350).

[11] As análises da carga, base de dados, capacidade de *hardware* rede de computadores e à exploração sistema são do Roff por este apresentar maior clareza em relação aos outros estudados.

- Distribuição por período;
- Distribuição por processos;
- Distribuição por utilizador.

Análise da BD do sistema consiste em:

- Desempenho da BD;
- Crescimento da BD (tablespaces, tabelas, extent);
- Disponibilidade e recuperação da BD (*backup online*, *backup offline* e a sua periodicidade);
- Permissões de acesso a BD;
- Verificação de tablespaces;
- Verificação de tabelas;
- Verificação de índices.

Análise da capacidade de *hardware* do sistema SAP/R3 consiste em:

- Configuração do sistema;
- Utilização do processador;
- Utilização da memória.

Análise da rede de computadores que correm os dados do sistema SAP/R3 consiste em:

- Gestão da rede;
- Segurança lógica e física da rede;
- Falhas e interrupções do serviço;
- *Software* de rede;
- Controlo de alterações;
- Plano de contigência.

Análise à exploração do sistema SAP/R3 consiste em:

- *Dumps* no sistema;
- Erros no *log* do sistema;
- Erros de *update*;
- Programas de reorganização;

- Qualidade dos *buffers*[12] do sistem.

A visita presencial como técnica de auditoria do sistema SAP/R3 no estudo das autorizações e permissões configuradas no sistema visa:

- Averiguar se autorizações configuradas estão sendo devidamente implementadas;
- Reportar anomalias verificadas nas autorizações configuradas.

A visita presencial como técnica de auditoria do sistema SAP/R3 no estudo das senhas dos utilizadores configuradas no sistema visa:

- Reportar as senhas usadas por mais de um usuário e os respectivos utilizadores;
- Reportar as senhas que tem feito tentativas fraudulentas ou acedido em módulos do sistema que não tem previlégio.

A entrevista como uma das técnicas usadas na auditoria do sistema SAP/R3 no estudo das autorizações e permissões configuradas no sistema visa verificar:

- As permissões de cada usuário do sistema;
- Os utilizadores que tem feito acções fraudulentas no sistema SAP/R3;
- As configurações feitas estão sendo devidamente implementadas.

A entrevista como técnica de auditoria do sistema SAP/R3 no estudo das senhas configuradas visa:

- Verificar o número de utilizadores que usam a mesma senha;
- Verificar e avaliar os problemas que normalmente tem ocorrido com os utilizadores que usam a mesma senha.

As parametrizações *standards* do sistema serão validadas pelo estudo do sistema e as dos programas desenvolvidos serão baseados em testes destes.

5.2.3 Verificar a Satisfação dos Utilizadores

Segundo Rosini e Palmisano (2003:66), os trabalhadores manuais e burocráticos estão deixando de existir, para dar lugar a trabalhadores de maior conhecimento, criatividade, competência, transparência e flexibilidade.

[12] Memória na qual são temporariamente conservadas informações e dados, que são produzidas e utilizadas a ritmo diferentes (Carneiro, 2001:274).

A satisfação dos utilizadores do sistema SAP/R3 começa pela sensibilização destes por parte da gestão da empresa, da formação contínua e qualitativa no uso do sistema, nas remunerações, no ambiente de trabalho existente na empresa e na própria robustez que o sistema SAP/R3 proporciona.

Esta actividade tem como principal objectivo o da análise do perfil dos utilizadores pois, a criação do perfil do utilizador é uma das tarefas mais difícies na administração do sistema SAP/R3.

São revistas nesta actividade as senhas dos utilizadores usadas ou compartilhadas por mais de um usuário, as senhas criadas no sistema e não são usadas por qualquer que seja o motivo e por fim, as senhas com perfis que são além das tarefas do utilizador no sistema. Tanto os perfis como as senhas dos utilizadores devem estar devidamente documentadas e qualquer alteração nestas também deve afectar a documentação resultante.

A verificação da satisfação dos utilizadores é também na intenção de aumentar a produtividade destes, começando por analisar aspectos sociais e humanos que possam causar um fraco desempenho dos utilizadores.

A insatisfação dos utilizadores pode fazer com que actos de vandalismo e fraudulentos sejam efectuados, sendo de uma forma geral a empresa em que estes se encontram a maior prejudicada, fazendo ainda com que, baixos níveis de desempenho da empresa sejam verificados.

Os principais objectivos da fase de planeamento são:

1) Conhecer o ambiente do sistema;
2) Analisar o sistema SAP/R3 instalado;
3) Verificar a satisfação do usuário.

5.3. Fase de Execução da Auditoria do Sistema SAP/R3

É considerada fase do modelo proposto pois, nela é mostrada a metodologia a ser usada na auditoria do sistema SAP/R3. A metodologia caracteriza- se por uma abordagem *top-down*, que em cada ponto a baixo descrito são mostrados constrangimentos, se estes existirem, e as recomendações, iniciando da seguinte forma:

- Descrever de forma sumária a empresa a ser auditada;
- Analisar o ambiente organizacional quanto à estrutura de implementação do sistema, sistema de alimentação eléctrica, segurança contra eventos catastróficos, segurança das TI, segurança dos utilizadores, sala do servidor;
- Verificar os contratos de hard e *software*, de aplicativos, de aquisição e/ou de manutenção do sistema e da rede de computadores;
- Verificar as licenças dos utilizadores do sistema;
- Verificar os controlos internos, os planos de contigência, os programas instalados e removidos;
- Verificar que o âmbito de acesso ao sistema está equilibrado;
- Verificar os perfis dos utilizadores e a parametrização do sistema standard e dos programas desenvolvidos;
- Analisar o sistema SAP/R3, os diversos módulos do sistema em uso, a carga do sistema, a exploração do sistema, a BD e a rede de computadores.

5.4. Fase de Análise da Informação Colhida na Fase Anterior

Nas fases anteriores foram colhidas informações que podem ser discrepantes, necessitando de uma análise exaustiva destas para um juízo final que corresponda a verdade do sistema SAP/R3 instalado na empresa auditada. Esta análise deve ser cuidadosamente feita pela equipa de auditoria para que a mesma reflicta uma auditoria transparente do sistema em operação.

É desta forma que após a análise, serão feitas reuniões onde serão expostos os factos identificados e é entregue um relatório ao representante da empresa auditada para que este analise e emita no caso de desacordo, um outro relatório por escrito, apresentando as razões de estar em desacordo.

Estas razões deverão ser revistas pela equipa de auditoria e no caso de permanência do juízo final divulgado pela equipa, as razões não aceites pela equipa de auditoria farão parte do relatório que é, segundo Fantinatti (1998:9), denominado Sumário Executivo, o qual será apresentado para o cargo máximo da empresa, ou seja, a presidência; isto em forma de apresentação.

Esta fase também caracteriza- se pela preparação da documentação da auditoria finda e os respectivos relatórios para que estes sejam conservados em locais seguros, pois estes poderão ser usados como base em futuras auditorias.

5.5. Fase de Conclusão

A fase de conclusão da Auditoria é nela que, o grupo auditor emite um relatório detalhado de suas actividades, composto dos seguintes itens (Fantinatti, 1998:9):

- Objectivo da Auditoria;
- Áreas cobertas pela revisão;
- Factos identificados (Anexo 16);
- Acções recomendadas (Anexo 16);
- Datas de realização da auditoria;
- Funcionários questionados ou entrevistados; e
- Avaliação global do ambiente auditado.

CAPÍTULO VI - CASO DE ESTUDO: AUDITORIA DO SISTEMA SAP/R3 DAS EMPRESAS DO GRUPO PETROMOC

O caso de estudo é referente a implementação do modelo conceptual de auditoria que consta no capítulo anterior, precisamente a **fase de execução**; Estão exclusas as restantes fases do modelo conceptual na presente implementação, por se tratar de uma auditoria meramente didáctica.

Sendo trabalho didáctico e fazendo parte da empresa em estudo, pressupôs-se o conhecimento do ambiente organizacional, os utilizadores e o sistema SAP/R3 instalado. Deste modo, às recomendações de cada ponto do estudo foram propostas por especialistas de cada área.

Assim, a fase de execução, apresenta a abordagem a ser seguida no momento da implementação do modelo conceptual obedecendo os seguintes pontos:

6.1. Introdução sobre a empresa Petromoc

A Petróleos de Moçambique (Petromoc) SARL, é uma companhia pública, criada em 1 de Maio de 1999, com o Estado a deter 80 % do seu capital e 20 % a que tem como accionistas os próprios trabalhadores. É a empresa pioneira na introdução e comercialização de combustíveis após o período da independência nacional, considerada líder no sector de distribuição e comercialização de derivados de petróleo (M-Global, 2002).

A empresa existe há mais de vinte e quatro (24) anos, e possui delegações por todo o país em forma de pontos de distribuição, depósitos e terminais. As suas facilidades de armazenamento compreendem dezanove (19) depósitos com aproximadamente 499,772 m3 de capacidade. As vendas e volumes totais situam-se em torno de 236,110 m3 e 93,515 m3 por ano respectivamente (ibidem)

Como forma de obtenção de maior produtividade e eficiência no tratamento dos processos da sua principal actividade, foram discentralizadas actividades formando-se pequenas empresas em que a Petromoc é o seu principal accionista ou seja, o accionista maioritário.

Deste processo de discentralização surgiram empresas como a PETROGÁS, PETROMOC E SASOL, SOMOTOR, E-BUSINESS SYSTEMS (EBS) e PETROAUTO. Sendo deste processo ainda que a área dos SI e TI da Petromoc fica na responsabilidade da EBS.

Segundo o modelo de referência proposto de auditoria do sistema SAP/R3, ilustrado no capítulo anterior, é feita de seguida a auditoria do SAP/R3 das empresas do grupo Petromoc seguindo cada uma das fases que do modelo fazem parte com a ilustração da metodologia que é mostrada na fase de execução da auditoria:

6.2. Ambiente Organizacional

6.2.1 Estrutura da Área de Implementação do SAP

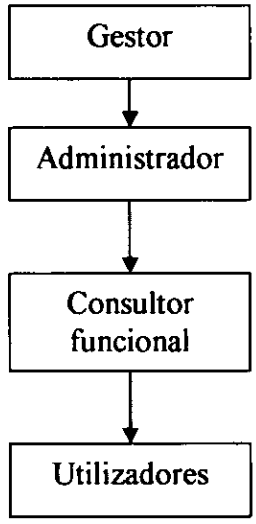


Fig.5: Estrutura da área de implementação do SAP

6.2.2 Sistema de Alimentação Eléctrica

A instalação eléctrica possui as seguintes características:

⇒ Voltagem entre terminais de neutro e terra: ~5v

⇒ Voltagem entre terminais de fase e terra: ~220v

⇒ oltagem entre terminais de fase e neutro: ~220v

Na instalação eléctrica com as características mostradas acima, existe um circuito extra de protecção que estão ligados aparelhos informáticos em cada andar do edifício da Petromoc sede e também UPS's que alimentam estes circuitos. Existe um (1) gerador de 175 kva de corrente para casos de abastecimento de corrente na falta de corrente.

Os equipamentos informáticos existentes na Petromoc estão dispostos por forma que estejam distantes das janelas que eventualmente haja incidência de raios solares sobre os equipamentos. Também as janelas possuem percianas que também impedem a entrada de raios solares sobre os equipamentos.

O soalho das salas em que existem equipamentos informáticos, são de parquet que não permitem descargas electromagnéticas que interfiram no funcionamento normal dos equipamentos informáticos da empresa.

Constrangimento:

Quando o gerador estiver em funcionamento pela falta de corrente eléctrica na sede da Petromoc, estando simultâneamente ligados os equipamentos informáticos e outros aparelhos como geleiras, ar condicionados, elevadores, fogões, após 3 horas de tempo o gerador descarrega-se causando deste modo a paralização do servidor e das actividades no sistema nos locais fora da sede em que tenham corrente eléctrica.

Recomendação

1) Adquirir um gerador com capacidade de 250 kva ou mais, para que possa levar muito tempo em funcionamento com estes equipamentos ligados, ou
2) Desligar aparelhos como elevadores, arcondicionados, geleiras, fogões, entre outros no momento de falta de corrente, permanecendo os equipamentos informáticos que a sua operacionalização é indispensável.

6.2.3 Segurança contra eventos catastróficos

Em cada andar do edifício sede da Petromoc sede, existem extintores e condutas para mangueiras de água no intuíto de extinguir eventual fogo intencionalmente ou não existente nas instalações.

Para o processo de extinção do fogo, existe uma pequena equipa afecta à sede para fogo de pequenas proporções e no caso de grandes proporções é solicitada uma equipa altamente treinada para o efeito que se encontra na terminal da Matola.

Constrangimento:

Falta de medidas ou mecanismos de prevenção contra inundações e que possivelmente possam destruir os equipamentos informáticos e os dados do sistema SAP/R3.

Recomendação

Estudar em colaboração com o Município o saneamento da zona e usar um servidor como *disaster recovery* estando localizado num edificio diferente e distante do edificio da Petromoc sede.

6.2.4 Segurança das Tecnologias de Informação

Visa proporcionar mecanismos para assegurar a devida operacionalização das TI reduzindo significativamente a destruição destas por eventos catastróficos e/ou negligência por parte dos utilizadores.

As TI estão num ambiente livre de poeiras, minimizando a acumulação de poeiras nos componentes, mantendo assim a capacidade de arrefecimento destas.

As TI estão também num ambiente com humidade normal evitando que chegue ao ponto de condensação.

Constrangimento:

Não tem definidas e/ou implementadas políticas de segurança das suas TI que tenham a ver com os aspectos ergonométricos, o que pode resultar na danificação das TI ou avarias frequentes destas se forem negligenciadas ou não consideradas.

Recomendação

Desenvolver e documentar políticas de segurança das TI que tenham em consideração à aspectos ergonométricos, isto para manter a devida operacionalização das TI.

6.2.5 Segurança dos Utilizadores

Para este caso, o sistema de controlo de acesso é semi-automático que é via interfones e por empresa especializada que garante a segurança fisica e permite a entrada de pessoas autorizadas ao edificio.

Os equipamentos informáticos estão dispostos em salas em que, são trancadas a chave após o final da jornada laboral.

Constrangimento:
Não é feito o controlo de presenças dos funcionários usando sistemas informáticos e muito menos manuais fazendo com que não exista o controlo da assiduidade destes.

Recomendação
Implementar um sistema automático que faz este controlo e esteja ligado ao SAP/R3 para o devido controlo de presenças dos funcionários desde a entrada até saída com o respectivo registo de horas.

6.2.6 Sala do Servidor do Sistema SAP/R3

O servidor do sistema SAP/R3 encontra-se numa sala de acesso restrito somente à pessoas autorizadas através da identificação por sistemas de controlo de acesso via cartão óptico, como forma de garantir a proteção do sistema contra possíveis actos de sabotagem ou perdas não intencionais dos dados nele armazenados.

Esta sala possui um sistema de frio composto por ar condicionado de 24000 BTU's com uma temperatura ambiente entre 18 °c – 20 °c fazendo com que os equipamentos estejem isentos de super aquecimento.

Existe um sistema automático de detenção de incêndio para casos de existência de fogo na sala do servidor e, o sinal é transmitido à empresa de seguros contratada para o efeito.

Constrangimento:

A disposição da sala não oferece muita segurança aos servidores nele existentes, devido a existência de janelas que ficam abertas por vezes para a passagem de ar quando o sistema de frio não está em funcionamento, deixando vulnerável os equipamentos imformáticos do recinto.

Recomendação

Manter a sala sem janelas e o sistema de frio nela existente deve estar em óptimas condições de funcionamento, ligado a gerador que permite a continuidade do funcionamento por muito tempo mesmo com a falta de corrente no recinto.

6.3. Contratos do Sistema Informático

Os contratos do sistema informático existentes nas empresas do grupo Petromoc estão subdivididos da seguinte forma:

- contratos de propriedade do sistema SAP/R3, contratos de manuntenção do SAP/R3, contratos de Manutenção das máquinas (computadores), Contratos de Manutenção de servidores, Contratos de Manutenção da rede de computadores.

O contrato de manutenção do sistema SAP/R3 é correspondente a uma assistência *offline*, isto é, envio de mensagem à SAP sobre certos constrangimentos verificados que posteriormente são respondidas. São disponibilizados *upgrades* do sistema em CD que a sua utilização não é obrigatória, dependendo do cliente.

O contrato de manutenção de servidores foi estabelecido com a empresa Cornastone em que figuram serviços de assistência respeitantes ao *hardware* e ao *software*.

O contrato de manutenção da rede e dos computadores está firmado com a empresa EBS de em que figuram serviços de assistência aos computadores e a rede de computadores, mantendo a devida operacionalização dos computadores e a comunicação entre os diversos pontos distribuídos ao longo da cidade e do país.

No que respeita aos contratos do sistema informático, não foram encontrados constrangimentos pois todos os contratos estão referentes aos padrões estabelecidos pela gestão das empresas, no que repeita às cláusulas.

6.4. Licenças dos Utilizadores

Correspondem a autorização formal dos utilizadores do sistema por forma a que seja garantida a utilização perfeita. As licenças estão de acordo com o tipo de utilizador do sistema dos quais os utilizadores operacional, do sistema, *basis component* e *workflow*.

O número de licenças do sistema adquiridas excedem o número de utilizadores permitindo assim a segurança do trabalho de cada utilizador. Algumas senhas nunca foram usadas mas estão alocadas aos utilizadores.

6.4.1 Constrangimento:

Partilha de senhas pelos utilizadores causando por vezes a adulteração de dados introduzidos por um determinado utilizador, responsabilização de erros cometidos ou transações ilegais praticadas intencionalmente ou não.

Recomendação

1) Distribuir senhas aos *keyusers* do sistema e que estas não sejam compartilhadas. Caso contrário, as senhas com previlégio de introdução e alteração dos dados são para os *keyusers* e que não sejam compartilhadas, e podem ser partilhadas senhas com previlégio de consulta aos restantes usuários, ou

2) Atribuir senhas que não são usadas ou as senhas ainda não exploradas aos utlizadores que pretendam usar o sistema, de modo que se tenha um uso minimamente perfeito destas.

6.4.2 Constrangimento:

Existem utilizadores com senhas que nunca foram usadas no sistema o que faz com que haja partilha de senhas pelos utilizadores e custos avultados pela aquisição de senhas que não são usadas.

Recomendação

Atribuir as senhas à utilizadores que possam fazer uso destas.

6.5. Controlos Internos

Existem políticas de controlo interno *online* que permitem garantir a extração de dados fiáveis no sistema.

Os controlos internos são concebidos e implementados pelo Departamento de Organização e Métodos (D.O & M) da Petromoc que, ainda não efectua controlos internos informáticos no concerne a actividades nos sistemas informáticos.

6.5.1 Constrangimento:

Inexistência de fidelidade dos dados gerados pelo sistema, isto devido a não fidelidade dos dados introduzidos no sistema.

Recomendação

Definir medidas de controlo interno eficientes dos dados manualmente tratados e da introdução feita ao sistema.

6.5.2 Constrangimento:

Inexistência de políticas de confidencialidade das informações tratadas pelo sistema.

Recomendação

Elaborar políticas de confidencialidade das informações tratadas pelo sistema e documentar para que após a sensibilização aos trabalhadores estas sejam seguidas.

6.5.3 Constrangimento:

Descontentamento da maior parte dos utilizadores do sistema devido a falta de conhecimento suficiente para a exploração adequada do sistema.

Recomendação

Seleccionar *keyusers* à formação e que os mesmos podem ser responsáveis pela formação "*on job*" dos restantes users.

6.6. Planos de Contigência

Dos diversos tipos de contigência importa realçar os seguintes:

1) *Processo de contigência em caso de falha do servidor*

A realização de cópias eficientes (*backups*) confere segurança contra perda de dados, mas não oferece proteção contra interrupção do funcionamento do sistema.

Constrangimento:

Paralização do sistema devido as falhas do servidor afectando as actividades de lençamentos e pesquisas nas terminais.

Recomendação

Usar *disaster recovery* e com exactamente os mesmos dados que o servidor principal, que sejam activados automaticamente após a interrupção do servidor principal.

2) *Processo de contigência no caso de destruição do servidor*

Pela execução frequente de *backups* em *tapes* auxiliares na Petromoc, estas são usadas como forma de salvaguardar as informações perdidas no caso de perda do servidor.

Constrangimento:

No caso de destruição do servidor ou da sala do servidor em que também estão as *tapes* de *backups* do sistema causa a perda total dos dados no sistema, isto pela não existência de mecanismos para a recuperação deste.

Recomendação

Usar *tapes* que não ficam na sala do servidor e/ou um servidor espelho em que esteja num outro local fora do edifício da Petromoc sede e distante.

3) *Processo de contigência no caso de paralização da rede de computadores*

Para este caso é feita a solicitação aos técnicos da EBS.

Constrangimento:

Tem sido constante a espera de técnicos para a solucionar problemas de desconexação dos cabos que causam a paralização da rede, fazendo com que actividades no sistema sejam interrompidas.

Recomendação

Formar simples equipas internas de identificação de avarias ou constrangimentos na rede e que possam solucionar simples paragens da rede.

4) *Contigência de paralização da corrente eléctrica*

Este processo inevitável logo pela qualidade de corrente eléctrica no país, a Petromoc tem usado gerador de 175 kva e UPS's ligados aos computadores existentes.

Os constrangimentos e recomendações não se diferem com os do ponto 2.2 do sistema de alimentação eléctrica.

6.7. Programas Instalados e Removidos

No sistema foram instalados programas basicamente que consistem na apresentação ou aparência de relatórios. Outros programas desenvolvidos são basicamente para tarefas meramente específicas e que por vezes são usados uma vez e abandonados.

6.7.1 Constrangimento:

Inexistência de "*authority check*[13]" nos programas desenvolvidos fazendo com que qualquer utilizador possa executar o programa e possivelmente a eliminação de tabelas, da BD, lançamentos feitos ou alterar a parametrização do sistema.

Recomendação

Criar "*authority check*" em cada programa desenvolvido para permitir que só os utilizadores autorizados executem os programas desenvolvidos.

[13] Refere-se ao teste para verificar se um determinado utilizador tem autorização para executar um objecto do SAP/R3.

6.7.2 Constrangimento:

Os programas são desenvolvidos e simultaneamente testados pelos mesmos técnicos fazendo com que não seja garantida a perfeição e a satisfação dos requisitos para o programa desenvolvido.

Recomendação

Testar todos programas desenvolvidos por técnicos que não tenham participado no desenvolvimento de modo que tanto a rotina (*authority check*) esteja em todos programas como também exista fidelidade dos programas desenvolvidos.

6.7.3 Constrangimento:

Os 463 *Backups* dos programas desenvolvidos estão armazenados em simples computadores que a qualquer momento podem ser formatados sem o devido cuidado de salvar os dados nele existentes, computadores susceptíveis para o uso não controlado originando deste modo a perda dos *Backups* de programas desenvolvidos.

Recomendação

Armazenar os *Backups* em servidores só para o efeito de cópias de segurança dos programas desenvolvidos.

6.8. Âmbito de Acesso ao Sistema

Referem-se aos mecanismos empreedidos por forma que se tenha acesso controlado evitando a entrada de intrusos no sistema, que para tal, são usados *firewalls*.

6.8.1 Constrangimento:

As *passwords* são estáticas o que faz com que a meio ou longo prazo possam ser descobertas ou divulgadas para possíveis actos de sabotagem.

Recomendação

Criar mecanismos para que as *passwords* sejam reinicializadas num prazo máximo de 2 meses por forma que, dificilmente estas sejam conhecidas para aceder o sistema e os dados que nele existem.

6.8.2 Constrangimento:

As *Passwords* de utilização do sistema tem três (3) caractéres o que faz com que a *password* seja descoberta em um menor número de tentativas, isto pelos interessados na descoberta para o acesso ao SAP/R3 efectuando actos fraudulentos ou não.

Recomendação

Alterar o número de caractéres da *password* para o mínimo de cinco (5), tornando difícil a descoberta pelo elevado número de tentativas requeridas para o efeito.

6.9. Perfil dos Utilizadores do Sistema

Este ponto é o mais crucial na auditoria do sistema SAP/R3 pois criar perfis é a tarefa mais difícil na administração do SAP/R3 e porque os utilizadores tem que ser devidamente criados simplesmente para que estes executem só e somente só, as suas tarefas específicas no sistema.

6.9.1 Constrangimento:

Existem utilizadores que acedem módulos que o seu trabalho não exige, ou seja, os seus perfis são além do seu trabalho dando lhes a possibilidade de modificar dados no sistema.

Recomendação

Criar novamente os perfis dos utilizadores no SAP/R3.

6.9.2 Constrangimento:

Certos utilizadores da contabilidade usam senhas distintas para execução das suas actividades porque os seus perfis não cobrem as suas necessidades, fazendo com que, tenham acesso e/ou modificação dos dados que não corresponde ao seu trabalho.

Recomendação

Criar novamente os perfis dos utilizadores no SAP/R3 de modo que a cada perfil cubra as necessidades do utilizador em termos de actividades a desempenhar.

6.9.3 Constrangimento:

Muitos utilizadores tem perfil para criação de objectos no sistema o que originará a criação de contas e mexer a parametrização do sistema.

Recomendação

Criar novamente os seus perfis pois se não, ter-se-ão objectos indesejáveis.

6.9.4 Constrangimento:

Usuários do ABAP usam senha com perfil para desenvolver programas directamente no mandante Produtivo tornando assim o sistema vulnerável a eliminação de certos objectos.

Recomendação

Eliminar este perfil, de modo que nenhum utilizador possua este perfil e que todos programas desenvolvidos são feitos no mandante Desenvolvimento para evitar o desaparecimento de objectos no mandante Produtivo.

6.10. Parametrizações do Sistema

Esta é uma verificação das parametrizações standard do sistema e dos programas desenvolvidos.

Constrangimento:

Não é feita parametrização periódica ao sistema, fazendo com que a parametrização da antiga estrutura da Petromoc seja diferente da actual originando dificuldades nas pesquisas de trabalhadores afectos em novos departamentos da empresa.

Recomendação

Parametrizar periódicamente o sistema SAP/R3 em conformidade com o desenvolvimento da empresa.

6.11. Análise do Sistema

6.11.1. Sistema SAP/R3

Por forma a auxiliar o tratamento dos seus processos de negócio, foi adquirido o sistema SAP/R3 e estão implementados pela EBS os módulos das áreas de Logística, Finânças e Recursos Humanos.

A empresa Petromoc por estar representada em quase todo o país através das suas instalações, depósitos e postos de abastecimento, faz com que um grande volume de dados sejam manuseados, daí a necessidade de sistemas com grande poder de tratamento dos seus processos seja prioridade. É deste elevado volume de dados, da possibilidade de produção de inúmeros documentos e gráficos após a introdução unívoca de dados, e da monitoração destes em tempo real que foram algumas das razões da aquisição do SAP/R3.

Na Petromoc foram implementados os Mandantes[14] Produtivo e Desenvolvimento, em que no Produtivo estão os dados em operação e no segundo os dados usados para desenvolver programas e testes; Estão os módulos SD, MM, FI, CO, HR, PM, TR e cuja manutenção está a cargo da EBS com consultores para cada módulo do sistema.

6.11.1.1 Constrangimento:

O sistema SAP/R3 implementado na Petromoc não possibilita um controle interno por forma que não sejam alterados certos campos vitais tais como, o preço de compra de combustíveis. O que supõe-se fraudes por parte dos utilizadores do sistema.

Recomendação

Parametrizar o sistema de modo que campos cruciais do sistema não sejam alterados pelos utilizadores.

[14] Mandante é a entidade legal organizacional no sistema SAP, em que todos os dados gerênciados de negócio são aqui protegidos para que outros mandantes não possam-os alcançar. O objetivo principal do mandante é manter os dados isolados, tal que, os dados em um mandante podem ser somente visíveis dentro desse mandante (Mohapatra S., 1998).

6.11.1.2 Constrangimento:

Não existem procedimentos documentados que definem o formato dos dados a introduzir, por forma a assegurar a entrada de dados no campo correcto e com o formato adequado.

Recomendação

Documentar os procedimentos para a introdução dos dados no sistema.

6.11.1.3 Constrangimento:

Discrepância de dados nos mandantes Desenvolvimento e Produtivo, o que permite a realização de testes no Produtivo deixando vulnerável à eliminação ou perda os dados deste mandante.

Recomendação

Efectuar passagens de mandantes nos momentos em que são feitos *Backups* diários do sistema como forma de garantir que os testes e programas sejam efectuados no Desenvolvimento.

De acordo com os módulos do sistema SAP/R3 implementados e/ou usados, são mostrados os factos constatados na utilização de cada módulo:

6.11.2 Módulo de Recursos Humanos (HR)

Este módulo está implementado na Direcção de Recursos Humanos (DRH) que possui um total de quatro (4) senhas para utilização do sistema.

6.11.2.1 Constrangimento:

Dificuldades nas pesquisas de trabalhadores de acordo com os departamentos que estão afectos, pois, alguns departamentos fundiram-se dando origem a outros cujos trabalhadores não estão directamente alocados no novo, fazendo com que pesquisas de trabalhadores por departamento sejam dificultadas.

Recomendação

Parametrizar periódicamente o sistema segundo o desenvolvimento da empresa.

6.11.2.2 Constrangimento:

Dificuldade em gerir o plano de férias anuais dos trabalhadores, mapas de trabalhadores que gozaram férias, o mapa com o número de trabalhadores com férias acumuladas e o mapa de subsídio de férias no sistema.

Recomendação

Formar utilizadores no módulo de Administração do pessoal.

6.11.2.3 Constrangimento:

Partilha de uma senha por utilizadores que tratam promoções, actualização de dados pessoais, tornando deste modo vulnerável e inseguro o acesso à dados que não são do seu respectivo domínio.

Recomendação

1. Adquirir mais senhas para que cada área tenha a(s) sua(s) respectiva(s) senha(s), ou
2. Partilhar senhas que não permitem actualização dos dados no sistema.

6.11.2.4 Constrangimento:

Certos dados de trabalhadores no sistema não refletem à sua situação real, apesar de terem entregue documentos formais para a devida actualização, isto porque, há casos em que permanecem descontos salariais que os mesmos são inexistentes fazendo com que mapas (estatísticas) tiradas no sistema não sejam verdadeiras.

Recomendação

Adoptar uma política ou prazos relativamente curtos, para a actualização imediata no sistema SAP/R3 após a aprovação da inexistência do desconto.

6.11.2.5 Constrangimento:

Certos trabalhadores quando tem um aumento salarial por promoção, os seus dados não são actualizados no sistema antes do respectivo processamento salarial sendo de certo modo transtornante para o DRH por causa das discrepâncias verificadas nos mapas do sistema e manualmente processados.

Recomendação

Adoptar uma política ou prazos relativamente curtos, para a actualização imediata no sistema SAP/R3 após a corfirmação do aumento salarial do trabalhador.

6.11.3. Módulo de Contabilidade (FI)

Constrangimento:

Dificuldades em executar as amortizações de forma automática, fazer avaliação cambial, extrair os resultados dos testes para Mapa de avaliação cambial (anexos ao balanço) fazendo com que os utilizadores desenvolvam programas na aplicação Ms Excel.

Recomendação

Formar utilizadores no uso do SAP/R3.

6.11.4 Carga do Sistema

6.11.4.1 Capacidade do Hardware

Algumas terminais com o SAP/R3 instalado tem em termos de capacidade de memória RAM variável 128 Mb à 500 Mb. Uma boa parte destas apresentam uma capacidade de RAM que varia de 866Mb à 1Gb.

Constrangimento:

Terminais com capacidade abaixo de 128Mb de RAM em que está instalado o sistema, são por vezes reportadas falhas quando o sistema necessitar de mais espaço em termos de memória.

Recomendação

Aumentar a capacidade para um mínimo de 1 Ghz de memória para que o sistema possa funcionar sem dificuldades.

6.11.5 Base de Dados

6.11.5.1 Arquitectura da Base de Dados

O SAP/R3 usado nas empresas do grupo Petromoc possui uma BD com uma arquitectura cliente/servidor implementado pelo sistema de gestão de bases de dados (SGBD) de Oracle. As *tablespaces, tables, filesystems* e índices são *standards* do SAP.

É usado um servidor para a gestão da BD da Petromoc e um para as empresas que fazem parte do grupo Petromoc.

Constrangimento:
Destruição inesperada do servidor causada por avaria do *hardware* ou por um evento catastrófico, tendo como consequêcia a perda total da BD e a paralização das actividades no SAP/R3.

Recomendação
Implementar um *disaster recovery* que não esteja localizado na Petromoc sede, por forma que seja dada a contínuidade das actividades no sistema.

6.11.5.2 Desempenho da Base de Dados

A BD atinge uma *performance* de 95% e os restantes 5% são referentes a falhas em termos de localização de dados na memória provisória do sistema.

Não foram registados constrangimentos pois, a percentagem acima mostrada em termos de *performance* encontra- se num intervalo aceitável.

6.11.5.3 Recuperação da Base de Dados

São feitos diariamente *backups online* e *offline* que ficam armazenados no servidor e em *tapes* no mesmo período que são armazenadas no centro de computação.

Constrangimento:

Inexistência de formas seguras de recuperação da BD no caso de eventos catastróficos que ocorram no centro de computação.

Recomendação

1. Efectuar *backups* diários em *tapes* e não armazenar no edifício da Petromoc sede, ou
2. Colocar em outro edifício uma máquina que sirva para *backup* remoto da BD.

6.11.5.4 Permissões de Acesso à Base de Dados

Foram devidamente implementadas as permissões de acesso à BD de modo que apenas os administradores da BD é que possuem *passwords* para o acesso.

Não foram verificados contrangimentos pois, o acesso à BD deve ser a prior restrito somente ao(s) admintrador(es) do sistema.

6.11.6 Rede de Computadores

A EBS criou um esboço sintetizado da estrutura organica ou funcional da rede montada em que figura a topologia adoptada que é estrela em cada andar e por todo edificio da sede da Petromoc. A comunicação entre a sede da Petromoc, as filiais e as empresas que fazem parte do grupo é feita por via de radio link.

A configuração da rede impede que a ocorrência de uma falha em um dos seus pontos provoque a queda de toda rede.

Estão implementados componentes de rede como *gateways* e *firewalls*, que restrigem o acesso não autorizado por estranhos.

É feita a inventariação e a respectiva actualização periódica pelos responsáveis dos equipamentos de rede que se encontram no local de trabalho.

Os responsáveis da rede estão devidamente capacitados para executarem actividades que tem a ver com a rede de forma eficaz e rápida.

Constrangimento:

Paralização da rede devido a fraca qualidade das tomadas instaladas, tornando vulnerável à interrupções do sinal na rede.

Recomendação

Substituir as tomadas que tem provocado interrupções do sinal e tomadas com as mesmas caracteríticas.

6.12. Resultados da Auditoria do Sistema SAP/R3

Dado não existirem medidas concretas da eficiência na utilização do sistema SAP/R3, a gestão de topo formula apenas uma percepção dessa eficiência através do volume de negócios, dos resultados líquidos, activo líquido, capitais próprios, custos operacionais número de trabalhadores, etc.

Os resultados relevantes do processo de auditoria abaixo apresentados foram baseados na utilização das técnias de auditoria como análise de relatórios do sistema, entrevistas e questionários a uma população de 50 funcionários das empresas alvo, dos quais 40 são utilizadores do sistema e os restantes não.

Baseando-se nos relatórios do sistema no universo das 140 licenças, foram apontados como relevantes os seguintes resultados:

- 75 usuários tem perfil inadequado às suas necessidades de trabalho;
- 36 licenças de utilizadores ainda não foram exploradas;
- 4 utilizadores nunca usaram as suas senhas no sistema;
- 25 utilizadores tem perfil para a criação de objectos no sistema;
- As *passwords* dos utilizadores são estáticas e com 3 caractéres;

Baseando-se nas entrevistas e questionários ao número de funcionários acima apresentado, forma apontados como relevantes os seguintes resultados:

- A parametrização do sistema é referente a antiga estrutura da empresa Petromoc que a mesma não corresponde a actual;
- 11 utilizadores não foram treinados para a devida utilização do SAP/R3, daí o receio destes na exploração do sistema;
- 24 utilizadores foram treinados no uso do SAP/R3 mas, mesmo assim, apresentam dificuldades na utilização do sistema;
- 5 utilizadores foram treinados no uso do SAP/R3 e apresentam bons conhecimentos de utilização do sistema;
- 14 utilizadores estão afectos em áreas onde lidam com o sistema sem o devido conhecimento da área específica. Daí também resulta o receio por parte destes na exploração do sistema;

- 296 programas foram desenvolvidos no mandante Produtivo e os mesmos são testados pelo técnico que os desenvolveu;
- 167 programas foram desenvolvidos no mandante Desenvolvimento e testados pelo técnico que os desenvolveu;
- Arbitrariedade na utilização das senhas por parte dos utilizadores, constatando-se por vezes a partilha por mais de um utilizador;
- Não existe possibilidade de recuperação de *Backups* dos programas desenvolvidos após a destruição dos computadores em que estão armazenados ou eliminação intencional ou não destes no referido computador;
- Inexistência de políticas documentadas de confidencialidade da informação advinda do sistema SAP/R3;
- Inexistência do *authority check* nos programas desenvolvidos;
- Quanto ao controlo de presença dos utilizadores, a Petromoc afirma estar para implementar um sistema de controlo de presenças desde a entrada até a saída dos trabalhadores e que o mesmo estará directamente ligado ao sistema SAP/R3;
- Em termos de perda do sistema existente na empresa, a Petromoc afirma que está em curso a montagem de dois novos servidores adquiridos que não estarão no edifício e sirvam de *disaster recovery*.

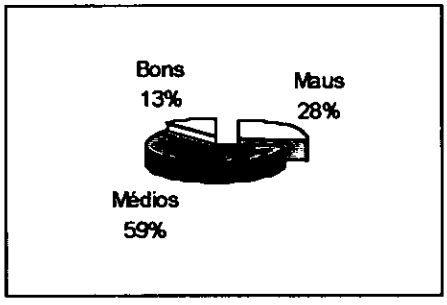
Como também resultado da auditoria, são vistas as seguintes causas da origem de ameaças do sistema SAP/R3:

- Inexistência de gerador com grande capacidade;
- Inexistência de rigorosidade no controlo sobre as pessoas que entram no edifício e posteriormente abandonam;
- Inexistência de servidor e *tapes* com dados do sistema armazenados fora da sede da empresa Petromoc.

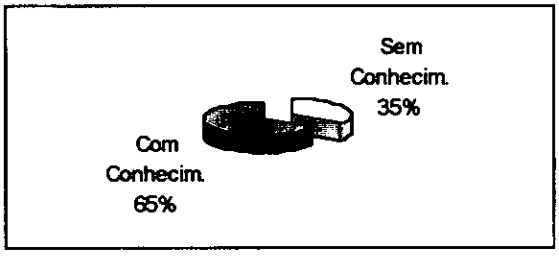
6.13. Discussão dos Resultados

Da análise baseada na totalidade de funcionários que participaram na implementação do modelo conceptual de auditoria do sistema SAP/R3 nas empresas do grupo Petromoc, constatou-se o seguinte:

1) Os utilizadores do SAP/R3 são classificados em relação ao domínio do sistema de acordo com os seguintes critérios:
   - Maus - 28% dos utilizadores do SAP/R3 não tem bons conhecimentos de utilização do sistema e não tiveram formação adequada;
   - Médios - 59% dos utilizadores passaram pela formação mas denotam ligeiras dificuldades na operação do sistema;
   - Bons - 13% dos utilizadores tiveram formação e com bons conhecimentos de utilização do sistema;

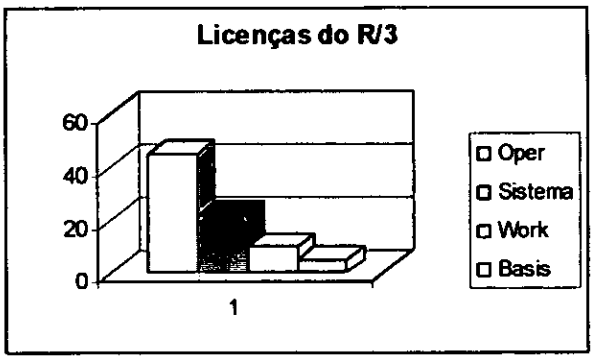


2) Os utilizadores do SAP/R3 são classificados em relação ao conhecimento da área específica:
   - Sem conhecimento - 35% dos utilizadores do SAP/R3 estão afectos em áreas em que não tiveram formação específica;
   - Com conhecimento - 65% dos utilizadores estão em áreas com formação específica;



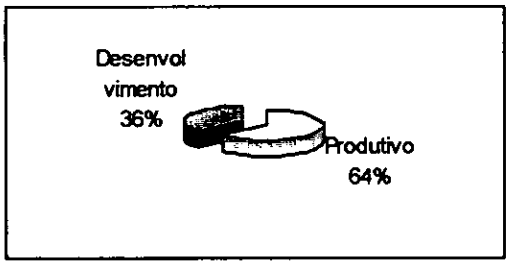
3) Numa amostra de 80 Licenças para utilização do sistema verifica-se que:

- 80% são correspondentes aos utilizadores operacionais (Oper);
- 14% são correspondentes aos utilizadores do sistema (Sistema);
- 3% são correspondentes aos utilizadores *worflow* (*Work*);
- 3% são correspondentes aos utilizadores *basis component* (*Basis*).



4) Dos 463 programas desenvolvidos verifica-se que:

- 64 % correspondem aos desenvolvidos no mandante Produtivo;
- 36 % correspondem aos desenvolvidos no mandante Desenvolvimento;



6.14. Conclusões

O estudo de auditoria e segurança de SI permitiu de forma equilibrada uma familiarização de termos e/ou conceitos novos que causaram maior interesse na execução do presente trabalho. Dentre os vários aspectos assimilados neste estudo, são destacados o historial da auditoria, o controlo interno, as funções e relatório final do auditor de sistemas, a auditoria dos utilizadores, dos especialistas em TI e a auditoria do ambiente organizacional. Foi também interessante a familiarização das técnicas de auditoria de sistemas a destacar os questionários, entrevistas, análise de relatórios e visitas presenciais, para a sua devida adequação no desenho do modelo conceptual e posterior implementação.

Constituiu maior motivação deste trabalho o estudo do SAP/R3 sendo este, um sistema bastante complexo composto por módulos parametrizáveis na prespectiva do negócio desenvolvido na organização. É sim um sistema que, está em contínuo desenvolvimento acompanhando a evolução do mercado fornecendo solução eficiente de gestão empresarial. Gestão em tempo real dos recursos da empresa de forma optimizada, projectando índices de *performance* bastante elevados e uma decisão baseada em dados que refletem a situação actual da empresa.

O SAP/R3 é um sistema que apresenta como maior desvantagem o elevado custo de implementação e formação dos funcionários que, em termos compartivos, são superadas com as ilimitadas vantagens como, a redução dos custos da empresa e o controlo das operações das áreas críticas.

Este estudo teve como base a bílbliografia disponível que impulsionou a concepção do modelo de auditoria, que possa na medida do possível ajudar as organizações a terem o controlo exacto das actividades desenvolvidas no sistema em causa.

Como forma de teste do modelo, este foi implementado e que claramente está notória a sua abrangência e complexidade de um modo coerente na auditoria dos sistemas das empresas.

6.15. Recomendações

Por forma a que se tenha um bom conhecimento de auditoria nas suas diversas vertentes, recomenda-se a pesquisa bibliográfica sobre o assunto em causa nos mais variados autores que o abordam.

Neste mesmo contexto mas para o sistema SAP/R3, recomenda-se um estudo mais aprofundado e suas implicações sobre o sistema SAP/R3 no que se refere à carga do sistema, exploração do sistema, BD do sistema, assim como, a operação do sistema na óptica de administrador por forma que se tenha uma implementação do modelo mais precisa e completa na execução de transações no sistema para o posterior registo das ocorrências.

Como a implementação do modelo conceptual teve maior incidência à parte técnica, faz se uma recomendação ao estudo cuidadoso dos processos de negócio configurados no sistema para que seja feita uma auditoria mais consistente abrangindo a parte funcional, pois, nesta parte são notórios constrangimentos por parte dos utilizadores na sua concepção.

6.16. Bibliografia

1. Auditoria sistemas (2004), Auditoria de sistemas informáticos, www.auditoriasistemas.com, consultado em 10-05-05;
2. Audy J. (2002), Auditoria de Sistemas de Informação, www.inf.pucrs.br, consultado em 16-02-2005;
3. Brand H. (1998), The Official SAP Guide: SAP/R3 Implementation with ASAP, Sybex Inc., USA
4. Carneiro A. (2001), Auditoria de Sistemas de Informação, Lisboa, FCA - Editora de Informática;
5. Carneiro A. (2004), Auditoria de Sistemas de Informação, Lisboa, FCA - Editora de Informática;
6. Coelho P. (1998), Criação de Páginas World Wide Web com Html 4 & Java, 2ª edição, FCA- Editora de Informática;
7. Costa C. B. (2000), Auditoria Financeira – Teoria e Prática, Lisboa, 7ª edição, Editora Rei dos Livros;
8. Datasoft (2000), Alcance da Auditoria, www.datasoft.com.br/auditoria.htm, consultado em 08-10-2004;
9. Fantinatti J. M. (1998), Auditoria em Informática: Metodologia e Prática, Sao Paulo: Mcgraw-hill;
10. Gil A. L. (1989), Auditoria de Computadores, São Paulo, Editora Atlas;
11. Best P. (2000), Authorizations, www.business.vu.edu.au/sap/paper%207.doc, consultado em 18-05-2005;
12. Kate V. (2000), Implementing SAP/R3: The Guide For Business And Technology Managers, USA, Sams Publishing;
13. Lawrence B. S. (2000), Auditoria Interna, www.unb.br/aud/a_essencia.htm, consultado em 18-05-2005;
14. Mangalhães A. F., Lunkes I. C. e Muller A. N. (2001) Auditoria das Organizações, São Paulo, Editora Atlas S.A;
15. Metzger S. M. e Roehrs S. (1998), The Official SAP Guide: SAP/R3 Change and Transport Management, USA, Sybex Inc;
16. M-Global (2002), Petroleos de Mocambique, www.petromoc.co.mz, consultado em 28-02-05;

17. Miller S. S., AcceleratedSAP (1998): Implementation At The Speed Of Business, USA, The McGraw-Hill Companies;
18. Mohapatra S. (2001), Everthing about SAP Clients, www.planetsap.com, consultado em 20-04-2005
19. Morea L. (1997), La Auditoria Informatica dentro de las Etapas de Análises de Sistema Administrativos, www.monografias, consultado em 01-06-2005;
20. Nabais C. (1993), Noções Práticas de Auditoria, Lisboa, 2ª edição;
21. Norris G., Hurley J., Dunleavy J. e Ballas J. (2001), E-Business e ERP: Transformando as Organizações, Brasil, Qualitymark Editora;
22. Roff (2005), Auditoria Técnica à exploração dos sistemas SAP, www.roff.pt/artigo.asp?ID=29&tipo=solucao, consultado em 13-12-04;
23. Rosini A. M. e Palmisano A. (2003), Administração de Sistemas de Informação e a Gestão do Conhecimento, São Paulo, Pioneira Thomson Learning;
24. Santos L. D. (1996), Observatório em Tecnologias e Sistemas de Informação, Braga, Universidade do Minho;
25. Silva S. M (2000), www.students.fct.unl.pt/users/smss/erp/trabalho.htm, consultado em 20-12-2004;
26. Smith P. (1992), Client/Server Computing: All-in-one Reference for Total Systems Development, USA, Sams Publishing;
27. Schneider T. (1998), The Official SAP Guide: SAP/R3 Performance Optimization, USA, Sybex Inc;
28. Ucpel, Auditoria de Segurança, www.redes.ucpel.tche.br/documentos/auditoria/conteudo.html, consultado em 24-02-05;
29. Will L. (1998), The Official SAP Guide: SAP/R3 System Administration, Berlin.

GLOSSÁRIO

ABAP: *Advanced Business Application Programming* – é a linguagem de programação do sistema R/3 (Brand, 1998:530);

***Authority Check*:** é o teste para verificar se um determinado utilizador tem autorização para executar um objecto do SAP/R3;

Avaliação: é o conceito que exprime a idéia de julgamento e emissão de opinião (Gil, 1989:26);

***Backup*:** é uma organização fisica de dados em que a base de dados inteira é duplicada em unidade de disco separada. O objectivo principal deste procedimento é garantir a segurança fisica dos dados em caso de ocorrência de alguma falha física com o disco onde os dados residem (Rosini e Palmisano, 2003:190);

Base de dados: conjunto integrado de dados, inter-relacionados, armazenados num dispositivo de armazenamento com acesso directo (Carneiro, 2001:274);

***Batch input*:** refere-se ao método e ferramentas para a importação rápida dos dados dos ficheiros sequenciais na base de dados R/3 (Brand, 1998:532).

***Batch Total*:** é o somatório de um conjunto lógico de dados, como por exemplo, quantidades;

***Buffer*:** Memória na qual são temporariamente conservadas informações e dados, que são produzidas e utilizadas a ritmo diferentes (Carneiro, 2001:274);

***Check-list*:** Lista de tarefas, perguntas e outros elementos que pode ser utilizada pelo auditor como um auxiliar da memória (Carneiro, 2001:275);

Cliente/Servidor: é a filosofia de funcionamento de aplicações, na qual existe dispersa (pelos servidores), em vez de estar concentrada centralmente e é consultada pelos chamados "clientes", lógica e geograficamente dispersos (Coelho, 1998:346);

CPI-C: *Common Programming Interface-Communication* - relação de programação, a base para sincronizar, sistema-a -sistema, uma comunicação do programa-à-programa (Brand, 1998:534);

***Disaster recovery*:** é o processo de planeamento estabelecido e teste dos procedimentos de recuperação, com a finalidade de prover serviços (Fantinatti, 1998:30);

EDI: *Electronic Data Interchange* - intercâmbio eletrônico intercompany de dados estruturados (por exemplo, documentos de negócio) entre o sócio de negócio num país e no exterior quem pode usar a hardware, o software, e os serviços diferentes de uma comunicação (Brand, 1998:536);

***Ethernet*:** refere-se a um tipo de comunicações de rede local muito usado hoje em dia. Está em migração para o tipo *Fast Ethernet*, que permite velocidades na ordem dos 100Mbps (Coelho, 1998:347);

***Firewall*:** É um conjunto formado por hardware e *software* cuja função é de erguer uma "barreira electrónica" contra intrusos externos que querem entrar numa rede privada. O firewall faz o reconhecimento dos usuários autorizados, direcionando-os para áreas previamente autorizadas a cada um (Rosini e Palmisano, 2003:197);

GUI: *Graphical User Interface* - é o meio com que um usuário pode trocar informação com o computador. Usa-se o GUI para selecionar comandos, iniciar programas, exibir ficheiros, e executa outras operações selecionando chaves ou teclas de função, opções do menu, e ícones com o rato (Brand, 1998:537);

***Hash Total*:** é o somatório de um conjunto ilógico de dados, como por exemplo, datas;

Internet: refere-se ao maior conjunto de rede de dados do mundo, tendo em comum apenas a utilização do protocolo TCP/IP (Coelho, 1998:348);

Mandante: é a entidade legal organizacional no sistema SAP, em que todos os dados gerênciados de negócio são aqui protegidos para que outros mandantes não possam-os alcançar. o objetivo principal do mandante é manter os dados isolados, tal que, os dados em um mandante podem ser somente visíveis dentro desse mandante (Mohapatra , 2001).

ODBC: *Open Data Base Connectivity*;

OLE: *Object Linking and Embedding*;

Parametrização: conjunto de operações que visam assegurar a existência dos processos organizacionais de negócio

***Password*:** é um método muito usado nas aplicações de software para garantir a segurança de acesso (Coelho, 1998:350);

Performance: é a medida da eficiência dum sistema de TI (Brand, 1998:542);

R/3: *Runtime System* 3;

***Router*:** é um equipamento de comunicações, usado para interligar equipamentos por meio de múltiplos protocolos de comunicações. Na *internet* usam-se para ligar equipamentos em TCP/IP (Coelho, 1998:351);

SQL: *Structured Query Language*. Linguagem de base de dados para aceder à base de dados relacionais (Schneider, 1998:502);

TCP/IP: *Transmission Control Protocol / Internet Protocol* – refere-se a um protocolo de comunicações utilizado com base para fluxos de informações e dados na internet e que é suportado pela maioria dos sistemas operacionais, sendo um factor de unificação de todas as redes de comunicações (Carneiro, 2001:279);

Transação: entende- se como sendo o conjunto de dados que identifica as alterações (actualizações) que foram feitas nos ficheiros de um arquivo. (Carneiro, 2001:279);

Validação: é o conceito que exprime a idéia de teste (Gil, 1989:26).

Anexos

Anexo 1: Entrevista ao Gestor do sistema

Perguntas	Resposta
1. Quantos computadores existem na organização? E quantos estão configurados o SAP/R3?	
2. Existem contratos de configuração e manutenção da rede?	
3. Existem licenças para utilização do sistema, e quantos utilizadores estão licenciados?	
4. Existem planos de formação periódicos para os utilizadores do sistema SAP/R3?	
5. Quais os módulos do SAP/R3 que foram implementados ou configurados?	
6. Existiu formação especializada para o(s) administrador(es) do sistema?	
7. Existem definidos os pontos de controlo tanto para administração, como para os utilizadores?	
8. É feita a inventariação do hardware e software do sistema?	
9. Quantos utilizadores do sistema SAP/R3 estão criados?	
10. Quantos mandantes estão configurados?	
11. Existe responsável pelo transporte dos dados de um mandante para o outro?	
12. Estão documentadas as alterações feitas ao sistema?	
13. A organização definiu e documentou as responsabilidades de todas as pessoas envolvidas na administração, desenvolvimento e consultoria do sistema?	

Anexo 2: Entrevista à Administração do sistema

Perguntas	Resposta
1. Quais são as características do servidor que está instalado o SAP/R3?	
2. Quais os programas desenvolvidos que foram configurados no sistema?	
3. Quais os erros comumente reportados pelo sistema no que respeita aos programas desenvolvidos?	
4. No caso de eventos catastróficos, tem se feito backups do sistema? E qual a periodicidade da execução dos backups online e offline?	
5. Como tornar o sistema operacional no caso de danificar-se ou inundar-se a sala do servidor e as tapes de backup existentes?	
6. Quais as políticas de segurança e protecção do sistema existentes?	
7. Quantos utilizadores foram criados sem o devido licenciamento e porquê essa criação?	
8. As passwords criadas tem prazo de utilização?	
9. Qual é a dimensão das passwords?	
10. Existem grupos de utilizadores?	

Anexo 3: Entrevista aos programadores do ABAP

Perguntas	Resposta
1. Possui formação especifica da área ou função que se encontra?	
2. Existe documentação dos programas desenvolvidos?	
3. Em que mandante tem sido criados os programas?	
4. Existe responsável pelo teste dos programas desenvolvidos?	
5. Qual dos mandantes é usado para o teste dos programas criados?	
6. Os programas desenvolvidos são amigáveis (comentários, *background*,etc)?	
7. Existem actualizações de emergência ao sistema?	

Anexo 4: Entrevista aos utilizadores do sistema

Perguntas	Resposta
1. Possui formação específica da área ou função que se encontra?	
2. Quais os problemas comumente encontrados?	
3. Teve formação do módulo do SAP que está usando?	
4. Tem auxilio de utilização para casos de constrangimentos?	
5. Como tem solucionado os constrangimentos encontrados?	
6. São respeitadas as normas de segurança do sistema pré-definidas pela administração do sistema?	

Anexo 5: Entrevista do Hardware

Perguntas	Resposta
1. Os contratos de *hardware* estão por meio de aquisição, aluguer, manutenção ou *leasing*?	
2. Existe segurança física do *hardware*?	
3. O *hardware* cumpre com as especificidades requeridas pelo sistema?	
4. Como são solucionados erros do *hardware* no caso positivo destes?	
5. É feita a manutenção correctiva e adaptativa do *hardware*?	
6. Quem o responsável pela manutenção do *hardware* do sistema?	
7. Exitem planos de contigência para o *hardware*?	

Anexo 6: Entrevista do Software

Perguntas	Resposta
1. Existem contratos de aquisição e manutenção do *software*?	
2. Existe segurança lógica do *hardware*?	
3. Quais os tempos de resposta para programas desenvolvidos?	
4. Quem é o responsável pela manutenção do *software*?	

Anexo 7: Entrevista do Ambiente organizacional

Perguntas	Resposta
1. Existem estabilizadores ou geradores de corrente?	
2. Quais os planos de contigência no caso de incêndios, inundações, etc.?	
3. Existem sistemas de detenção de fogo e equipas de socorro de incêndios?	
4. Que tipo de protecção existe nos locais em que se encontram os servidores do sistema?	
5. Existe arcondicionado na sala do servidor?	

Anexo 8: Entrevista da Base de Dados do sistema

Perguntas	Resposta
1. Como cresce a base de dados?	
2. Como são feitos os *backups* da base de dados?	
3. Quem é o responsável pela base de dados?	
4. Qual é a arquitectura da base de dados?	
5. Qual é a performance da base de dados?	

Anexo 9: Entrevista da Rede de Computadores

Perguntas	Resposta
1. Existe o desenho da arquitectura da rede implementada?	
2. Qual é o tipo de cablagem usada?	
3. Quais os constrangimentos verificados na rede? E como são solucionados?	
4. Quanto tempo em média tem se esperado para o normal funcionamento da rede?	
5. A largura de banda dos meios de transmissão torna eficiente o volume de dados que trafegam na rede?	
6. Existe uma política de *backup* para a rede?	

Anexo 10: Questionário - Avaliação do controlo interno

Questão	Resposta (sim/não)	Comentário
1. Existem controlos internos e são usados?		
2. São eficazes os controlos internos definidos?		
3. Tem se feito ajustamentos nos controlos internos adoptados?		

Anexo 11: Questionário - Validação e Avaliação do Hardware do sistema

Questão	Resposta (sim/não)	Comentário
1. Existem contratos de aquisição, manutenção e aluguer do *hardware*?		
2. Existem planos de contigência no caso de eventos catatróficos?		
3. Tem sido reportados erros do *hardware*?		
4. Existem políticas de segurança e protecção ao *hardware*?		
5. É feita a inventariação do *hardware*?		
6. O *hardware* encontra- se em bom estado de conservação?		

Anexo 12: Questionário - Validação e Avaliação do Software do sistema

Questão	Resposta (sim/não)	Comentário
1. Há contratos de aquisição e manutenção *software*?		
2. O *software* tem reportado erros de configuração do sistema?		
3. Existem planos de contigência no caso de eventos catastróficos?		
4. Existe incompatibilidade do *software* com o *hardware*?		
5. Existe segurança e protecção adoptada ao *softaware*?		

Anexo 13: Questionário – Base de Dados

Questão	Resposta (sim/não)	Comentário
1. Existem *passwords* de acesso à base de dados? E quantas são no caso positivo?		
2. Tem sido feitos os *backups*?		
3. Existe programa de reorganização da base de dados?		

Anexo 14: Questionário – Utilizadores do sistema

Questão	Resposta (sim/não)	Comentário
1. Existem constrangimentos no uso do sistema SAP/R3?		
2. Tem apoio para solucionar os contrangimentos encontrados no uso do sistema?		
3. Alguma vez já participou numa formação para o uso do sistema?		
4. Existem controles adoptados para validação do dados introduzidos?		
5. É experiente na função em que se encontra ou desempenha?		
6. Quantos usuários existem no sistema?		
7. Quantos usuários estão activos?		
8. Quantos usuários foram removidos? E quando foram removidos?		

Anexo 15: Questionário - Validação e avaliação da Rede de computadores

Questão	Resposta (sim/não)	Comentário
1. Existem contratos de configuração ou manutenção?		
2. Existem constrangimentos ligados a rede?		
3. Existem erros de configuração?		
4. Existem planos de contigência?		
5. Tem sido feita a manutenção preventiva da rede?		
6. Existem procedimentos documentados e responsabilidades atribuídas para as actividades de supervisão e recuperação de defeitos de funcionamento?		

Anexo 16: Mapa de Oportunidade de Melhoramento

Área	Pontos fracos no sistema	Gravidade	Impacto da informação na gestão	Nossa sugestão de melhoria	Opinião do responsável
A1					
A2					
A3					
A4					
A5					
A6					
A7					
A8					
A9					
A10					

Tabela 1: Mapa de Oportunidade de Melhoramento

Anexo 17: Relatório final do Auditor

Relatório Final

Nome da entidade a auditar: _

Nomes das actividades auditadas: _
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Nome do responsável pela actividade _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Nome do responsável da entidade: _

Equipa de auditores: _
_ _

Objectivo(s) da auditoria: (total, parcial, sectorial)_ _ _ _ _ _ _ _ _ _ _ _
_ _

Áreas (Sectores) abrangidos: _
_ _

Factos constatados: (ver o Anexo10) _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
_ _
_ _
_ _
_ _

Conclusões: (normalmente com dados estatíticos ou outras conclusões sumário)_ _
_ _
_ _
_ _

Responsável pela auditoria: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Data de início: _ _/_ _/_ _ Data de término: _ _/_ _/_ _

Figura 5: Relatório Final da entidade que realizou auditoria