CENTRO UNIVERSITÁRIO FEEVALE

ANDREY SIMON UNGARETTI NOVAES DA SILVEIRA

AUDITORIA DE SISTEMAS - PROPOSTA DE SOLUÇÃO PARA GERENCIAMENTO E CONTROLE DE AUDITORIAS

Novo Hamburgo, Julho de 2009.

ANDREY SIMON UNGARETTI NOVAES DA SILVEIRA

AUDITORIA DE SISTEMAS - PROPOSTA DE SOLUÇÃO PARA GERENCIAMENTO E CONTROLE DE AUDITORIAS

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Ciência da Computação
Trabalho de Conclusão de Curso II

Professor orientador: Ms. Alexandre Zamberlam

Novo Hamburgo, julho de 2009.

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização desse trabalho e, em especial:

A minha família pelo incentivo, compreensão e apoio.

Ao meu orientador Ms. Alexandre Zamberlam pela ajuda e presteza sempre demonstrada no decorrer do trabalho, o que foi de fundamental importância nessa jornada.

Aos meus avaliadores pelas considerações emitidas que foram de grande valia para um melhor desenvolvimento do trabalho.

RESUMO

Este trabalho apresenta um estudo acerca dos trabalhos de auditoria de TI, verificando a importância e abrangência da mesma para as organizações, como uma ferramenta que auxilie a avaliação de aspectos relativos à Segurança da Informação e, desta forma, validar determinados controles internos. Com base nos dados pesquisados, foi efetuado estudo de caso em uma empresa que possui auditoria interna na área de TI, com o objetivo de verificar as vulnerabilidades existentes nos processos de auditoria atualmente utilizados e sugerir melhorias, por meio de uma proposta de modelo computacional, visando uma maior eficiência nos trabalhos da auditoria interna.

Palavras-Chaves: Controle Interno, Auditoria de TI, Análise de Risco.

ABSTRACT

Title: IT Audit

This work presents a study about IT Audit, verifying its importance and range for the organizations as a tool that aid the features assessments related with the Information Security and, this way, validating some internal controls. By the research done, it was applied a case in a company that uses internal controls in IT Audit. In fact, it was proposed a computational model to increase the efficiency in internal audit process.

Keywords: Internal Control, IT Audit, risk analysis

.

LISTA DE FIGURAS

Figura 1-1: Ciclo de vida da informação, considerando os conceitos básicos da segurança. ..17

Figura 1-2: Ciclo de vida do Ponto de Controle e Ponto de Auditoria.....27

Figura 3-1**:** Organograma da empresa**.**.....38

Figura 3-2: Organograma da auditoria interna**.**.....40

Figura 5-2- Diagrama entidade relacionamento.....76

Figura 5-3- Tela inicial de acesso ao sistema.....77

Figura 5-4- Consulta, inclusão e exclusão de auditorias.....78

Figura 5-5- Auditores.....79

Figura 5-6- Cadastramento de auditores.....80

Figura 5-7- Sistemas.....81

Figura 5-8- Inclusão de sistemas.....82

Figura 5-9- Inclusão de sistemas (continuação).....83

Figura 5-10- Roteiros.....84

Figura 5-11- Alteração de controle macro.....85

Figura 5-12- Dados de um ponto de controle 86

Figura 5-13- Avaliações 87

Figura 5-14- Roteiro – Atribuição do risco do sistema 88

Figura 5-15- Recomendações para plano de ação 89

Figura 5-16- Modelo de plano de ação 90

Figura 5-17- Tela de relatórios 91

Figura 5-18: Análise de risco de um sistema 92

Figura 5-19: Comparação de risco entre sistemas 93

LISTA DE ABREVIATURAS

CPD	Centro de Processamento de Dados
ISO	International Standardization Organization
ITF	Integrated Test Facility
NBR	Norma Brasileira
SI	Sistemas de Informação
TCU	Tribunal de Contas da União
TI	Tecnologia de Informação
TIC	Tecnologia da Informação e Comunicação
UML	Unified Modeling Language
CD	Compact Disc
MER	Modelo Entidade-Relacionamento
DER	Diagrama Entidade-Relacionamento
BD	Banco de dados
SOX	Sairbanes Oxley

SUMÁRIO

INTRODUÇÃO 12

1 SEGURANÇA DA INFORMAÇÃO E CONTROLE INTERNO 15

1.1 Importância da informação 15

1.2 Classificação da informação 15

1.3 Ciclo de vida da informação 16

1.4 Segurança da informação 18

1.5 Definição de controle interno 19

1.6 Controle interno e auditoria 20

1.7 Parâmetros de controle interno 20

1.7.1 Fidelidade da informação em relação ao dado 21

1.7.2 Segurança física 22

1.7.2.1 Controle de acesso físico 22

1.7.2.2 Controle ambiental 23

1.7.3 Segurança lógica 23

1.7.4 Confidencialidade 24

1.7.5 Obediência à legislação 24

1.7.6 Eficácia 25

1.7.7 Eficiência 25

1.7.8 Obediência às diretrizes da alta administração 25

1.8 Ponto de controle e ponto de auditoria 25

2 AUDITORIA 29

2.6 Tipos de auditoria 30

2.7 Natureza da auditoria 31

2.8 Auditoria de TI 32

2.9 Conceitos e objetivos 33

3 ESTUDO DE CASO 36

3.6 Dados da empresa 37

3.7 Estrutura organizacional da auditoria interna 39

3.7.1 Chefe da auditoria 40

3.7.2 Gerência de auditoria de sistemas 41

3.8 Metodologia de trabalho da auditoria de sistemas 42

3.8.1 Processos envolvidos na auditoria de sistemas 43

3.8.2 Limitações da metodologia utilizada 44

4 ANÁLISE DE RISCOS 46

5 SOLUÇÃO PROPOSTA 51

5.1 Requisitos do sistema proposto 53

5.2 Metodologia de projeto/desenvolvimento 55

5.2.1 Técnica de modelagem utilizada 55

5.2.2 Linguagem de modelagem 55

5.2.3 Ferramentas utilizadas para o desenvolvimento da aplicação 56

5.2.4 Diagramas 56

5.2.5 Diagramas de Caso de Uso 56

5.2.6 Modelo Entidade-Relacionamento (ER) 75

5.2.7 Protótipo de Telas do Sistema 77

CONSIDERAÇÕES FINAIS 94

REFERÊNCIAS BIBLIOGRÁFICAS 95

INTRODUÇÃO

O surgimento da informática e do processamento eletrônico de dados trouxe diversas facilidades para as pessoas e, sobretudo, para as corporações, que passaram a utilizar os Sistemas de Informação (SI) para auxiliar no processo de decisão gerencial da empresa.

Em um mundo competitivo e dinâmico, torna-se vital para as empresas que busquem eficiência e eficácia nos sistemas de informação utilizados, além de garantir a segurança das informações geradas pelos mesmos.

Para que a empresa consiga obter um grau de confiabilidade satisfatório e possa verificar a conformidade de suas informações, torna-se fundamental que sejam efetuadas verificações e testes em seu ambiente de TI. Testes estes efetuados pelo departamento responsável pela Auditoria de TI da empresa.

Nota-se que Auditoria não se limita simplesmente em auditar Sistemas de Informação. A mesma utiliza um conjunto de procedimentos que formam um conjunto de verificações e averiguações que permitem obter e analisar as informações necessárias à formulação da opinião do auditor. Geralmente em listas de pontos a serem verificados durante a Auditoria.

Porém, a grande quantidade de sistemas e ambientes existentes nas empresas aliada ao número reduzido de funcionários para realizar os trabalhos de auditoria, demanda a utilização de critérios para eleição dos sistemas a serem auditados, aproveitando melhor os recursos humanos disponíveis na empresa.

Segundo o estatístico William Edwards Deming, “O que não pode ser medido, não pode ser gerenciado”. Baseando-se nessa premissa, é necessária a utilização de uma métrica definida para que a empresa possa efetuar a análise de priorização de auditorias.

Além disso, torna-se complexo o gerenciamento dessas análises sem uma ferramenta de apoio que, a partir da métrica aplicada, retorne indicadores que auxiliem no planejamento dos trabalhos de auditoria.

Também é fundamental a utilização de uma ferramenta de apoio que vise automatizar o trabalho dos auditores e auxiliar no gerenciamento das recomendações efetuadas, uma vez que o controle manual das recomendações gera re-trabalho e fragilidades ao processo, visto que não há um controle automatizado do mesmo.

Neste trabalho são abordados assuntos relacionados a Auditoria de TI, tais como: informação, controle interno, auditoria em geral, etc., com utilização de uma empresa para estudo de caso, verificando as dificuldades encontradas na realização de suas auditorias.

A partir disso, é proposta a construção de uma ferramenta que ajude a sanar as dificuldades dos profissionais da área.

Sendo assim, para um melhor entendimento do apresentado, dividiu-se o trabalho em seis capítulos.

O capítulo um aborda a importância e a segurança da informação. Além disso, apresenta controle interno e seus parâmetros existentes, relacionando-o com auditoria. Também é efetuado comparativo entre ponto de controle e ponto de auditoria.

O capítulo dois trata sobre auditoria, apresentando o seu conceito, os tipos existentes, suas classificações, com ênfase em auditoria em TI, visto que esse assunto é o foco da pesquisa realizada, abordando o conceito e objetivos desse tipo de auditoria.

Após a apresentação do tema de pesquisa, é efetuado estudo de caso em uma empresa que possui um departamento de auditoria interna voltado a TI, buscando verificar possíveis limitações na metodologia utilizada atualmente pela mesma.

Finalizando o levantamento das necessidades da empresa, é apresentada no capítulo quatro análise de risco, indicando como pode ser utilizada para resolução dos problemas detectados no estudo de caso.

No capítulo cinco, é apresentado um comparativo das soluções existentes no mercado, seguido da proposta de uma ferramenta que venha a resolver os problemas identificados

durante o estudo de caso, com o objetivo de auxiliar nos processos que envolvem a auditoria de TI da empresa, seguido da apresentação de um modelo funcional da solução proposta, a metodologia, as técnicas utilizadas, a modelagem e o protótipo de telas da mesma.

1 SEGURANÇA DA INFORMAÇÃO E CONTROLE INTERNO

Neste capítulo, é abordada a importância da segurança da informação e o papel do controle interno nesse processo, além de conceitos e definições acerca do tema.

1.1 Importância da informação

A informação é um poderoso instrumento estratégico para as empresas nos dias atuais, sendo considerado como um ativo de valor inestimável para as organizações.

Sêmola (2003, p. 47) afirma que todas as empresas, independente de seu segmento de mercado, em todas as fases de existência, sempre usufruem a informação como apoio à tomada de decisão para suas ações e seus planos.

A NBR ISO 17799 define que:

> A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.

1.2 Classificação da informação

As informações podem ter diferentes tipos, de acordo com sua importância, seu valor, requisitos legais, sensibilidade e criticidade para a organização.

Segundo Cláudia Dias (2000, p.54), a informação pode ser classificada em:

1. Pública - Informação de domínio público;
2. Interna – Informação exclusiva para os funcionários de uma organização;
3. Confidencial – Informação para determinado grupo de pessoas ou departamentos;
4. Restrita – Informação restrita a um número reduzido de pessoas;

Porém, a autora afirma que, cada empresa, de acordo com sua necessidade pode classificar a informação a sua maneira.

1.3 Ciclo de vida da informação

Segundo Sêmola (2003, p. 10), independente da forma com que uma informação é apresentada, são quatro as principais fases em que se pode dividir seu ciclo de informação.

- A primeira fase refere-se ao manuseio da informação, ou seja, quando a informação é criada e manipulada.
- A segunda fase refere-se ao armazenamento da informação, que refere-se a todas as formas possíveis de armazenamento, que pode ocorrer tanto eletronicamente quanto manualmente;
- A terceira fase diz respeito ao transporte da informação, não importando qual meio foi utilizado para o transporte da mesma, podendo ser eletronicamente, fisicamente ou até mesmo verbalmente;
- A quarta e última fase referem-se ao descarte da informação, quando a informação é destruída.

É de fundamental importância que, em todos os momentos do ciclo de vida da informação, sejam observados e preservados todos os atributos referentes aos controles que devem ser mantidos em relação às informações, para salvaguardar suas propriedades básicas.

Conforme Sêmola:

> "Toda a informação é influenciada por três propriedades principais: confidencialidade, integridade e disponibilidade, além dos aspectos autenticidade e legalidade que complementam esta influência". (SÊMOLA, 2003, p. 9).

Para um melhor entendimento, a figura a seguir ilustra as fases da informação, bem como suas propriedades básicas:

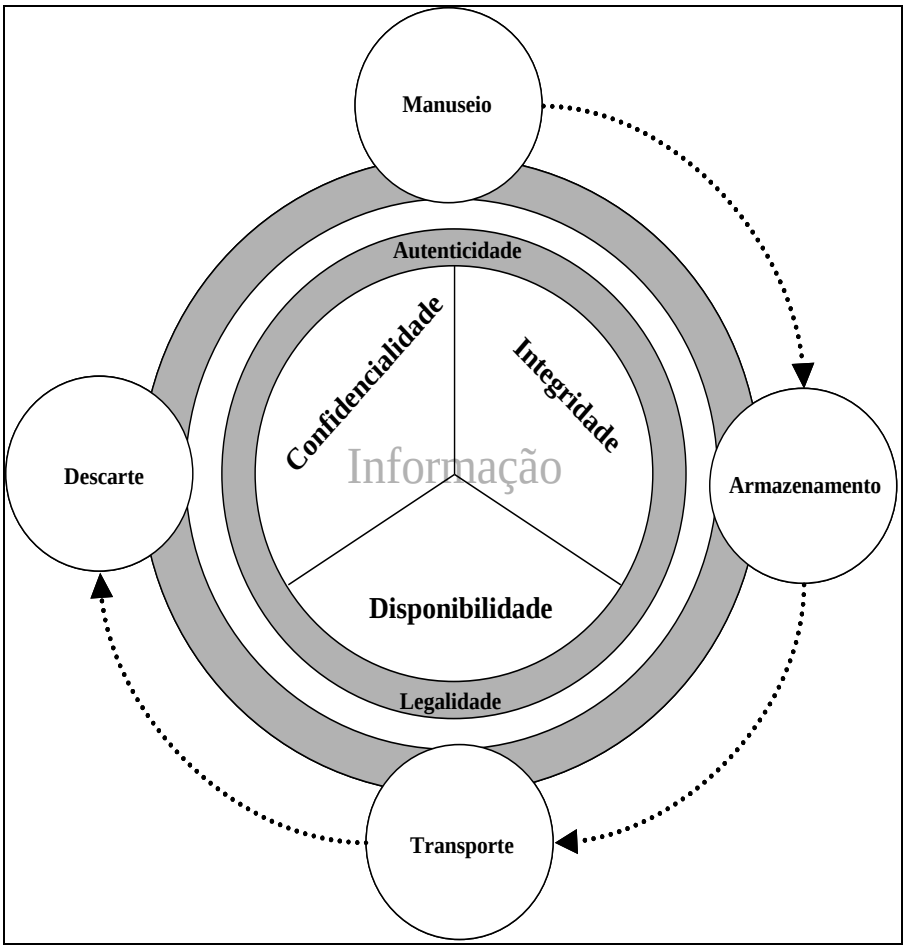


Figura 1-1: Ciclo de vida da informação, considerando os conceitos básicos da segurança.

Fonte: SÊMOLA (2003, p. 11).

Visando garantir que não sejam alteradas as propriedades da informação, torna-se fundamental que seja aplicada uma política que vise a segurança da informação, conforme consta no próximo item abordado.

1.4 Segurança da informação

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida.

Segundo a Norma NBR ISO 17799, a informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.

Com o crescente dinamismo da evolução tecnológica e sua participação no mundo corporativo, foi crescendo a ameaça na qual as informações ficam expostas e, consoante a isto, um maior impacto para as organizações.

Cláudia Dias (2000, p. 40), afirma que:

Na sociedade da informação, ao mesmo tempo que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isto, a segurança de informações tornou-se um ponto crucial para a sobrevivência das instituições.

A segurança da informação visa proteger a informação, bem como o ambiente de TI da empresa, de possíveis falhas que venham a afetar a integridade, a disponibilidade e a confidencialidade das informações.

Dias (2000) define segurança da informação como sendo “a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança.”

Para que sejam protegidos os ativos das organizações, são observados certos controles, denominados de Controles Internos, conforme será tratado no item seguinte.

1.5 Definição de controle interno

Carlos Hideo Arima, em sua obra Metodologia de Auditoria de Sistemas, todo plano de organização da empresa, composto de métodos e medidas coordenadas e aplicadas, visa proteger os bens, conferir a exatidão e a fidelidade dos dados contábeis, promover a eficiência operacional e estimular a obediência às diretrizes administrativas estabelecidas.(ARIMA, 1994, p.12)

Neste caso, deve o auditor, avaliar determinados controles, através de um trabalho de auditoria, procurando documentar e manter em dia a documentação de programas, inclusive das possíveis alterações, instruir de forma escrita e precisa os operadores, não aceitando informações verbais de programadores, manter ponto de controle em toda a extensão do processamento, assim como, um controle de todos os *hardwares* (equipamentos) e *softwares* (programas), as licenças e demais equipamentos físicos, da manutenção preventiva e corretiva, dos treinamentos realizados, das responsabilidades de cada usuário etc.

Para tanto, as organizações devem elaborar um Plano Organizacional, definindo com clareza deveres e responsabilidades, e um plano de contas que possibilite capturar a realidade.

A correta observação dos princípios de controle interno envolvendo TI é de fundamental importância para as empresas que utilizam meios eletrônicos de processamento de dados. Os documentos que explicam e servem de suporte aos programas de auditoria devem ser cuidadosamente elaborados e mantidos.

Controles internos podem ser definidos como todas as políticas adotadas pelas empresas com intuito de mitigar riscos e melhorar processos. Para o Instituto Americano de Contadores Públicos Certificados apud Arima (1994, p.12), os principais objetivos dos controles internos são:

- proteger os ativos da empresa;

- obter informações adequadas;
- promover a eficiência operacional da organização;
- estimular a obediência e o respeito às políticas da administração.

Em outras palavras, os controles internos devem assegurar que as várias fases do processo decisório e do fluxo de informações se revistam da necessária confiabilidade.

1.6 Controle interno e auditoria

A existência de sistema de controles internos apropriados propicia às empresas proteção menos onerosa e mais eficaz. Com base nos Sistemas de Controle Interno (SCI) existentes nas empresas, é que a auditoria determina a extensão de seu exame e os procedimentos a serem aplicados, os quais, inclusive, devem prever investigações mais detalhadas em contas ou áreas perigosas da companhia.

A finalidade da revisão da adequação do sistema de controles internos é determinar se o mecanismo estabelecido é eficaz para assegurá-los com eficiência e economia. Para tanto, torna-se necessário que sejam utilizados certos parâmetros, conforme é abordado no próximo item.

1.7 Parâmetros de controle interno

Conforme Arima (2006, p. 13), para permitir melhor identificação dos seus parâmetros, pode-se separar o controle interno em dois conjuntos, ou seja:

1. Controle Interno Contábil;
2. Controle Interno Administrativo;

Essa divisão torna-se muito importante para definir objetivos e responsabilidades da auditoria externa e interna. Ficando a auditoria externa com maior ênfase em controle interno contábil e a auditoria interna atuando predominantemente com o controle interno

Administrativo. A tabela a seguir apresenta a classificação de controle interno como contábil e administrativo, adequando-o às necessidades e aos requisitos de um Sistema de Informação.

Tabela 1:1: Parâmetros de Controle Interno

CONTROLE INTERNO	
CONTÁBIL	ADMINISTRATIVO
Fidelidade da informação em relação ao dado	Eficácia
Segurança física	Eficiência
Segurança lógica	Obediência às diretrizes da alta administração
Confidencialidade (Privacy)	
Obediência à legislação em vigor	

Fonte: Arima (2006, p. 13)

Adiante serão detalhados os itens relativos ao controle interno contábil e administrativo.

1.7.1 Fidelidade da informação em relação ao dado

Fidelidade da informação em relação ao dado, quer dizer que, os dados extraídos estão corretos e são condizentes aos que deram origem aos mesmos, ou melhor, os dados que deram entrada no sistema.

Consiste na validação dos resultados do sistema de informação ao nível de registros, informações e dados. Entende-se por sistema de informações os arquivos lógicos, banco de dados, documentos de entrada de dados e relatórios de saída.

A validação da fidelidade da informação em relação ao dado pode levar a tomar medidas corretivas para os processos falhos ou errôneos, pelo grau de falha ou erro detectado na confrontação.

Cabe ao auditor, neste controle, certificar-se de que não foram alterados dados e nem perdidos durante o processamento dos dados em informação.

1.7.2 Segurança física

Entende-se como segurança física a avaliação dos recursos materiais e humanos aplicados ao ambiente de TI. (DIAS, 2000, p. 99)

De acordo com Dias (2000, p. 100), *"a segurança física pode ser abordada de duas formas: segurança de acesso, que trata das medidas de acesso físico não autorizado, e segurança ambiental, que trata da prevenção de danos por causas naturais."*

1.7.2.1 Controle de acesso físico

Pode-se definir controle de acesso físico, como sendo as medidas a serem tomadas visando proteger equipamentos e informações contra usuários não autorizados, prevenindo que os mesmos tenham acesso a esses recursos. (DIAS, 2000, p. 100)

Dias (2000, p. 100), informa que os recursos a serem protegidos pelo controle de acesso físico são:

> "os equipamentos (servidores, estações de trabalho, CPU's, placas, vídeos, mouses, teclados, unidades de disco, impressoras, scanners, modems, linhas de comunicação, roteadores, cabeamento elétrico, etc.), a documentação sobre hardware e software, aplicativos, política e procedimentos de segurança, os suprimentos (disquetes, fitas, formulários, papel) e as próprias pessoas"

A proteção física dos recursos apresentados constitui-se em uma barreira adicional e anterior às medidas de segurança de acesso lógico, protegendo também os recursos lógicos, tais como programas e dados.

1.7.2.2 Controle ambiental

Assim como o controle de acesso físico, é de fundamental importância que o controle ambiental conste na política de segurança da empresa, pois estão diretamente relacionados a disponibilidade e integridade dos recursos computacionais. (DIAS, 2000, p. 82)

Esse controle visa proteger os recursos de TI da empresa contra possíveis danos causados por desastres naturais/ambientais, tais como enchente, incêndios, etc..

As principais ameaças à segurança física que se pode identificar são o calor, poeira, magnetismo, quedas, empenamento, incêndios, enchentes, umidade, etc..

1.7.3 Segurança lógica

A segurança lógica consiste em estimar o nível de segurança e controle empregado com recursos tecnológicos nos *softwares* e *hardwares* de um determinado sistema de informações. (DIAS, 2000, p. 85)

Para implementar segurança lógica, torna-se necessário que a empresa aplique medidas de controle de acesso lógico, afim de proteger seus recursos computacionais (equipamentos, *softwares*, aplicativos e arquivos de dados) contra perda, danos ou modificação não autorizada.

Para Dias (2000, p 84), controle de acesso lógico é:

> um conjunto de medidas e procedimentos, adotados pela organização ou intrínsecos aos softwares utilizados, cujo objetivo é proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por usuários ou outros programas.

É de vital importância a manutenção adequada das rotinas de falhas ou erros, identificadas a partir das informações geradas pela reconstituição dos dados originais pelas trilhas de auditoria, garantindo assim a segurança lógica do sistema. (DIAS, 2000, p. 85)

1.7.4 Confidencialidade

Confidencialidade é o controle das informações que uma pessoa consegue manter perante o acesso de pessoas não autorizadas, sejam elas internas ou externas, ou informações consideradas privativas ou de sigilo, devendo estar disponível somente para a alta administração. (ARIMA, 1994, p 26)

Cabe salientar que de nada adianta ter confidencialidade no sistema de informações, no uso de sofisticados recursos tecnológicos, se o usuário deixar à vista de terceiros os relatórios de saída.

Para Dias (2000, p 90) convêm que a informação seja classificada de acordo com seu valor, requisitos legais, sensibilidade e criticidade para a organização.

Segundo a ISO 17799 (2005, p. 23), *"convém que seja responsabilidade do proprietário do ativo, definir a classificação de um ativo, analisando-o criticamente a intervalos regulares, e assegurar que ele está atualizado."*.

Finalizando os itens relativos ao controle interno contábil, temos a obediência a legislação em vigor, que será abordado a seguir.

1.7.5 Obediência à legislação

É a constatação de que os processos e rotinas do sistema de informações estão de acordo com as leis vigentes no país, estado, município e entidades externas responsáveis pelo estabelecimento de normas e procedimentos.

Conforme Arima (1994, p.17), *"a validação sob essa especificação ou parâmetro de controle interno, está vinculada à necessidade de estar atendendo as regulamentações e condicionantes do ambiente externo..."*.

Os próximos itens de controle, referentes ao Controle Interno Administrativo, são os controles que se referem principalmente à eficácia e eficiência operacionais e obediência às diretrizes administrativas, que no modo geral incluem controles como análise, estatísticas,

estudos de tempo e movimento, relatórios de desempenho, programas de treinamento de empregados e controles de qualidade.

1.7.6 Eficácia

A eficácia do sistema de informações consiste no atendimento adequado dos objetivos e necessidades das empresas, através dos seus recursos tecnológicos de informação.

Pode ser medida através do grau de atendimento adequado e do nível de satisfação do usuário, quanto ao operacional, tático e estratégico do sistema informatizado.

1.7.7 Eficiência

Um sistema de informação eficiente é aquele que apresenta uma ótima combinação entre os recursos humanos, materiais e tecnológicos, resultando num melhor custo/benefício dos processos computacionais.

Para Arima (1994, p.18), eficiência *"ao nível do sistema de informação representa uma otimização na aplicação dos recursos tecnológicos, humanos e materiais, implicando na agilização do seu processo produtivo"*.

1.7.8 Obediência às diretrizes da alta administração

Este ponto de controle consiste em verificar se o sistema informatizado de informações atende as normas e procedimentos determinados pelos diversos setores operacionais e administrativos da empresa. (ARIMA, 1994, p.18). Este item trata especificamente do atendimento a normatização interna da empresa, avaliando a adequação dos processos às políticas e normal estabelecidas pela alta administração.

1.8 Ponto de controle e ponto de auditoria

Neste item é tratado ponto de controle, traçando um paralelo com ponto de auditoria, verificando as diferenças entre os dois pontos.

Arima (1994, p 29) define que ponto de controle é "...uma situação levantada que merece ser validada pela Auditoria de Sistemas, segundo determinados parâmetros de controle interno.".

Ponto de Controle é a situação do ambiente computacional, composta pela combinação das rotinas operacionais e de controle e os recursos humanos, materiais e tecnológicos agrupados.

Pode-se definir recursos tecnológicos, as informações componentes dos arquivos trabalhados e instruções componentes do programa de atualização do sistema informatizado e, os recursos materiais podem ser, a configuração do computador onde é processado o programa de atualização e dispositivos (*drive* de disco, formulário contínuo etc.), onde são colocadas as informações e, por sua vez, recursos humanos seria o operador do computador no momento do processamento do programa de atualização.

O ponto de auditoria é o ponto de controle eleito para avaliação e que apresentou fraqueza em relação aos parâmetros do controle interno, conforme demonstra o fluxograma da figura 1-2.

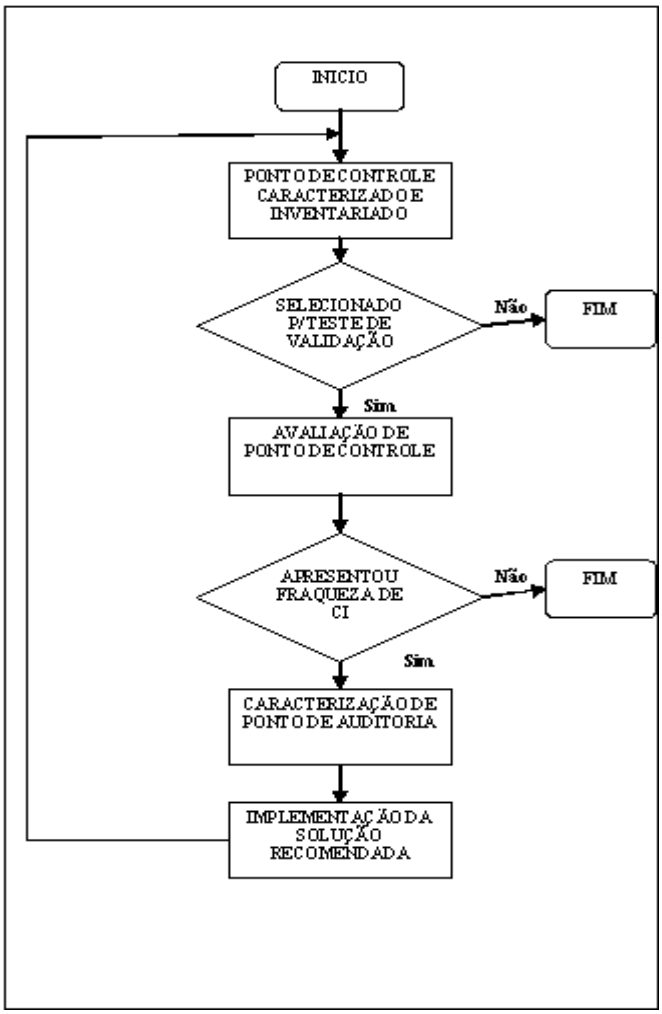


Figura 1-2: Ciclo de vida do Ponto de Controle e Ponto de Auditoria

Fonte: Arima (2006, p.31)

A figura 1.2 apresenta o fluxo de avaliação de ponto de controle efetuado pelo auditor em suas análises efetuadas durante um processo de auditoria. Caso o ponto de controle avaliado apresente fraqueza, torna-se um ponto de auditoria, caso contrário, o ponto de controle será considerado adequado e encerra-se a avaliação.

Neste capítulo foi abordado controle interno, seu conceito, parâmetros utilizados e traçando um paralelo entre controle interno e auditoria. Verificou-se que a auditoria é uma maneira de atestar a adequação dos controles internos da empresa.

Desta forma, no próximo capítulo é abordado o tema Auditoria, seus conceitos, tipos existentes e técnicas utilizadas.

2 AUDITORIA

A busca pela eficiência operacional tornou-se constante em grandes empresas e conglomerados. Um dos pontos-chave para alcançar tal propósito é a integração e a sinergia entre as diversas áreas. Neste capítulo, aborda-se a importância do envolvimento da auditoria no processo de avaliação dos controles internos das instituições. *(PEREZ JUNIOR, 1995, p. 9)*

Wilian Attie em seu livro *Auditoria Conceitos e Aplicações* informa que *"A auditoria é uma especialização contábil voltada a testar a eficiência e a eficácia do controle patrimonial implantado com o objetivo de expressar uma opinião sobre determinado dado"*. (ATTIE, 1998, p.25)

Como pode-se entender, auditoria é um conjunto de procedimentos técnicos, através dos quais o profissional da área baseia-se para elaborar sua opinião sobre determinado dado da entidade.

Para José Hernandes Perez Junior, em seu livro Auditoria de Demonstrações contábeis:

> "A auditoria pode ser definida como o levantamento, o estudo e a avaliação sistemática de transações, procedimentos, rotinas e de demonstrações contábeis de uma entidade, com o objetivo de fornecer a seus usuários uma opinião imparcial e fundamentada em normas e princípios sobre sua adequação." *(PEREZ JUNIOR, 1995, p11)*

Maria Goreth M. A. Paula, no livro Auditoria Interna: embasamento conceitual e suporte tecnológico, define auditoria como a:

> "atividade de avaliação independente e de assessoramento da administração, voltada para o exame e para a avaliação da adequação, eficiência e eficácia dos sistemas de controle e da qualidade do desempenho das áreas, em relação às atribuições e aos planos, metas objetivos e políticas definidas para elas". *(PAULA, 1999, p.31)*

Entende-se que a auditoria não só contribui para a contabilidade, mas também para a administração, fornecendo-lhe subsídios para o controle, ajuste e a orientação dos sistemas de controle das áreas em relação ao que foi proposto.

Paula (1999) define ainda auditoria como:

> "uma atividade de avaliação independente, que atua em parceria com administradores e especialistas, deverá avaliar a eficiência e a eficácia dos sistemas de controle de toda entidade, agindo pro*a*tivamente, zelando pela observância às políticas traçadas e provocando melhorias, fornecendo subsídios aos proprietários e administradores para a tomada de decisão, visando ao cumprimento da missão da entidade".

Constata-se que, em ambos os conceitos apresentados, a auditoria tem como premissa a proteção e orientação, a fim de que tudo se passe com exatidão e eficiência para o alcance da administração.

Para que esse propósito seja alcançado, a auditoria divide-se em várias áreas/tipos para que obtenha a abrangência desejada, conforme abordado a seguir:

2.6 Tipos de auditoria

De acordo com o manual de Auditoria do Tribunal de Contas da União (1998) existem cinco tipos de auditoria das quais se pode citar:

- Auditoria Contábil - Destina-se a examinar e avaliar os componentes das demonstrações financeiras no que concerne à adequação dos registros e procedimentos contábeis, sistemática dos controles internos, observância de normas, regulamentos e padrões aplicáveis, bem como sujeição aos princípios fundamentais de contabilidade.

- Auditoria de Gestão - Direcionada para a avaliação da eficiência e eficácia dos resultados em relação aos recursos materiais e humanos disponíveis.

- Auditoria Operacional - Tem por finalidade emitir opinião com vistas a certificar a regularidade das contas; verificar a execução de contratos, convênios, acordos, guarda e administração dos valores e bens da empresa.

- Auditoria Especial – Abrange os trabalhos especiais de auditoria, não compreendidos na programação anual estabelecida.

- Auditoria de Sistemas – Compreende a análise dos processos automatizados para processamentos e emissão das demonstrações contábeis, com o objetivo de expressar opinião sobre a integridade das informações demonstradas. Tal análise proporciona também uma avaliação do seu ambiente tecnológico, uma vez que, para a análise dos processos automatizados, há a necessidade de avaliar o ambiente físico e o ambiente lógico.

Os tipos de auditoria descritos são definidos por área de atuação, entretanto cada um possui uma natureza, como segue.

2.7 Natureza da auditoria

De acordo com Dias (2000, p.10), "*não há uma na literatura especializada uma classificação ou denominação padronizada para a natureza ou dos diversos tipos de auditoria existentes*", porém, cita que os tipos mais comuns encontrados são:

- Auditoria Interna - auditoria realizada por departamento interno responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma empresa.

- Auditoria Externa – Auditoria realizada por agente externo e independente da empresa, geralmente com vista a fornecer informações para o mercado e acionistas da empresa.

- Auditoria Articulada – Trabalho Conjunto de auditorias internas e externas, devido a superposição de responsabilidade dos órgãos fiscalizadores, caracterizado pelo uso comum de recursos e comunicação recíproca dos resultados.

Tanto a auditoria interna quanto auditoria externa em auditoria de sistemas utilizam-se de técnicas de auditoria específicas, que são detalhadas na próxima seção.

Neste item foi abordada auditoria, seus tipos existentes e a natureza de cada uma. Adiante é abordado especificamente auditoria de TI, apresentando seus conceitos e objetivos, visto que trata-se do foco do trabalho.

2.8 Auditoria de TI

O termo tecnologia da informação surgiu inicialmente como uma classificação do departamento de comércio dos Estados Unidos da América para industrias cujos serviços e ou produtos correspondem a *hardware*, *software*, serviços de informática, equipamentos e serviços de comunicação. Na verdade, a nomenclatura mais completa seria tecnologia da informação e comunicação (TIC), porém sua forma mais simplificada, sem a palavra comunicação, foi a denominação que mais se difundiu nos últimos anos. (DIAS, 2000, p. 131)

Conforme Dias (2000, p.136), pode-se dizer que a nomenclatura tecnologia da informação engloba termos como informática, sistemas, telecomunicações, ciência da computação, processamento de dados, engenharia de sistemas e *software*.

Como conseqüência disso, a auditoria de sistemas, como era conhecida passou a ser utilizada como sinônimo de auditoria de TI.

Visto que junto aos autores não há um consenso em relação ao nome utilizado para esta auditoria, serão utilizados os dois termos neste trabalho, dependendo do autor referenciado.

Na auditoria de TI, é analisado um conjunto de controles gerenciais e procedimentos que afetam todo o ambiente de informática e, conseqüentemente, todos os sistemas aplicativos.

Para Dias (2000, p.137), a auditoria de TI tem por função verificar os padrões e políticas adotadas pela organização, a operação sobre sistemas e dados, a disponibilidade e a manutenção do ambiente computacional, a utilização de recursos computacionais, a gerencia de banco de dados e de rede, além de todos os aspectos relacionados à segurança das informações, como segurança física, lógica e ambiental, e continuidade dos serviços de informática.

2.9 Conceitos e objetivos

Desde os registros da história da auditoria, até bem pouco tempo, ela era basicamente direcionada para o setor financeiro, devido a sua importância dentro da gestão empresarial, porque, aí que era controlado e manipulado o patrimônio da entidade.

Nos dias de hoje, a memória, a história, os projetos, as pesquisas e quase todas as informações da empresa são armazenadas, condicionadas em arquivos eletrônicos dos sistema eletrônico de dados, visto que o a própria dinâmica do setor empresarial e suas demandas de negócios, faz com que a empresa dependa do sistema de informações que possui. Sistema este, que enfrenta uma série de riscos.

Em anãlise a Joaquim Rubens Fontes, em seu livro *Manual de Auditoria de Sistemas:*

> Os principais ativos da empresa são as informações e os recursos humanos que delas se utiliza. Essas informações são colhidas, processadas, armazenas e fornecidas para orientarem as decisões e rotinas. A qualidade e a confiabilidade desses dados influem decisivamente no sucesso dos negócios. Por essa importância vital, fica visível a necessidade e a utilidade de se garantir a sua qualidade. *(FONTES, 1991 p337)*

Pode-se acrescentar a essa citação, que a auditoria deve ter uma especialização a mais, para poder atender a essas necessidades das empresas.

A Auditoria de TI pode ser conceituada como sendo uma função que estuda, analisa e avalia um ambiente, um bem, um serviço ou, informação, de forma sistemática e periódica, com o objetivo de verificar se as normas/políticas em vigor estão sendo cumpridas, se o que deve ser feito, é realmente aquilo que acontece, se existem problemas ou irregularidades, e se há medidas de controle de segurança, que garantam a redução e combate aos riscos existentes para, posteriormente, relatar os resultados do trabalho e recomendar as correções necessárias, maximizando o uso de recursos.

O Conselho Regional de Contabilidade do Estado de São Paulo (CRC-SP), define auditoria de sistemas como um meio que:

> avalia o ambiente de processamento de dados para identificar e avaliar os possíveis riscos (erros, falhas, irregularidade, ineficiência etc.) que estejam ocorrendo, ou que possam ocorrer, e faz recomendações para correção e melhoria dos controles internos para diminuição dos riscos levantados. *CRC-SP (1999, p92)*

Sabendo que a maioria das atividades em uma empresa estão, direta ou indiretamente, fortemente ligadas ao processamento eletrônico de dados e a complexidade resultante dessas atividades, exigem da empresa criação de auditoria especializada para que possam, de certa forma, certificar-se de que, nessas atividades, não estão sendo lesadas.

Já em outra conceituação mais sucinta tem-se:

> Auditoria de sistemas é uma atividade voltada à avaliação dos procedimentos de controle e segurança vinculados ao processamento eletrônico das informações. CRC-SP (1999, p 92)

Ressalta-se que, em ambos os conceitos apresentados, a auditoria tem como preocupação fundamental a segurança e objetiva uma sugestão para a correção e melhoria.

Já como objetivos, entende-se que a auditoria deve propiciar aos usuários do sistema, a segurança de que as informações que estão sendo manipuladas estão corretas e os resultados alcançados espelham os dados inseridos.

A colocação mais contundente dos objetivos da auditoria de sistemas foi encontrada na obra do CRC-SP intitulada Auditoria por Meios Eletrônicos.

> A auditoria de sistemas objetiva certificar-se que:
>
> - As informações são corretas e oportunas;
> - Existe um processamento adequado das informações;
> - As informações estão protegidas contra fraudes;
> - Existe a proteção das instalações e equipamentos;
> - Existe a proteção contra situações de emergência (paralisação de processamento, perda de arquivos, inundações, incêndios, etc.) CRC-SP (1999, p 93).

Pode-se entender a auditoria de sistemas como uma assessoria que atende a alta administração da organização, fornecendo um relatório completo de todas as tarefas que podem ser desenvolvidas com segurança por um sistema, tanto que Gil estabelece que a auditoria de sistemas deve: “*buscar a otimização do emprego dos recursos do Processamento*

Eletrônico de Dados e a melhoria das atividades empresariais com a aplicação desses recursos”. (1999, p 64)

Aí está a base do sucesso de muitas empresas, saber aproveitar ao máximo os recursos da informática para melhorar e agilizar suas rotinas e atividades, para maximizar os resultados almejados.

- Para implantar auditoria de Tecnologia da informação dentro de uma empresa com sucesso, é de fundamental importância que sejam seguidas as seguintes premissas:
- ter aprovação e apoio da alta administração da empresa;
- ter a colaboração dos profissionais e usuários da área de TI da empresa;
- ter total independência para auditar e relatar irregularidades sem interferência ou coação de terceiros;
- ter livre acesso dentro de todos os departamentos da empresa;
- ter métodos apropriados, técnicas de auditoria e definição clara dos objetivos (curto, médio e longo prazo);
- controle e planejamento dos trabalhos de auditoria e acima de tudo a localização em posição privilegiada dentro da estrutura funcional da empresa;

Além dessas premissas, devem ser observados outros aspectos que podem ser decisivos para a eficiência de uma auditoria, como por exemplo, o conhecimento técnico dos auditores, cuja não observância poder vir a ocasionar possíveis limitações a atuação da auditoria.

3 ESTUDO DE CASO

Yin (2001, p. 13) define estudo de caso com base nas características do fenômeno em estudo e com base num conjunto de características associadas ao processo de recolha de dados e às estratégias de análise dos mesmos. Para este autor, o estudo de caso é um processo de investigação empírica com o qual se pretende estudar um fenômeno contemporâneo no contexto real em que este ocorre, sendo particularmente adequado ao seu uso quando as fronteiras entre o fenômeno em estudo e o contexto em que ele ocorre não são claramente evidentes.

Para Yin (2001, p. 13) o estudo de caso é uma metodologia de investigação particularmente apropriada quando procuramos compreender, explorar ou descrever acontecimentos e contextos complexos, nos quais estão simultaneamente envolvidos fatores.

Neste estudo é realizado um apanhado geral da empresa, com objetivo de avaliar a situação atual da auditoria de TI, verificar as limitações da metodologia utilizada e buscar propor uma solução para os problemas encontrados. Após implementação da solução proposta será efetuada análise da solução, para verificar se a mesma atingiu os objetivos esperados.

Visto que o foco deste trabalho é auditoria de TI, será dada maior atenção à Gerencia de Auditoria de Sistemas da empresa.

3.6 Dados da empresa

Ramo de atuação: Mercado Financeiro

Tipo: Instituição Financeira

Funcionários: 11000

Nº de Agências: 410 espalhas em diversos estados brasileiros, tais como Bahia, Ceará, Minas Gerais, Pernambuco, Paraná, Rio de Janeiro, Santa Catarina, São Paulo, Rio Grande do Sul e Distrito Federal, além de representação em Buenos Ayres, na Argentina, Nova York, nos Estados Unidos e Cayman, na Suíça.

Para possibilitar um melhor entendimento sobre a estrutura interna da empresa, identificando onde a auditoria se enquadra no interior da mesma, é apresentado um organograma da empresa.

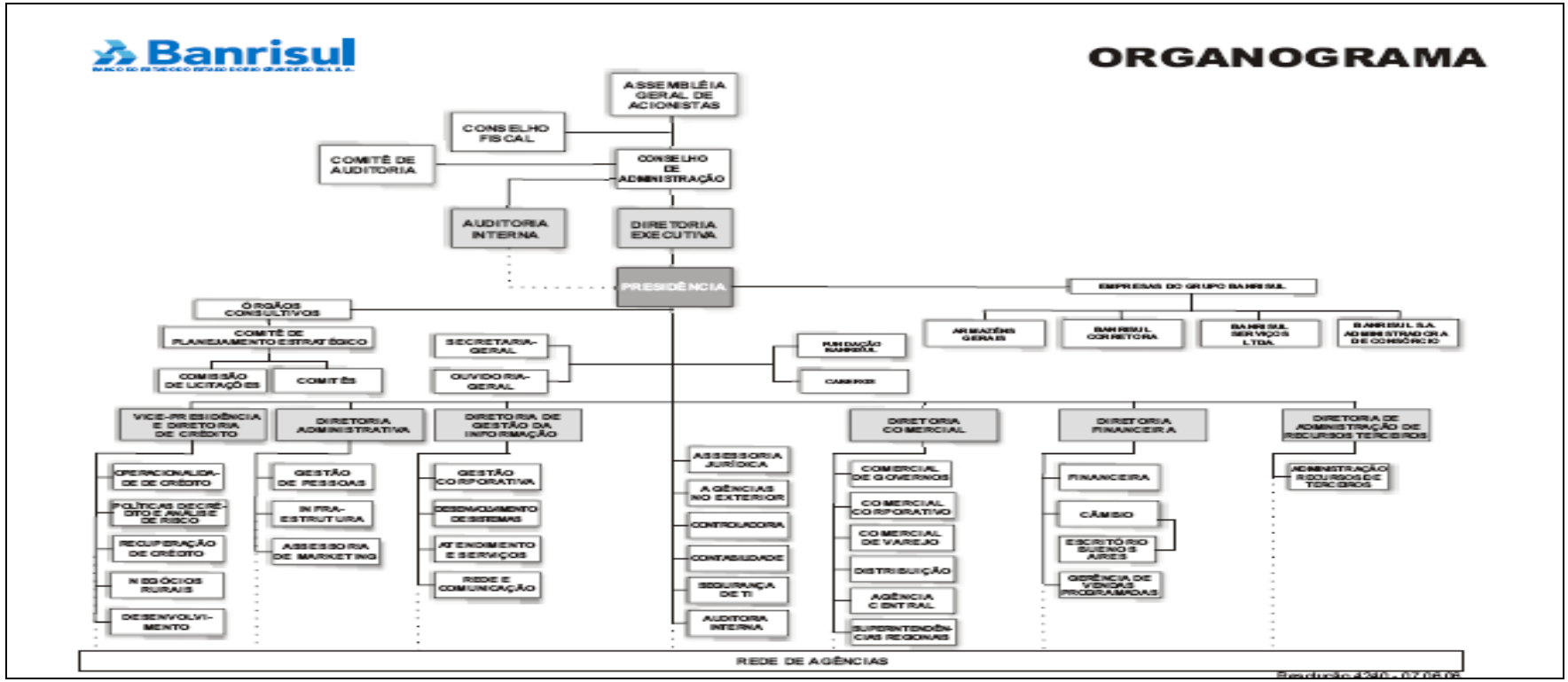


Figura 3-1**:** Organograma da empresa**.**

Fonte: a empresa

Através do organograma é possível observar que a auditoria interna não está vinculada a nenhuma diretoria da empresa, a mesma é ligada diretamente ao conselho de administração e ao comitê de auditoria da empresa e serve como assessoria para a presidência.

O fato de não estar subordinada a nenhuma diretoria, deve-se à necessidade de independência necessária à função da auditoria interna.

3.7 Estrutura organizacional da auditoria interna

Através da Resolução 4105, de 30 de maio de 2003, redefiniu-se a estrutura organizacional da Auditoria Interna, a qual passou a apresentar a seguinte composição:

a) chefe da auditoria;

b) gerência de auditoria de sistemas;

c) gerência administrativa;

d) gerência de auditoria operacional;

Para melhor compreensão, a figura 3-2 mostra o organograma da unidade de auditoria interna da empresa.

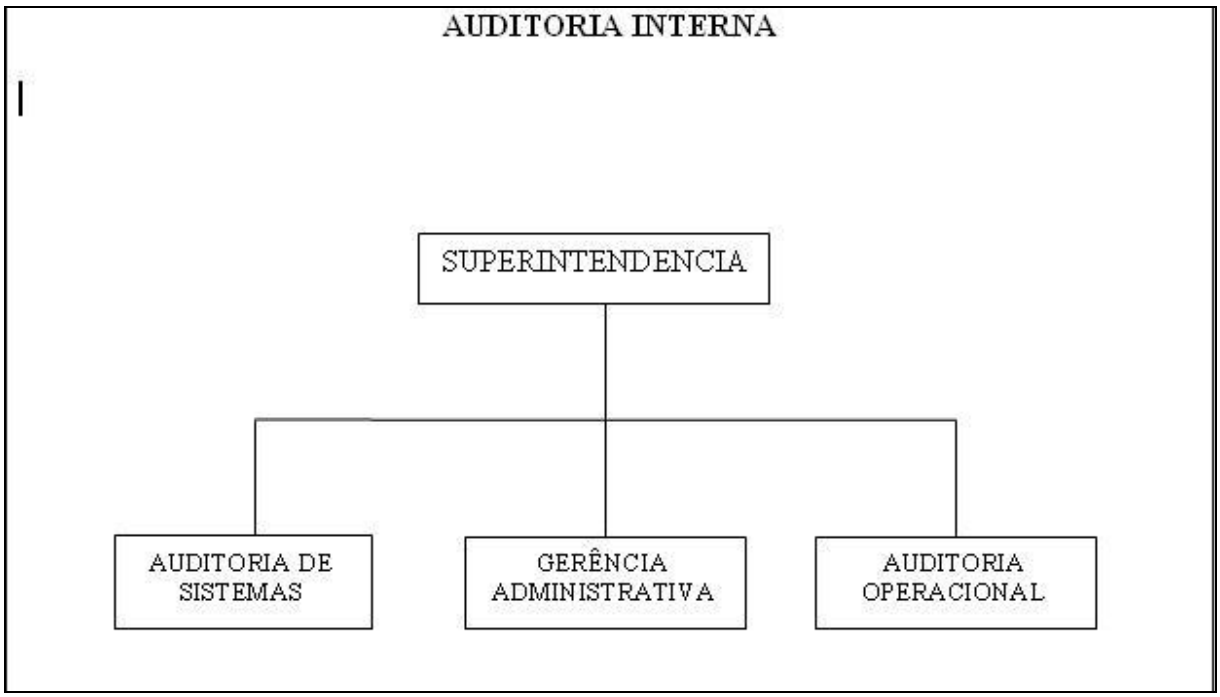


Figura 3-2: Organograma da auditoria interna**.**

Fonte: Banrisul

Os dados apresentados neste estudo de caso, até a página 45 tem como fonte a empresa objeto de pesquisa.

3.7.1 Chefe da auditoria

O chefe da auditoria é subordinado ao comitê de auditoria, conselho de administração ou, por delegação deste, a um diretor designado por resolução.

O chefe de auditoria é o responsável pela gestão dos serviços na Área de Auditoria Interna da empresa, relacionados ao desenvolvimento de programas de auditoria interna em todos os sistemas e fluxos de operações financeiras; avaliação dos Controles Internos Aplicados; verificação do fiel cumprimento dos procedimentos operacionais e

administrativos, comerciais e contábeis; orientação no preparo de relatórios parciais e globais das auditagens realizadas e execução de auditoria especiais. Observando a legislação e as normas vigentes.

3.7.2 Gerência de auditoria de sistemas

O gerente executivo desta área estará subordinado diretamente ao chefe da auditoria e será responsável pelas seguintes atividades:

- Realizar auditorias em sistemas de informação em desenvolvimento e em produção, avaliando e validando os controles internos durante o processo de construção, alteração e implementação dos sistemas em desenvolvimento e revisando os controles internos e aspectos de segurança nos sistemas em produção.

- Efetuar auditorias extraordinárias nos casos de episódios envolvendo sistemas de informação ou recursos tecnológicos, levantando e analisando as causas da ocorrência, identificando fragilidades ou insuficiência de controles que propiciaram a mesma;

- Auditar o ambiente de tecnologia da informação (TI), verificando a existência e a adequação dos controles internos e aspectos de segurança dos recursos tecnológicos, dos dados, informações, produtos e programas.

Para a realização das auditorias, são utilizadas as seguintes técnicas:

- Visita in loco;

- Análise Física de Documentos;

- Análise de log’s;

- Entrevistas;

- Questionários;

- Análise de relatórios.

- Simulação Paralela;

Os auditores podem efetuar o acompanhamento de todas as etapas do desenvolvimento de um sistema, testes, até sua implantação, para verificar questões relativas à segurança do sistema em desenvolvimento e resguardar a empresa de possíveis falhas decorrentes da inobservância de controles internos.

3.8 Metodologia de trabalho da auditoria de sistemas

A partir do planejamento estratégico definido para a instituição, anualmente é elaborado o planejamento de atividades previstas para o exercício seguinte. Esse documento, no qual são identificadas as áreas prioritárias para serem realizadas auditorias, é encaminhado para análise do conselho de administração e presidência do Banco.

Os trabalhos de auditoria são efetuados a partir das definições do Plano Anual de auditoria em que estão priorizadas as áreas com maior relevância, ou seja, com um nível maior de importância para a empresa.

Até o corrente ano essa avaliação é baseada em informações coletadas durante as auditorias e, sobretudo, no conhecimento do gerente da auditoria de sistemas.

A metodologia utilizada nos trabalhos de auditoria contempla a verificação do cumprimento das normas internas, legislação e recomendações do Banco Central, além das melhores práticas de mercado, tanto na auditoria de rotina, quanto nas verificações especiais.

As auditorias contemplam a realização de reunião de abertura, com o registro da respectiva ata, onde são expostos os objetivos da auditoria interna e do trabalho.

Se durante os trabalhos de auditoria forem identificadas ocorrências de natureza grave, será solicitada manifestação formal dos responsáveis e da administração da unidade auditada.

Na reunião final é apresentado o resultado da auditoria e são discutidos os prazos e os responsáveis para realização das ações corretivas registradas no plano de ação, cuja verificação é efetuada conforme os prazos acordados entre o auditor e a unidade auditada.

De acordo com a gravidade da ocorrência, determina-se a imediata regularização ou prazo compatível com a natureza da gravidade.

Nos casos em que as ocorrências de maior relevância ou gravidade não foram regularizadas, as auditorias são concluídas com ressalvas e os resultados são encaminhados à Diretoria Executiva.

No próximo item, é apresentado os processos envolvidos na auditoria de sistemas da empresa.

3.8.1 Processos envolvidos na auditoria de sistemas

De acordo com os auditores de sistemas da empresa, são efetuadas auditorias periódicas, de acordo com o cronograma existente, com o intuito de validar os controles existentes no sistema ou ambiente de TI auditado.

Os auditores são divididos em áreas de atuação inicialmente entre Rede e Sistemas.

Devido à complexidade de alguns sistemas operacionais do banco, o que demanda um grande tempo de estudo para que o auditor conheça a arquitetura do sistema, alguns sistemas operacionais ficam somente com um auditor, aumentando assim a eficiência da auditoria.

De acordo com o cronograma e disponibilidade dos auditores, é repassado ao auditor que efetuará a auditoria, pela gerência da unidade, o que será tema de auditoria.

Após esse momento, o auditor confecciona um documento denominado de programa de auditoria, onde constam as técnicas que serão utilizadas, os recursos necessários e o tempo previsto para a realização da auditoria.

Após ser efetuado o estudo do objeto a ser auditado, é elaborado um documento denominado roteiro de auditoria, onde constam os pontos de controle que serão verificados.

Quando todos os itens constantes no roteiro, mais os itens que por ventura forem identificados no decorrer da auditoria foram verificados, é elaborado o Relatório de Auditoria, onde irão constar todas as averiguações realizadas pelo auditor.

No relatório, o auditor, além de descrever o ambiente auditado, são enumerados os pontos de controle auditados, informando se o ponto de controle está ou não adequado às normas relacionadas e boas práticas de mercado.

Para os pontos de controle que não estão adequados, são colocados os riscos resultantes da não conformidade e a recomendação do auditor.

Depois de concluído o relatório, é elaborado encaminhamento à unidade/área envolvida, onde constam as considerações referentes aos pontos de controle auditados, marcando uma reunião para que seja discutido o plano de ação referente à auditoria realizada.

Em reunião, são discutidas as recomendações do auditor e, de acordo com o entendimento dos auditados, é estipulado, para cada ponto, prazo para correção das irregularidades.

O auditor, de acordo com o plano de ação, quando se esgota o prazo para atendimento da recomendação, entra em contato com a área auditada para verificar se o ponto de controle foi ou não atendido, caso o ponto tenha sido atendido, o auditor encerra aquele ponto, senão foi atendido, é verificado porque do não atendimento e, conforme o caso, estipula-se nova data para adequação do ponto de controle.

3.8.2 Limitações da metodologia utilizada

Uma das maiores dificuldades existentes na auditoria de TI encontra-se na falta de ferramenta que automatize os procedimentos de auditoria.

O auditor necessita replicar informações em diversos locais para geração dos documentos necessários em sua auditoria, o que além de demandar tempo, aumenta a possibilidade de erros

Outro ponto observado é o controle das recomendações, pois há a necessidade do auditor entrar em contato com os responsáveis para verificação do atendimento das recomendações contidas no plano de ação. Por serem observados diversos pontos de controle nas auditorias, torna-se necessário que a auditoria de TI efetue um correto gerenciamento do

atendimento às suas recomendações, o que nem sempre é passível de ser efetuado pelo auditor isoladamente, visto que certas recomendações podem demorar indefinidamente para serem atendidas.

Para que seja possível um maior gerenciamento das auditorias, torna-se necessário a utilização de uma ferramenta de apoio que efetue o controle das auditorias realizadas e forneça informações de apoio a decisão à gerência da auditoria.

No capítulo seguinte é abordada a análise de riscos como uma métrica para a tomada de decisão no processo do planejamento de auditorias a serem realizadas.

4 ANÁLISE DE RISCOS

Conforme o guia de referência denominado “Guia Sairbanes Oxley”, criado pela empresa de auditoria Deloitte, eventos envolvendo grandes fraudes financeiras em empresas como Enron e WorldCom, cujos administradores alegaram “não ter conhecimento”, fizeram os Estados Unidos da América criar a lei Sarbanes Oxley (SOX) com objetivo de redefinir as regras para governança corporativa e proteger os investidores de todo o mundo.

Similar a esta lei, está a resolução 3380 do Banco Central (BACEN) que dispõe sobre a implementação de estrutura de gerenciamento do risco operacional nas instituições bancárias que operam no Brasil, caso da empresa objeto do estudo.

Considerando ser a informação, um ativo de alto valor para as empresas e, a Auditoria de TI tratar a segurança da informação, entende-se como um bom parâmetro para priorização dos sistemas auditados, a análise dos mesmos em função do risco que apresentam.

Sendo assim, nesta parte do trabalho é abordada Análise de Risco, apresentando o assunto e em seguida a proposta de aplicação no trabalho.

Por entender se tratar de um *framework* reconhecido junto ao mundo corporativo, foi utilizado como principais referências as ISO 17799 e 27005.

De acordo com a ISO 17799 :

> “O nível de risco aumenta de acordo com as ameaças recebidas e a sua vulnerabilidade frente a estas ameaças.”

Análise de riscos, conforme define Cardella (1999), "*é o estudo detalhado de um objeto, com a finalidade de identificar perigos e avaliar os riscos ou danos que possam causar ações indesejadas*", ou seja a análise de risco serve para a empresa analisar os seus sistemas e processos, visando inventariar seus riscos com vistas a prevenção de futuras ocorrências.

De acordo com a ISO27005 (2008, p.14) pode-se utilizar diferente níveis de detalhamento para a apuração da análise de riscos, dependendo da criticidade dos ativos, da extensão das vulnerabilidades e do histórico de incidentes envolvendo a organização.

A ISO define ainda que podem ser utilizadas estimativas quantitativas, qualitativas ou uma combinação de ambas.

Neste trabalho, por achar mais indicado para a análise e a dificuldade de valoração dos sistemas, é abordada a análise quantitativa.

Para CARDELLA (1999, p.37):

> o risco é definido como sendo a combinação da freqüência de ocorrência do evento e as suas conseqüências. Assim, o risco é a relação da descrição do evento acidental, da freqüência de ocorrência acidental e a severidade das conseqüências (perdas e danos).

A ISO 27005 define: Risco = P x C x R, sendo P a probabilidade de ocorrência de um evento, C a conseqüência para a instituição em termos financeiros e R a relevância do ativo para o negócio da empresa.

Embora conste na fórmula, a relevância do ativo não é considera em um primeiro momento na análise, servindo apenas para desempate em caso de ameaças com mesma probabilidade e conseqüência.

É sugerida pela ISO a utilização de matriz de risco para apuração e comparação de riscos entre diferentes ativos, como consta na tabela 4.1.

Tabela 4:1: Matriz de Risco

Rótulo identificador da ameaça (a)	**Valor da conseqüência (do ativo)**	**Probabilidade de ocorrência da ameaça**
Ameaça A	5	2
Ameaça B	2	4
Ameaça C	3	5
Ameaça D	1	3
Ameaça E	4	1
Ameaça F	2	4

Fonte: ISO 27005 (2008, p.51)

Considerando que na Auditoria de TI da empresa analisada são verificados pontos de controle relacionados a diferentes ameaças, a partir da valoração dos controles analisados na Auditoria e a atribuição da probabilidade de ocorrência e a relevância do sistema para o negócio da empresa, é possível apurar o nível de risco de um sistema.

Sendo assim, sugere-se que cada ponto de controle avaliado no decorrer da auditoria, receba um de probabilidade de ocorrência e a conseqüência associada, para que possa ser apurada a medida de risco de um sistema.

Além da informação da probabilidade e conseqüência atrelada a cada controle interno, é necessária diferenciação de acordo com a relevância do sistema para o negócio da empresa, fazendo com que seja possível obter uma priorização entre sistemas que apresentem o mesmo valor de risco apurado.

A NBR ISO 27005 define que podem ser utilizados tantos intervalos quanto forem necessários para a análise do risco, dependendo da necessidade da empresa e dá um exemplo de intervalo que pode ser utilizado em uma análise quantitativa, conforme consta adiante:

Tabela 4:2: Valores para Riscos qualitativos

Descrição Qualitativa	**Valor associado**
Muito Baixo	0
Baixo	1
Médio	2
Alto	3
Muito Alto	4

Fonte: NBR ISO 27005

Sendo assim, o risco apurado de um sistema se dará pela soma do produto de sua vulnerabilidade e conseqüência de todos os pontos que não apresentarem controles satisfatórios; ou seja, utilizando os dados da matriz de risco sugerida pela ISO, chega-se ao seguinte resultado para um sistema X que apresenta a relevância 3:

Tabela 4:3: Matriz de Risco

Rótulo identificador da ameaça (a)	**Valor da conseqüência (do ativo)**	**Probabilidade de ocorrência da ameaça**	**Medida do Risco**	**Ordem da ameaça**
Ameaça A	5	2	**10**	2
Ameaça B	2	4	**8**	3

Ameaça C	3	5	**15**	1
Ameaça D	1	3	**3**	5
Ameaça E	4	1	**4**	4
Ameaça F	2	4	**8**	3
RISCO TOTAL			**48**	
RISCO TOTAL CONSIDERANDO A RELEVÂNCIA			**48*3=144**	

Fonte: ISO 27005 (2008, p.51)

Analisando a tabela, pode-se verificar que a medida total de risco para o sistema X é 48 e o valor apurado levando em consideração uma relevância definida aleatoriamente como sendo 3 para o sistema .

Ao aplicar a mesma métrica aos demais sistemas auditados, será possível hierarquizar os sistemas através da análise do risco e a representatividade para os negócios da empresa.

No item seguinte é efetuado uma análise das ferramentas existentes no mercado, com o objetivo de verificar a existência ou não de ferramentas que atendam a demanda da empresa.

5 SOLUÇÃO PROPOSTA

De acordo com o estudo efetuado junto à auditoria de sistemas da empresa pesquisada, verificou-se a necessidade de uma ferramenta de apoio às auditorias, que armazene dados e efetue o cálculo de risco dos sistemas para a equipe de auditores.

A partir do resultado obtido com o estudo de caso, buscou-se às ferramentas para automação de auditorias existentes no mercado, verificando as características, funcionalidades e preço, e com isso verificar a viabilidade de aquisição de uma ferramenta para suprir as demandas identificadas, conforme consta adiante:

Além das ferramentas específicas para controle de auditorias, também foram analisadas algumas ferramentas de gestão de projetos, com vistas a verificar a possibilidade de adoção de uma ferramenta dessa natureza para solução dos problemas da empresa.

Porém, devido a impossibilidade de implementação de métricas para comparação entre os sistemas, chegou-se a conclusão de que ferramentas de gestão de projetos não atendem aos requisitos de negócio da empresa.

Foram identificadas no mercado três ferramentas com solução para auditorias, cujas características estão apresentadas na figura 5.1:

Tabela 5:1: Comparativo de Sistemas

	WebGovernance	Auto Audit	Audit Automation Facilities	Sistema proposto
Plataformas suportadas				
- Windows Vista	x		x	x
- Windows XP	x	x	x	x
- Windows 2000	x	x	x	x
- Windows 2003 Server	x	x	x	x
- Plataforma	WEB	Windows	WEB	WEB
- Editor Associado	BrOffice/MSOffice	MSOffice	MSOffice	MSOffice
Planejamento de Auditoria				
- Diversos tipos de auditorias	x	x	x	
- Baseado em matriz de risco	x	x	x	x
- Mostra disponibilidades de funcionarios		x	x	
- Alteração de itens a ser verificados				x
Realização da Auditoria				
- Utilização de pontos a serem verificados	x	x	x	x
- Inserçãq de novos controles a serem verificados	x	x	x	
- Emissão de relatórios pré formatados				
- Emissão de relatórios parciais		x	x	
- Repositório de arquivos	x	x	x	
- Geração de relatórios em PDF	x	x	x	x
Acompanhamento de Auditorias				
- Controle de Auditoriasrealizadas	x	x	x	
- Consulta auditorias por auditor	x			
- Consulta auditorias por unidade gestora	x			
- Exportação dos dados	x	x		
- Perfil segregado de Usuários	x	x	x	
Acompanhamento das recomendações efetuadas				
- Acompanhamento das recomendações	x	x	x	
- Visualização Inconformidades/Resposta Auditado	x	x	x	
- inserção da resposta direta pelo auditado	x		x	
Custo por licença (sem customização)	26.333,33	4.600,00	2.783,33	

Fonte: Fabricantes

Devido ao preço elevado constatado através da análise das soluções existentes no mercado e a necessidade de customização da ferramenta, o que elevaria ainda mais o preço final do produto, sugere-se o desenvolvimento de um aplicativo que vise o atendimento das demandas específicas da empresa analisada, gerando dados estatísticos que sirvam de apoio ao planejamento das auditorias de TI da empresa, risco dos sistemas aplicando o método apresentado neste trabalho, além da geração de documentos utilizados pelas auditorias.

Diante disso, sugere-se a modelagem de uma ferramenta de apoio ao gerenciamento dos processos que envolvem a auditoria de sistemas, contendo algumas funcionalidades, abordadas no próximo item.

5.1 Requisitos do sistema proposto

Através da análise efetuada pela gerência de auditoria de sistemas, segue requisitos do sistema proposto:

Requisitos de negócio

- Possibilitar a elaboração do planejamento anual da Auditoria Interna;
- Possibilitar que o planejamento anual seja baseado em matriz de risco e alinhado aos objetivos e estratégias do negocio;
- Proporcionar a padronização do processo de auditoria;
- Permitir o acompanhamento das recomendações realizadas;
- Possibilitar comunicação entre a auditoria interna e as áreas auditadas de acordo com as atividades executadas, pro meio de notificações;
- Proporcionar a revisão, elaboração e compartilhamento dos relatórios de auditoria e acompanhamento dos planos de ação;
- Permitir a documentação da auditoria de forma eletrônica;
- Utilizar recursos de editoração de texto para elaborar papéis de trabalho.

Requisitos gerais da administração do sistema

- Permitir concessão e administração de acessos;
- Permitir cadastro e administração de probabilidades e conseqüência de uma ameaça e relevância de um sistema;
- Permitir a administração de roteiros a partir de outros já formatados, bem como a sua administração;
- Possibilitar a parametrização e a geração de consultas e relatórios;
- Possibilitar a geração de relatórios estatísticos de auditorias de sistemas;

Requisitos das etapas do processo de auditoria

- permitir a definição de atividades com base nas informações atualizadas dos riscos sistêmicos;
- permitir consulta as auditorias anteriores;
- permitir a atribuição de um trabalho de auditoria interna para um ou mais auditores;
- permitir a seleção de áreas auditadas, responsáveis e envolvidos;
- permitir notificação dos auditores sobre agendamentos;
- permitir seleção de pontos a serem auditados;
- possibilitar a criação de um roteiro de auditoria permitindo seleção de pontos macros e pontos de controle previamente cadastrados, bem como o cadastramento de novos pontos de controle;

Reporte dos resultados

- possibilitar geração de relatório de modo parcial ou integral;
- possibilitar geração de relatório formatado para apreciação do auditado, contendo os pontos de auditoria e recomendações;

Acompanhamento / Follow-up

- permitir que as recomendações sejam acessadas, atualizadas e acompanhadas pelos auditores;
- permitir a inserção de comentários no plano de ação;
- possibilitar notificação no vencimento de prazos de atendimento das recomendações;

- permitir que sejam estipulados status da recomendação, como: atendida, não atendida, em avaliação, etc.

- permitir que sejam estipulados status da auditoria tais como: ativa, pendente, concluída, entre outros.

No item seguinte é apresentada a metodologia que será utilizada no projeto de desenvolvimento da ferramenta

5.2 Metodologia de projeto/desenvolvimento

Neste item, são apresentadas as técnicas que serão utilizadas para o desenvolvimento do sistema proposto.

5.2.1 Técnica de modelagem utilizada

Durante o processo de modelagem do sistema será utilizada a abordagem orientada a objetos.

5.2.2 Linguagem de modelagem

Para a modelagem será utilizada a UML (*Unified Modeling Language*), que é uma linguagem padrão para a elaboração da estrutura de projetos de software. (BOOCH, 2000, p. 12)

De acordo com Booch (2000, p.13), “a UML é uma linguagem muito expressiva, abrangendo todas as visões necessárias ao desenvolvimento e aplicação de sistemas.”

Booch (2000, p.14) afirma ainda que “a UML é uma linguagem destinada a:

- Visualizar

- Especificar

- Construir

- Documentar

os artefatos de um sistema complexo de software".

5.2.3 Ferramentas utilizadas para o desenvolvimento da aplicação

Para a modelagem UML foi escolhida a ferramenta JUDE, pelo conhecimento prévio da ferramenta, a facilidade de utilização, bem como as funcionalidades que a mesma apresenta, tais como exportação dos diagramas em diversos formatos e geração automática de documetação.

Para confecção do Modelo ER, foi utilizado o DBdesigner pelo conhecimento obtido da ferramenta e a mesma atender aos objetivos propostos inicialmente.

No próximo item, são apresentados os diagramas utilizados no desenvolvimento da aplicação.

5.2.4 Diagramas

Para Booch (2000, p.89), "um diagrama é uma apresentação gráfica de um conjunto de elementos...".

A UML define nove tipos de diagramas, que podem ser combinados para determinar cada visão. A seguir são apresentados os diagramas que serão utilizados na implementação da ferramenta proposta. (BLAHA, 2006, p. 34)

5.2.5 Diagramas de Caso de Uso

De acordo com Blaha (2006, p. 45), casos de uso descrevem, do ponto de vista dos atores, um grupo de atividades num sistema que produz um resultado concreto e tangível. São descrições de interações típicas entre os usuários de um sistema e o sistema propriamente dito. Eles representam a interface externa do sistema e especificam um conjunto de exigências do que o sistema deve fazer, informando apenas 'o quê' o sistema deve fazer e não 'como' deve fazer.

Diagramas de Caso de Uso descrevem relacionamentos e dependências entre um grupo de Caso de Uso e os Atores participantes no processo. São feitos para facilitar a comunicação com os futuros usuários do sistema, e com o cliente, e são especialmente úteis para determinar os recursos necessários que o sistema deve ter. (BLAHA, 2006, p. 47)

Segundo Booch (2000, p 233) “aplica-se casos de uso para fazer a modelagem da visão estática do caso de uso do sistema. Essa visão proporciona suporte para o comportamento de um sistema”.

A figura 5.2 apresenta o diagrama de caso de uso da ferramenta proposta:

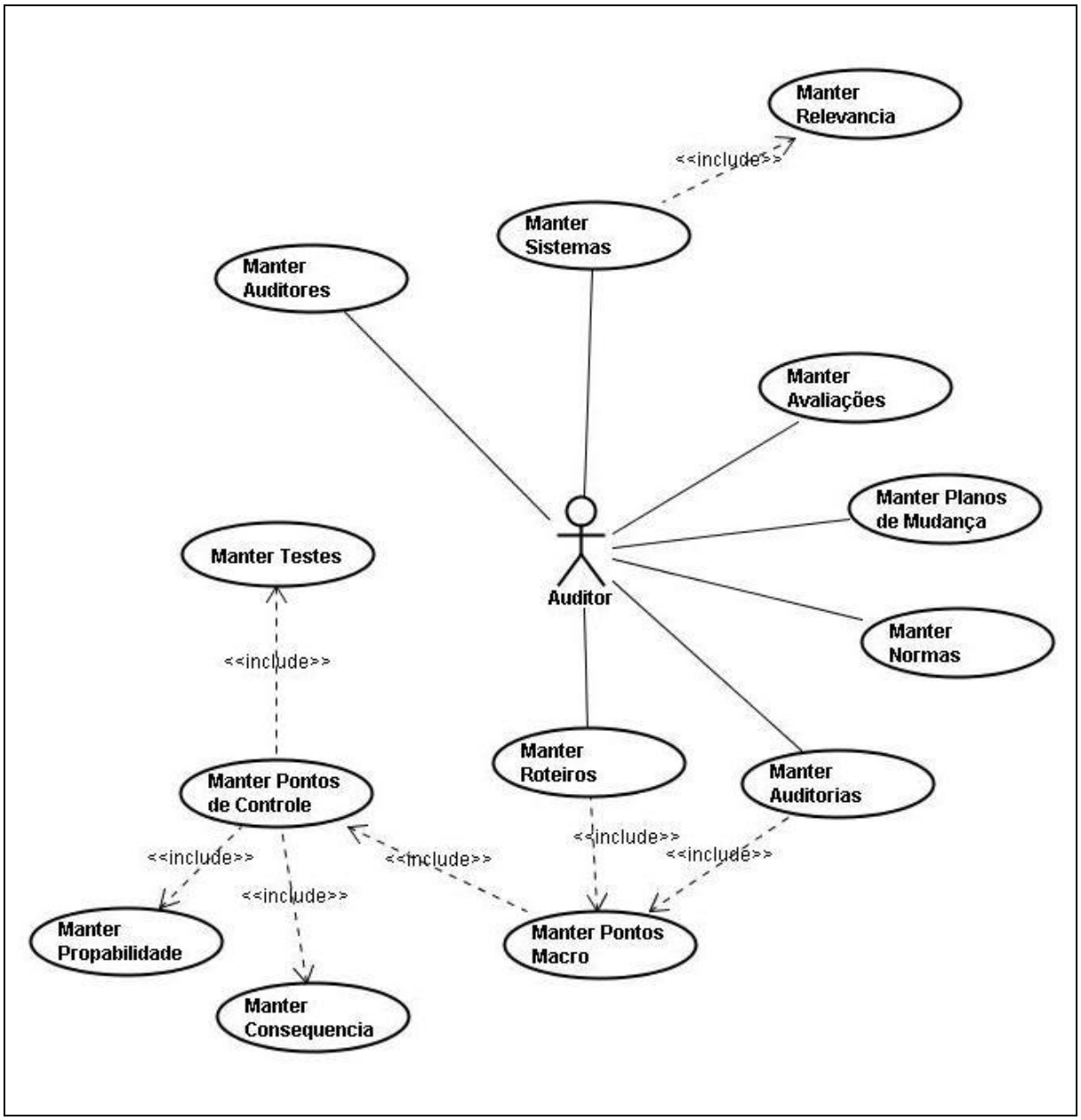


Figura 5-1- Diagrama de casos de uso do projeto

Fonte: o autor

Para melhor entendimento sobre o diagrama seguem as descrições de caso de uso:

Manter Auditores

1. O ator inicia o caso de uso selecionando "Auditores";

2. O programa exibe uma lista com os auditores cadastrados;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	
Fluxo Alternativo A1 – Inclusão	Tratamento de Exceções
3. O usuário clica na opção "Incluir Auditor"; 3.1. O programa oferece a interface para preenchimentos dos dados do auditor; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 - Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Auditor"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir o auditor; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 – Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 – Alteração	
3. O usuário clica sobre o nome do auditor na lista;	Fluxo Alternativo A3.1 - Erro ao alterar 3.3. O programa informa que houve erro

3.1. O programa oferece o formulário preenchido com os dados do auditor selecionado; 3.2. O ator altera os dados que julgar necessário e confirma; 3.3. O programa informa que a operação foi realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

Quadro 5:2 – Manter Auditores

Fonte: o autor

Manter Auditorias

1. O ator inicia o caso de uso selecionando "Auditoria";

2. O programa exibe uma lista com as auditorias cadastradas;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	
Fluxo Alternativo A1 – Inclusão	Tratamento de Exceções
3. O usuário clica na opção "Incluir Auditoria"; 3.1. O programa oferece a interface para preenchimentos dos dados da auditoria; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 – Exclusão	

3. O usuário marca um registro e clica na opção "Excluir Sistema"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir o sistema; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 - Alteração	
3. O usuário clica sobre o nome do sistema na lista; 3.1. O programa oferece o formulário preenchido com os dados do sistema selecionado; 3.2. O ator altera os dados que julgar necessário e confirma [A.3.1]; 3.3. O programa informa que a operação foi realizada com sucesso [A3.2]; 3.4. Retorna para ponto 2 do fluxo básico.	Fluxo Alternativo A3.1 - Ver Roteiro 3.2. O ator clica em "Administrar Roteiro"; 3.2.1. O programa exibe a lista de pontos macro para o tipo de sistema selecionado na auditoria; Utiliza caso de uso "Manter Pontos Macro"; Fluxo Alternativo A3.2 - Erro ao alterar 3.3. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

Quadro 5:3 - Manter auditorias

Fonte: o autor

Manter Avaliações

1. O ator inicia o caso de uso selecionando "Avaliações";

2. O programa exibe uma lista com as avaliações cadastradas;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	
Fluxo Alternativo A1 – Inclusão	Tratamento de Exceções
3. O usuário clica na opção "Incluir Avaliação"; 3.1. O programa oferece a interface para avaliação de cada teste do roteiro; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 - Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Avaliação"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir a avaliação; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 - Alteração	
3. O usuário clica sobre o nome da avaliação na lista; 3.1. O programa oferece o formulário preenchido os dados dos testes realizados; 3.2. O ator altera os dados que julgar necessário e confirma; 3.3. O programa informa que a operação foi	Fluxo Alternativo A3.1 - Erro ao alterar 3.3. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	

Quadro 5:4 - Manter avaliações

Fonte: o autor

Manter Planos de Mudança

1. O ator inicia o caso de uso selecionando "Planos de Mudança";

2. O programa exibe uma lista com os planos cadastrados;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	
Fluxo Alternativo A1 – Inclusão	Tratamento de Exceções
3. O usuário clica na opção "Incluir Plano de Mudança"; 3.1. O programa oferece a interface para preenchimento dos dados; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 - Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Plano de Mudança"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir o plano; 3.2. O ator confirma sua intenção [A2.1];	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na

3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 - Alteração	
3. O usuário clica sobre o nome do plano de mudança na lista; 3.1. O programa oferece o formulário preenchido com os dados dos testes realizados; 3.2. O ator altera os dados que julgar necessário e confirma; 3.3. O programa informa que a operação foi realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	Fluxo Alternativo A3.1 - Erro ao alterar 3.3. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

Quadro 5:5 - Manter planos de mudança

Fonte: o autor

Manter Pontos de Controle

1. O ator inicia o caso de uso selecionando um ponto macro para alterar;

2. O programa exibe uma lista com os pontos de controle cadastrados para o ponto macro;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	
Fluxo Alternativo A1 – Inclusão	Tratamento de Exceções
3. O usuário clica na opção "Incluir Ponto de Controle"; 3.1. O programa oferece a interface para preenchimentos dos dados do ponto macro; 3.2. O ator preenche os dados no formulário e	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;

confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	
Fluxo Alternativo A2 – Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Ponto de Controle"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir o sistema; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 – Alteração	
3. O usuário clica sobre o nome do sistema na lista; 3.1. O programa mostra uma lista de teste; Utiliza "Manter Testes"; 3.2. Retorna para ponto 2 do fluxo básico.	

Quadro 5:6 - Manter pontos de controle

Fonte: o autor

Manter Probabilidade

1. O ator inicia o caso de uso selecionando um ponto de controle para alteração;

2. O programa exibe uma lista com os testes cadastrados para o ponto de controle;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	Tratamento de Exceções
Fluxo Alternativo A1 – Inclusão	

3. O usuário clica na opção "Incluir Probabilidade"; 3.1. O programa oferece a interface para preenchimentos dos dados; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 – Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Probabilidade"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir a informação; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 - Alteração	
3. O usuário clica sobre o ponto de controle na lista lista; 3.1. O programa oferece o formulário preenchido com os dados; 3.2. O ator altera a probabilidade e confirma; 3.3. O programa informa que a operação foi realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	Fluxo Alternativo A3.2 - Erro ao alterar 3.1. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

Quadro 5:7 - Manter probabilidade

Fonte: o autor

Manter Consequência

1. O ator inicia o caso de uso selecionando um ponto de controle para alteração;

2. O programa exibe uma lista com os testes cadastrados para o ponto de controle;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	Tratamento de Exceções
Fluxo Alternativo A1 – Inclusão	
3. 3. O usuário clica na opção "Incluir consequência"; 3.1. O programa oferece a interface para preenchimentos da relevância; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 – Exclusão	
3. O usuário marca um registro e clica na opção "Excluir consequência"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir a informação; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 - Alteração	
3. O usuário clica sobre o nome do sistema na	Fluxo Alternativo A3.2 - Erro ao alterar

lista; 3.1. O programa oferece o formulário preenchido com a consequência; 3.2. O ator altera o dado e confirma; 3.3. O programa informa que a operação foi realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	3.1. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

Quadro 5:8 - Manter consequência

Fonte: o autor

Manter Consequência

1. O ator inicia o caso de uso selecionando "Normas";

2. O programa exibe uma lista com as normas cadastradas;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	Tratamento de Exceções
Fluxo Alternativo A1 – Inclusão	
3. O usuário clica na opção "Incluir Normas"; 3.1. O programa oferece a interface para preenchimento dos dados; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 – Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Normas"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir a norma;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico;

3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	 Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 - Alteração	
3. O usuário clica sobre o nome da norma na lista; 3.1. O programa oferece o formulário preenchido com a descrição da norma; 3.2. O ator altera os dados que julgar necessário e confirma; 3.3. O programa informa que a operação foi realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	Fluxo Alternativo A3.2 - Erro ao alterar 3.1. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

Quadro 5:9 - Manter normas

Fonte: o autor

Manter Pontos Macro

1. O ator inicia o caso de uso selecionando um tipo de sistema;

2. O programa exibe uma lista com os pontos cadastrados para o tipo selecionado;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	
Fluxo Alternativo A1 – Inclusão	Tratamento de Exceções
3. O usuário clica na opção "Incluir Ponto Macro";	Fluxo Alternativo A1.1 - Erro ao incluir

3.1. O programa oferece a interface para preenchimentos dos dados do ponto macro; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 – Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Ponto Macro"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir o sistema; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 – Alteração	
3. O usuário clica sobre o nome do sistema na lista; 3.1. O programa mostra uma lista de pontos de controle; Utiliza "Manter Pontos de Controle"; 3.2. Retorna para ponto 2 do fluxo básico.	

Quadro 5:10 - Manter pontos macro

Fonte: o autor

Manter Roteiros

1. O ator inicia o caso de uso selecionando "Roteiros";

2. O programa exibe uma lista com os tipos de sistema cadastrados;

3. O usuário clica na opção "Voltar" [A1];

Fluxo	
Fluxo Alternativo A1 – Alteração	
3. O usuário clica sobre o nome do tipo de sistema na lista; 3.1. O programa oferece uma lista com os pontos macro; Utiliza "Manter Pontos Macro"; 3.2. Retorna para ponto 2 do fluxo básico.	

Quadro 5:11 - Manter roteiros

Fonte: o autor

Manter Sistemas

1. O ator inicia o caso de uso selecionando "Sistemas";

2. O programa exibe uma lista com os sistemas cadastrados;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	
Fluxo Alternativo A1 – Inclusão	Tratamento de Exceções
3. O usuário clica na opção "Incluir Sistema"; 3.1. O programa oferece a interface para preenchimentos dos dados do sistema; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;

realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	
Fluxo Alternativo A2 – Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Sistema"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir o sistema; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 – Alteração	
3. O usuário clica sobre o nome do sistema na lista; 3.1. O programa oferece o formulário preenchido com os dados do sistema selecionado; 3.2. O ator altera os dados que julgar necessário e confirma; 3.3. O programa informa que a operação foi realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	Fluxo Alternativo A3.1 - Erro ao alterar 3.3. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

Quadro 5:12 - Manter sistemas

Fonte: o autor

Manter Relevância

1. O ator inicia o caso de uso selecionando "Sistemas";

2. O programa exibe uma lista com os sistemas cadastrados;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	Tratamento de Exceções
Fluxo Alternativo A1 – Inclusão	
3. 3. O usuário clica na opção "Incluir Relevância"; 3.1. O programa oferece a interface para preenchimentos da relevância; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 – Exclusão	
3. O usuário marca um registro e clica na opção "Excluir relevância"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir a informação; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2]; 3.4. Retorna ao ponto 2 do fluxo básico;	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 - Alteração	
3. O usuário clica sobre o nome do sistema na lista; 3.1. O programa oferece o formulário preenchido com a relevância; 3.2. O ator altera o dado e confirma; 3.3. O programa informa que a operação foi	Fluxo Alternativo A3.2 - Erro ao alterar 3.1. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	

Quadro 5:13 - Manter relevância

Fonte: o autor

Manter Testes

1. O ator inicia o caso de uso selecionando um ponto de controle para alteração;

2. O programa exibe uma lista com os testes cadastrados para o ponto de controle;

3. O usuário clica na opção "Voltar" [A1][A2][A3];

Fluxo	
Fluxo Alternativo A1 – Inclusão	Tratamento de Exceções
3. O usuário clica na opção "Incluir Teste"; 3.1. O programa oferece a interface para preenchimentos dos dados do teste; 3.2. O ator preenche os dados no formulário e confirma a inclusão; 3.3. O programa informa que a operação foi realizada com sucesso [A1.1]; 3.4. Retorna para o ponto 2 do fluxo básico;	Fluxo Alternativo A1.1 - Erro ao incluir 3.3. O programa informa que houve erro na inclusão; retorna para o ponto 3.1 do fluxo A1;
Fluxo Alternativo A2 – Exclusão	
3. O usuário marca um registro e clica na opção "Excluir Teste"; 3.1. O programa pergunta se o usuário tem certeza de que deseja excluir o teste; 3.2. O ator confirma sua intenção [A2.1]; 3.3. O programa informa o sucesso da operação [A2.2];	Fluxo Alternativo A2.1 - Desistência 3.2. O ator cancela a operação; retorna para o ponto 2 do fluxo básico; Fluxo Alternativo A2.2 - Falha na exclusão 3.3. O programa informa que não pode

3.4. Retorna ao ponto 2 do fluxo básico;	excluir o registro; retorna para o ponto 2 do fluxo básico;
Fluxo Alternativo A3 – Alteração	
3. O usuário clica sobre o nome do teste na lista; 3.1. O programa oferece o formulário preenchido com os dados do teste selecionado; 3.2. O ator altera os dados que julgar necessário e confirma; 3.3. O programa informa que a operação foi realizada com sucesso [A3.1]; 3.4. Retorna para ponto 2 do fluxo básico.	Fluxo Alternativo A3.1 - Erro ao alterar 3.3. O programa informa que houve erro ao salvar registro; retorna ao ponto 3.1 do fluxo A3;

Quadro 5:14 - Manter testes

Fonte: o autor

5.2.6 Modelo Entidade-Relacionamento (ER)

Diagrama ER (DER), é uma representação das entidades e dos relacionamentos entre as mesmas a serem armazenadas em um banco de dados (BD).

Modelo ER (MER) é uma representação baseada em uma percepção de um mundo real que consiste em uma coleção de objetos básicos chamados entidades, e em relacionamentos entre estes objetos. Uma entidade é um objeto que é distinguível de outro objeto por um conjunto específico de atributos.

Através do diagrama ER é possível representar graficamente toda a estrutura lógica de um banco de dados.

A figura 5.3 apresenta o diagrama ER concebido para o sistema proposto no presente trabalho:

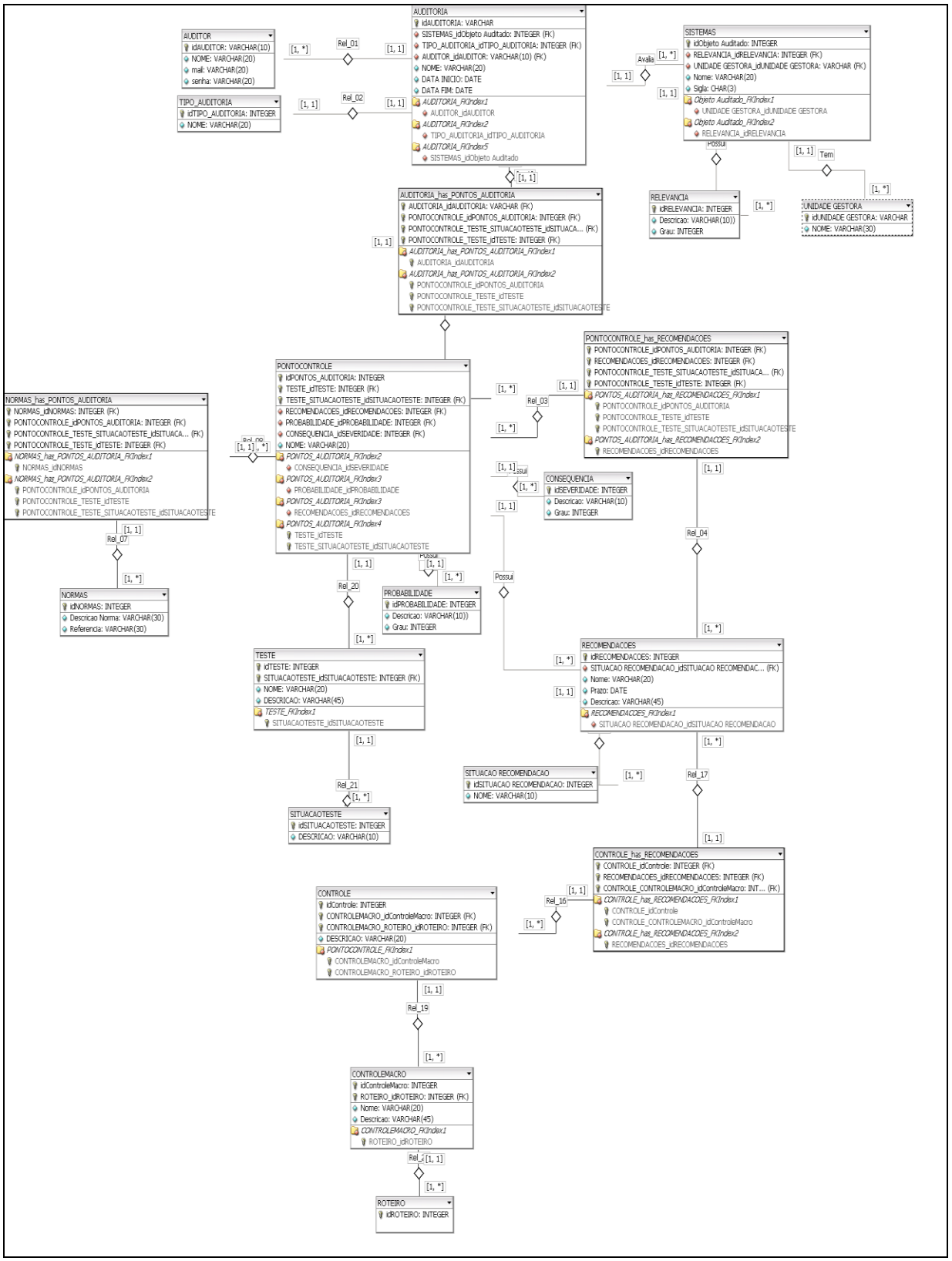


Figura 5-2- Diagrama entidade relacionamento

Fonte: o autor

A partir da análise do modelo ER do sistema é apresentado protótipo de telas para o sistema.

5.2.7 Protótipo de Telas do Sistema

A partir do modelo proposto e com o intuito de demonstrar o que se espera do sistema, foi desenvolvido um protótipo contendo algumas telas para o mesmo.

A figura 5.3 ilustra como seria a tela inicial de acesso ao sistema. Nesta tela, além das opções contidas na esquerda, consta, quando for o caso, um aviso ao auditor que há ações cujo prazo de conclusão já se encontra esgotado.

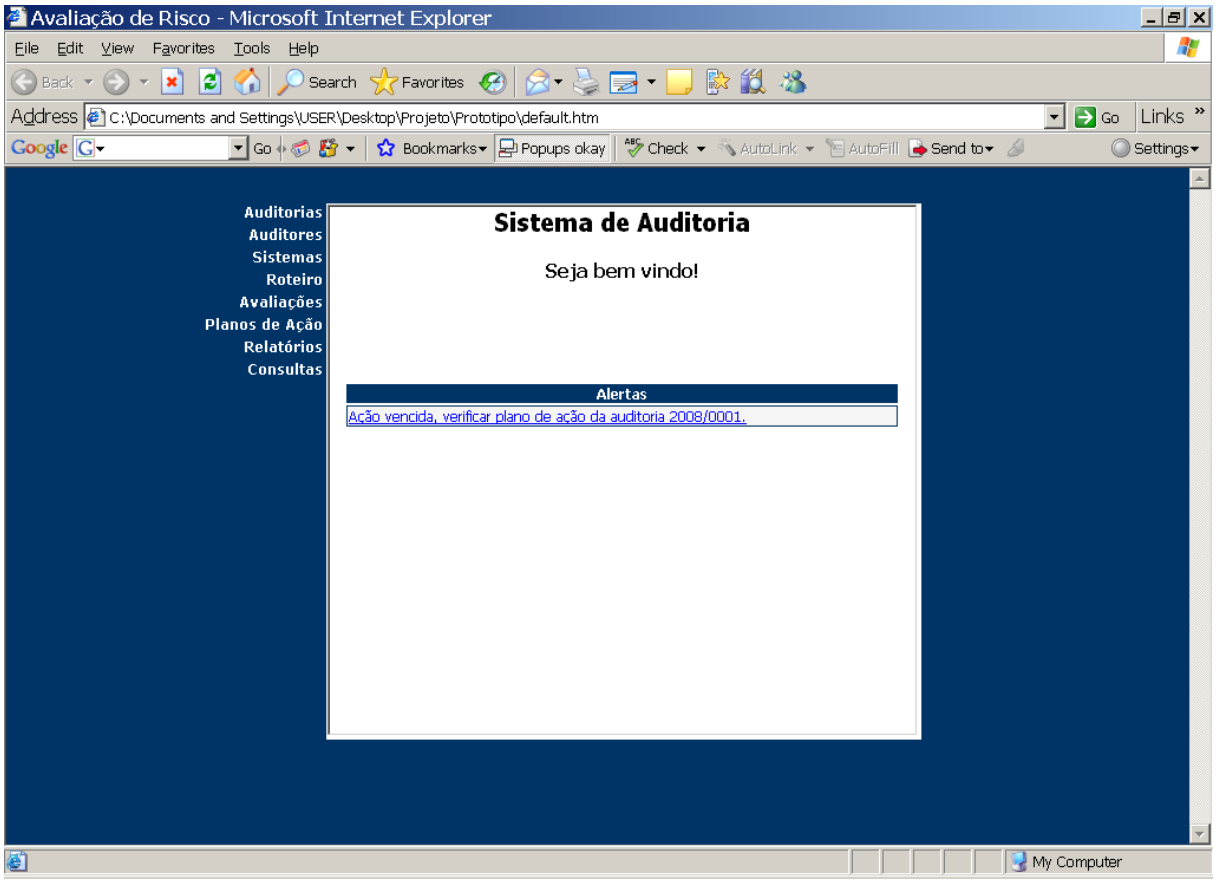


Figura 5-3- Tela inicial de acesso ao sistema

Fonte: o autor

Na tela mostrada na figura 5.4 há a opção de inclusão de auditorias através do link Incluir Auditoria, consulta dados de uma auditoria, selecionando o código da mesma e exclusão selecionando a caixa de marcação ao lado da auditoria e selecionando excluir auditoria. Para inclusão de auditoria em um sistema é necessário primeiramente realizar o cadastramento do sistema, na guia sistemas e do auditor na guia auditores.

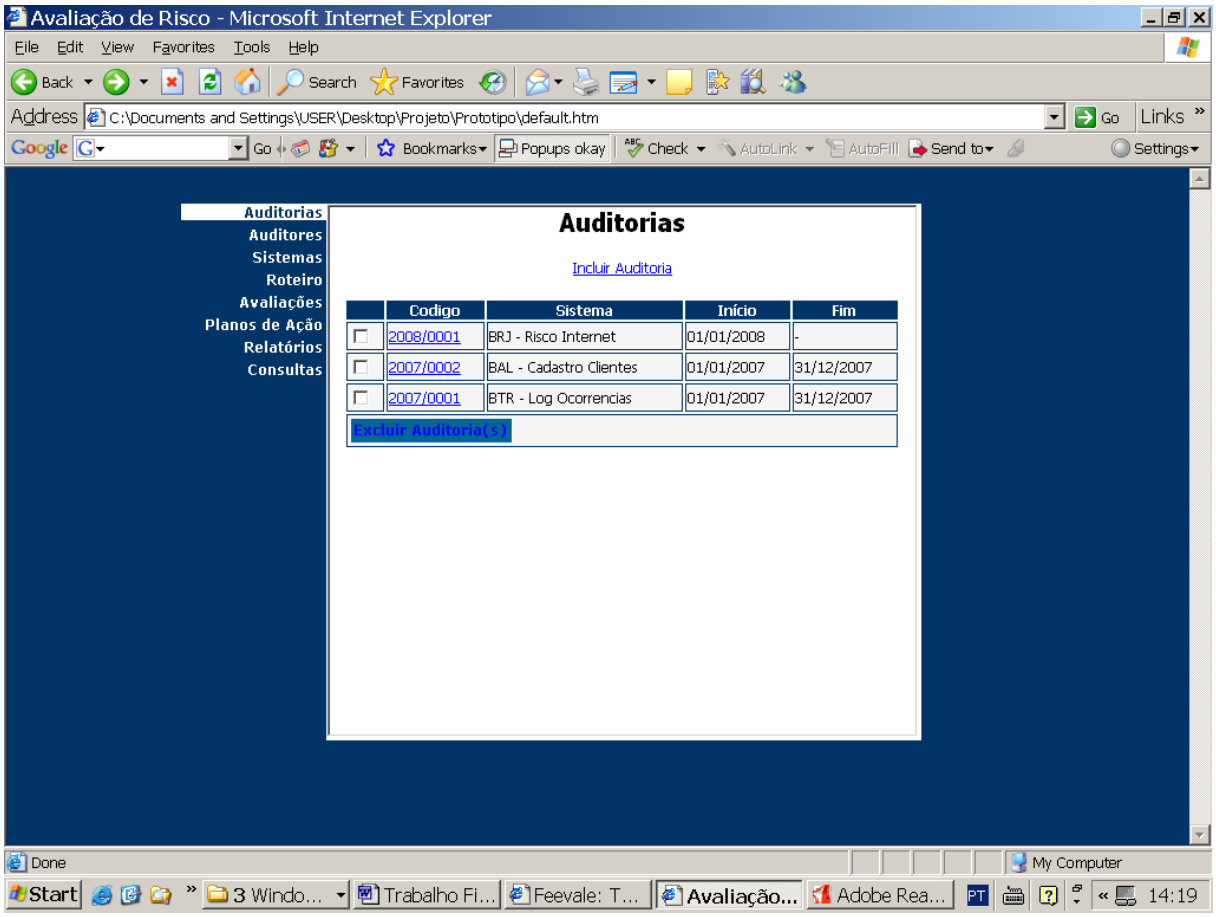


Figura 5-4- Consulta, inclusão e exclusão de auditorias

Fonte: o autor

Na figura 5.5 é realizada a consulta, inclusão e exclusão de auditores.

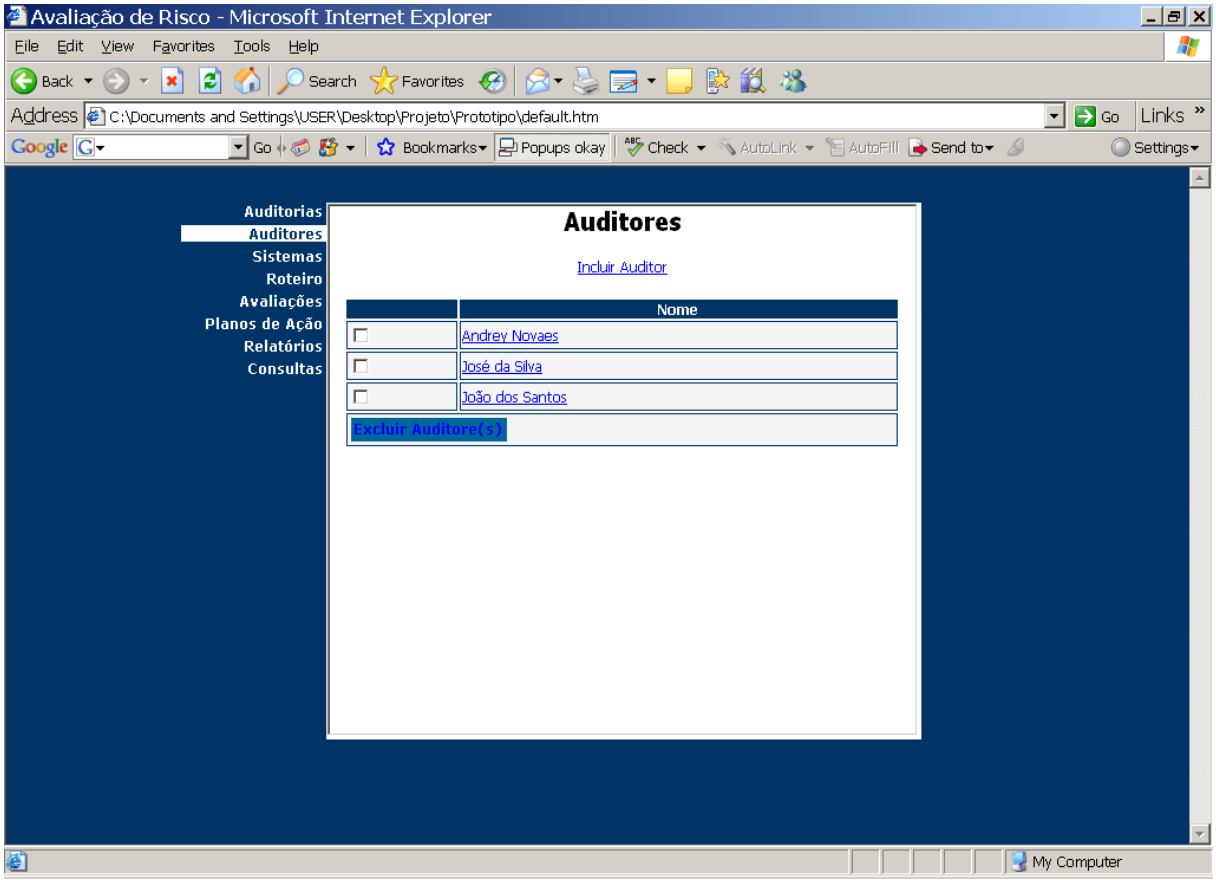


Figura 5-5- Auditores

Fonte: o autor

Na figura 5.6 consta o exemplo de cadastramento de um auditor.

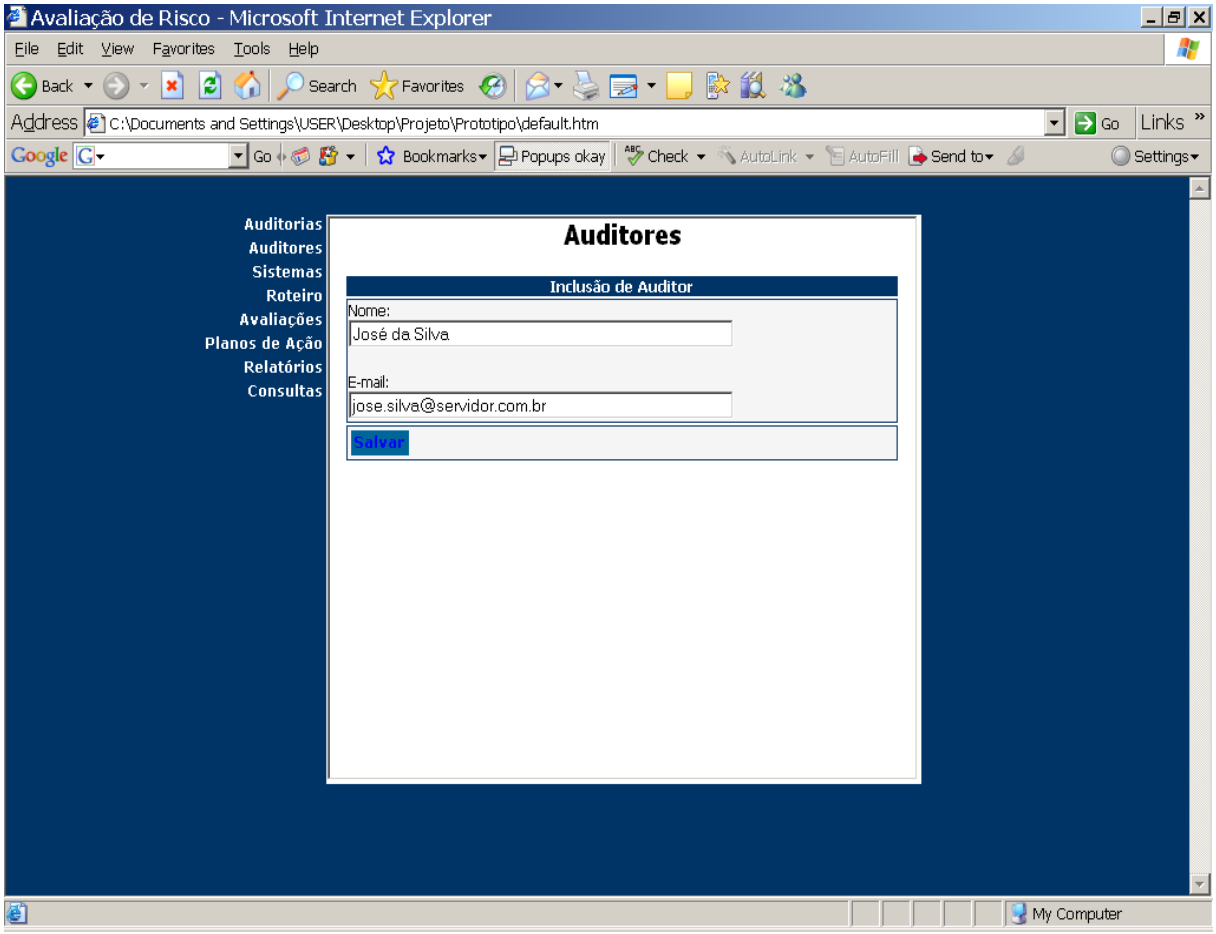


Figura 5-6- Cadastramento de auditores

Fonte: o autor

A figura 5.7 demonstra a tela de gerenciamento dos sistemas.

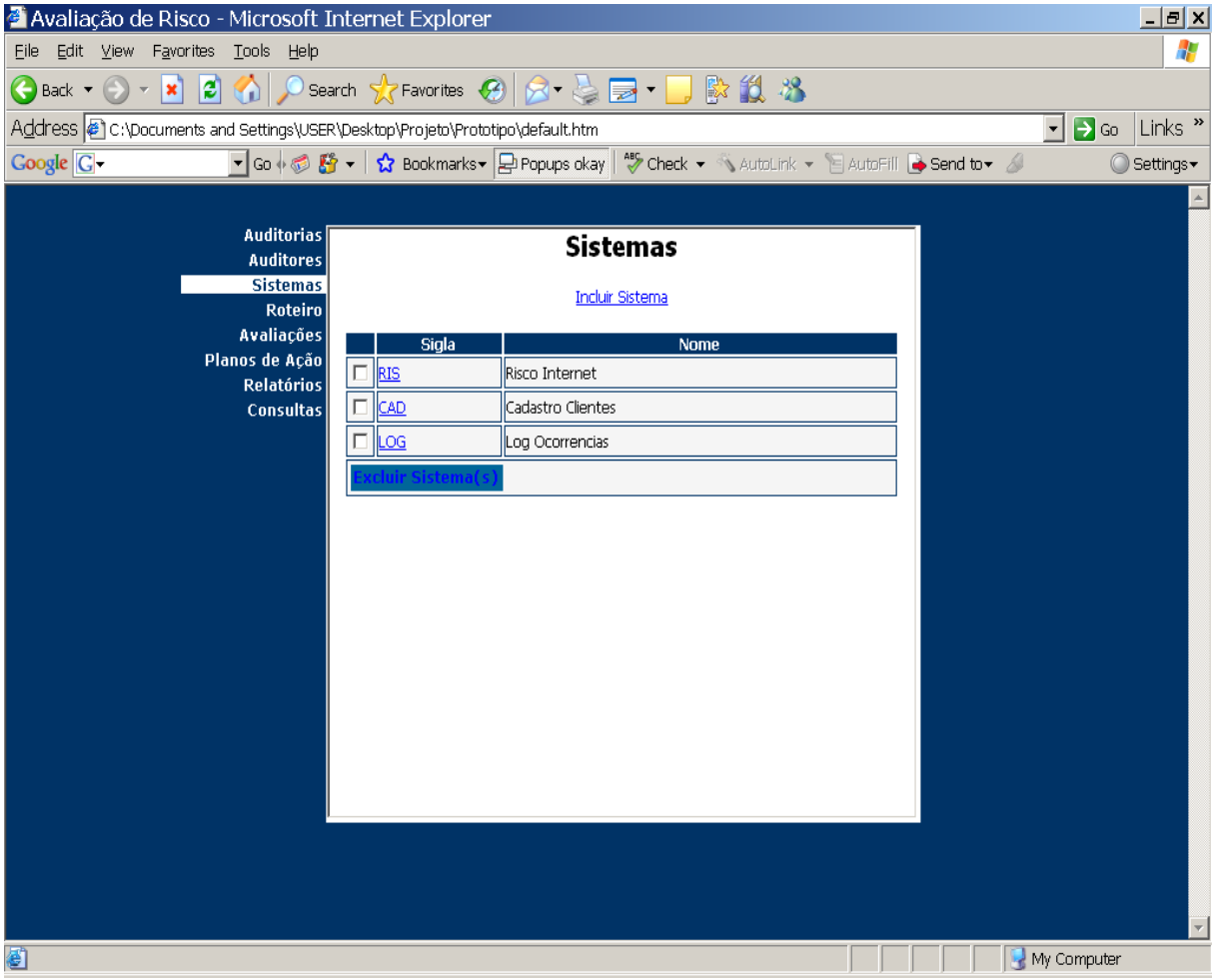


Figura 5-7- Sistemas

Fonte: o autor

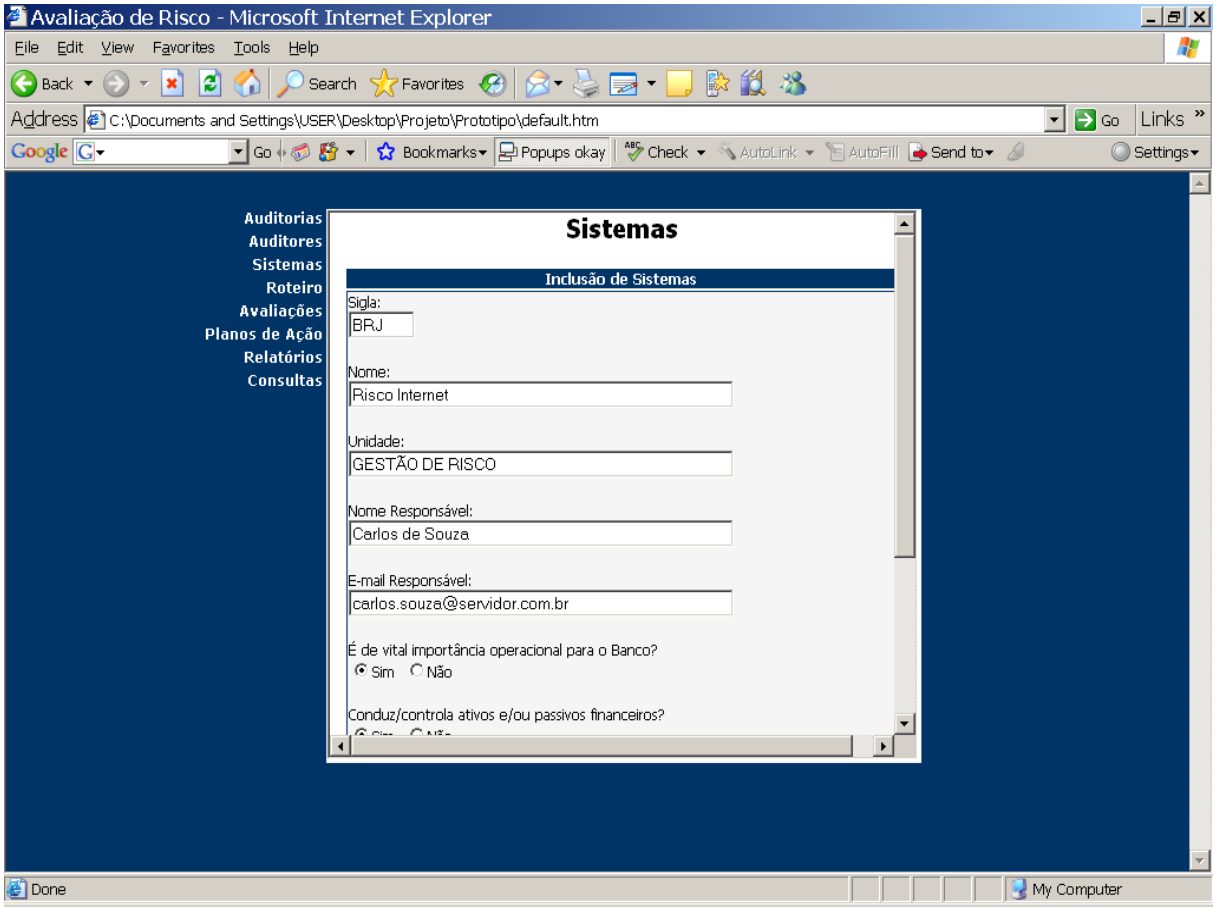


Figura 5-8- Inclusão de sistemas

Fonte: o autor

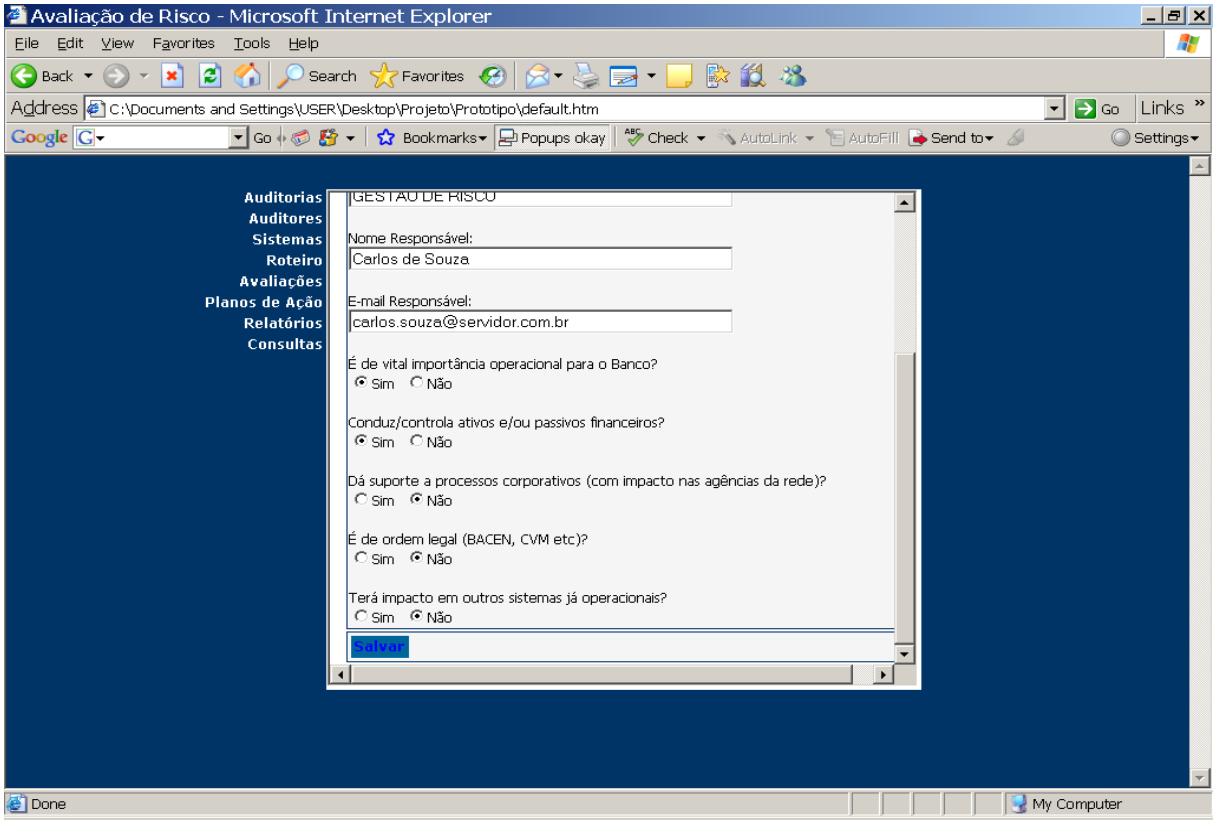


Figura 5-9- Inclusão de sistemas (continuação)

Fonte: o autor

A figura 5.9 exemplifica a inclusão de um sistema. Quando do cadastramento do sistema, é respondido pelo auditor questões referentes a relevância do sistema, conforme foi abordado anteriormente na metodologia.

Na próxima tela, consta o roteiro com os pontos macros a serem verificados na auditoria.

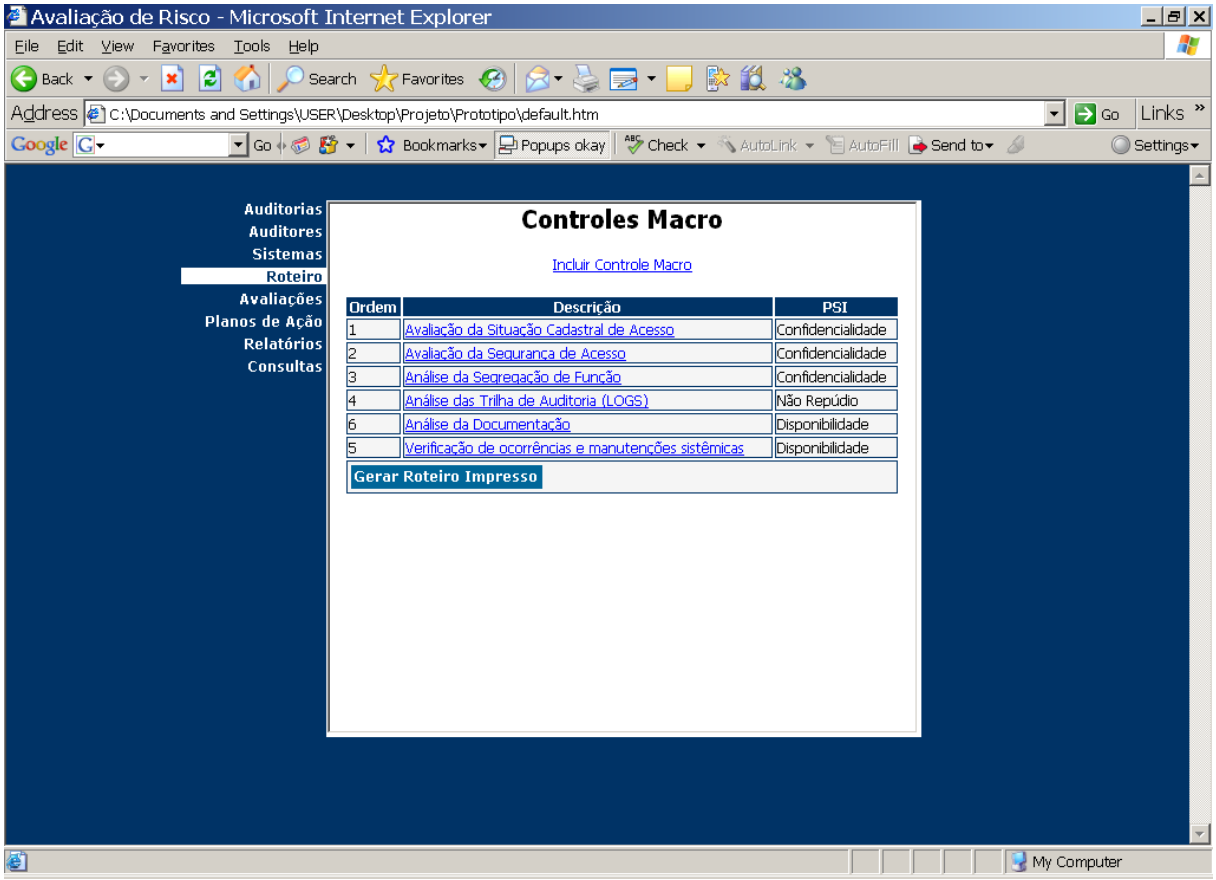


Figura 5-10- Roteiros

Fonte: o autor

Cada ponto macro está composto por diversos testes a serem efetuados. Ao lado de cada ponto macro há a propriedade de segurança da informação (PSI) na qual o mesmo está associado.

Ao selecionar um ponto macro, pode-se visualizar os pontos de controle contidos, como consta na próxima tela.

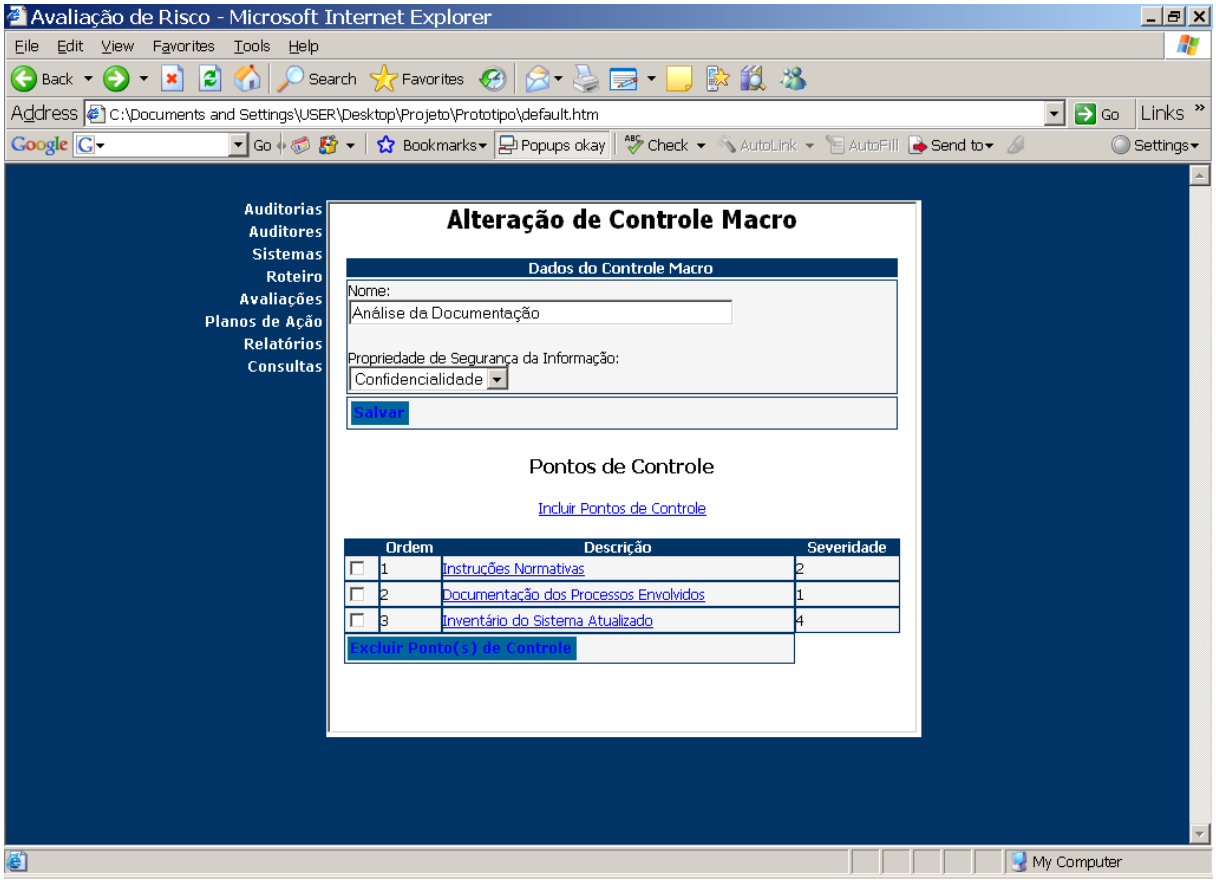


Figura 5-11- Alteração de controle macro

Fonte: o autor

Na figura 5.11 pode-se alterar um ponto macro, bem como visualizar, incluir e excluir um ponto de controle. Nesta tela também pode ser visualizada a severidade de cada ponto de controle.

Ao clicar em cima de um ponto de controle consegue-se consultar os dados do ponto selecionado, conforme demonstrado na figura 5.12.

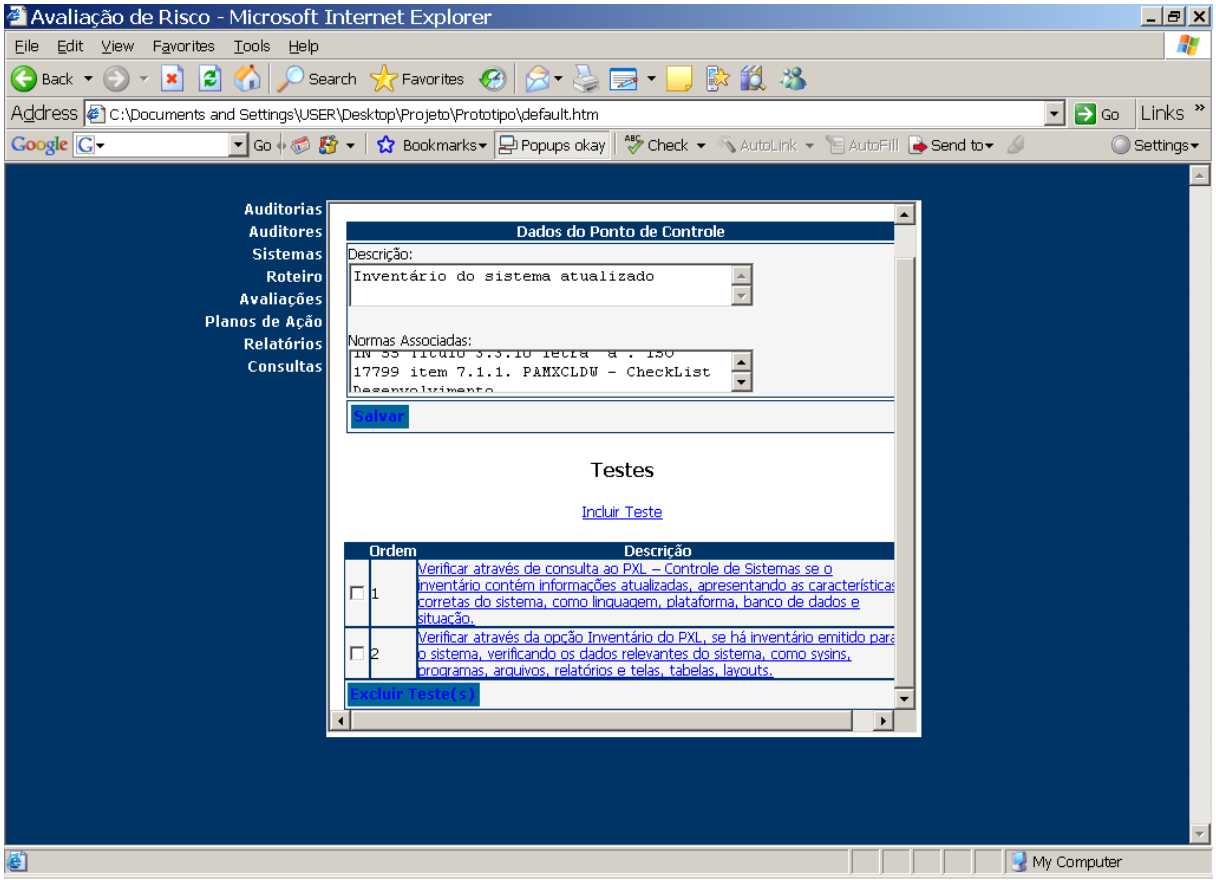


Figura 5-12- Dados de um ponto de controle

Fonte: o autor

Nesta tela consta a descrição do ponto de controle, as normas associadas, bem como os testes necessários para validação do ponto de controle. Caso necessário, pode ser incluídos mais testes no roteiro ou excluir algum teste desnecessário.

A figura 5.13 mostra a tela de avaliação dos pontos de controle a ser preenchida pelo no decorrer dos trabalhos de auditoria.

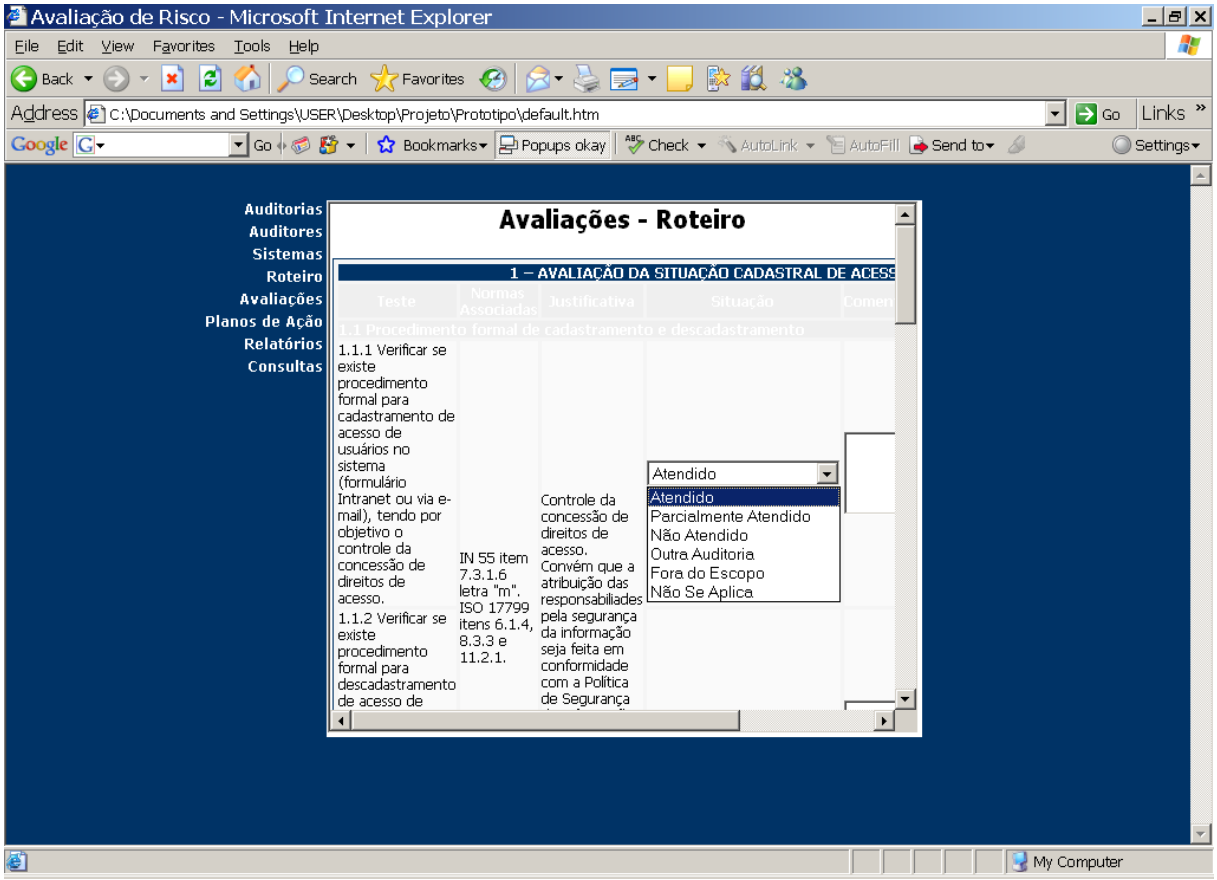


Figura 5-13- Avaliações

Fonte: o autor

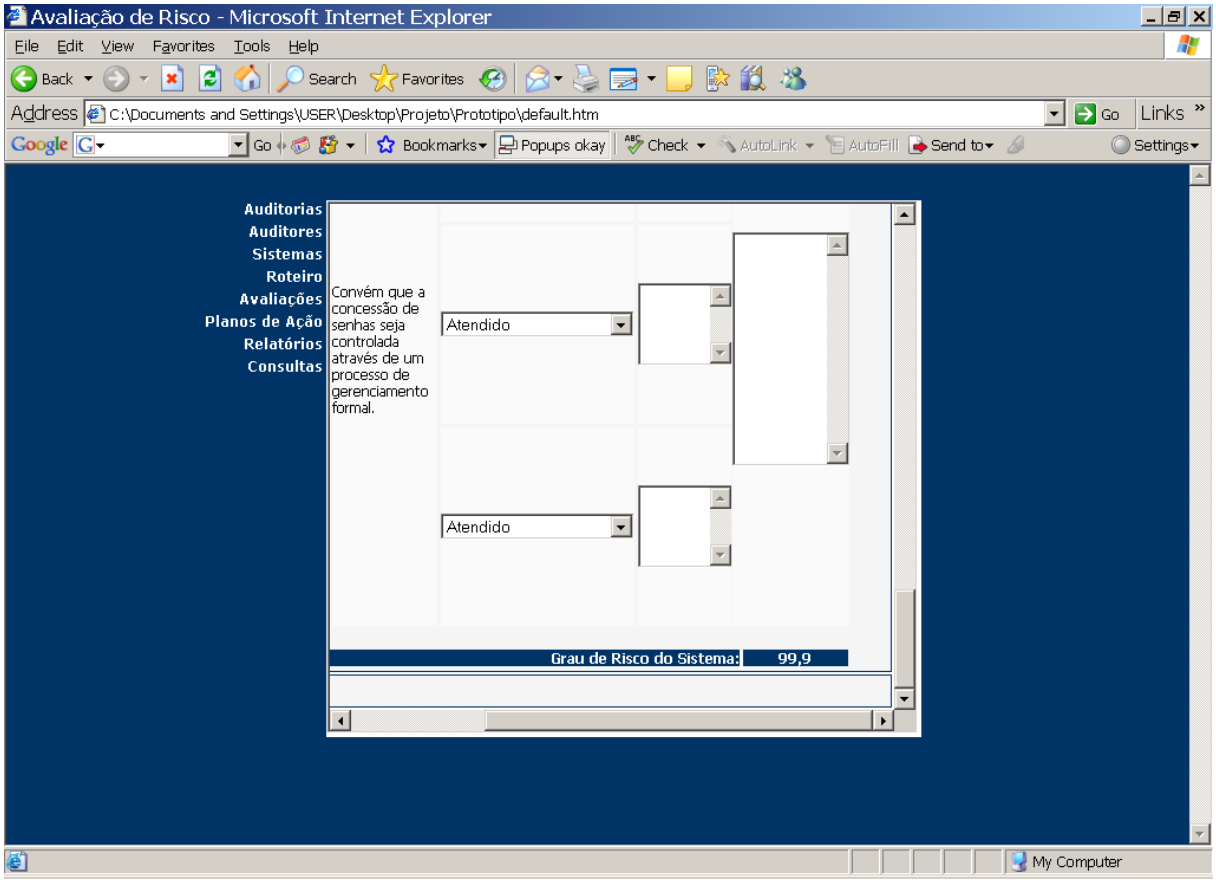


Figura 5-14- Roteiro – Atribuição do risco do sistema

Fonte: o autor

Ao final dos testes, os pontos de controle que se encontram com situação diferente de atendido, vão para o plano de ação da auditoria, conforme consta na figura 5.15.

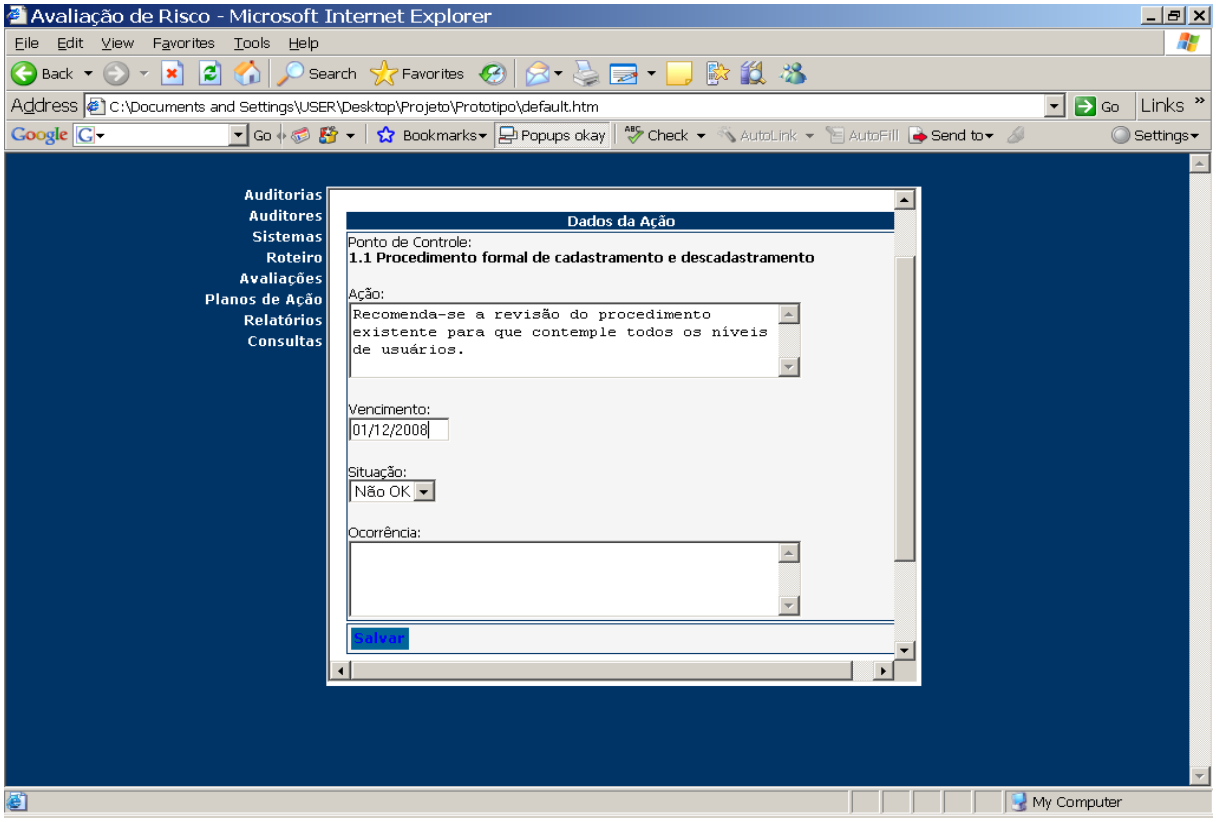


Figura 5-15- Recomendações para plano de ação

Fonte: o autor

Os dados do plano de ação são repassados para o gestor responsável pelo cumprimento da recomendação, quando são acordados os prazos necessários para atendimento de cada recomendação. Para a reunião, é emitido pelo sistema o plano de ação.

Na figura 5.16 há um exemplo do documento gerado.

Plano de Ação — **Auditoria Interna**

Gerência de Auditoria de

Código da 20080100AU *Tipo de Auditoria:* Auditoria de Sistemas em Produção

Objeto Auditado: RIS Risco Interno *Período* 01/10/2008 a 01/01/2009

Auditor(es): Audrey Simon Ungaretti N Silveira - -

Unidade(s): Unidade de Infra Estrutura de Tecnologia - -

	Ação	*Prazo*	*Situação*
1	Documentação	01/12/2008	Pendente
	Atualizar Documentação	*Responsáveis:*	
	Comentário da	*Unidade:* Unidade de Infra Estrutura de Tecnologia	
2	Segurança de Acesso	01/12/2008	Pendente
	Revisar usuários com Acesso ao Sistema	*Responsáveis:*	
	Comentário da	*Unidade:* Unidade de Infra Estrutura de Tecnologia	
3	Trilhas de Auditoria	01/12/2008	Pendente
	Implementar Logs no Sistema	*Responsáveis:*	
	Comentário da	*Unidade:* Unidade de Desenvolvimento de Sistemas	
4	Segregação de Função	01/12/2008	Pendente
	Efetuar análise dos usuários cadastrados, visando verificar a necessidade de acesso	*Responsáveis:*	
	Comentário da	*Unidade:* Unidade de Infra Estrutura de Tecnologia	

Figura 5-16- Modelo de plano de ação

Fonte: o autor

Além de auxiliar nas auditorias, também são gerados relatórios estatísticos para acompanhamento dos trabalhos. A figura a seguir mostra a tela de consulta de relatórios do sistema.

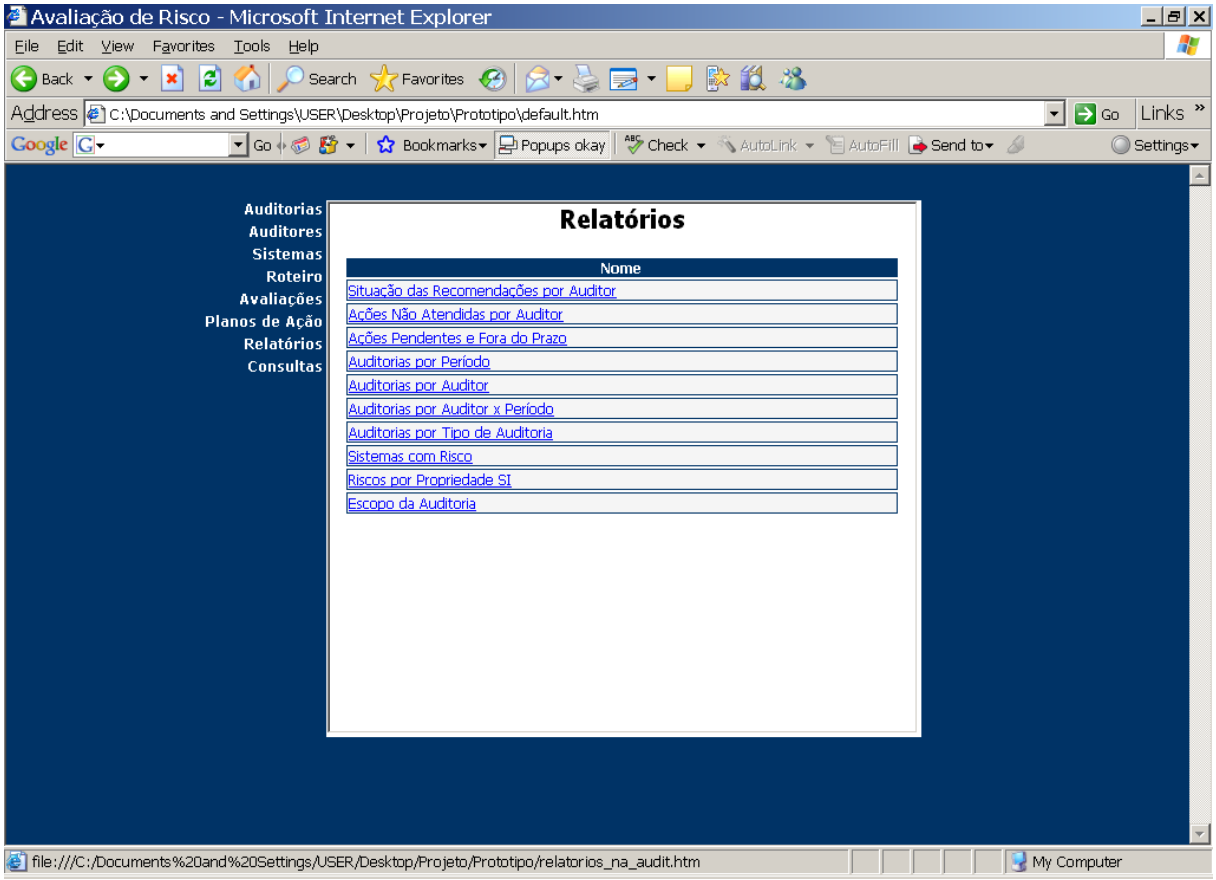
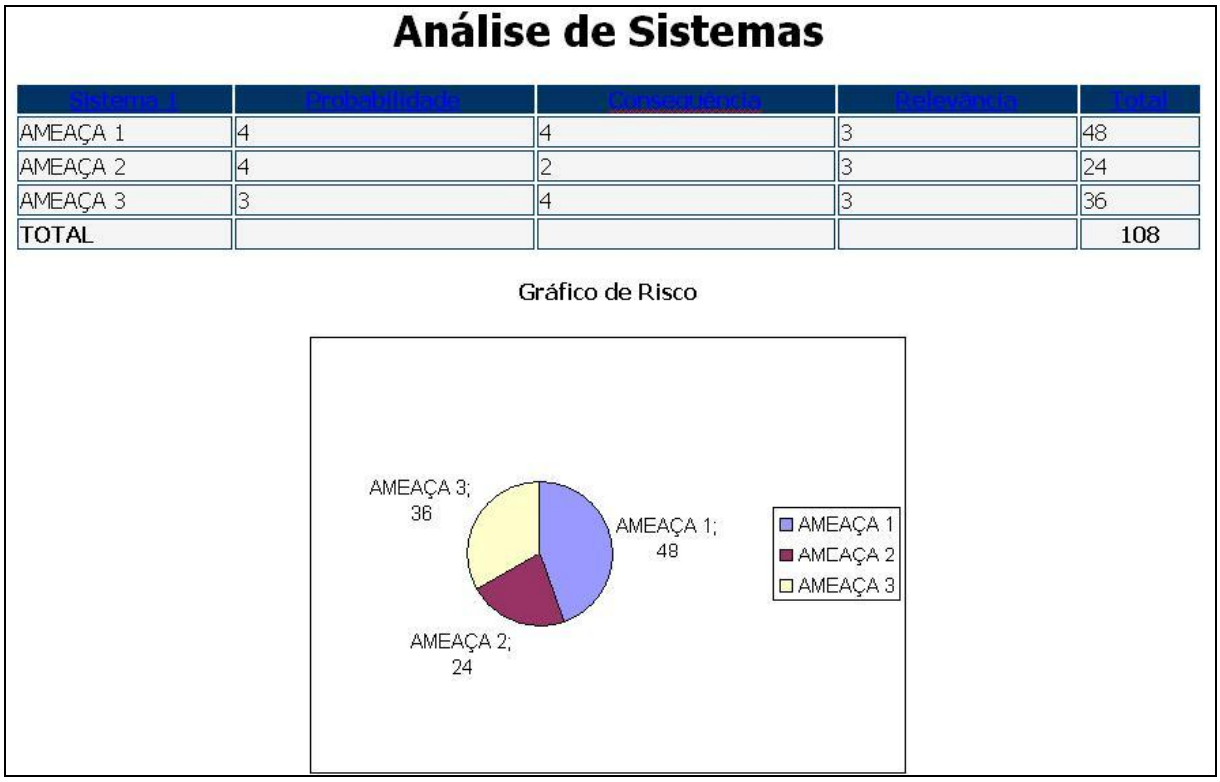


Figura 5-17- Tela de relatórios

Fonte: o autor

A figura 5-18 apresenta a apuração de risco de um sistema a comparação do sistema. Com isso é possível ao auditor efetuar a análise do risco separando-as pela ameaça.



Análise de Sistemas

Sistema 1	Probabilidade	Consequência	Relevância	Total
AMEAÇA 1	4	4	3	48
AMEAÇA 2	4	2	3	24
AMEAÇA 3	3	4	3	36
TOTAL				108

Figura 5-18: Análise de risco de um sistema

Fonte: o autor

A figura 5-19 demonstra a comparação de três sistemas já auditados, com foco no risco apresentado. Com isso pode-se facilmente auferir qual sistema apresenta maior índice de risco.

Sistema	Total
SISTEMA 1	140
SISTEMA 2	118
SISTEMA 3	90

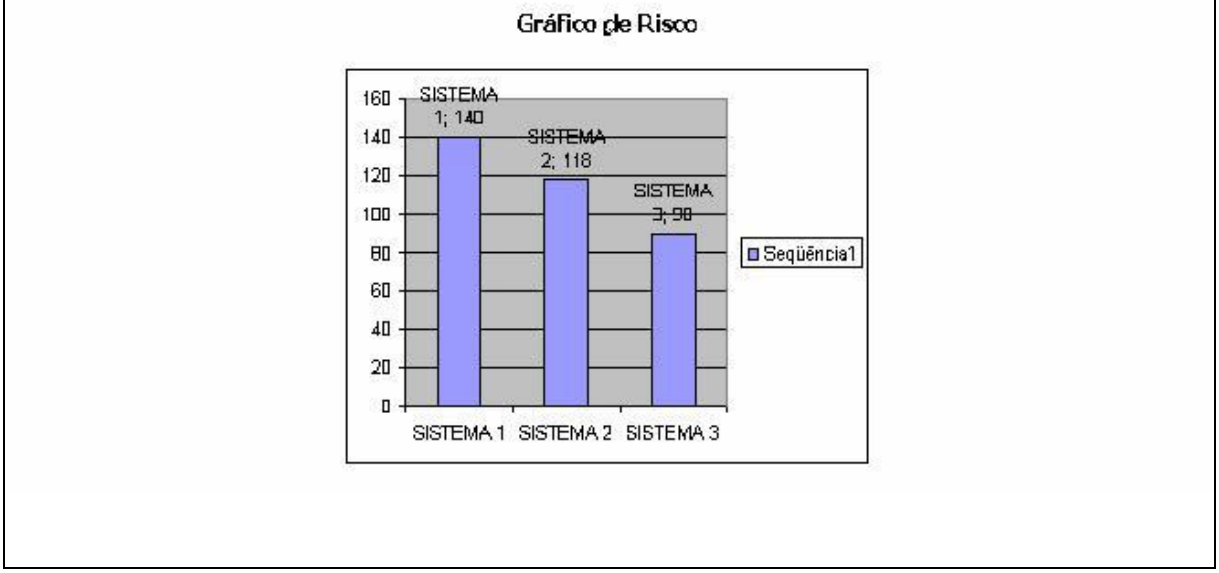


Figura 5-19: Comparação de risco entre sistemas

Fonte: o autor

A seguir são apresentadas as configurações finais resultantes do trabalho efetuado.

CONSIDERAÇÕES FINAIS

Através dos estudos realizados, verificou-se a importância dos controles internos para garantir a segurança da informação nas empresas. Considerando a importância cada vez maior dos sistemas de informação, torna-se imprescindível que as empresas possuam uma auditoria que busque verificar e atestar a confiabilidade dos dados apresentados. Porém, devido ao grande volume de sistemas a serem auditados, torna-se vital para as empresas, buscarem uma maior eficiência em seus trabalhos de auditoria.

Nos estudos realizados junto à empresa do caso de estudo, identificou-se a necessidade de uma ferramenta que venha a auxiliar nos trabalhos de auditoria, gerando os papéis de trabalho da auditoria e, além disso, de acordo com os dados obtidos no decorrer das auditorias, efetuar o levantamento do risco dos sistemas, possibilitando uma hierarquização (ou ordenação) de sistemas a serem auditados primeiramente.

Este trabalho não teve a pretensão de esgotar o assunto relativo à auditoria, pois além de ser um assunto extenso, não é a proposta de contribuição do trabalho.

Na seqüência, sugeriu-se a modelagem de uma ferramenta visando atender às necessidades da empresa objeto da pesquisa.

Como continuação deste trabalho, sugere-se o desenvolvimento de roteiros de auditoria para os diversos tipos de auditoria de TI existentes, associando os pontos de controle com as ameaças constantes na ISO 27705.

A partir disso, pode-se implementar uma aplicação baseada na modelagem desenvolvida neste trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

ARIMA, Carlos Hideo. **Metodologia de auditoria de sistemas**. 10.ed. São Paulo: Érica, 1994.

ATTIE, William. **Auditoria Interna**. 10.ed. São Paulo: Érica, 1994.

ATTIE, William. **Auditoria: conceitos e aplicações.** 3.ed. São Paulo: Atlas, 1998.

BOOCH, Grady; RUMBAUGH, James; JACOBSON, Ivar. **UML – Guia do Usuário.** 12.ed. São Paulo: Campus, 2000.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 1994.0

FONTES, Joaquim Rubens. **Manual de Auditoria de Sistemas**, 1. ed. São Paulo: Ciência Moderna, 1991.

GIL, Antônio de Loureiro. **Auditoria de computadores.** 5.ed. São Paulo: Atlas, 2000.

HEUSER, Carlos Alberto. **Projeto de Banco de Dados.** 4. ed. Porto Alegre: Sagra Luzzatto, 2001.

IMONIANA, Joshua Onome. **Auditoria de sistemas de informação.** 1.ed. São Paulo: Atlas, 1994.

JUNIOR, José Hernandes Perez. **Auditoria de demonstrações contá*beis.*** 1. ed. São Paulo: Atlas, 1995.

Manual de Auditoria do Tribunal de Contas da União, Brasília, 1998. 109 páginas, disponível em: www.tcu.gov.br – Acesso em 28/08/2006

PAULA, Maria Goreth Miranda Almeida. **Auditoria interna.** 1. ed. São Paulo: Atlas, 1999.

PRODANOV, Cléber Cristiano. **Manual de metodologia científica**. 3. ed. Novo Hamburgo: Feevale, 2003.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. 1.ed. Rio de

Janeiro: Campus, 2003.

SHIMIDT, Paulo; SANTOS, José Luiz dos; ARIMA, Carlos Hideo. **Fundamentos de auditoria de sistemas.** 1.ed. São Paulo: Atlas, 2006.

Manual Sairbanes Oxley da Deloitte Tomatsu São Paulo, 2003 47 páginas, disponível em: www.deloitte.com.br – Acesso em 14/04/2009.

CARDELLA, B. **Segurança no trabalho** – Uma abordagem holística: São Paulo: Atlas, 1999.

YIN, Robert K. **Estudo de caso: planejamento e métodos.** 2. ed. Porto Alegre, RS: Bookman, 2001. 205 p.

BLAHA, Michael; RUMBAUGH, James. **Modelagem e projetos baseados em objetos com UML** 2. 2. ed., rev. atual. Rio de Janeiro, RJ: Elsevier, 2006