UNIVERSIDADE REGIONAL DE BLUMENAU

CENTRO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE CIÊNCIAS DA COMPUTAÇÃO

(Bacharelado)

SOFTWARE PARA AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO DE UMA EMPRESA CONFORME A NORMA NBR ISO/IEC 17799

TRABALHO DE CONCLUSÃO DE CURSO SUBMETIDO À UNIVERSIDADE REGIONAL DE BLUMENAU PARA A OBTENÇÃO DOS CRÉDITOS NA DISCIPLINA COM NOME EQUIVALENTE NO CURSO DE CIÊNCIAS DA COMPUTAÇÃO — BACHARELADO

DOUGLAS ROSEMANN

BLUMENAU, NOVEMBRO/2002.

2002/2-14

SOFTWARE PARA AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO DE UMA EMPRESA CONFORME A NORMA NBR ISO/IEC 17799

DOUGLAS ROSEMANN

ESTE TRABALHO DE CONCLUSÃO DE CURSO FOI JULGADO ADEQUADO PARA OBTENÇÃO DOS CRÉDITOS NA DISCIPLINA DE TRABALHO DE CONCLUSÃO DE CURSO OBRIGATÓRIA PARA OBTENÇÃO DO TÍTULO DE:

BACHAREL EM CIÊNCIAS DA COMPUTAÇÃO

_____

Prof. Carlos Eduardo Negrão Bizzotto - Orientador na FURB

_____

Prof. José Roque Voltolini da Silva - Coordenador do TCC

BANCA EXAMINADORA

_____

Prof. Carlos Eduardo Negrão Bizzotto

_____

Prof. Everaldo Artur Grahl

_____

Prof. Ricardo A. de Azambuja

AGRADECIMENTOS

Agradeço a Deus que deu força e esperança para a realização deste trabalho e para conseguir superar todas as etapas que nos são apresentadas na vida, sendo na superação de desafios ou na alegria de poder estar compartilhando coisas boas.

Um agradecimento especial a aquela que esteve junto comigo e me apoiou em todos os momentos, minha mãe Ilsa. Aos demais colegas e amigos que compartilharam deste trabalho de uma forma direta ou indireta o meu muito obrigado.

Agradeço ao meu orientador professor Carlos Eduardo Negrão Bizzotto, cujo conhecimento e dedicação para esta orientação, foi essencial para o desenvolvimento desse trabalho.

Agradecimentos também para com a banca examinadora deste trabalho de conclusão de curso.

SUMÁRIO

LISTA DE FIGURAS

RESUMO

O presente trabalho tem por objetivo o desenvolvimento de um protótipo de *Software* para auxiliar na avaliação da adequação de uma empresa à norma **NBR ISO/IEC 17799, tecnologia da informação – Código de prática para a gestão da segurança da informação**. Inicialmente é feita a apresentação das preocupações que as organizações possuem sobre a segurança de suas informações armazenadas. Em seguida, a norma **NBR ISO/IEC 17799** é apresentada em detalhes, apontando os sistemas que a empresa deve implementar para se adequar à referida norma. Para que se possa avaliar a adequação de uma empresa com relação à norma descrita, foi desenvolvido um *check-list*, através do qual pode-se verificar o grau de segurança da informação. O protótipo de *Software* proposto permite a inclusão, alteração e / ou remoção de tópicos do *check-list* elaborado. Os tópicos constantes do *check-list* poderão ser quantificados conforme o grau de importância dentro da organização. No final de cada avaliação, o grau de adequação da empresa será representado por uma nota, a qual é obtida a partir da média ponderada das notas fornecidas a cada uma das perguntas do *check-list*.

ABSTRACT

The present work has for objective the development of an archetype of Software to assist in the evaluation of the adequacy of a company to norm **NBR ISO/IEC 17799, technology of the information – Code of practical for the management of the security of the information**. Initially the presentation of the concerns is made that the organizations possess on the security of its stored information. After that, norm **NBR ISO/IEC 17799** is presented in details, having pointed the systems that the company must implement to adjust itself to the cited norm. So that if it can evaluate the adequacy of a company with relation to the described norm, a check-list was developed, through which can be verified the degree of security of the information. The archetype of considered Software allows the inclusion, alteration and/or removal of topics of the elaborated check-list. The constant topics of the check-list could inside be quantified in agreement the degree of importance of the organization. In the end of each evaluation, the degree of adequacy of the company will be represented by a note, which is gotten from the weighed mean of notes supplied to each one of the questions of the check-list.

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO / JUSTIFICATIVA

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local (Dias, 2000). Com as mudanças tecnológicas e a difusão do uso dos computadores por todas as áreas da empresa, essa simplicidade nos procedimentos de segurança deixou de existir. A complexidade aumentou não só em função do número de pessoas que têm acesso às informações quanto das diferentes formas através das quais essas informações podem ser acessadas. Com isso, além da segurança física (controle de acesso, locais reservados etc.) surge à necessidade de se criar controles lógicos, de forma a aumentar a probabilidade de que somente pessoas autorizadas possam acessar, modificar e / ou excluir as informações armazenadas em meio digital.

Conforme ressalta Albernaz (2001), a informação é um recurso vital em todas as organizações, tendo influência em muitos aspectos do negócio e da própria sobrevivência da organização. Assim, observa-se que a informação é um ativo importante das organizações e que sua segurança é essencial tanto para o retorno dos investimentos quanto para a continuidade dos negócios. Casanas (2001) afirma que, nos anos recentes, a informação assumiu importância vital para manutenção dos negócios, os quais são marcados pela dinamicidade da economia globalizada e permanentemente *on-line*. Dessa forma, são poucas as organizações que não dependem da tecnologia de informações, direta ou indiretamente. Com isso, o comprometimento do sistema de informações por problemas de segurança pode causar grandes prejuízos ou mesmo levar a organização à falência.

Neste sentido, desde a década de 80 vêm sendo criadas normas para segurança da informação. Em 1987 o *Department Of Trade Centre* (UK DTI) criou o *Comercial Computer Security Centre* (CCSC) o qual possuía dois objetivos principais:

1. auxiliar companhias britânicas que comercializavam produtos para segurança de tecnologia da informação através da criação de critérios para avaliação da segurança;
2. criação de um código de segurança para os usuários das informações.

Em 1989 foi publicada a primeira versão do código de segurança denominado PD0003 – Código para Gerenciamento da Segurança da Informação. Em 1995 esse código foi revisado

e publicado como uma norma britânica, a BS7799:1995. Essa norma foi revisada e alterada mais algumas vezes até que em 1º de dezembro de 2000 foi homologada pela *International Standartization Organization* (ISO) como ISO/IEC 17799:2000. No Brasil sua homologação ocorreu pela Associação Brasileira de Normas Técnicas (ABNT) sendo denominada como NBR ISO/IEC 17799:2001.

Nascimento (2001) ressalta que a partir da publicação da norma NBR ISO/IEC 17799, passa a existir um referencial de aceitação internacional. Essa norma, de acordo com Saldanha (2002), estabelece um referencial para as organizações desenvolverem, implementarem e avaliarem a gestão da segurança de informação, além de promover a confiança nas transações comerciais entre organizações, realizadas através dos computadores.

De acordo com Souza (2001), a norma NBR ISO/IEC 17799 define 127 controles divididos em 10 itens. Esta divisão tem por objetivo permitir que sejam identificadas as necessidades específicas de cada ambiente.

Os tópicos propostos pela norma NBR ISO/IEC 17799 são:

1. política de segurança;
2. segurança organizacional;
3. classificação e controle de ativos de informação;
4. segurança em pessoas;
5. segurança ambiental e física;
6. gerenciamento das operações e comunicações;
7. controle de acesso;
8. desenvolvimento e manutenção de sistemas;
9. gestão da continuidade do negócio;
10. conformidade.

Torna-se importante ressaltar que a norma esclarece que não é necessária a implementação de todos os tópicos integrantes. Para se definir os tópicos necessários em um dado ambiente, deve-se realizar uma análise de risco ou diagnóstico de vulnerabilidade. Para realizar essa análise, deve-se identificar quais são os ativos a serem protegidos e qual é o grau de proteção desejado. Entretanto, é importante salientar que os controles de segurança da informação são consideravelmente mais baratos e mais eficientes quando incorporados nos estágios do projeto e da especificação dos requisitos.

Portanto, é essencial que a empresa tenha, ao implementar a norma NBR ISO/IEC 17799, uma visão abrangente de todos os tópicos incluídos e o grau de adequação da empresa

com relação a cada um deles. A partir desse diagnóstico inicial é possível, então, realizar uma implantação planejada da norma.

É dentro desse contexto que se enquadra o presente trabalho, uma vez que seu objetivo é justamente o desenvolvimento de um protótipo de *Software* que permita a realização de um diagnóstico inicial sobre o grau de adequação da empresa aos tópicos propostos pela norma NBR ISO/IEC 17799.

1.2 OBJETIVOS

O objetivo principal deste trabalho de conclusão de curso é desenvolver um protótipo de *Software* para auxiliar na avaliação da adequação de uma empresa à norma NBR ISO/IEC 17799, tecnologia da informação – Código de prática para a gestão da segurança da informação.

Os objetivos específicos do trabalho são:

a) inclusão de um *check-list* com perguntas sobre os tópicos propostos pela norma;
b) estabelecimento da quantificação do grau de conformidade da empresa em relação a cada tópico da norma;
c) inclusão e exclusão de novos tópicos, permitindo a definição do peso de cada tópico incluído;
d) inclusão e exclusão de novas perguntas;
e) disponibilizar para a empresa avaliada um relatório apontando críticas sobre a situação da empresa frente a cada item da norma.

1.3 ORGANIZAÇÃO DO TRABALHO

O trabalho está organizado em cinco capítulos.

O capítulo dois apresenta conceitos sobre segurança da informação trazendo as principais preocupações de uma empresa com confidencialidade de sua informação. O mesmo capítulo apresenta ainda algumas normas de segurança de informação que foram projetadas para efetuar a proteção de empresas contra o acesso não autorizado das informações consideradas sensíveis. Ao final deste capítulo é apresentado então um estudo sobre a norma NBR ISO/IEC 17799, abordando seu objetivo principal, e os tópicos o qual sugere a serem seguidos para implantação da segurança da informação.

O capítulo três apresenta uma breve descrição das metodologias e tecnologias que são utilizadas no *Software*, bem como o ambiente de desenvolvimento utilizado.

No capítulo quatro são apresentadas a especificação e a implementação do software proposto.

O capítulo cinco contém as conclusões provenientes da execução desse trabalho, bem como as possíveis extensões que dele podem ser desenvolvidas.

No Anexo A é apresentado um modelo proposto para efetuar avaliações.

No Anexo B é apresentada parte da implementação de uma classe orientada a objetos.

2 SEGURANÇA DA INFORMAÇÃO

2.1 PREOCUPAÇÃO COM A SEGURANÇA DA INFORMAÇÃO

Conceitualmente a segurança pode ser definida como a proteção de informações, sistemas, recursos e serviços contra desastres, erro e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança (Dias, 2000).

A informação pode ser definida como um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegida (ABNT, 2001).

Dias (2000) afirma que quando existe o pensamento da segurança de informação, imagina-se a proteção das informações, não importando onde estejam (no papel, na memória do computador, em um disquete ou trafegando pela linha telefônica). A expectativa de todo usuário é que a informação esteja disponível no computador, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo. Segundo a ABNT (2001), segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

Conforme Casanas (2001) a segurança da informação é caracterizada pela preservação dos seguintes atributos básicos:

a) confidencialidade: segurança de que a informação pode ser acessada apenas por quem tem autorização;
b) integridade: certeza da precisão da informação;
c) disponibilidade: garantia de que os usuários autorizados tenham acesso a informação e aos recursos associados, quando necessário.

Não há organização humana que não depende da tecnologia de informação, em maior ou menor grau (Casanas, 2001). Sendo assim, a segurança da informação é preocupação de todos que integram a empresa e sua cadeia de valor. Acionistas, executivos, funcionários, clientes, fornecedores e parceiros devem estar atentos em preservar seus ativos e preocupados com a proteção adequada de informações e sistemas da empresa. Isso acontece porque a segurança da informação está se tornando um importante diferencial competitivo (Bastos, 2002).

Bastos (2002) afirma que ações de segurança da informação podem:

a) viabilizar aplicações e processos que otimizem as atividades da empresa, reduzindo custos;
b) viabilizar novos produtos e serviços, aumentando a receita da empresa;
c) reduzir e administrar os riscos do negócio;
d) fortalecer a imagem da empresa;
e) criar valor para a empresa e para o acionista.

Mas por outro lado, Bastos (2002) enfatiza que a ausência de processos e controles sobre a segurança pode acarretar diferentes impactos, que levarão a perda de faturamento, custos e despesas e, no final das contas, perder de valor da empresa. Segundo Ramos (2002), uma falha em um sistema informatizado, seja esta intencional ou não, pode causar a paralisação das atividades da organização com perdas muito significativas, quando não irreparáveis. Casanas (2001) também ressalta que o comprometimento do sistema de informações por problemas de segurança pode causar grandes prejuízos ou senão levar a organização à falência.

Segundo Dias (2000), nunca foi tão fácil atacar os sistemas informatizados, já que os sistemas de informações institucionais conectados em redes externas aumentam significativamente os riscos de segurança e muitas das ferramentas de ataque utilizadas antigamente apenas por agências de inteligência, hoje estão disponíveis a qualquer pessoa.

Quando se tem em mente a implantação de um programa de segurança de informação, é interessante responder a algumas questões. Dias (2000) propõe as seguintes questões:

- o que se quer proteger?
- contra que ou quem?
- quais são as ameaças mais prováveis?
- qual a importância de cada recurso?
- qual o grau de proteção desejado?
- quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados?
- quais as expectativas dos usuários e clientes em relação à segurança de informações?
- quais as conseqüências para a instituição se seus sistemas e informações forem corrompidos ou roubados?

Dias (2000) descreve que quando as respostas a essas perguntas são obtidas, pode-se então definir uma política de segurança de informações e fazer a análise das ameaças de acordo com a política, incluindo análise de riscos, requerimentos legais e padrões técnicos.

A política de segurança de informações, para que seja realmente colocada em prática com seriedade por todos os membros da organização, deve ter o total apoio da alta administração, pois sem esse apoio, o assunto é assumido como uma prioridade mínima em relação a outros projetos da organização. Em alguns casos a gerência se lembra da segurança somente quando algum desastre ocorre, ou consideram muito dispendiosa sua implantação, além de ser vista às vezes como inibidor ou camisa de força, ao invés de uma garantia de disponibilidade e qualidade das informações. Estes e outros casos fazem com que a segurança da informação não alcance a devida importância nas organizações atuais.

Tedeschi (2001) afirma que um sistema de segurança eficiente não significa necessariamente possuir o mais caro e moderno conjunto de soluções tecnológicas. Este erro, muito comum, de valorizar excessivamente o aspecto técnico da questão, pode permitir a existência de brechas de segurança perigosas na organização.

Segundo Vangelotti (2002) um dos fatores que muitas vezes é esquecido no processo de proteção da informação é o desenvolvimento e a manutenção de sistemas. Albernaz (2001) ainda sugere que uma organização não execute apenas o jogo dos controles e dos procedimentos para a segurança da informação, mas também os controle e os mantenha. É neste sentido na criação, como na manutenção da segurança da informação, que grandes empresas, agências governamentais e instituições internacionais têm trabalhado para estabelecer padrões (Nascimento 2001).

Conforme Nascimento (2001) a segurança dos sistemas e informações foi um dos primeiros itens a ter padrões definidos. Esta necessidade de segurança foi importante principalmente nas transações via internet.

2.2 TIPOS DE SEGURANÇA

Os controles de segurança de informações são geralmente agrupados em três tipos de controle: Físico, Lógico e Administrativo. As empresas necessitam desses três tipos de controles. As políticas de segurança de informações da empresa, através da documentação dos Padrões de Segurança de Informações associados, governam o uso desses controles.

Broderick (2001) e ABNT (2001) citam alguns exemplos de cada tipo de controle:

a) físico: portas, trancas, guardas, travas de acesso a disquetes, sistemas de travamento por cabos para mesas/paredes, circuito interno de TV, retalhadora de papéis e sistemas de controle de incêndio;
b) lógico (Técnico): senhas, permissões para arquivos, listas de controle de acesso, privilégios de contas e sistemas de proteção de energia;
c) administrativo: conscientização sobre segurança, revogação de contas de usuários e políticas.

2.3 NORMAS DE SEGURANÇA

Normas de segurança são pesquisadas desde final da década de 80. Em 1987 o *Department Of Trade Centre* (UK DTI) criou o *Comercial Security Centre* (CCSC) com o objetivo de auxiliar as companhias britânicas que comercializavam produtos para segurança de tecnologia da informação através da criação de critérios para avaliação da segurança e a criação de um código de segurança para os usuários das informações (Machado, 2002).

Na busca de um código de segurança para os usuários das informações, em 1989 foi publicada a primeira versão do código de segurança, denominado PD0003 – Código para gerenciamento da segurança da informação (Machado, 2002).

Em 1995 esse código foi revisado e publicado como uma norma britânica a BS7799:1995. Em 1996, essa norma foi proposta ao ISO para homologação mas essa foi rejeitada. Uma segunda parte desse documento foi criada posteriormente e publicada em novembro de 1997, para consulta pública e avaliação (Machado, 2002).

Machado (2002) traz ainda que em 1998 esse documento foi publicado como BS 7799-2:1998. Nesse ano, a lei britânica, denominada Ato de Proteção de Dados, recomendou a aplicação da norma na Inglaterra. Albernaz (2001) comenta que foram feitos consultas e debates públicos, sendo emitida uma nova versão da BS 7799 em 1999. Esta versão conteve todos os controles originais e novos controles que estendiam e elogiavam o espaço da BS 7799. Albernaz (2001) afirma que nele estão incluídos novos controles para as áreas de comércio eletrônico, *teleworking* e *outsourcing*. Machado (2002) também ressalta que o principal objetivo da BS 7799 é manter os aspectos básicos da informação como a integridade, confidencialidade e disponibilidade.

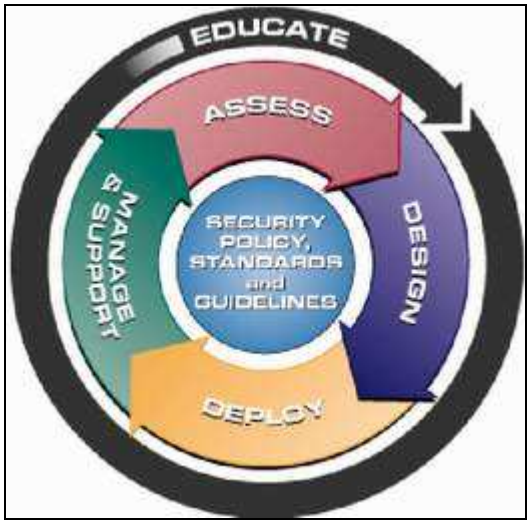
Bastos (2002) estabelece que a norma BS 7799 é dividida em duas partes:

a) código de prática para gestão da segurança da informação: seu conteúdo propõe apenas recomendações de segurança, mas não é objeto de certificação;
b) especificação de sistema de gestão de segurança da informação: nesta parte é definido um Sistema de Gestão de Segurança da Informação (SGSI) que representa o objeto de certificação.

Em abril de 1999 as duas partes da norma foram publicadas após uma revisão como BS 7799:1999. A norma foi adotada não só pela Inglaterra como por outros países da Comunidade Britânica, tal como Austrália, África de Sul e Nova Zelândia. A parte 1 desse documento foi levada à ISO e proposta para homologação pelo mecanismo do tipo *Fast Track* para um trâmite acelerado, pois normalmente, uma norma leva até cinco anos para ser avaliada e homologada pela ISO (Machado, 2002). Nascimento (2001) completa que esta publicação foi fruto de um trabalho do qual empresas privadas de grande porte e órgãos governamentais da Inglaterra participaram.

A dinâmica da norma BS 7799 consiste na segurança e monitoramento da empresa, através de padrões e normas para projeto, implementação (*deploy*), administração/suporte e avaliação. Conforme mostrado na Figura 2.1, ao longo das fases do ciclo apresentado, ocorre o processo de educação da equipe que trabalha com a segurança de informação.

Figura 2.1 – Dinâmica da BS 7799



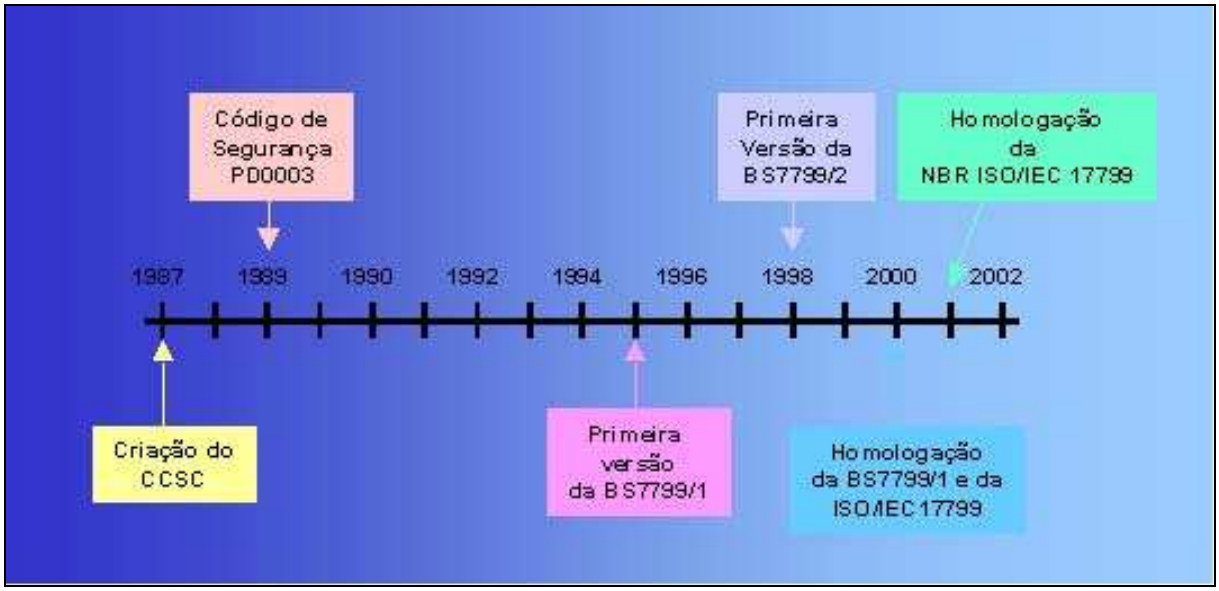
Fonte: Machado, 2002

Em maio de 2000 a *British Standard Institute* (BSI) homologou a primeira parte da BS7799. Em outubro do mesmo ano, na reunião do comitê da ISO em Tóquio, a norma foi votada e aprovada pela maioria dos representantes. Os representantes dos países ricos, excetuando a Inglaterra, foram todos contra a homologação, mas, sob votação, venceu a

maioria, e a norma foi homologada, em 1º de dezembro como ISO/IEC 17799:2000 – *Code Of Pratices for Infomation Security Management* (Machado, 2002).

Em abril de 2001 a versão brasileira da norma ISO foi posta em consulta pública. Em setembro de 2001, a ABNT homologou a versão brasileira da norma, denominada NBR ISO/IEC 17799, estando a mesma disponível, desde então, para os brasileiros (Machado, 2002). Na Figura 2.2 é mostrado todo percurso do processo, desde a criação do CCSC até a homologação da NBR ISO/IEC 17799.

Figura 2.2 – Linha do tempo



Fonte: Machado, 2002

2.4 NBR ISO/IEC 17799

De acordo com Nascimento (2001) a norma NBR ISO/IEC 17799 é exatamente a BS-7799/1 de 1999. Ramos (2002) afirma que a análise normativa da NBR ISO/IEC 17799 pode ser aplicada a qualquer organização, não importando o segmento, tamanho ou a tecnologia utilizada na gestão do seu negócio. Ramos (2002) também comenta que é comum a aplicação dos padrões em setores (ex.: financeiro) para depois estendê-las por toda a empresa.

Casanas (2001) ressalta que a ISO 17799 é bem abrangente, pretendendo contemplar todos os aspectos da segurança da informação. É dividida em 12 capítulos, cada qual abordando um aspecto da segurança da informação. Os capítulos que compõem a norma são os seguintes:

1. objetivo;
2. termos e definições;
3. política de segurança;
4. segurança organizacional;
5. classificação e controle dos ativos de informação;
6. segurança em pessoas;
7. segurança ambiental e física;
8. gerenciamento das operações e comunicações;
9. controle de acesso;
10. desenvolvimento de sistemas e manutenção;
11. gestão de continuidade do negócio;
12. conformidade.

2.4.1 OBJETIVOS

Conforme a ABNT (2001) esta norma possui recomendações para a gestão da segurança da informação, para ser usado pelos responsáveis na introdução, implementação ou manutenção da segurança em suas organizações. O propósito desta norma é prover uma base padrão de desenvolvimento de normas de segurança da organização, como também para as práticas de gestão de segurança provendo confiança no relacionamento entre as organizações.

2.4.2 TERMOS E DEFINIÇÕES

Neste capítulo a norma traz alguns termos e definições usadas no decorrer dos capítulos da norma, como a segurança da informação que trata da confidencialidade, integridade e disponibilidade, como também da avaliação e gerenciamento de risco a tudo que se refere ao processamento e segurança da informação.

2.4.3 POLÍTICA DE SEGURANÇA

O objetivo para o relacionamento dos principais assuntos de uma política de segurança em uma organização é prover a direção apoio para segurança da informação (Tedeschi, 2001). Conforme Nascimento (2001) a administração deve estabelecer uma política clara e demonstrar apoio e comprometimento com a segurança da informação através da emissão e manutenção de uma política de segurança da informação para toda a organização.

2.4.4 SEGURANÇA ORGANIZACIONAL

A segurança organizacional tem o objetivo de gerenciar a segurança da informação na organização (Tedeschi, 2001). Esta estrutura de gerenciamento deve ser estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. Nascimento (2001) ressalta que este tópico aborda o estabelecimento de responsabilidades com terceiros e fornecedores de serviços. O acesso por terceiros às instalações de processamento da informação da organização precisa ser controlado. Este controle pode ser efetuado através de um acordo entre as partes, que deve considerar os riscos, controles de segurança e procedimentos para os sistemas de informação, rede de computadores e/ou estações de trabalho.

2.4.5 CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO

Tedeschi (2001) afirma que este tópico tem por objetivo garantir que os ativos de informação recebam um nível adequado de proteção. Esta proteção pode ser feita através da classificação, registro e controle dos ativos da organização. Segundo Nascimento (2001) todos os princípios ativos da informação da organização devem ser inventariados e ter um proprietário responsável. O inventário de ativos ajuda a garantir que a proteção está sendo mantida de forma adequada. Aos proprietários responsáveis dos principais ativos devem ser identificados e a eles deve ser atribuída a responsabilidade pela manutenção apropriada dos controles.

2.4.6 SEGURANÇA EM PESSOAS

A segurança em pessoas objetiva a redução dos riscos de erro humano acidental ou intencional, roubo, fraude ou uso indevido de instalações (Tedeschi, 2001). São abordadas inclusões de responsabilidades relativas, que devem ser atribuída na fase de recrutamento, incluída em contratos e monitorada durante a vigência do contrato de funcionários. A segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados a segurança. Usuários devem ser treinados nos procedimentos de segurança e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança. Os incidentes que afetam a segurança devem ser notificados através dos canais apropriados o mais rápido possível. Todos os funcionários e prestadores de serviço

devem estar conscientes dos procedimentos para notificação dos diversos tipos de incidentes que possam ter impactos na segurança dos ativos organizacionais (Nascimento, 2001).

2.4.7 SEGURANÇA AMBIENTAL E FÍSICA

De acordo com Tedeschi (2001) este tópico têm por objetivo a prevenção de acesso não autorizado, dano, perda e interferência às instalações físicas da organização e à sua informação. Nascimento (2001) afirma que recursos e instalações de processamento de informações críticas, ou sensíveis do negócio, devem ser mantidas em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano ou interferência.

2.4.8 GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

Têm por objetivo garantir a operação segura e correta dos recursos de processamento da informação, e proteger a integridade dos programas e da informação (Tedeschi, 2001). Neste tópico são apresentados quais são as principais áreas que devem ser objeto especial de atenção. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de *backup*, controle de documentação, segurança de correio eletrônico, entre outras. Os procedimentos e responsabilidades pela gestão e operação de todas as instalações de processamento das informações devem ser definidos. Isto abrange o desenvolvimento de procedimentos operacionais e de resposta a incidentes (Nascimento, 2001).

2.4.9 CONTROLE DE ACESSO

O controle de acesso procura controlar o acesso à informação e aos meios de acesso a mesma (Tedeschi, 2001). Nascimento (2001) afirma que neste tópico são definidas competências, sistema de monitoração de acesso e uso, a utilização de senhas, dentre outros assuntos. Os acessos às informações e processos do negócio devem ser controlados na base dos requisitos de segurança e do negócio. Procedimentos formais devem ser estabelecidos, para controlar a concessão das chaves de direitos de acesso aos sistemas de informação e serviços. A cooperação dos usuários autorizados é essencial para a eficácia da segurança. Os usuários devem estar cientes de suas responsabilidades para a manutenção efetiva dos

controles de acesso, considerando o uso de senhas e a segurança dos equipamentos de sua utilização.

2.4.10 DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Este tópico procura garantir que a segurança está implantada nos sistemas de informação (Tedeschi, 2001). São abordados neste item os requisitos de segurança dos sistemas, controles de criptografia, controle de arquivos, segurança do desenvolvimento e suporte de sistemas. Incluirá infra-estrutura, aplicações específicas ao negócio e aplicações desenvolvidas pelo usuário. Requisitos de segurança devem ser identificados e acordados antes do desenvolvimento dos sistemas de informação. O acesso aos sistemas de arquivos deve ser controlado (Nascimento, 2001).

2.4.11 GESTÃO DA CONTINUIDADE DO NEGÓCIO

O objetivo deste tópico é a não interrupção das atividades do negócio e proteger os processos críticos contra efeitos de grandes falhas ou desastres (Tedeschi, 2001). O processo de continuidade deve reduzir a interrupção para um nível aceitável através de uma combinação de ações e de recuperação. As conseqüências de desastres, falhas de segurança e perda de serviços devem ser analisados. Os planos de contingência devem ser desenvolvidos e implementados, para garantir que os processos de negócio possam ser recuperados no tempo devido (Nascimento, 2001).

2.4.12 CONFORMIDADE

A conformidade vai procurar evitar a violação de qualquer lei, estatutos, regulamentações ou obrigações contratuais, e de quaisquer requisitos de segurança (Tedeschi, 2001). Nascimento (2001) afirma que projetos, operações, uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentos ou estatutos. Consultorias em requisitos legais específicos podem ser procuradas em organizações de consultoria jurídica ou em profissionais liberais, adequadamente qualificados nos aspectos legais.

2.5 GERAÇÃO DO *CHECK-LIST*

No Anexo A, deste trabalho, encontra-se um *check-list*, detalhado sobre os tópicos da norma. Os tópicos foram abrangidos a partir da Política de Segurança até a Conformidade, que são os tópicos específicos para conceber a normalização dentro de uma organização. Este *check-list*, foi gerado a partir da leitura detalhada da norma, com apoio de livros e artigos. Este check-list, está inserido no banco de dados do protótipo, que será detalhado nos próximos capítulos do trabalho.

3 TECNOLOGIAS E AMBIENTES DE DESENVOLVIMENTO

Este capítulo pretende trazer informações breves para conhecimento do leitor de quais tecnologias foram empregadas para especificação e implementação do protótipo de *Software*, servindo para um leitor leigo que não possui conhecimento sobre as ferramentas aqui utilizadas.

No capítulo 3.1 será explanado sobre a orientação a objetos, trazendo conceitos e a facilidade de manutenção de um sistema desenvolvido orientado a objetos. No mesmo capítulo é descrita a UML, que é uma linguagem de modelagem utilizada para modelar objetos. No capítulo 3.2 será dada uma introdução sobre o *Rational Rose*, ferramenta para modelagem da UML, trazendo o objetivo de sua existência e suas facilidades de uso. No capítulo 3.3 será apresentado o Borland Delphi 5, que tem por objetivo contemplar os capítulos anteriores e trazer suas ferramentas de auxílio ao programador de sistemas. Ao final no capítulo 3.4, serão apresentados conceitos sobre o banco de dados Interbase, responsável em armazenar as informações, para utilização futura como processamento ou consulta.

3.1 ORIENTAÇÃO A OBJETOS

Montenegro (1994) afirma que exigência crescente dos usuários tem forçado a industria do *Software* a estabelecer um acelerado ritmo de produtividade e de melhoria da qualidade de seus sistemas. Esta pressão tem tornado os sistemas cada vez maiores e mais complexos.

A complexidade e tamanho são problemas para as técnicas, ferramentas e abstrações tradicionais da construção de sistemas. Neste aspecto há um certo consenso de que a programação orientada a objetos possa ser útil no controle da complexidade e na manutenção dos sistemas (Montenegro, 1994) .

Um objeto é uma ocorrência específica (instância) de uma classe e é similar a uma entidade/tabela no modelo relacional somente até o ponto onde representa uma coleção de dados relacionados com um tema em comum (Furlan, 1998).

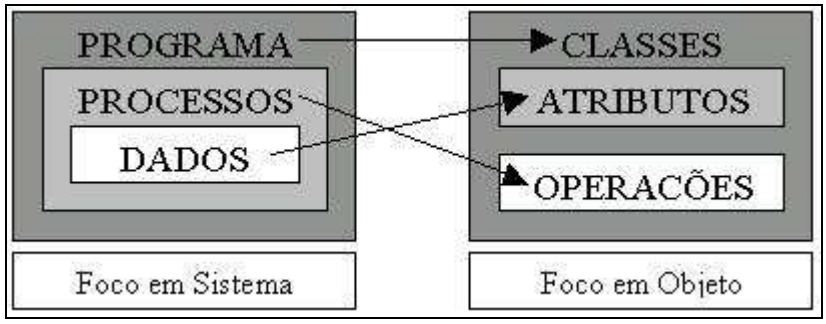
Neste aspecto há um certo consenso de que a programação orientada a objetos possa ser útil no controle da complexidade e na manutenção dos sistemas. Além disso, cada vez mais são utilizadas tecnologias diferentes simultaneamente na solução de um problema. Sobre

este ponto a orientação a objetos possui uma forma de definição diferenciada de seus elementos, podendo ser aproveitada como ferramenta de integração dos módulos distintos do sistema.

A programação orientada a objetos possui obstáculos naturais como resistência dos programadores a mudança na forma de programar. O ponto forte na orientação a objetos consiste no reaproveitamento de código e a maior facilidade de manutenção, quando comparados aos programas estruturados. Vale salientar que o tamanho do código gerado por programas desenvolvidos segundo o paradigma da Programação Orientada a Objetos é menor (Montenegro, 1994).

Na Figura 3.1, Furlan (1998) traz um comparativo entre sistemas e classes, mencionando que o programa equivale a classes do objeto, enquanto os processos dos sistemas equivalem às operações das classes e os dados equivalem aos atributos das classes.

Figura 3.1 – Enfoque em Sistemas Versus Enfoque em Objetos



Fonte: Furlan, 1998

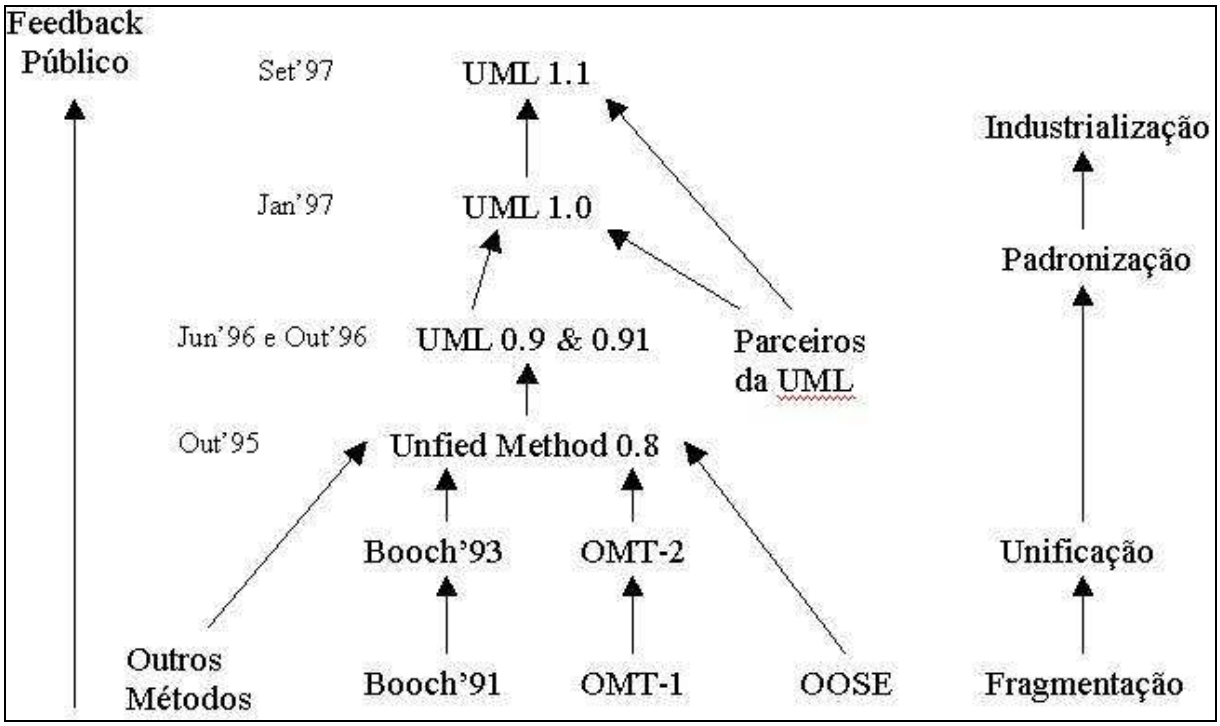
Conforme Furlan (1998) o sucesso em desenvolvimento de *Software* depende em grande parte do conhecimento, que não só envolve programação e habilidade de gerenciamento, mas também conhecimento e compreensão das mais recentes inovações na indústria do *Software*. Um fato curioso da tecnologia da informação é que sempre a última inovação tecnológica nos parece ser definitiva e que nada mais será possível ser inventado para substitui-la. Isso ocorreu com todas tecnologias e certamente irá acontecer com a tecnologia de objetos.

3.2 ORIENTAÇÃO A OBJETOS UTILIZANDO A UML

A *Unified Modeling Language* (UML), é uma linguagem de modelagem, não uma metodologia. A UML foi a junção de vários métodos, ganhando parceiros importantes como a Microsoft, Hewlett-Packard, Oracle, IBM entre outras (Furlan, 1998).

A Figura 3.2 mostra a evolução da UML, começando com o desenvolvimento e evolução de várias idéias, passando pelos processos de fragmentação, unificação, padronização e industrialização, até que a versão da UML 1.1 foi gerada.

Figura 3.2 – Evolução da UML



Fonte: Furlan, 1998

A UML pode ser usada para:

a) mostrar as fronteiras de um sistema e suas funções principais utilizando atores e casos de uso;
b) ilustrar a realização de casos de uso com diagramas de interação;
c) representar uma estrutura estática de um sistema utilizando diagramas de classe;
d) modelar o comportamento de objetos com diagramas de transição de estado;
e) revelar a arquitetura de implementação física com diagramas de componente e de implantação;
f) estender sua funcionalidade através de estereótipos.

Abaixo são relacionados alguns pontos, considerados importantes para utilização básica da UML, como:

a) atores: representam pessoas ou coisas que interagem com o sistema em desenvolvimento;

b) casos de uso: também conhecidos como *use-case*, especificam as ações de um

sistema, subsistema, ou classe, de forma seqüencial, com um dos atores envolvidos no processo;

c) classes: considerados os elementos mais importantes de qualquer sistema orientado objetos, tem por objetivo armazenar os atributos, relacionamentos, operações e a semântica;

d) diagrama de classes: considerados como os principais diagramas estruturais da UML, um diagrama de classe, mostra as interfaces e os relacionamentos entre esses elementos, especificando a estrutura e o comportamento dos objetos;

e) diagrama de seqüência: irá visualizar um conjunto de objetos, seus relacionamentos e as mensagens que podem ser enviadas entre eles, dando ênfase a ordenação destas mensagens.

3.3 RATIONAL ROSE

Qualquer método de desenvolvimento é melhor suportado com apoio de uma ferramenta, e neste objetivo é que foi desenvolvido o *Rational Rose*. Conforme Quatrani (2001) a família do produto *Rational Rose* é projetada para oferecer ao desenvolvedor de *Software* um conjunto completo de ferramentas de modelagem visual para o desenvolvimento de soluções fortes, eficientes para as verdadeiras necessidades comerciais nos ambiente cliente/fornecedor. A modelagem na ferramenta *Rational Rose* é acessível para programadores que desejam modelar processos comerciais, bem como a programadores que desejam modelar aplicativos lógicos. O *Rational Rose* permite executar análises de exigências comerciais, analise de cenário comercial, com diagramas de seqüência e colaboração, posição de modelagem, capacidades de geração de código adicional para DDL e IDL, juntamente com a inclusão de um script de linguagem, para fornecer acesso ao domínio *Rose*. O *Rational Rose* permite a criação de documentação dos diagramas de uso, classes e seqüência, podendo também gerar código de implementação para facilitar o trabalho do desenvolvedor.

3.4 BORLAND DELPHI 5

Conforme Oliveira (2000) a ferramenta Delphi foi lançada em 1994, baseada na linguagem *object* pascal, que é uma versão do Pascal, mas orientada a objetos. Lischner (2000) complementa que a linguagem *object* Pascal, além de ser uma linguagem moderna

orientada a objeto, possui elegância e a simplicidade do Pascal. O Delphi oferece inúmeras ferramentas para tornar o desenvolvimento para Windows, fácil, rápido e seguro.

Algumas características do Delphi que podem ser citadas:

a) interface gráfica para desenvolvimento conhecida como *Integrated Development Environment* (IDE), que é definido como sendo um conjunto coeso de programas que automatiza e centraliza o ciclo de vida da criação e distribuição de código de programa. Nesta interface, através de clique e arrastos de mouse, pode-se criar formulários sofisticados rapidamente, para os mais diversos tipos de aplicações;
b) possui um conjunto de componentes para realizar diversas operações, como entrada de dados, conexão com banco de dados, geração de relatórios, etc. Estes componentes estão agregados na *Visual Component Library* (VCL), e podem originar novos componentes adaptados as suas necessidades;
c) *sites* na internet que possuem componentes especiais para serem utilizados em outras funcionalidades;
d) um editor de código que oferece mensagens de erro, com cores diferentes para os comandos padrões sendo este editor integrado a um depurador profissional;
e) um compilador que gera um programa executável como código nativo e otimizado;
f) possibilidade de desenvolvimento de aplicações para Windows 98, Windows NT, Windows 2000, Windows ME e Windows XP;
g) facilidade e rapidez na criação de aplicativos que manipulam bancos de dados de diversos formatos, como Paradox, FoxPro, Access, SQL Server, Interbase e Oracle;

Conforme Lischner (2000) o Delphi possui classes e objetos, tratamento de exceções, programação *multithreaded*, programação modular, vínculo dinâmico e estático, automação OLE e outros recursos.

3.5 BANCO DE DADOS INTERBASE

Conforme Valley (1995) o Interbase é um sistema de gerência de banco de dados relacional (RDBMS), que provê processamento de transações rápidas e compartilhamento de dados em ambiente monousuário ou multiusuário. O padrão de uso do Interbase é o padrão SQL-92.

Interbase é uma tecnologia de servidor que oferece suporte transparente através de redes heterogêneas. Pode ser executado na maioria das plataformas Windows e em muitas implementações nos sistemas operacionais UNIX.

O Interbase roda sob duas formas: Local Interbase (monousuário), Interbase *Server* (remoto, multiusuário). Ambos servidores vem com opções cliente windows: Windows ISQL para definição dos dados e manipulação e o *Server Manager* para usuários autorizados e administradores de banco de dados.

Na criação do banco de dados o Interbase oferece características para criação do local onde o banco de dados com suas tabelas e estruturas serão criadas, como também o tamanho da página de dados, tamanho máximo do arquivo principal da base de dados, e número máximo de usuários que irão acessar a base de dados. No capítulo 3.5.1 são apresentados os tipos de dados que o Interbase suporta.

3.5.1 TIPOS DE DADOS SUPORTADOS PELO INTERBASE

Tabela 3.1 – Tipos de dados suportados pelo Interbase

Tipos	Descrição
BLOB	*Binary large object*. Armazena dados grandes tais como gráficos textos e voz digitalizada.
CHAR(n)	Tamanho fixo de caractere ou tipo de texto.
DATE	Data armazenando também horas na informação.
DECIMAL (precisão, escala)	Número com ponto e escala de digitação decimal a direita. Por exemplo: Decimal (10,3).
DOUBLÉ PRECISION	Científico: 15 dígitos de precisão.
FLOAT	Precisão simples: 7 dígitos de precisão.
INTEGER	Número com valor alto.
NUMERIC (precisão, escala)	Número com ponto e escala de digitação decimal a direita. Por exemplo: Numeric (10,3).
SMALLINT	Número com valor baixo.
VARCHAR(n)	Tamanho variável de caractere ou tipo de texto. Alterna entre variações de caractere e char.

São suportados pelo Interbase, até dez tipos de dados, que são apresentados na Tabela 3.1 para simples conferência. O Interbase permite opcionalmente aplicar certas obrigações para as colunas, estas obrigações são chamadas de obrigações de integridade. As construções de integridade dirigem-se de colunas para tabelas e de tabelas para tabelas, relacionando e validando as entradas de dados.

Na definição de índices o Interbase define automaticamente índices desde que sejam declaradas *primary keys*. O Interbase possui também as *TRIGGERS* que são blocos de código de manipulação de dados que são executados automaticamente quando uma operação de inserção, atualização e remoção em uma determinada tabela ocorre no banco de dados.

Amplamente utilizado em *TRIGGERS*, temos os *GENERATORS*, que funciona como um contador, fornecendo um número seqüencial e visam atribuir um valor para campos chaves.

4 DESCRIÇÃO DO PROTÓTIPO

4.1 REQUISITOS

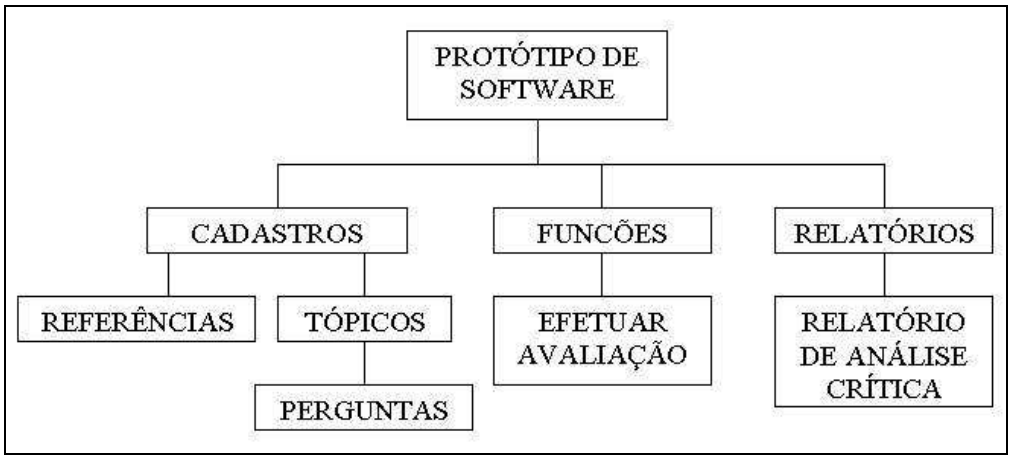
Este protótipo terá sua funcionalidade aplicada diretamente sobre a segurança da informação, comportando o *check-list* elaborado neste trabalho, e abrindo a possibilidade da alteração dos tópicos bem como das perguntas, permitindo a atualização constante do *check-list*. Também é importante, que os *sites* sejam armazenados, da onde são extraídas algumas das informações que vão compor as atualizações do *check-list*, sendo que a atualização mais importante, será quando a norma sofrer alguma atualização. Exige-se do protótipo a flexibilidade da escolha dos tópicos, o qual a organização deseja ser avaliada, conseqüentemente a atribuição dos pesos destes tópicos na avaliação, para que ocorra a quantificação conforme a necessidade. Ao final de cada avaliação, será apresentada para a organização, a disponibilidade de emitir um relatório que listará os tópicos selecionados com suas respectivas perguntas e respostas, e caso as respostas não possuam um grau positivo, sugerir análises críticas para que ocorra o processo de adequação para com a norma. Juntamente com estas análises, serão apresentadas médias por tópico e a média geral alcançada

4.2 ESPECIFICAÇÃO

Este capítulo apresenta o protótipo de *Software* que irá auxiliar uma organização para avaliar a segurança de suas informações conforme a norma NBR ISO/IEC 17799.

O protótipo de *Software* foi organizado em três módulos, como mostra a Figura 4.1

Figura 4.1 – Organograma do funcionamento do protótipo



Os objetivos dos módulos apresentados na Figura 4.1 são os seguintes:

a) cadastro de Referências: seu objetivo principal é servir de apoio ao usuário que deseja manter seu *check-list* atualizado através de artigos que se encontram na rede mundial, não possuindo ligação direta ao processo de avaliação. Este cadastro contém o nome e a URL do *site*;
b) cadastro de Tópicos: serão informados os tópicos que serão utilizados na avaliação como títulos para as perguntas;
c) cadastro de Perguntas: serão cadastradas as perguntas referentes aos tópicos, podendo aplicar algumas observações opcionais das perguntas informando o que pode acontecer caso a resposta tenha aspecto negativo. Também contém um campo para a análise crítica, que trará sugestões para poder alcançar um grau de quantificação adequado para esta pergunta;
d) efetuar Avaliação: esta função é responsável pela execução da avaliação na organização perante a norma;
e) relatório de Análise: este relatório será então o responsável em trazer as perguntas e respostas calculando as médias parciais e ponderadas, trazendo para cada pergunta menor do que três uma análise crítica para poder elevar esta nota.

O usuário que se utilizar deste protótipo de *Software* terá uma ferramenta de fácil manuseio, por ser um *Software* flexível no sentido da manipulação de suas informações e transparente, pois todas as informações estão visíveis para consultar e alterar.

Como principal vantagem do protótipo, tem-se a facilidade do processo de avaliação da segurança da informação dentro da organização, trazendo perguntas objetivas. Para isso, é interessante que o usuário ou equipe tenha o mínimo de conhecimento sobre os procedimentos de segurança da informação na organização. No entanto, não é necessário que se tenha conhecimento das funcionalidades da norma para responder ao *check-list*.

Na versão atual do protótipo, é fornecida uma proposta inicial dos tópicos a serem utilizados. Cada tópico é dividido em tópicos principais e sub-tópicos, sendo que os tópicos principais são os dez tópicos da norma, apresentados anteriormente. Cada tópico terá um peso associado a ele, o qual que será utilizado ao final de cada avaliação para gerar a média ponderada e conseqüentemente a análise crítica. O protótipo oferece também um conjunto de perguntas, as quais permitem a avaliação da conformidade da empresa com relação à norma em questão.

Os tópicos, bem como as perguntas, ficam armazenadas em banco de dados, podendo ser utilizado sempre que necessitar fazer uma nova avaliação. Embora o protótipo contenha todos os tópicos propostos pela norma NBR ISO IEC 17799, não é necessário que a avaliação de uma empresa envolva todos eles. Pode-se, por exemplo, avaliar a conformidade da empresa somente com relação à Política de Segurança.

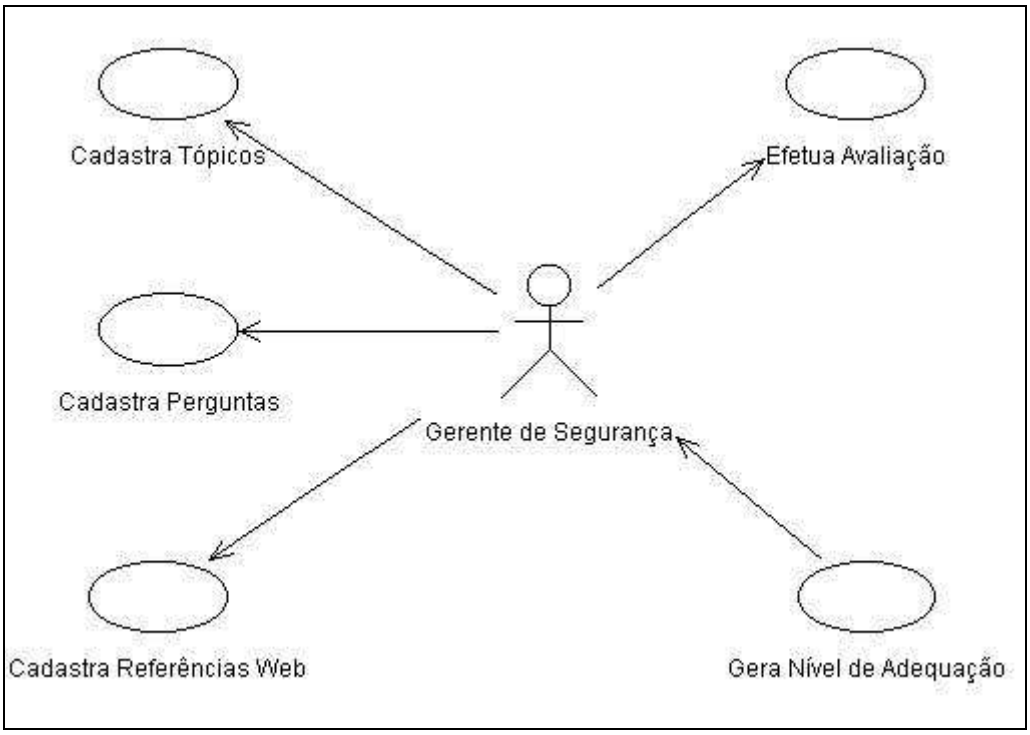
Quando a avaliação for concluída pelo usuário, o mesmo poderá imprimir o relatório da avaliação contendo a média ponderada das respostas dos tópicos, juntamente com uma análise crítica gerada pelo protótipo referente a cada um dos tópicos escolhidos.

Para a especificação foi utilizada a análise orientada a objetos através da linguagem de modelagem UML, sendo apresentados o caso de uso, como também as classes criadas durante a implementação deste protótipo.

4.2.1 VISÃO GERAL DO PROTÓTIPO

Esta seção apresenta uma visão geral da especificação do protótipo, mostrando seus principais processos, através dos casos de uso ou *use-case*, e suas classes, atributos e métodos, através de diagramas de classe utilizando a *Unified Modeling Language* (UML) com o auxílio da ferramenta *Rational Rose*. A Figura 4.2 apresenta o *use-case* com os processos que envolvem o protótipo deste trabalho.

Figura 4.2 – *Use-case* representando os processos do protótipo

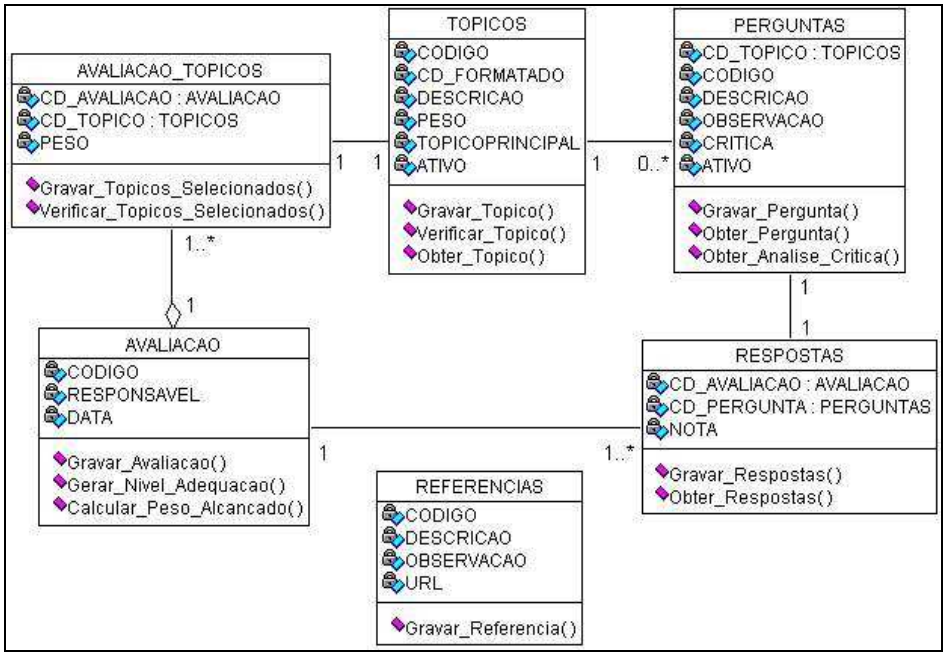


Abaixo, é apresentada a definição de cada caso de uso:

- cadastra tópicos : neste processo será aberta uma janela para o usuário informar os dados dos tópicos.
- cadastra perguntas : neste processo será aberta uma janela para o usuário informar as perguntas referentes aos tópicos;
- cadastra referência *web*: neste processo será aberta uma janela para o usuário informar os *sites* da internet, que possuam como conteúdo a segurança da informação;
- efetua avaliação: este processo será responsável pela execução da avaliação através de duas janelas, uma que será informados os dados da avaliação e a outra que fará perguntas para o usuário responder com notas;
- gera nível de adequação: este processo trará um relatório separado por tópicos que contém o grau de quantificação, juntamente com análises críticas de adequação.

Tendo uma visão geral dos processos que envolvem este protótipo, pode-se agora detalhar um pouco mais as classes que compõe o mesmo, e logo após os processos serão vistos em detalhes através de diagramas de seqüência. A Figura 4.3 apresenta o diagrama de classes com seus respectivos atributos e métodos.

Figura 4.3 – Diagrama de Classes do Protótipo



A tabela 4.1 apresenta em detalhes a existência de cada classe, com seus atributos e métodos, sendo que nos capítulos posteriores, os atributos e métodos referenciados nesta Tabela serão tratados em mais detalhes, exemplificando a usabilidade de cada um.:

Tabela 4.1 – Definição dos Atributos e Métodos das Classes

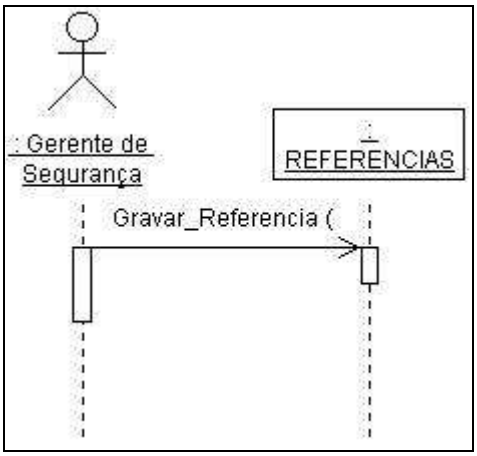
Classe TÓPICOS	
Abriga todos os tópicos cadastrados que irão compor as perguntas	
Atributos	**Definição**
CODIGO	Numeração auto-incremento
CD_FORMATADO	Texto, para armazenar o código em níveis do tópico (4 níveis)
DESCRICAO	Texto, para armazenar a descrição do tópico
PESO	Decimal, armazena o peso padrão do tópico
TOPICOPRINCIPAL	Caractere, especifica se é um tópico principal
ATIVO	Caractere, especifica se o tópico é utilizado em novas avaliações
Métodos	**Definição**
Gravar_Topico	Efetua a gravação das informações impostas pelo usuário no banco de dados
Verificar_Tópico	Verifica se o tópico em questão existe
Obter_Tópico	Obtém o tópico para ser visualizado (consulta, relatório)
Classe PERGUNTAS	
Abriga todas as perguntas cadastradas que irão ser utilizadas na avaliação	
Atributos	**Definição**
CD_TOPICO	Numeração, possui relação ao código do tópico
CODIGO	Numeração auto-incremento
DESCRICAO	Texto, responsável em armazenar a pergunta
OBSERVAÇÃO	Texto, responsável em armazenar a importância da pergunta
CRITICA	Texto, crítica da pergunta, caso a resposta não alcance avaliação positiva
ATIVO	Caractere, especifica se a pergunta é utilizada em novas avaliações
Métodos	**Definição**
Gravar_Pergunta	Efetua a gravação das informações impostas pelo usuário no banco de dados
Obter_Pergunta	Obtém a pergunta para ser visualizada (consulta, relatório)
Obter_Analise_Critica	Obtém a analise crítica caso a resposta não alcance avaliação positiva
Classe AVALIACAO	
Abriga dados essenciais da avaliação para identificação no momento de gerar o relatório	
Atributos	**Definição**
CÓDIGO	Numeração auto-incremento
RESPONSAVEL	Texto, nome do responsável pela avaliação
DATA	Data, data e hora da avaliação
Métodos	**Definição**
Gerar_Nível_Adequacao	Inicia o processo de geração do relatório
Calcular_Peso_Alcancado	Calcula a média alcançada
Gravar_Avaliacao	Inicia o processo da avaliação, e grava no banco de dados
Classe AVALIACAO_TÓPICOS	
Abriga os tópicos principais selecionados pelo usuário para efetuar a avaliação. Está agregada a classe avaliação	
Atributos	**Definição**
CD_AVALIACAO	Numeração, possui relação ao código da

	avaliação
CD_TOPICO	Numeração, possui relação ao código do tópico
PESO	Decimal, peso específico para a avaliação
Métodos	**Definição**
Gravar_Topicos_Selecionados	Grava os tópicos selecionados no inicio da avaliação no banco de dados
Verificar_Tópicos_Selecionados	Verifica quais tópicos foram selecionados
Classe RESPOSTAS	
Abriga as respostas informadas para as perguntas associadas na avaliação	
Atributos	**Definição**
CD_AVALIACAO	Numeração, relacionado ao código da avaliação
CD_PERGUNTA	Numeração, relacionado ao código da pergunta
NOTA	Inteiro, nota alcançada na pergunta (1 a 4)
Métodos	**Definição**
Gravar_Respostas	Grava a resposta informada pelo usuário no banco de dados
Obter_Respostas	Obtém a resposta do banco de dados
Classe REFERÊNCIAS	
Abriga as referências da internet, não possui ligação direta ao processo de avaliação	
Atributos	**Definição**
CODIGO	Numeração, auto-incremento
DESCRICAO	Nome do *site*
OBSERVACAO	Dados complementares do *site*
URL	Endereço do *site*
Métodos	**Definição**
Gravar_Referencia	Efetua a gravação dos dados informados pelo usuário no banco de dados

4.2.2 CADASTRO DE REFERÊNCIAS DA WEB

O processo de cadastramento de referências é aquela que abre a janela de comandos que o usuário poderá utilizar para cadastrar um determinada referência. Neste processo acontece a instanciação de um objeto da classe `REFERENCIAS` que inicializa todos os componentes que compõe a janela para cadastrar as referências. A Figura 4.4 ilustra o diagrama de seqüência do processo de cadastramento de referências.

Figura 4.4 – Processo para Cadastrar Referências

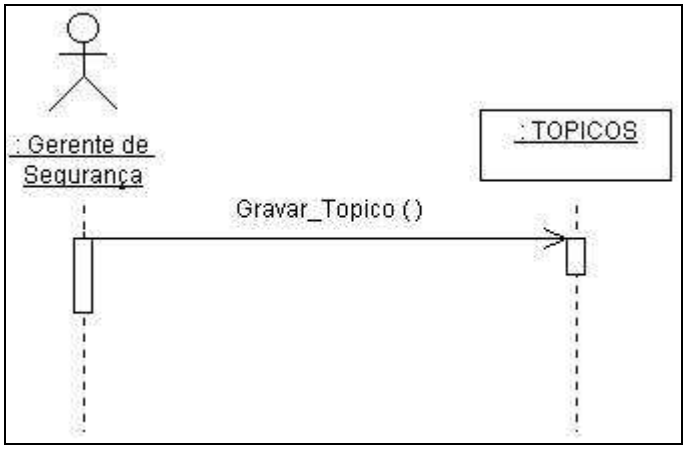


O diagrama da Figura 4.4, ilustra a chamada do método `Gravar_Referencia`, que é responsável em capturar todas informações impostas pelo usuário, na interface e efetuar a gravação, internamente é verificado se os dados estão completos para gravar e se é uma referência nova ou não. A implementação principal desta classe, se encontra no Anexo B, para consulta.

4.2.3 CADASTRO DE TÓPICOS

O processo de cadastramento de tópicos é aquela que abre a janela de comandos que o usuário poderá utilizar para cadastrar um determinado tópico. Neste processo acontece a instanciação de um objeto da classe `TOPICOS` que inicializa todos os componentes que compõe a janela para cadastrar os tópicos. A Figura 4.5 ilustra o diagrama de seqüência do processo de cadastramento de tópicos.

Figura 4.5 – Processo para Cadastrar Tópicos



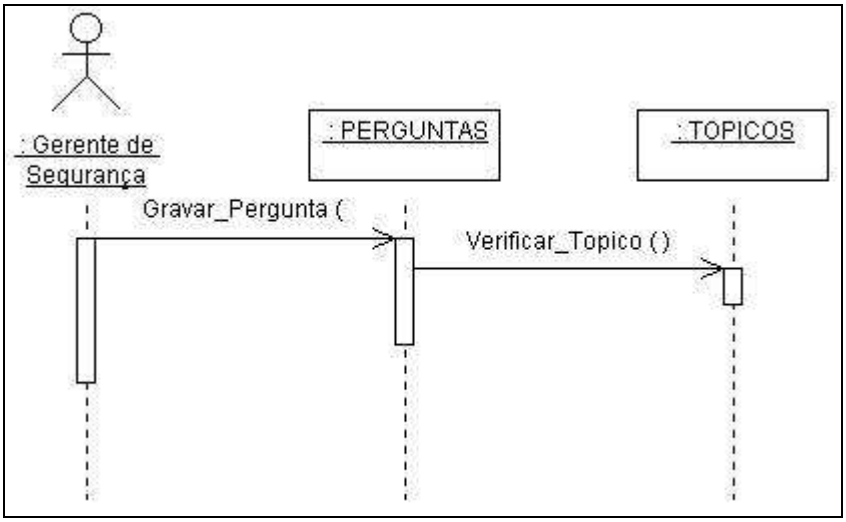
O diagrama da Figura 4.5, ilustra a chamada do método `Gravar_Topico`, que é responsável em capturar todas informações impostas pelo usuário, na interface e efetuar a gravação. Internamente é verificado se os dados estão completos para gravar, e se é um tópico novo ou não.

4.2.4 CADASTRO DE PERGUNTAS

O processo de cadastramento de perguntas abre uma janela de comandos para cadastrar uma determinada pergunta conforme um tópico escolhido pelo usuário. Neste processo acontece a instanciação de um objeto da classe `TOPICOS` para poder consultar os tópicos e outro objeto `PERGUNTAS` que inicializa todos os componentes que compõe a janela

para cadastrar as perguntas. A Figura 4.6 ilustra o diagrama de seqüência do processo de cadastramento de perguntas.

Figura 4.6 – Processo para Cadastrar Perguntas

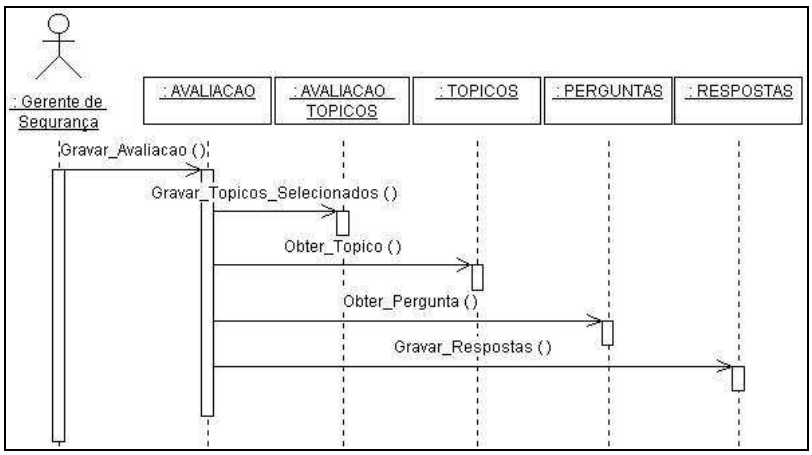


O diagrama da Figura 4.6, ilustra a chamada do método `Gravar_Pergunta`, que é responsável em capturar todas informações impostas pelo usuário na interface, e efetuar a gravação, internamente é verificado se o tópico informado existe, chamando o método `Verificar_Topico`, que verifica se os dados estão completos para gravar, e verifica se a pergunta é nova ou não.

4.2.5 EFETUANDO A AVALIAÇÃO

O processo de efetuar avaliação abre duas janelas de comandos, uma para cadastrar algumas informações da avaliação, e a outra que irá trazer as perguntas para o usuário responder. Neste processo são instanciados os objetos das classes `AVALIACAO`, `AVALIACAO_TOPICOS`, `TOPICOS`, `PERGUNTAS` e `RESPOSTAS`. A Figura 4.7 ilustra o diagrama de seqüência do processo de avaliação.

Figura 4.7 – Processo para Efetuar Avaliação

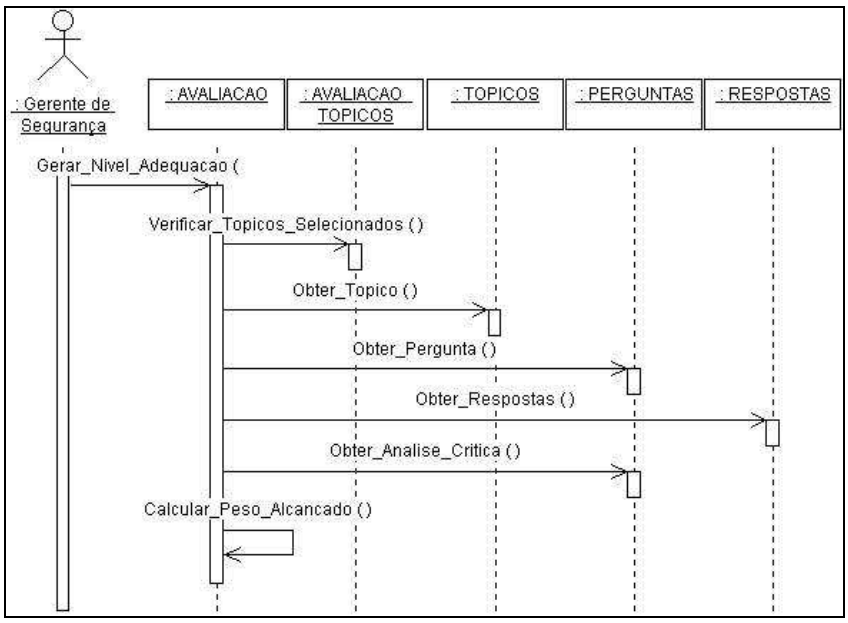


O diagrama da Figura 4.7, ilustra a chamada do método `Gravar_Avaliacao`, que é responsável em capturar todas informações impostas pelo usuário na interface. São gravados também os tópicos selecionados utilizando o método `Gravar_Topicos_Selecionados`. Após gravadas as informações básicas, é iniciada a avaliação, obtendo o primeiro tópico através do método `Obter_Topico` e conseqüentemente busca-se a primeira pergunta através do método `Obter_Pergunta`. O usuário, por sua vez, terá que informar uma nota, que será gravada através do método `Gravar_Respostas`, até que avaliação termine, podendo então efetuar o processo de geração do nível de adequação.

4.2.6 GERAR O NÍVEL DE ADEQUAÇÃO

O processo de geração do nível de adequação consiste em gerar um relatório que estará separado por tópicos, sendo que cada tópico, terá abaixo uma seqüência de perguntas com suas respostas, trazendo uma média das notas e a média ponderada conforme o tópico, juntamente com uma análise crítica para a organização poder adequar-se. Neste processo são instanciados os objetos das classes `AVALIACAO`, `AVALIACAO_TOPICOS`, `TÓPICOS`, `PERGUNTAS` e `RESPOSTAS`. A Figura 4.8 ilustra o diagrama de seqüência do processo da geração do nível de adequação.

Figura 4.8 – Processo para Gerar o Nível de Adequação



O diagrama da Figura 4.8, ilustra a chamada do método `Gerar_Nivel_Adequacao`, que é responsável em capturar todas informações armazenadas na classe, e disponibiliza-las na interface do relatório. Neste processo também são verificados quais tópicos foram selecionados para a avaliação em questão, utilizando o método `Verificar_Topicos_Selecionados`. Após, é obtido o primeiro tópico através do método `Obter_Topico`, e conseqüentemente busca-se a primeira pergunta, através do método `Obter_Pergunta`, que será suficiente para buscar a resposta, através do método `Obter_Respostas`. Caso a resposta não venha a ter uma avaliação positiva, será chamado o método `Obter_Analise_Critica`. Com todas as respostas carregadas, então é calculado o nível de adequação, através do método `Calcular_Peso_Alcancado`.

4.3 MODELO ORIENTADO OBJETOS PARA BANCO DE DADOS RELACIONAL

A modelagem do banco de dados relacional não sofreu nenhuma alteração comparado a estrutura da modelagem orientada a objetos, sendo que foram somente utilizadas algumas facilidades do banco de dados Interbase, na geração do banco. Para a criação dos campos auto-incrementos foram utilizados *TRIGGERS*, associados aos *GENERATORS*, que foram comentados no capítulo 3.5.1. A Tabela 4.2 mostra as tabelas que foram criadas para conceber o *check-list*.

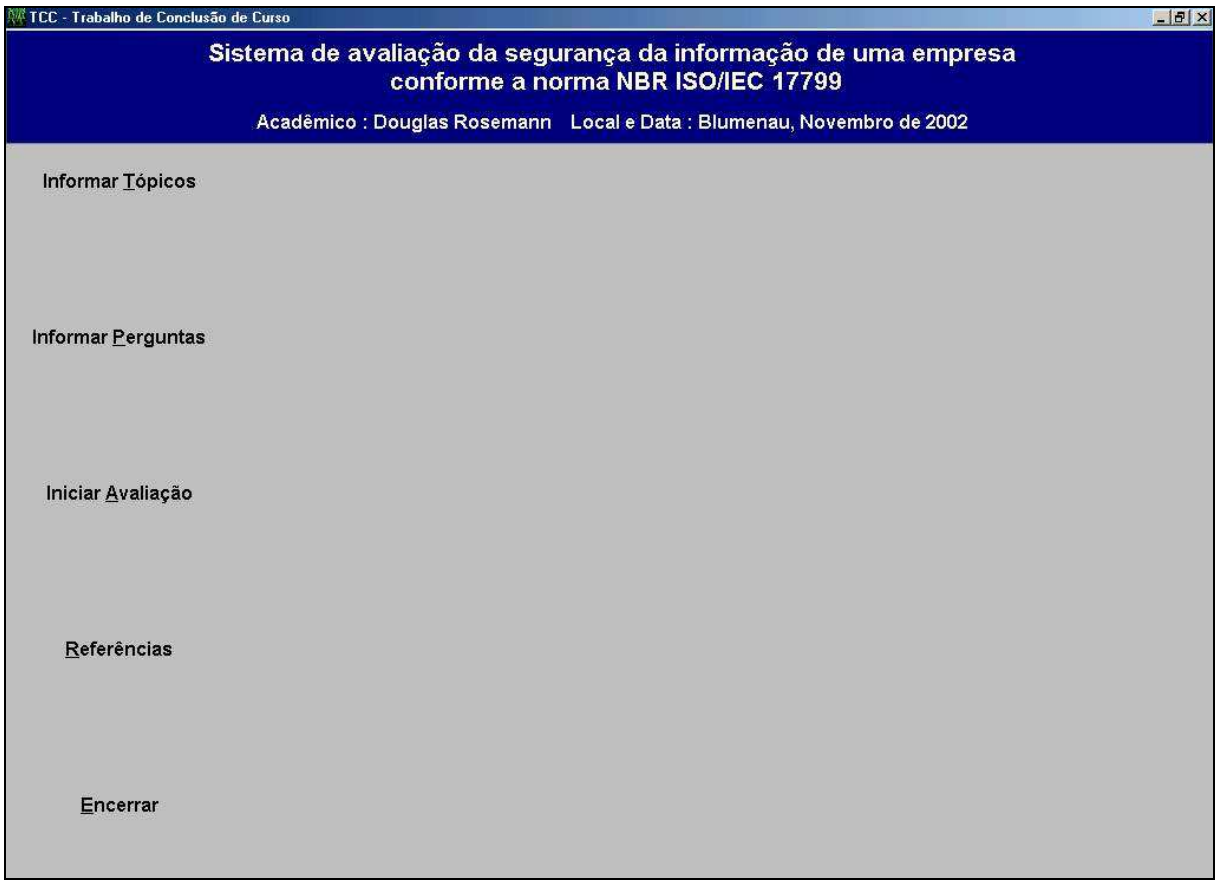
Tabela 4.2 – Tabelas criadas no Interbase

AVALIACÃO				
Campo	**Referência**	**Tipo**	**Tamanho**	**Permite Nulo**
CODIGO	Primary Key	Integer	4	Não
RESPONSAVEL		Char	60	Não
DATA		Date	8	Não
AVALIACAO_TÓPICOS				
Campo	**Referência**	**Tipo**	**Tamanho**	**Permite Nulo**
CD_AVALIACAO	Foreign Key	Integer	4	Não
CD_TOPICO	Primary Key	Integer	4	Não
PESO		Numeric	8	Não
PERGUNTAS				
Campo	**Referência**	**Tipo**	**Tamanho**	**Permite Nulo**
CD_TOPICO	Foreign Key	Integer	4	Não
CODIGO	Primary Key	Integer	4	Não
DESCRICAO		VarChar	500	Não
OBSERVACAO		VarChar	500	Sim
CRITICA		VarChar	500	Sim
ATIVO		Char	1	Não
REFERENCIAS				
Campo	**Referência**	**Tipo**	**Tamanho**	**Permite Nulo**
CODIGO	Primary Key	Integer	4	Não
DESCRICAO		Char	60	Não
OBSERVACAO		VarChar	500	Não
URL		Char	60	Não
RESPOSTAS				
Campo	**Referência**	**Tipo**	**Tamanho**	**Permite Nulo**
CD_AVALIACAO	Foreign Key	Integer	4	Não
CD_PERGUNTA	Foreign Key	Integer	4	Não
NOTA		Integer	4	Não
TÓPICOS				
Campo	**Referência**	**Tipo**	**Tamanho**	**Permite Nulo**
CODIGO	Primary Key	Integer	4	Não
CD_FORMATADO	Secondary Key	Char	20	Não
DESCRICAO		Char	100	Não
PESO		Numeric	8	Não
TOPICO_PRINCIPAL		Char	1	Não
ATIVO		Char	1	Não

4.4 FUNCIONAMENTO DO SISTEMA

Nesta seção será apresentada a interface do *Software*, bem como seu funcionamento. Ao inicializar o software, o usuário tem acesso ao menu principal, a partir do qual poderá ter acesso a todas as funções do sistema. A Figura 4.9 apresenta a tela com o menu principal do sistema.

Figura 4.9 – Tela com o Menu Principal do Sistema



4.4.1 REALIZANDO UMA AVALIAÇÃO

Essa versão do software já vem com o *check-list* dos itens da norma NBR ISO / IEC 17799. Em função disso, uma vez inicializado o software, o usuário já pode iniciar a avaliação da organização, clicando sobre a opção **Iniciar Avaliação**, do menu principal. Ao clicar sobre essa opção o usuário tem acesso ao módulo de avaliação.

Na tela de avaliação, o primeiro passo é definir o código da avaliação, o nome do responsável e a data de realização da avaliação. Em seguida, conforme indicado na Figura 4.10, o avaliador deve definir os tópicos a serem avaliados e indicar seus respectivos pesos.

Figura 4.10 – Iniciando uma Avaliação

É importante observar que quando um tópico não estiver marcado, como ocorreu com o tópico **Segurança Física e do Ambiente** na Figura 4.10, o mesmo não será utilizado na avaliação em questão. Uma vez definidos os tópicos a serem avaliados e seus respectivos pesos, o usuário deve clicar sobre o botão **Iniciar Avaliação**.

Quando o usuário clica sobre o botão **Iniciar Avaliação**, o software apresenta, seqüencialmente, as perguntas a serem respondidas para cada tópico selecionado. A Figura 4.11 apresenta a primeira pergunta relativa ao tópico **Política de Segurança**.

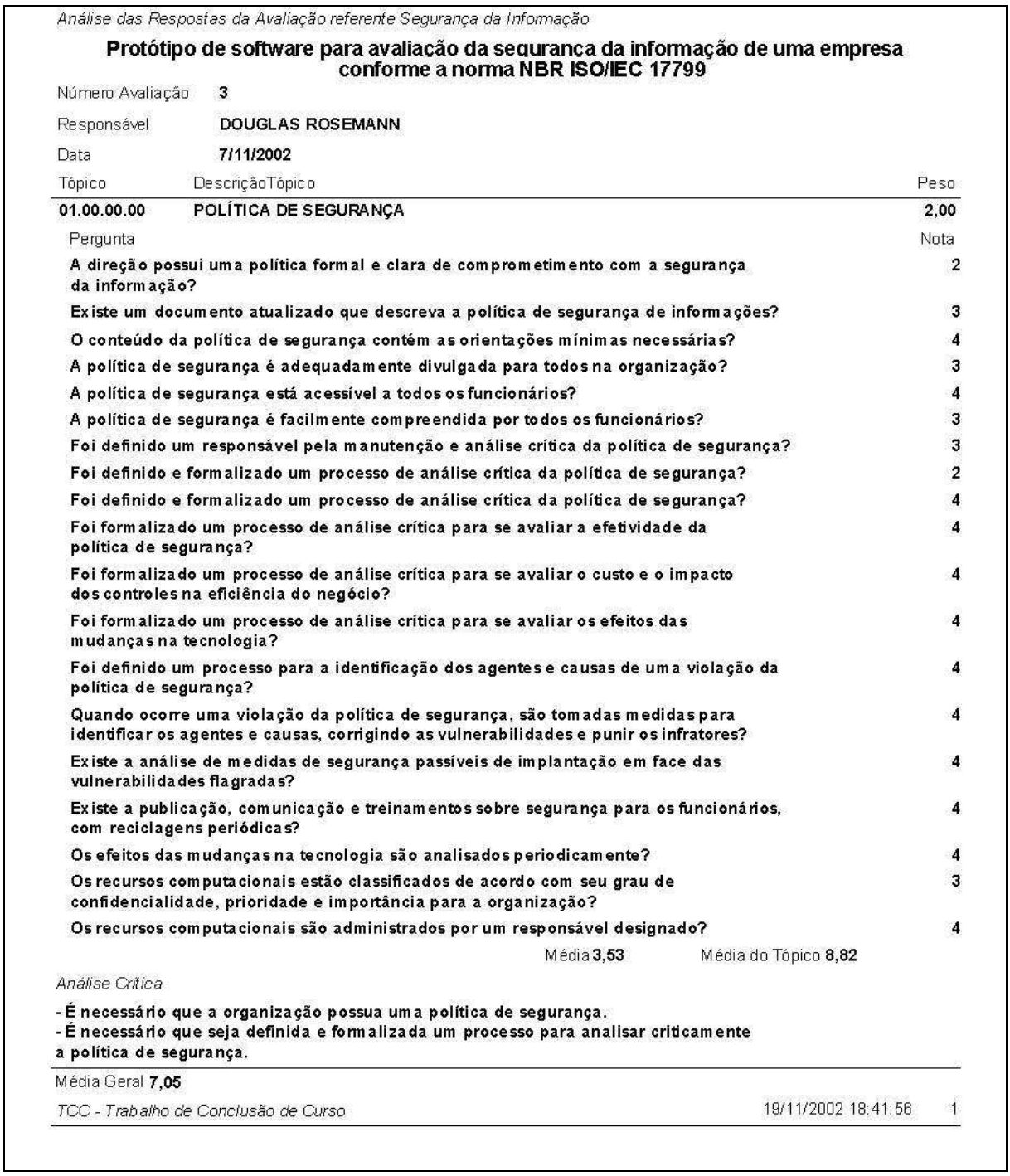
Figura 4.11 – Resposta às Perguntas do *Check List*

Neste momento são lidos os tópicos, e conseqüentemente as perguntas e observações previamente cadastradas, tendo que o usuário ler e decidir por uma nota. As notas foram definidas em uma seqüência de um a quatro. As notas um e dois são consideradas como negativas, e são alvos de críticas no relatório. Enquanto as notas três e quatro, são consideradas positivas. Após indicar a nota para a pergunta em questão, o usuário deve clicar sobre o botão **Avançar**, para responder às demais perguntas dos tópicos selecionados para a avaliação atual. Ao responder todas as perguntas do *check-list*, o *software* retorna à tela referente ao início da avaliação. Agora, conforme pode ser observado na Figura 4.12, o botão **Imprimir** está habilitado.

Figura 4.12 – Avaliação efetuada pronta para imprimir

Ao clicar sobre o botão **Imprimir**, será iniciado o processo de geração do relatório do nível de adequação com a análise crítica, abrindo uma tela de visualização do relatório, antes de envia-lo para uma impressora. A Figura 4.13 mostra o *layout* do relatório a ser impresso.

Figura 4.13 – *Layout* do relatório



Análise das Respostas da Avaliação referente Segurança da Informação

Protótipo de software para avaliação da segurança da informação de uma empresa conforme a norma NBR ISO/IEC 17799

Número Avaliação **3**

Responsável **DOUGLAS ROSEMANN**

Data **7/11/2002**

Tópico	DescriçãoTópico	Peso
01.00.00.00	**POLÍTICA DE SEGURANÇA**	**2,00**

Pergunta	Nota
A direção possui uma política formal e clara de comprometimento com a segurança da informação?	**2**
Existe um documento atualizado que descreva a política de segurança de informações?	**3**
O conteúdo da política de segurança contém as orientações mínimas necessárias?	**4**
A política de segurança é adequadamente divulgada para todos na organização?	**3**
A política de segurança está acessível a todos os funcionários?	**4**
A política de segurança é facilmente compreendida por todos os funcionários?	**3**
Foi definido um responsável pela manutenção e análise crítica da política de segurança?	**3**
Foi definido e formalizado um processo de análise crítica da política de segurança?	**2**
Foi definido e formalizado um processo de análise crítica da política de segurança?	**4**
Foi formalizado um processo de análise crítica para se avaliar a efetividade da política de segurança?	**4**
Foi formalizado um processo de análise crítica para se avaliar o custo e o impacto dos controles na eficiência do negócio?	**4**
Foi formalizado um processo de análise crítica para se avaliar os efeitos das mudanças na tecnologia?	**4**
Foi definido um processo para a identificação dos agentes e causas de uma violação da política de segurança?	**4**
Quando ocorre uma violação da política de segurança, são tomadas medidas para identificar os agentes e causas, corrigindo as vulnerabilidades e punir os infratores?	**4**
Existe a análise de medidas de segurança passíveis de implantação em face das vulnerabilidades flagradas?	**4**
Existe a publicação, comunicação e treinamentos sobre segurança para os funcionários, com reciclagens periódicas?	**4**
Os efeitos das mudanças na tecnologia são analisados periodicamente?	**4**
Os recursos computacionais estão classificados de acordo com seu grau de confidencialidade, prioridade e importância para a organização?	**3**
Os recursos computacionais são administrados por um responsável designado?	**4**

Média **3,53** Média do Tópico **8,82**

Análise Crítica

- É necessário que a organização possua uma política de segurança.
- É necessário que seja definida e formalizada um processo para analisar criticamente a política de segurança.

Média Geral **7,05**

TCC - Trabalho de Conclusão de Curso 19/11/2002 18:41:56 1

A Figura 4.13, apresenta um exemplo de impressão relativo somente ao tópico da **Política de Segurança**, permitindo observar como os dados estarão distribuídos no relatório, contendo as perguntas com suas respectivas respostas (notas). A média é representada pela soma de todas as notas dividido pelo numero de notas, na Figura 4.13, está representado pela média 3,53. A Média do Tópico é o resultado da conversão de uma escala de um a quatro para uma escala de zero a dez, na Figura 4.13, está representado pela média 8,82. Isso foi feito para facilitar a interpretação por parte do avaliador.

Abaixo da Média do Tópico, é apresentada uma análise crítica do resultado da avaliação, indicando os pontos que merecem maior atenção por parte da organização. Esta análise é proveniente do cadastro de perguntas, cadastrada juntamente com a pergunta em si. No final do relatório mostrado na Figura 4.13 é apresentada a Média Geral da avaliação, a qual é calculada através da média do tópico e multiplicado pelo peso do tópico, na Figura 4.13 o peso equivale a 2, enquanto que a média geral está sendo representada pela média 7,05.

No caso dos sub-tópicos, que não estão sendo representados na Figura 4.13, eles passam pelo mesmo processo de cálculo, porém o resultado da média ponderada (média x peso) deste sub-tópico, é adicionado ao tópico “pai” como se fosse uma nota de uma pergunta. Este processo ocorre nos quatro níveis que um tópico pode alcançar.

4.4.2 ATUALIZANDO O *CHECK LIST*

As normas de segurança são periodicamente modificadas de forma a refletir às mudanças na tecnologia e nas necessidades das organizações. Por esse motivo, o software desenvolvido permite a modificação dos tópicos cadastrados, bem como de suas respectivas perguntas. Isso permite que a organização esteja utilizando sempre as versões mais atualizadas das normas existentes.

Adicionalmente, o software permite a inclusão de novos tópicos e perguntas. Com isso, a organização pode incluir tópicos e perguntas não considerados explicitamente pela norma. Para fazer as alterações de tópicos, o usuário deve utilizar, a partir do menu principal mostrado na Figura 4.9, a opção **Informar Tópicos**.

Ao clicar sobre o botão **Informar Tópicos**, o usuário tem acesso à tela **Inclusão de Tópicos**, conforme mostrado na Figura 4.14. Para incluir um novo tópico, basta clicar sobre o botão **Novo** e informar: o código, a descrição e o peso.

Figura 4.14 – Tela do Cadastro de Tópicos

É importante observar que na tela mostrada na Figura 4.14 existem duas opções para serem marcadas: **Tópico Principal** e **Tópico Ativado**. A opção **Tópico Principal** deve ser marcada quando o tópico em questão for um dos tópicos principais da norma que está sendo utilizada. Já a opção **Tópico Ativado** indica se o código que está sendo incluído estará ou não ativo nas avaliações. Quando a opção **Tópico Ativado** estiver desmarcada, o tópico em questão não será incluído quando da realização de uma avaliação.

Outro aspecto importante a ser ressaltado na Figura 4.14 é que o código utilizado indica o nível do tópico ao qual ele se refere, da seguinte forma:

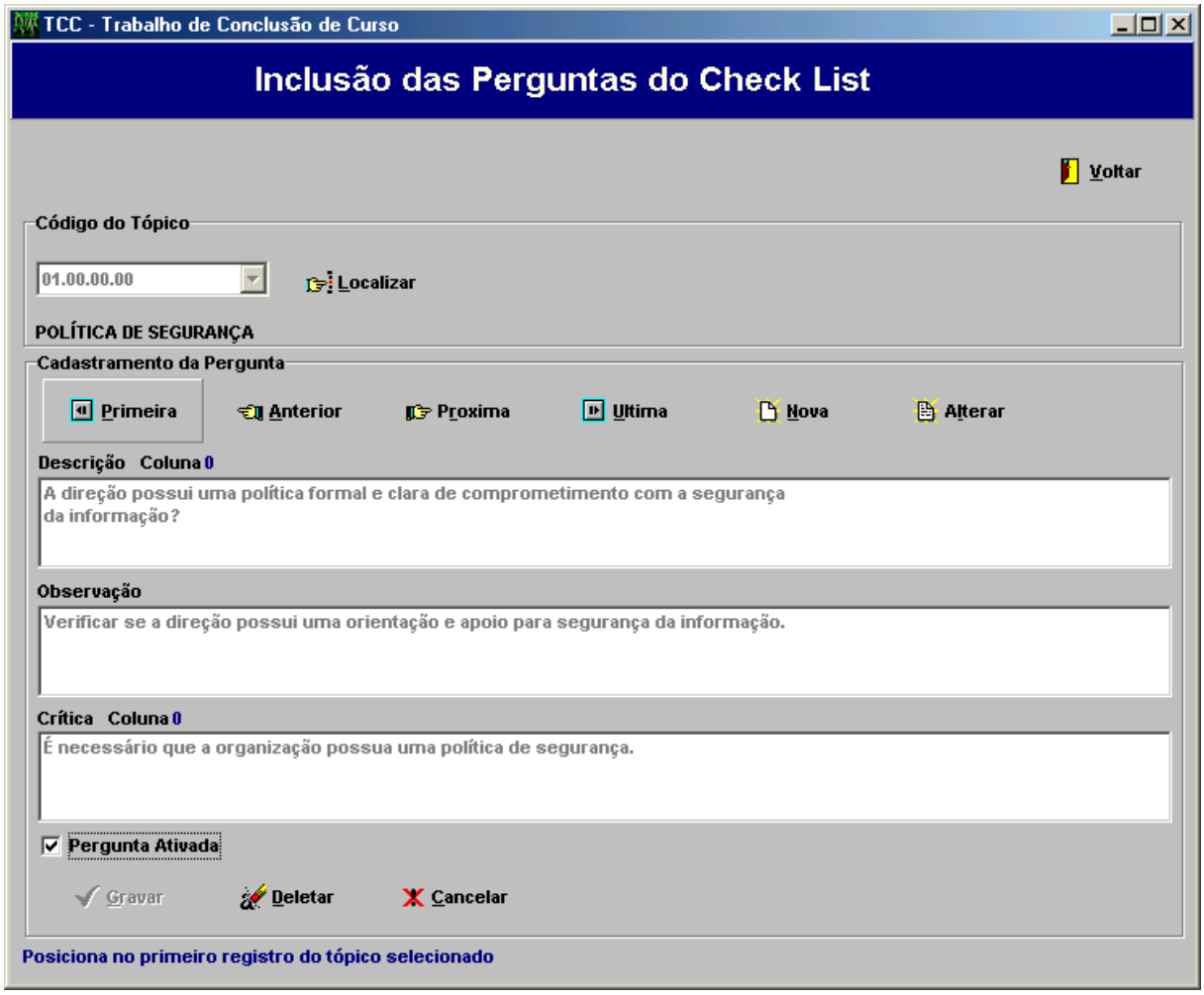
- 01. Nível de primeira ordem
- 01.10. Nível de segunda ordem
- 01.10.10. Nível de terceira ordem
- 01.10.10. 10 Nível de quarta ordem

Além dos tópicos, os usuários podem alterar e incluir as perguntas que serão utilizadas durante a avaliação. Para fazer essas alterações, o usuário deve utilizar, a partir do menu principal mostrado na Figura 4.9, a opção **Informar Perguntas**.

Ao clicar sobre o botão **Informar Perguntas**, o usuário tem acesso à tela **Inclusão de Perguntas do *Check-List***, conforme mostrado na Figura 4.15. Para incluir uma nova

pergunta, o primeiro passo é escolher o tópico ao qual a pergunta pertence. Após essa escolha, o usuário deve digitar o texto da pergunta que será mostrado ao usuário durante a avaliação.

Figura 4.15 – Tela de Cadastro de Perguntas



Conforme mostrado na Figura 4.15, após a digitação do texto da pergunta, o usuário pode colocar uma observação sobre a pergunta em questão. Esse item é opcional, mas pode ajudar na inclusão informações importantes a serem consideradas durante a avaliação.

No campo **Crítica**, o usuário deve digitar o texto que será mostrado quando a pergunta em questão não receber uma avaliação positiva na avaliação, que seriam as notas um e dois. Da mesma forma que no caso dos tópicos, o usuário deve decidir se a pergunta estará ativa ou não durante as avaliações.

4.4.3 REGISTRANDO REFERÊNCIAS

O software desenvolvido pode se transformar no referencial sobre segurança da informação da organização. Para isso, é importante que o software permita a inclusão / registro de endereços na internet que tratem do tema segurança da informação. Para fazer isso, o usuário deve utilizar, a partir do menu principal mostrado na Figura 4.9, a opção **Referências**.

Ao clicar sobre o botão **Referências**, o usuário tem acesso à tela **Referências para Pesquisa**, conforme mostrado na Figura 4.16. Nessa tela, o usuário pode consultar os endereços já cadastrados e, adicionalmente, incluir novos endereços. Para incluir uma nova referência, o usuário deve clicar sobre o botão **Nova**. Após isso, basta informar o nome do *site* e o endereço de acesso. Quando o usuário desejar visitar o *site* basta pressionar o botão **Ir**.

Figura 4.16 – Tela de Cadastro de Referências

Com as referências cadastradas, o usuário terá um acesso rápido a estes endereços de internet, sempre que desejar obter alguma notícia, artigo ou qualquer outro assunto relacionado ao tema Segurança da Informação.

4.4.4 CONSIDERAÇÕES DA IMPLEMENTAÇÃO

Foram utilizadas as facilidades do Interbase, ao que se refere na utilização de *TRIGGERS* e *GENERATORS*, o que facilita na geração dos números auto-incremento. Para a criação do banco de dados, tabelas, índices, foram todos gerados a partir do Interbase Interactive SQL, uma das ferramentas que são instaladas juntamente com a instalação do Banco de Dados Interbase.

No Anexo B, deste trabalho é disponibilizado para consulta, parte do código para gravar uma referência, pois foi considerado como modelo padrão de desenvolvimento para o restante das classes geradas. As implementações das classes estão separadas das implementações das interfaces, o que dá uma ordenação da disposição das informações do, protótipo, gerando um código limpo, pequeno e fácil para gerar manutenção. Os relatórios foram gerados todos através de componentes padrões do Delphi 5, não necessitando de nenhuma atualização para poderem ser gerados.

5 CONCLUSÕES

Para proteger a informação de diversos tipos de ameaças, é necessário que exista a cultura de segurança da informação, para que a continuidade dos negócios esteja garantida, minimizando assim, os danos aos negócios e maximizando o retorno dos investimentos e as oportunidades de negócio.

Sendo assim é possível afirmar que as informações que estão disponibilizadas para pessoas não autorizadas podem gerar danos e prejuízos a organização. É importante que esta conscientização seja discutida dentro da organização bem como pelos gerentes que fazem parte dela, buscando constantemente a segurança dos dados e informações em suas organizações.

Acessos às redes não podem ser controlados totalmente, pois a possibilidade de violação existe e ocorre quando menos se espera, sendo as soluções de segurança as únicas que podem servir como base para a solução.

Um dos objetivos da norma NBR ISO/IEC 17799, é garantir que a integridade, a disponibilidade, e a confiabilidade dos recursos incorporados à informação, estejam presentes. Os controles essenciais, bem como as boas maneiras, também são tratados pela norma, os quais precisam ser separados para que o *check-list* fique consistente. O mesmo, que se encontra no Anexo A, foi gerado a partir da leitura detalhada da norma, com apoio de livros e artigos para consultas de dados técnicos. O resultado desta leitura gerou uma listagem de no total de cento e setenta e cinco tópicos e quinhentos e setenta e quatro perguntas, todos dando ênfase sobre a segurança da informação. Este *check-list* se encontra inserido no Banco de Dados gerado para o protótipo, para ser utilizado em avaliações prontamente.

Realizando-se uma análise do presente trabalho, observa-se que o objetivo principal foi atingido, uma vez que o software desenvolvido auxilia na avaliação do grau de adequação de uma empresa à norma NBR ISO/IEC 17799. Apesar de não ter sido utilizado em situações reais (em empresas), o software forneceu os resultados desejados nas simulações realizadas.

O software permite que sejam incluídos novos tópicos e perguntas, o que permite adequá-lo, rapidamente, às mudanças da norma ou da empresa. Adicionalmente, o software quantifica, através das notas estabelecidas pelo avaliador, o grau de conformidade da empresa em relação a cada tópico da norma.

Ao concluir uma avaliação, o usuário pode imprimir um relatório apontando críticas sobre a situação da empresa frente a cada item da norma. É a partir desse relatório é que a empresa pode estabelecer as estratégias e ações a serem implementadas para melhorar o grau de adequação com relação à norma NBR ISO/IEC 17799.

Trabalhos que são fundamentados sobre normas de padronização, são considerados às vezes, como não importantes para utilização futura. Mas foi comprovado com este trabalho que o critério segurança é importante, e que organizações que não estão com suas informações bem resguardadas, correm sérios riscos de ver perder parte de suas informações, ou senão todo, a qualquer hora. E ainda aquelas que ignorarem estas informações, ficarão ultrapassadas perante as outras organizações que investem nesta área.

Vale lembrar, que não somente normas de segurança são importantes, outras normas também possuem sua grande importância, isto pode ser comprovado pela procura dessa padronização, e pelas organizações que já adotaram estes padrões.

O produto final gerado, a partir deste trabalho, está pronto para ser utilizado em um processo de avaliação da segurança da informação de uma organização. Pode-se dizer que este trabalho é um dos primeiros trabalhos deste nível sobre a norma NBR ISO/IEC 17799, e já está conceitualmente adaptado para a realidade, ao que se refere a segurança nas organizações em geral.

5.1 EXTENSÕES

As possíveis extensões que podem ser feitas a partir desse trabalho estão enumeradas a seguir:

a) Integrar o software desenvolvido com softwares de outros TCC’s relacionados à qualidade de software, como também soluções de redes e outras ferramentas que possam ser empregadas;

b) Disponibilizar a ferramenta na WEB, para que a avaliação possa ser feita via internet, de forma que pessoas em locais diferentes da empresa possam realizar a avaliação ao mesmo tempo;

c) Incrementar a geração de relatórios gráficos, onde se possa visualizar, rapidamente, o desempenho da empresa nos diferentes tópicos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERNAZ, Valéria Almeida. **Introdução da british standard – BS7799**, Brasília, set. 2001. Disponível em: <http://www.iso17799.hpg.com.br/artigos.htm>. Acesso em: 20 abr. 2002.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

BASTOS, Alberto. **Os novos rumos da gestão de segurança com as normas ISO 17799 e BS 7799**, [S.l], ago. 2002. Disponível em: <http://www.modulo.com.br>. Acesso em: 16 ago. 2002.

BRODERICK, Stuart. **Proteção de informações -** Por que é importante? (Parte II), [S.l.], 2002. Disponível em: <http://www.symantec.com/region/br/enterprisesecurity/content/content_vul6.html.> Acesso em: 15 set. 2002.

CASANAS, A. D.; MACHADO, C. S. **O impacto da implementação da norma NBR SO/IEC 17799**, Florianópolis, abr. 2001. Disponível em: <http://www.iso17799.hpg.com.br/artigos.htm>. Acesso em: 20 abr. 2002.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação.** Rio de Janeiro: Axcel, 2000. 218 p.

FURLAN, Davi. **Modelagem de objetos através da UML** – the unified modeling language. São Paulo: Makron Books, 1998. 329 p.

LISCHNER, Ray. **Delphi** : o guia essencial. Tradução Daniel Vieira. Rio de Janeiro: Campus, 2000. 605 p.

MACHADO, Cesar S. **Histórico**, Florianópolis, abr. 2002. Disponível em: <http://www.iso17799.hpg.ig.com.br/hist.htm>. Acesso em: 20 abr. 2002.

MONTENEGRO, Fernando; PACHECO, Roberto. **Orientação a objetos em C++**. Rio de

Janeiro: Ciência Moderna, 1994. 394 p.

NASCIMENTO, Neide L. T. **ISO 17799**, Brasília, set. 2001. Disponível em: <http://www.iso17799.hpg.com.br/artigos.htm>. Acesso em: 20 abr. 2002.

OLIVEIRA, Adeliza; MEDEIROS, Marcelo. **Delphi 5** : conceitos básicos, Florianópolis: Advanced, 2000. 224 p.

QUATRANI, Terry. **Modelagem visual com rational rose 2000 e UML**. Tradução Savannah Hartmann. Rio de Janeiro: Ciência Moderna, 2001. 206 p.

RAMOS, Fabio F. **NBR ISO/IEC 17799:** benefícios e aplicações, [S.l], mar. 2002. Disponível em: <http://www.iso17799.hpg.com.br/artigos.htm>. Acesso em: 20 abr. 2002.

SOUZA, Mauro J. *et al.* **ISO 17799**, [S.l], [2001?]. Disponível em: <http://www.e-trust.com.br/iso>. Acesso em: 20 abr. 2002.

TEDESCHI, Fabio. **Segurança em tecnologia da informação**, [S.l.], [2001?]. Disponível em: <http://www.portalsi.com.br/artigos>. Acesso em: 20 abr. 2002.

VALLEY, Scotts. **Borland Interbase:** Getting Started, 1995.

VANGELOTTI, Ivan M. B. **Segurança no ambiente de produção e desenvolvimento**, [S.l.], 2002. Disponível em: <http://www.modulo.com.br>. Acesso em: 16 ago. 2002.

ANEXO A: PROPOSTA DO MODELO DE AVALIAÇÃO (TÓPICOS DA NBR ISO/IEC 17799)

1 POLÍTICA DE SEGURANÇA

1 - A direção possui uma política formal e clara de comprometimento com a segurança da informação?

Obs.: Verificar se a direção possui uma orientação e apoio para segurança da informação.

2 - Existe um documento atualizado que descreva a política de segurança de informações?

3 - A política de segurança é adequadamente divulgada para todos na organização?

4 - A política de segurança está acessível a todos os funcionários?

5 - A política de segurança é facilmente compreendida por todos os funcionários?

6 - Foi definido um responsável pela manutenção e análise crítica da política de segurança?

7 - Foi definido e formalizado um processo de análise crítica da política de segurança? (identificar qualquer mudança que venha a modificar a avaliação de risco original)

8 - Foi formalizado um processo de análise crítica para se avaliar a efetividade da política de segurança? (tipo, volume e impacto dos incidentes de segurança registrados).

9- Foi formalizado um processo de análise crítica para se avaliar o custo e o impacto dos controles na eficiência do negócio?

10 - Foi formalizado um processo de análise crítica para se avaliar os efeitos das mudanças na tecnologia?

11 - Foi definido um processo para a identificação dos agentes e causas de uma violação da política de segurança?

12 - Quando ocorre uma violação da política de segurança, são tomadas medidas para identificar os agentes e causas, corrigindo as vulnerabilidades e punir os infratores?

13 - Existe a análise de medidas de segurança passíveis de implantação em face das vulnerabilidades flagradas?

Obs.: É necessário fazer uma análise de custo-benefício antes de tomar qualquer medida.

14 - Existe a publicação, comunicação e treinamentos sobre segurança para os funcionários, com reciclagens periódicas?

Obs.: No treinamento pode ser aplicado procedimentos de segurança pessoal para reduzir ou evitar erro humano, mau uso de recursos computacionais, fraude ou roubo.

15 - Os efeitos das mudanças na tecnologia são analisados periodicamente?

16 - Os recursos computacionais estão classificados de acordo com seu grau de confidencialidade, prioridade e importância para a organização?

Obs.: Recursos tais como *hardware*, *software*, dados, documentação, etc.

17 - Os recursos computacionais são administrados por um responsável designado?

1.1 ORIENTAÇÕES MÍNIMAS QUE COMPÕE A POLÍTICA DE SEGURANÇA

1 - A política contém uma definição de política de segurança?

2 - Existe um resumo das metas relacionadas a segurança da informação?

3 - Foi incluído o escopo da política de segurança?

4 - É ressaltada a importância da segurança como um mecanismo que habilita o compartilhamento da informação?

5 - Contém a declaração de comprometimento da alta direção, apoiando as metas e princípios da segurança da informação?

6 - Existe uma breve explanação das políticas, princípios, padrões e requisitos de conformidade importantes para a organização?

7 - Foram definidas responsabilidades gerais e específicas na gestão da segurança da informação?

8 - A política de segurança faz referências a outros documentos mais detalhados que a complementam?

2 SEGURANÇA ORGANIZACIONAL

2.1 INFRA-ESTRUTURA DA SEGURANÇA DA INFORMAÇÃO

1 - Existem fóruns apropriados de gerenciamento com liderança da direção?

Obs.: São estabelecidos para aprovar a política de segurança da informação.

2 - É utilizado de fonte especializada em segurança da informação dentro da organização?

3 - A organização faz contatos com especialistas de segurança externos?

Obs.: Mantendo este contato a organização vai se encontrar mais atualizada com tendência do mercado, com monitoração de normas e métodos de avaliação, recebendo apoio durante os incidentes de segurança.

4 - Existe enfoque multidisciplinar na segurança da informação com envolvimento de todas as pessoas que participam de alguma forma no processo de segurança?

5 - Existe enfoque multidisciplinar na segurança da informação com cooperação de todas as pessoas que participam de alguma forma no processo de segurança?

6 - Existe enfoque multidisciplinar na segurança da informação com colaboração de todas as pessoas que participam de alguma forma no processo de segurança?

7 - As responsabilidades pela proteção de cada ativo e pelo cumprimento do processo de segurança específico, estão claramente definidas?

8 - Os ativos físicos e de informação bem como os processo de segurança (plano de continuidade de negócio) estão sob responsabilidade de pessoa designada em cada local?

9 - Processos de segurança que envolvem a implementação bem como os vários ativos estão associados a cada sistema?

10 - Processos de segurança que envolvem a implementação bem como os vários ativos estão claramente definidos?

11 - O responsável por cada ativo de segurança está de acordo com esta responsabilidade?

12 - O responsável por cada processo de segurança está de acordo com esta responsabilidade?

13 - Os detalhes da responsabilidade dos ativos estão documentados?

14 - Os detalhes da responsabilidade dos processos estão documentados?

2.1.1 ATRIBUIÇÃO DAS RESPONSABILIDADES EM SEGURANÇA DA INFORMAÇÃO

1 - Os níveis de autorização estão claramente definidos e documentados?

2.1.2 PROCESSO DE AUTORIZAÇÃO PARA AS INSTALAÇÕES DE PROCESSAMENTO DA INFORMAÇÃO

1 - Novos recursos de processamento da informação possuem um processo de gestão de autorização?

2 - *Hardwares* são verificados para garantir que são compatíveis com outros componentes do sistema?

3 - *Softwares* são verificados para garantir que são compatíveis com outros componentes do sistema?

4 - O uso de recursos pessoais de processamento de informação no ambiente de trabalho é avaliado e autorizado?

Obs.: Quando se trata de rede de computadores isto se faz necessário.

2.1.3 COOPERAÇÃO ENTRE ORGANIZAÇÕES

1 - São mantidos contatos apropriados com autoridades legais para garantir apoio especializado caso ocorra os incidentes de segurança?

2 - São mantidos contatos apropriados com organismos reguladores para garantir apoio especializado caso ocorra os incidentes de segurança?

3 - São mantidos contatos apropriados com provedores de serviço de informação para garantir apoio especializado caso ocorra os incidentes de segurança?

4 - São mantidos contatos apropriados com operadores de telecomunicações para garantir apoio especializado caso ocorra os incidentes de segurança?

5 - Trocas de informações de segurança são restritas para garantir informações confidenciais?

2.2 SEGURANÇA NO ACESSO DE PRESTADORES DE SERVIÇOS

1 - O acesso de prestadores de serviços aos recursos de processamento da informação da organização é controlado?

2.2.1 TIPO DE ACESSO

1 - O acesso físico é restrito por pessoas autorizadas?

2 - O acesso lógico é restrito por pessoas autorizadas?

2.2.2 CONTRATADOS PARA SERVIÇOS INTERNOS

1 - Existem muitos prestadores de serviços contratados dentro da organização?

Obs.: Muitos prestadores podem aumentar a fragilidade da informação.

2 - Se existir a necessidade de acesso de prestadores de serviços aos recursos de processamento da informação, é feita uma avaliação de riscos, para determinar implicações e controles necessários?

3 - O controle de acesso dos prestadores de serviço é definido através de contrato assinado?

2.3 TERCEIRIZAÇÃO

1 - Os requisitos de segurança com prestadores de serviços terceirizados para gerenciamento e controle de sistemas de informação estão descritos por contrato?

2 - Os requisitos de segurança com prestadores de serviços terceirizados para gerenciamento e controle de redes de computadores estão descritos por contrato?

3 - Os requisitos de segurança com prestadores de serviços terceirizados para gerenciamento e controle de e/ou estações de trabalho estão descritos por contrato?

3 CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO

3.1 CONTABILIZAÇÃO DOS ATIVOS

1 - Os principais ativos de informação são inventariados?

2 - Os principais ativos de informação possuem um proprietário responsável?

Obs.: Entenda-se por ativos de informação: base de dados e arquivos, documentação de sistemas, manuais de usuário, informações armazenadas. Ativos de *software*: aplicativos ferramentas de desenvolvimento e utilitários. Ativos físicos equipamentos (processadores, monitores) comunicação (fax, secretária eletrônica), mídia magnética (fitas e discos), mobília acomodações.

3 - A classificação de segurança está em conformidade?

4 - A classificação de segurança está documentada?

5 - A responsabilidade pela prestação de contas está com o proprietário nomeado do ativo?

3.2 CLASSIFICAÇÃO DA INFORMAÇÃO

3.2.1 RECOMENDAÇÕES PARA CLASSIFICAÇÃO

1 - A informação é classificada conforme as necessidades dos negócios para compartilhar ou restringir as informações?

2 - Os controles são classificados conforme as necessidades dos negócios para compartilhar ou restringir as informações?

3 - São verificados os impactos no negócio quando se utiliza o compartilhamento ou restrição das informações?

Obs.: Se refere aos acessos não autorizados ou danos à informação.

4 - Informações e resultados de sistema que processam dados são rotulados conforme seu valor e sua sensibilidade para a organização?

5 - A quantidade de categorias de classificação estão esquematizados de forma que seu uso seja fácil para classificar os ativos?

6 - A definição da classificação de um item de informação está sob responsabilidade do autor ou com o proprietário responsável pela informação?

3.2.2 RÓTULOS E TRATAMENTO DA INFORMAÇÃO

1 - Relatórios, telas, mídias magnéticas (fitas, discos, CD's, cassetes) considerados como informações sensíveis ou críticas possuem rótulos de classificação?

4 SEGURANÇA EM PESSOAS

4.1 SEGURANÇA NA DEFINIÇÃO E NOS RECURSOS DE TRABALHO

4.1.1 INCLUINDO SEGURANÇA NAS RESPONSABILIDADES DO TRABALHO

1 - As responsabilidades de segurança são atribuídos na fase de recrutamento?

2 - Estas responsabilidades estão incluídas em contrato?

3 - Existe o monitoramento do trabalho durante a vigência de cada contrato de trabalho?

4.1.2 SELEÇÃO E POLÍTICA DE PESSOAL

1 - No momento da seleção do candidato, existem verificações de controle da equipe permanente?

2 - Possui-se a disponibilidade de referências de caráter satisfatório?

Obs.: Referência profissional e pessoal.

3 - As informações do *curriculum vitae* do candidato são verificadas?

4 - As qualificações acadêmicas e profissionais são confirmados?

5 - É feita a verificação da identidade?

Obs.: Passaporte ou documento similar.

6 - Para aquelas pessoas que terão acesso a informações sensíveis, tais como informações financeiras, é verificado se o candidato possui condições para manuseá-la?

7 - Para posições com níveis consideráveis de autoridade, o procedimento de verificação de idoneidade é feito periodicamente?

8 - Funcionários novos e inexperientes que lidam com informações sensíveis são revistos e aprovados pelo membro mais experiente da equipe?

9 - Problemas pessoais do funcionário são avaliados?

4.1.3 ACORDOS DE CONFIDENCIALIDADE

1 - É exigida assinatura dos colaboradores ou prestadores de serviços antes de ter acesso a instalações de processamento da informação?

2 - Acordos de confidencialidade são revisados quando existem modificações nos termos de contratação?

4.1.4 TERMOS E CONDIÇÕES DE TRABALHO

1 - Existem termos e condições de trabalho que determinem as responsabilidades dos funcionários pela segurança da informação?

2 - Quando existe o termino do contrato de trabalho a responsabilidade continua sendo aplicada por um período de tempo definido?

3 - Caso ocorra desrespeito ao acordo estão incluídas ações no contrato?

4 - Leis de direitos autorais ou de proteção de dados, são esclarecidos e incluídos dentro dos termos e condições de trabalho?

5 - Nos caso de execução de atividades fora das dependências de trabalho, em casa, por exemplo, as responsabilidades continuam sendo aplicadas?

6 - Responsabilidades pela classificação e gestão dos dados do empregador também são incluídas no contrato?

4.2 TREINAMENTO DOS USUÁRIOS

1 - Os usuários são treinados para que usem corretamente as instalações de processamento da informação?

4.3 RESPONDENDO AOS INCIDENTES DE SEGURANÇA E AO MAU FUNCIONAMENTO

4.3.1 NOTIFICAÇÃO DOS INCIDENTES DE SEGURANÇA

1 - Quando ocorre algum incidente de segurança, ela é reportada em canais apropriados para a direção, o mais rápido possível?

2 - Procedimentos de resposta ao incidente são estabelecidos?

3 - Funcionários e prestadores de serviços são instruídos a relatar incidentes de segurança o mais rápido possível?

4 - Ações de *feedback* são tomadas para ter certeza que incidentes foram tratados e encerrados?

4.3.2 NOTIFICANDO FALHAS NA SEGURANÇA

1 - Os usuários dos serviços de informação são instruídos a registrar e notificar quaisquer fragilidades ou ameaças, suspeitas ou ocorridas, na segurança de sistemas ou serviços?

2 - Assuntos sobre falhas são notificados o mais rápido possível para seus superiores ou para os provedores?

3 - Os usuários são instruídos para não tentar averiguar a fragilidade por si próprios?

Obs.: Pode ser interpretado como uso impróprio dos sistemas.

4.3.3 NOTIFICANDO MAU FUNCIONAMENTO DE *SOFTWARE*

1 - São estabelecidos procedimentos para notificar mau funcionamento do *software*?

2 - Sintomas de problemas, ou mensagens apresentadas, são anotadas?

3 - Quando ocorre detecção de algum problema, o computador é isolado incluindo a desconexão da rede e o isolamento de seus disquetes, ou qualquer, componente capaz de transferir informações?

4 - Problemas com mau funcionamento do *software* é notificado imediatamente ao gestor da segurança da informação?

5 - Usuários são notificados para a não remoção do *software*, a menos que seja autorizado, caso mau funcionamento do mesmo?

6 - Existe uma equipe adequadamente treinada para tratar da remoção e recuperação do *software* suspeito?

4.3.4 APRENDENDO COM OS INCIDENTES

1 - Existem mecanismos para permitir que tipos, quantidades e custos dos incidentes e dos maus funcionamentos sejam quantificados e monitorados?

4.3.5 PROCESSO DISCIPLINAR

1 - Funcionário que viola os políticas e procedimentos de segurança, passa por um processo disciplinar?

5 SEGURANÇA FÍSICA E DO AMBIENTE

5.1 ÁREAS DE SEGURANÇA

5.1.1 PERÍMETRO DA SEGURANÇA FÍSICA

1 - As organizações usam perímetro de segurança para proteger as áreas que contém os recursos e instalações de processamento de dados?

2 - O perímetro de segurança está claramente definido?

3 - O perímetro de um prédio ou local que contenha recursos de processamento de dados é fisicamente consistente (sem brechas onde pode ocorrer uma invasão)?

4 - As paredes possuem construção sólida e as portas externas são protegidas de forma apropriada contra acessos não autorizados?

Obs.: exemplo de segurança como travas, alarmes, grades etc.

5 - Existe uma recepção ou outro meio de controle alternativo de acesso ao local ou prédio?

6 - Somente pessoal autorizado possui acesso ao local ou prédio?

7 - Existem barreiras físicas do piso ao teto contra acessos não autorizados ou contaminação ambiental como fogo e inundações?

8 - As portas de incêndio no perímetro de segurança possuem sensores de alarme com molas para fechamento automático?

5.1.2 CONTROLES DE ENTRADA FÍSICA

1 - Aos visitantes que possuem acesso as áreas de segurança tem registrado a data e hora de sua entrada e saída?

2 - Os visitantes possuem acesso apenas à área específicas?

3 - Os acessos a áreas físicas seguem instruções baseadas nos requisitos de segurança e procedimentos de emergência própria da área considerada?

4 - Informações sensíveis, instalações e recursos de processamento de informações é controlado e restrito apenas para pessoal autorizado?

5 - São utilizados controles de autenticação para validar qualquer acesso a informações sensíveis, instalações e recursos de processamento de informações?

6 - Os funcionários que acessam as instalações e recursos de processamento de informações, possuem sua identificação visível?

7 - Os funcionários são incentivados a informar para a segurança sobre a presença de qualquer pessoa não identificada, ou estranho não acompanhado, nas instalações e recursos de processamento de informações?

8 - Os direitos de acesso às áreas de segurança são regularmente revistos e atualizados?

5.1.3 SEGURANÇA EM ESCRITÓRIOS, SALAS E INSTALAÇÕES DE PROCESSAMENTO

1 - Na seleção do projeto de uma área de segurança foi considerado possibilidades de danos causados pelo meio ambiente (fogo, inundações, por exemplo)?

2 - As instalações críticas estão localizados de forma a evitar o acesso público?

3 - O prédio é sem obstruções ao seu acesso, com indicações mínimas do seu propósito?

4 - Os serviços de suporte e equipamentos são instalados de tal forma que não comprometa a informação?

Obs.: Suporte e equipamento como fotocopiadoras e máquinas de fax.

5 - As portas e janelas das instalações do processamento são mantidas fechadas?

6 - Sistema de detecção de intrusos é instalado por profissionais especializados e testados regularmente?

7 - Áreas não ocupadas como sala de computadores ou salas de comunicação possuem um sistema de alarme ligado permanentemente?

8 - Áreas de processamento da informação gerenciada pela organização é fisicamente separada daquela gerenciadas por prestadores de serviço?

9 - Arquivos e listas de telefones internos que identificam os locais de processamento estão acessíveis ao público em geral?

10 - Materiais combustíveis são guardados de forma segura e distante da área de segurança?

11 - Equipamentos de contingência e meios magnéticos de reserva (*backup*) são guardados com distância segura da instalação principal?

Obs.: Esta medida é importante, caso desastres ocorram na instalação principal.

5.1.4 TRABALHANDO EM ÁREAS DE SEGURANÇA

1 - Funcionários da organização conhecem a área de segurança somente quando existe necessidade?

2- Existe supervisão nas áreas de segurança?

Obs.: Por segurança e para evitar atividades maliciosas.

3 - Áreas de segurança desocupadas são mantidas fechadas e verificadas periodicamente?

4 - Serviços de suporte terceirizado possuem acesso restrito as instalações a áreas de segurança de processamento de informações?

5 - O acesso de serviços de suporte terceirizado é autorizado e monitorado?

6 - O uso de equipamentos de gravação é restrito nas áreas de segurança?

Obs.: Equipamentos como máquina fotográfica, vídeo ou áudio?

5.1.5 ISOLAMENTO DAS ÁREAS DE EXPEDIÇÃO E CARGA

1 - Áreas de expedição e de carregamento é isolada das instalações de processamento da informação?

2 - Suporte de carga e descarga externa ao prédio é restrito ao pessoal identificado e autorizado?

3 - A área foi projetada para que o pessoal que descarrega os suprimentos não tenha acesso a outras partes do prédio?

4 - As portas externas estão protegidas quando as internas estão abertas?

5 - A entrada de material é inspecionado?

6 - O material recebido é registrado quando da sua recepção?

5.2 SEGURANÇA DOS EQUIPAMENTOS

5.2.1 INSTALAÇÃO E PROTEÇÃO DE EQUIPAMENTOS

1 - Os equipamentos são instalados, de forma que os acessos sejam reduzidos na área de trabalho?

2 - Instalações de processamento e armazenamento de informações consideradas sensíveis estão posicionadas a reduzir riscos de espionagem?

3 - Itens que necessitam de proteção especial estão isolados daqueles itens que necessitam de proteção geral?

4 - São adotados controles contra ameaças potenciais?

Obs.: Ameaças potenciais tais como roubo, fogo, explosivos, água, poeira entre outros.

5 - A organização possui alguma política específica para alimentação, bebida e fumo nas proximidades onde ocorre o processamento da informação?

6 - São adotados métodos na organização de proteção especial para equipamentos que se encontram em ambiente industrial?

Obs.: Capas para teclados.

5.2.2 FORNECIMENTO DE ENERGIA

1 - Existe alimentação múltipla de energia para evitar falha em um ponto do fornecimento elétrico?

2 - São utilizados *no-break´s Uninterruptable Power Supply* (UPS)?

3 - A organização possui gerador de reserva?

4 - Os *no-break´s* passam por revisão?

5 - O gerador de energia passa por revisão?

6 - Existe fornecimento adequado de óleo caso o gerador precise ser utilizado por mais tempo?

7 - Interruptores elétricos estão localizados próximos às saídas de emergência?

8 - A iluminação de emergência está disponível caso ocorra falha na fonte elétrica primária?

9 - Existe proteção contra raios e relâmpagos?

5.2.3 SEGURANÇA DO CABEAMENTO

1 - Linha elétricas e de telecomunicação estão submetidas à proteção alternativa adequada?

Obs.: Linhas subterrâneas.

2 - Os cabos de rede estão protegidos contra interrupções não autorizadas?

3 - Cabos elétricos estão separados dos cabos de comunicação?

Obs.: Para evitar interferências.

4 - Existe na organização a opção de utilização de rotas e meios alternativos?

5 - Foi feita uma varredura inicial para identificar dispositivos não autorizados conectados aos cabos?

5.2.4 MANUTENÇÃO DE EQUIPAMENTOS

1 - Os equipamentos possuem manutenção adequada conforme fabricante?

2 - Os reparos e serviços são executados por pessoal autorizado?

3 - As falhas e manutenções são registradas?

4 - Existe algum controle para equipamentos que necessitem manutenção fora da instalação física?

5.2.5 SEGURANÇA DE EQUIPAMENTOS FORA DAS INSTALAÇÕES

1 - Qualquer tipo de processamento da informação fora da organização é autorizado pela direção?

2 - Os equipamentos são deixados desprotegidos em áreas públicas?

3 - Computadores portáteis são carregados na mão e disfarçados em viagens?

4 - As instruções de fabricantes de equipamentos são respeitadas?

5 - Existe uma cobertura de seguro para equipamentos que são levados fora das instalações da organização?

5.2.6 REUTILIZAÇÃO E ALIENAÇÃO SEGURA DE EQUIPAMENTOS

1 - Equipamentos que são reutilizados ou alienados possuem sua informação destruída ou sobrescrita de forma segura?

5.3 CONTROLES GERAIS

1 - Existe uma política de mesa e tela limpa?

2 - Papéis e mídias são guardadas quando não está sendo feita da sua utilização?

3 - Computadores pessoais, terminais de computador são desligados quando não assistidos?

4 - Computadores pessoais, terminais de computadores possuem senha de acesso ou algum tipo de controle quando não estão em uso?

5 - As máquinas fax e telex recepção de envio de correspondências são protegidos?

6 - As copiadoras são travadas quando não estão sendo usadas?

7 - As informações impressas são imediatamente retiradas da impressora?

5.3.1 REMOÇÃO DE PROPRIEDADE

1 - Inspeção pontuais são realizadas para detectar remoção não autorizada de propriedade?

Obs.: São considerados propriedades os equipamentos, informações ou *software*.

2 - As pessoas sabem que inspeções pontuais são realizadas?

6 GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÃO

6.1 PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

6.1.1 DOCUMENTAÇÃO DOS PROCEDIMENTOS DE OPERAÇÃO

1 - Procedimentos operacionais são tratados como documentos formais?

2 - As mudanças são autorizadas pela direção?

6.1.2 CONTROLE DE MUDANÇAS OPERACIONAIS

1 - Modificações nos sistemas e recursos de processamento da informação são controlados?

2 - É utilizada uma formalização dos procedimentos e das responsabilidades nas mudanças de equipamentos, *software* ou procedimentos?

3 - Programas em produção possuem um controle específico de modificações?

4 - As modificações de programas em produção são registrados?

6.1.3 PROCEDIMENTOS PARA O GERENCIAMENTO DE INCIDENTES

1 - Foram definidos responsabilidades e procedimentos para gerenciamento de incidentes de segurança?

2 - São feitas auditorias e levantamento de evidencias similares para problemas internos?

3 - As tomadas de ações para recuperação de violações de segurança e falhas de sistema são cuidadosas e formalmente controladas?

6.1.4 SEGREGAÇÃO DE FUNÇÕES

1 - É considerada a separação da administração da administração ou execução de certas funções?

2 - Quando ocorre segregação de funções é verificada que as atividades requeiram cumplicidade para executar uma fraude?

6.1.5 SEPARAÇÃO DOS AMBIENTES DE DESENVOLVIMENTO E DE PRODUÇÃO

1 - Os ambientes de desenvolvimento, teste e produção são separadas?

2 - *Software* que está em desenvolvimento está separado do *software* em produção?

3 - Compiladores, editores e outros programas utilitários são acessíveis para o ambiente de produção?

4 - O processo de acesso ao ambiente de produção é diferente do acesso de desenvolvimento?

5 - Usuários são incentivados para usar senhas diferentes conforme ambiente?

6 - Pessoal de desenvolvimento recebem senha especial no acesso ao ambiente de produção?

7 - Quando o pessoal do desenvolvimento utiliza senha na produção, esta senha é alterada logo após o uso?

6.2 PLANEJAMENTO E ACEITAÇÃO DOS SISTEMAS

1 - Demandas de capacidade e projeção de cargas são feitas para garantir a capacidade adequada de processamento e armazenamento?

2 - Os computadores de grande porte são verificados quanto a sua capacidade?

3 - Os problemas de capacidade são identificados e evitados?

6.2.1 ACEITAÇÃO DE SISTEMAS

1 - São estabelecidos critérios de aceitação para novos sistemas?

2 - Atualizações e novas versões são testados antes da sua aceitação?

3 - Os requisitos para aceitação de novos sistemas, estão claramente definidos, acordados, documentados e testados?

4 - Para novos desenvolvimentos os usuários e funções de operação são consultados?

6.3 PROTEÇÃO CONTRA *SOFTWARE* MALICIOSO

6.3.1 CONTROLES CONTRA *SOFTWARE* MALICIOSO

1 - A organização possui controle para a detecção e prevenção de *software* malicioso?

2 - Os usuários estão conscientizados sobre os malefícios dos *softwares* maliciosos?

3 - Existe uma política formal exigindo conformidade com as licenças de *software* e proibindo o uso de *software* não autorizado?

4 - São instalados e atualizados *software* para detecção e remoção de vírus dos computadores e meios magnéticos?

5 - São feitas analises críticas regulares de *software* que suportam processos críticos do negócio?

6 - São feitas analises críticas regulares de dados dos sistemas que suportam processos críticos do negócio?

7 - Antes de serem utilizados, os arquivos são verificados se estão livres de vírus?

8 - Caso um vírus venha a atacar, existem procedimentos para salvar e recuperar dados e *software*?

9 - Informações e alertas referentes a *software* malicioso são averiguados quanto a sua veracidade?

10 - Os funcionários estão conscientizados a lidar com boatos referente a *software* malicioso e as conseqüências desses?

6.4 HOUSEKEEPING

6.4.1 CÓPIAS DE SEGURANÇA

1 - Cópias de segurança dos dados e *software* são feitas regularmente?

2 - Estão disponíveis recursos e instalações alternativas caso venha ocorrer algum problema?

3 - Os *backup´s* são testados, para verificar se atendem aos requisitos dos planos de continuidade de negócios?

4 - São mantidos um nível mínimo de cópias de segurança?

5 - As cópias são mantidas em local seguro da instalação principal?

6.4.2 REGISTROS DE OPERAÇÃO

1 - É mantido registro das atividades do pessoal de operação?

2 - As atividades dos operadores são submetidos à checagem regular e independente?

6.4.3 REGISTRO DE FALHAS

1 - As falhas são relatadas e ações são tomadas?

2 - As falhas informadas pelos usuários relativa ao processamento da informação são registradas?

3 - As falhas resolvidas, passam por analise crítica para confirmar a sua solução?

4 - As soluções tomadas perante a falha, são analisadas para garantir que não afetaram os controles e tenham sido devidamente autorizadas?

6.5 GERENCIAMENTO DA REDE

6.5.1 CONTROLES DA REDE

1 - É utilizado um conjunto de controles para obter e preservar a segurança nas redes de computadores?

2 - A responsabilidade operacional está segregada da operação dos computadores?

3 - São estabelecidos procedimentos e responsabilidades para gerenciamento de equipamentos remotos?

4 - São estabelecidos controles para a confidencialidade integridade dos dados que trafegam em rede pública?

5 - As atividade de gerenciamento são cuidadosamente coordenadas?

6.6 SEGURANÇA E TRATAMENTO DE MÍDIAS

6.6.1 GERENCIAMENTO DE MÍDIAS REMOVÍVEIS

1 - Os meios magnéticos reutilizáveis, quando não é mais utilizado o seu conteúdo é apagado?

2 - É requerida a autorização para remoção de mídias das instalações da organização?

3 - Quando é retirada da mídia da organização, é registrada sua saída?

4 - As mídias são guardadas em ambiente seguro?

5 - Existe documentação explicando os procedimentos e os níveis de autorização para gerenciamento de mídias?

6.6.2 DESCARTE DE MÍDIAS

1 - Mídias que possuem informações, sensíveis são guardados e descartadas de forma segura?

2 - O descarte de itens sensíveis é registrado?

6.6.3 PROCEDIMENTOS PARA TRATAMENTO DE INFORMAÇÃO

1 - A organização possui procedimentos estabelecidos para tratamento e armazenamento de informações?

2 - Os meios magnéticos possuem tratamento especial e são identificados?

3 - Existe a restrição de acesso para pessoal não identificado?

4 - Possui um registro formal dos destinatários que possuem acesso aos dados?

5 - Existe garantia da entrada dos dados, processamento e validação das saídas?

6 - As mídias são armazenadas conforme recomendação dos fabricantes?

7 - Os dados são mantidos e distribuídos no menor nível possível?

8 - As cópias de segurança são devidamente identificadas?

9 - É feita anáse das listas de distribuição e destinatários em intervalos regulares?

6.6.4 SEGURANÇA DA DOCUMENTAÇÃO DOS SISTEMAS

1 - A documentação dos sistemas são guardados de forma segura?

2 - Existe restrição de pessoas à documentação de sistemas?

3 - Precisa ter autorização do gestor da aplicação para ter acesso às documentações de sistemas?

4 - As documentações mantidas em rede pública são protegidas de forma apropriada?

6.7 TROCA DE INFORMAÇÕES E *SOFTWARE*

6.7.1 ACORDOS PARA A TROCA DE INFORMAÇÕES E *SOFTWARE*

1 - São formalizados acordos para distribuição de *software* entre organizações?

2 - É estabelecido o nível de sensibilidade das informações envolvidas no negócio?

6.7.2 SEGURANÇA DE MÍDIAS EM TRÂNSITO

1 - O transporte ou serviço de mensageiro é confiável?

2 - A embalagem utilizada para proteger o conteúdo está de acordo com as especificações dos fabricantes?

3 - Para proteção de informação crítica são utilizados controles especiais?

Obs.: Recipientes lacrados, entrega em mãos, entre outros.

6.7.3 SEGURANÇA DO COMÉRCIO ELETRÔNICO

1 - São aplicados controles para o comércio eletrônico, contra fraudes, violações, divulgação e modificação da informação?

2 - Acordos de comércio eletrônico são baseados em contrato formal?

6.7.4 SEGURANÇA DO CORREIO ELETRÔNICO

6.7.4.1 Riscos de Segurança

1 - São utilizados controles para a redução dos riscos no uso de correio eletrônico?

6.7.4.2 Política de uso do correio eletrônico

1 - A organização possui uma política clara para utilização do correio eletrônico?

6.7.5 SEGURANÇA DOS SISTEMAS ELETRÔNICOS DE ESCRITÓRIO

1 - Foram definidas políticas e diretrizes para controlar o negócio e os riscos de segurança?

6.7.6 SISTEMAS DISPONÍVEIS PUBLICAMENTE

1 - A integridade da informação divulgada eletronicamente é protegida?

2 - A publicação de uma informação passa por um processo de autorização?

3 - *Software* ou outras informações que necessitam de integridades e que são expostos em um sistema público são protegidos por mecanismos apropriados?

6.7.7 OUTRAS FORMAS DE TROCA DE INFORMAÇÕES

1 - É estabelecida uma política clara, com procedimentos na utilização de comunicação por voz, fax e vídeo?

7 CONTROLE DE ACESSO

7.1 REQUISITOS DO NEGÓCIO PARA CONTROLE DE ACESSO

7.1.1 POLÍTICA DE CONTROLE DE ACESSO

7.1.1.1 Requisitos do negócio e política

1 - Os requisitos do negócio controle de acessos estão definidos?

2 - Os requisitos do negócio controle de acessos estão documentados?

3 - As regras de acesso e direito para os usuários estão no documento da política de controle de acesso?

4 - Os usuários e provedores possuem um documento que possui os contrais de acesso e que satisfaçam os requisitos do negócio?

7.1.1.2 Regras de controle de acesso

1 - Existe diferenciação das regras de devem ser cumpridas daquelas regras opcionais ou condicionais?

2 - São feitas modificações de permissão de usuários do que aquela atribuída por um administrador?

7.2 GERENCIAMENTO DE ACESSOS DO USUÁRIO

7.2.1 REGISTRO DE USUÁRIO

1 - Existe na organização algum procedimento formal de registro e cancelamento de usuário para acessos aos sistemas de informação?

2 - Para acessos de informação multiusuário, são utilizados identificadores de usuário (ID) único?

3 - Existe a verificação se o usuário possui autorização do proprietário para utilização dos sistemas de informação ou serviço?

4 - Existe a verificação para saber se o nível concedido está adequado aos propósitos do negócio e consistente com a política de segurança?

5 - É feita entrega de documento escrito para os usuários sobre seus direitos de acesso?

6 - É cobrada assinatura dos usuários nos documentos de direitos de acesso?

7 - Existe a garantia de que o provedor não irá fornecer direito de acesso até que os procedimentos de autorização estejam concluídos?

8 - Existe um registro formal para saber quem são as pessoas que estão utilizando o serviço?

9 - Quando o usuário se desliga da organização seus acessos são cancelados imediatamente?

10 - Existe a verificação periódica de usuários e contas inativas?

11 - Existe garantia que as identificações de usuários redundantes não foram atribuídas para outros usuários?

12 - Nos contratos dos funcionários foram inseridas clausulas para acessos não autorizadas?

7.2.2 GERENCIAMENTO DE PRIVILÉGIOS

1 - A concessão de privilégios é restrito e controlado?

2 - Sistemas multiusuário possui um processo formal de autorização para privilégios?

7.2.3 GERENCIAMENTO DE SENHA DOS USUÁRIOS

1 - Existe um processo de gerenciamento formal para concessão de senhas?

2 - É solicitada a assinatura dos usuários para que mantenham a confidencialidade de suas senhas?

3 - Quando entrega de uma senha temporária para um usuário, este a altera imediatamente?

4 - Senhas temporárias são entregues de forma segura aos usuários?

5 - As senhas são armazenadas de forma segura?

7.2.4 ANÁLISE CRÍTICA DOS DIREITOS DE ACESSO DO USUÁRIO

1 - Os direitos de acesso dos usuários é analisado periodicamente?

2 - Os direitos de acesso privilegiado é analisado com mais freqüência do que aquelas com acesso geral?

7.3 RESPONSABILIDADE DO USUÁRIO

7.3.1 USO DE SENHAS

1 - Os usuários são informados para manter a confidencialidade das senhas?

2 - Os usuários matem suas senhas registradas em papel?

3 - São selecionadas senhas de qualidade?

Obs.: Com no mínimo seis caracteres, fáceis de lembrar, sem relação com coisas óbvias, caracteres diferentes.

4 - É exigida troca periódica das senhas dos usuários?

5 - Senhas temporárias são alteradas no primeiro acesso ao sistema?

6 - Os usuários são informados para não compartilhar senhas individuais?

7 - As senhas são incluídas em processo automático?

Obs.: Armazenadas em macros, ou teclas de função.

7.3.2 EQUIPAMENTOS DE USUÁRIO SEM MONITORAÇÃO

1 - Os usuários são orientados para encerrar sessões ativas, quando não possui proteção de tela?

2 - É Efetuada desconexão de computador de grande porte quando a sessão é finalizada?

3 - Microcomputadores ou terminais são protegidas por tecla de bloqueio ou senha quando não estão em uso?

7.4 CONTROLE DE ACESSO À REDE

7.4.1 POLÍTICA DE UTILIZAÇÃO DOS SERVIÇOS DE REDE

1 - Os usuários possuem acesso somente aos serviços que estão autorizados?

7.4.2 ROTA DE REDE OBRIGATÓRIA

1 - O caminho do usuário ao serviço do computador é controlado?

2 - As opções do menu e subimento é limitada para usuários individuais?

3 - São utilizados na organização *gateways* de segurança como os *firewalls*?

7.4.3 AUTENTICAÇÃO PARA CONEXÃO EXTERNA DO USUÁRIO

1 - Acesso de usuários remotos estão sujeitos a autenticação?

Obs.: Técnicas como a criptografia.

7.4.4 AUTENTICAÇÃO DE NÓ

1 - Conexões a sistemas remotos de computadores são autenticados?

7.4.5 PROTEÇÃO DE PORTAS DE DIAGNÓSTICO REMOTAS

1 - O acesso às portas de diagnóstico são seguramente controlados?

7.4.6 SEGREGAÇÃO DE REDES

1 - Para segregação de grupos de serviço de informação é considerada a introdução de controles na rede?

7.4.7 CONTROLE DE CONEXÕES DE REDE

1 - A organização possui redes compartilhadas que se estendem além dos limites físicos da organização?

2 - São incorporados controles que limitem a capacidade de conexão dos usuários?

7.4.8 CONTROLE DO ROTEAMENTO DE REDE

1 - Para redes compartilhadas são utilizados controle de roteamento?

2 - Os controles de roteamento são baseados em fontes confiáveis e mecanismos de checagem de endereço de destino?

3 - São utilizados tradutores de endereço?

4 - Os implementadores estão cientes do poder de qualquer mecanismo utilizado?

7.4.9 SEGURANÇA DOS SERVIÇOS DE REDE

1 - A organização utiliza serviços de rede?

2 - A organização está assegurada da descrição dos atributos de segurança de todos os serviços usados?

7.5 CONTROLE DE ACESSO AO SISTEMA OPERACIONAL

7.5.1 IDENTIFICAÇÃO AUTOMÁTICA DE TERMINAL

1 - É utilizada identificação automática de terminal para conexões locais específicas e para equipamento portáteis?

7.5.2 PROCEDIMENTOS DE ENTRADA NO SISTEMA *(LOG-ON)*

1 - Para entrar nos sistemas da organização é utilizado um processo seguro de entrada *(log-on)*?

2 - O procedimento de entrada mostra identificadores de sistema antes da entrada no sistema *(log-on)*?

3 - É mostrada mensagem que somente pessoas autorizadas tenham acesso ao computador?

4 - É fornecida ajuda para entrar no sistema?

5 - É limitada a tentativa de acesso no sistema?

6 - É limitado o tempo máximo e mínimo de acesso no sistema?

7 - São mostradas informações de entrada no sistema?

Obs.: Data e hora da última entrada, detalhes das tentativas sem sucesso.

7.5.3 IDENTIFICAÇÃO E AUTENTICAÇÃO DE USUÁRIO

1 - Todos os usuários dos sistemas possuem identificadores pessoais (ID)?

2 - São mostrados os privilégios do usuário?

3 - Quando da utilização de um ID para um grupo de usuários este é aprovado pelo gestor?

7.5.4 SISTEMA DE GERENCIAMENTO DE SENHAS

1 - O sistema de gerenciamento de senhas proporciona facilidade interativa e eficaz que assegura senha de qualidade?

2 - É obrigada a utilização de senhas individuais para manter responsabilidades?

3 - Os usuários estão autorizados a alterar suas senhas quando bem assim entenderem?

4 - É mantido o registro das senhas anteriores utilizadas?

5 - As senhas são visíveis quando digitadas?

6 - As senhas são armazenadas separadamente dos dados de sistemas e de aplicação?

7 - As senhas são armazenadas utilizando algoritmo de criptografia?

8 - As senhas padrão fornecidas pelo fabricante são alteradas?

7.5.5 USO DE PROGRAMAS UTILITÁRIOS

1 - A utilização de programas utilitários passa por um procedimento de autorização?

2 - Existe separação dos sistemas utilitários para os *softwares* de aplicação?

3 - A utilização dos programas utilitários é liberada somente para usuários confiáveis e autorizados?

4 - A utilização dos programas utilitários para uso particular, passa por processo de autorização?

5 - São registrados todos utilitários de sistema?

6 - É limitada a disponibilidade dos utilitários de sistema?

7 - É definida através de documento os níveis de autorização dos utilitários de sistema?

8 - É removido todos *softwares* utilitários e de sistemas desnecessários?

7.5.6 ALARME DE INTIMIDAÇÃO PARA A SALVAGUARDA DE USUÁRIOS

1 - São providos na organização alarme de intimidação?

2 - É avaliado os riscos na decisão de implantação de um alarme?

3 - São definidos responsabilidades e procedimento quanto ao alarme de intimidação?

7.5.7 DESCONEXÃO DE TERMINAL POR INATIVIDADE

1 - Terminais inativos em locais de alto risco, são desligados automaticamente após um período pré-determinado de inatividade?

Obs.: Prevenção de acesso não autorizado.

7.5.8 LIMITAÇÃO DO TEMPO DE CONEXÃO

1 - Existe limitação de horários de conexão a sistemas sensíveis?

2 - Existe restrição dos horários de conexão somente nas horas normais?

7.6 CONTROLE DE ACESSO ÀS APLICAÇÕES

7.6.1 RESTRIÇÕES DE ACESSO À INFORMAÇÃO

1 - São fornecidos menus para controlar o acesso as funções dos sistemas de aplicação?

2 - O conhecimento de função ou informações de aplicação é restrito?

3 - É controlado o direito dos acessos?

4 - É assegurado que as saídas são relevantes somente ao uso em questão?

7.6.2 ISOLAMENTO DE SISTEMAS SENSÍVEIS

1 - Sistemas sensíveis estão em ambiente isolado?

2 - A sensibilidade do sistema de aplicação é explicitamente identificada e documentada pelo proprietário?

3 - Quando a aplicação sensível é executada em ambiente compartilhado, são identificados quais são os sistemas de aplicação que irão compartilhar os recursos?

4 - Quando existe o compartilhamento de recursos, este é aprovado pelo proprietário de aplicação sensível?

7.7 MONITORAÇÃO DO USO E ACESSO AO SISTEMA

7.7.1 REGISTRO *(LOG)* DE EVENTOS

1 - Na organização é mantida trilha de auditoria de segurança?

2 - O *Log* possui a identificação do usuário?

3 - O *Log* possui registro das datas e horas de entrada e saída?

4 - O *Log* mantém a identidade do terminal?

5 - O *Log* mantém o acesso ao sistema aceito ou rejeitado?

7.7.2 MONITORAÇÃO DO USO DO SISTEMA

7.7.2.1 Procedimentos e áreas de risco

1 - São estabelecidos procedimentos e monitoração dos recursos de processamento da informação?

2 - É monitorado quais acesso foram autorizados?

3 - É monitorado as operações privilegiadas?

4 - É monitorado as tentativas de acesso não autorizado?

5 - É monitorado os alertas e falhas do sistema?

7.7.2.2 Fatores de risco

1 - As atividades de monitoração são analisadas em intervalos regulares?

7.7.2.3 Registro e análise crítica dos eventos

1 - A organização possui um segundo registro de *log* com as mensagens mais importantes?

Obs.: *Logs* podem conter grandes volumes de informação.

2 - É dada atenção especial à segurança dos recursos de registros (*Log*), contra adulteração?

7.7.3 SINCRONIZAÇÃO DOS RELÓGIOS

1 - Os relógios dos computadores estão ajustado na hora certa?

2 - Estes relógios passam por um ajuste periodicamente contra os atrasos que eles podem representar?

7.8 COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

7.8.1 COMPUTAÇÃO MÓVEL

1 - Na organização é estabelecida uma política formal do uso de computação móvel?

2 - São estabelecidos proteções para evitar o acesso não autorizado ou divulgação das informações armazenadas neste recurso?

3 - Os equipamentos estão disponíveis para possibilitar recuperação rápida e fácil das informações em caso roubo ou perda de informações?

4 - Quando ocorre a necessidade de conexão a rede existe um processo de identificação e autenticação?

5 - Os recursos de computação móvel estão protegidos contra roubo?

6 - O grupo de trabalho é conscientizado quanto aos riscos desta forma de trabalho e os controles necessários?

7.8.2 TRABALHO REMOTO

1 - Existe um processo de proteção apropriada para trabalho remoto?

2 - A autorização e controle para o acesso remoto parte do gestor?

3 - A segurança física do local de trabalho é analisada?

4 - O tipo de informação que vai trafegar é conhecida?

5 - Existe controle de acesso não autorizado?

6 - São verificados a mobília necessária para as atividades?

7 - São analisados as horas de trabalho?

8 - É verificada a segurança física?

9 - É previsto o suporte e manutenção do equipamento?

10 - São feitas cópias de segurança?

11 - A segurança é auditada e monitorada?

12 - Quando cessa as atividades de trabalho remoto o equipamento passa por um processo de devolução?

8 DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

8.1 REQUISITOS DE SEGURANÇA DE SISTEMAS

8.1.1 ANÁLISE E ESPECIFICAÇÃO DOS REQUISITOS DE SEGURANÇA

1 - Na especificação de requisitos de novos sistemas, os são especificados controles?

8.2 SEGURANÇA NOS SISTEMAS DE APLICAÇÃO

8.2.1 VALIDAÇÃO DE DADOS DE ENTRADA

1 - Os dados de entrada são validados, para garantir que estão corretos e apropriados?

2 - Os arquivos de dados passam por análise crítica para confirmar sua validade e integridade?

3 - Existem procedimentos á validação de erros?

4 - São definidos responsabilidade para o processo de entrada de dados?

8.2.2 CONTROLE DO PROCESSAMENTO INTERNO

8.2.2.1 Áreas de risco

1 - São feitos controles de sessão ou processamento em lote?

2 - São feitos controles de balanceamento?

3 - Os dados gerados pelo sistema são validados?

4 - A integridade dos dados são validados?

5 - Os programas de aplicação são executados no horário correto?

6 - É feita checagem para garantir que os programas estão sendo executados na ordem correta?

7 - É feita checagem para garantir que os programas estão terminando em caso de falha?

8 - É feita checagem para garantir que o processamento ficará suspenso até que o problema seja resolvido?

8.2.3 VALIDAÇÃO DOS DADOS DE SAÍDA

1 - Os dados de saída são validados por verificar se o processo de armazenamento está correto?

2 - É verificado se o dado de saída é razoável?

3 - É verificada se as informações de saída são suficientes para um leitor?

4 - Existe a definição de responsabilidades de todo pessoal envolvido na saída de dados?

8.3 CONTROLES DE CRIPTOGRAFIA

8.3.1 POLÍTICA PARA O USO DE CONTROLES DE CRIPTOGRAFIA

1 - Uma avaliação de riscos é executada para saber o nível de proteção a ser utilizada para a informação?

8.3.2 CRIPTOGRAFIA

1 - É considerada a proteção de informações críticas ou sensíveis através da codificação?

2 - As regulamentações e restrições nacionais para utilização de técnica de criptográfica é consultada para poder codificar a informação?

3 - É utilizada assessoria especializada para saber qual o nível de proteção a ser utilizada sobre a informação?

8.3.3 ASSINATURA DIGITAL

1 - Na utilização de assinatura digital a chave é mantida em segredo?

2 - As assinaturas digitais possuem chave criptográfica diferente daquela usadas na criptografia?

3 - Na utilização da assinatura digital a legislação é consultada para saber seu valor legal?

8.3.4 SERVIÇOS DE NÃO REPÚDIO

1 - Quando ocorrem disputas sobre a ocorrência ou não de alguma ação são utilizados serviços de não repudio?

8.3.5 GERENCIAMENTO DE CHAVES

8.3.5.1 Proteção de chaves criptográficas

1 - A organização possui um sistema de gerenciamento de chaves de acesso?

8.3.5.2 Normas, procedimentos e métodos

1 - A organização possui um sistema de gerenciamento de chaves baseados em normas procedimento e métodos seguros?

2 - As chaves possuem data de ativação e desativação definidas?

3 - Chaves públicas são geradas de tal maneira que elas relacionam as informações do proprietário do par de chaves pública/privada com chave pública considerada?

4 - O processo para geração de chaves é implementado por uma autoridade certificadora de confiança?

8.4 SEGURANÇA DE ARQUIVOS DO SISTEMA

8.4.1 CONTROLE DE *SOFTWARE* EM PRODUÇÃO

1 - A atualização de bibliotecas está sob responsabilidade de apenas uma pessoa?

2 - A organização mantém apenas o código executável do sistema operacional?

3 - Antes da implantação, o sistema operacional passa por teste e a aceitação do usuário, com as bibliotecas atualizadas?

4 - É mantido um *log* das atualizações das bibliotecas?

5 - As versões anteriores são retidas como medida de contingência?

6 - Quando existe necessidade de atualização, é verificada a segurança da versão?

7 - As correções de *software* são aplicadas quando existe a probabilidade de aumento da segurança?

8 - O acesso físico ou lógico de fornecedores é dado somente quando existe a necessidade de suporte e autorização da gerência?

9 - As atividade desses fornecedores é monitorado?

8.4.2 PROTEÇÃO DE DADOS DE TESTE DO SISTEMA

1 - É evitado o uso da base de dados da produção para testes?

2 - O controle de acesso para base de dados da produção é o mesmo aplicado para base de dados teste?

3 - Existe uma autorização quando uma informação da produção for copiada para teste?

4 - Quando da finalização dos testes, a base de dados teste é apagada?

5 - A cópia e uso de informações da base de dados teste é registrado para auditoria futura?

8.4.3 CONTROLE DE ACESSO A BIBLIOTECAS DE PROGRAMA-FONTE

1 - As bibliotecas de programas fonte são manipuladas pelo ambiente de produção?

2 - Existe um responsável designado pela biblioteca de programas fontes de cada aplicação?

3 - O pessoal de suporte e tecnologia possui acesso ilimitado as bibliotecas de código fontes?

4 - Os programas em desenvolvimento ou manutenção estão separadas das bibliotecas de programas fonte em produção?

5 - A atualização das bibliotecas de programas fontes e distribuição é feita somente pelo responsável da biblioteca?

6 - As listas de programa fontes é mantido em ambiente seguro?

7 - É mantido registro das atualizações das bibliotecas?

8 - As versões antigas de programas fontes são arquivadas por data e hora com informações relevantes referente ao seu uso?

9 - Manutenção e cópia de bibliotecas de programas fontes, estão sujeitas a procedimentos rígidos de controle de mudança?

8.5 SEGURANÇA NOS PROCESSOS DE DESENVOLVIMENTO E SUPORTE

8.5.1 PROCEDIMENTOS DE CONTROLE DE MUDANÇAS

1 - Existe um controle rígido sobre a implementação de mudanças?

2 - Procedimentos de mudança garantem que procedimentos de segurança e controle não serão comprometidos?

3 - Os programadores de suporte tem acesso somente às partes do sistema que irão trabalhar?

4 - É mantido um registro dos níveis de autorização?

5 - É garantido que as mudanças são feitas pro usuários autorizados?

6 - É analisada criticamente os controles e a integridade dos procedimentos?

7 - Existe uma aprovação formal antes do início dos trabalhos?

8 - O usuário é consultado para garantir sua aceitação antes do inicio dos trabalhos?

9 - A implementação garante o mínimo de transtorno para o negócio?

10 - A documentação é atualizada a cada modificação feita?

11 - A documentação antiga é destruída ou arquivada?

12 - É mantido controle da versão?

13 - É mantida uma trilha de auditoria para todas atualizações de *software*?

14 - A organização matem separada o ambiente de teste o ambiente de desenvolvimento e produção?

8.5.2 ANÁLISE CRÍTICA DAS MUDANÇAS TÉCNICAS DO SISTEMA OPERACIONAL DA PRODUÇÃO

1 - Quando existem modificações no sistema operacional estas modificações são analisadas e testadas para garantir que não ocorrerá nenhum impacto na produção ou na segurança?

8.5.3 RESTRIÇÕES NAS MUDANÇAS DOS PACOTES DE *SOFTWARE*

1 - Modificações dos pacotes de *software* são desencorajadas?

2 - Se for necessária à modificação, é verificado o comprometimento dos controles e a integridade dos processos?

3 - O *software* original é mantido como cópia?

4 - As modificações são testadas e documentadas?

8.5.4 *COVERT CHANNELS* E CAVALO DE TRÓIA

1 - A aquisição de programas é feita de fontes conhecidas e idôneas?

2 - É comprado programas fontes, onde o código possa ser verificado?

3 - É utilizado produtos que já foram analisados?

4 - É controlado o acesso ao código uma vez já instalado?

5 - É utilizado pessoal de confiança para trabalhar com os sistemas chave?

8.5.5 DESENVOLVIMENTO TERCEIRIZADO DE *SOFTWARE*

1 - A organização faz um acordo sobre as licenças, propriedade de código?

2 - O trabalho é certificado e a qualidade verificada?

3 - São feitos acordos caso há uma falha de prestador de serviços?

4 - São verificados requisitos contratuais para a qualidade de código?

5 - O *software* é testado para detecção de cavalos de tróia?

9 GESTÃO DA CONTINUIDADE DO NEGÓCIO

9.1 ASPECTOS DA GESTÃO DA CONTINUIDADE DO NEGÓCIO

9.1.1 PROCESSO DE GESTÃO DA CONTINUIDADE DO NEGÓCIO

1 - São verificados os riscos em que a organização está exposta?

2 - A organização está ciente dos impactos que interrupções terão sobre os negócios?

3 - São estabelecidos os objetivos de negócio quanto às instalações e recursos de processamento da informação?

4 - É considerado a contratação de um seguro compatível fazendo parte do processo de continuidade?

5 - Está definida e documentada a estratégia para o plano de continuidade?

6 - São testados e atualizados regularmente os planos e procedimentos implementados?

7 - É garantida que a gestão de continuidade de negócio esteja incorporada aos processos e estrutura da organização?

9.1.2 CONTINUIDADE DO NEGÓCIO E ANÁLISE DE IMPACTO

1 - O plano de continuidade teve seu ponto de partida na identificação dos eventos que podem causar interrupções nos processo do negócio?

2 - É feita uma avaliação para os impactos destas interrupções?

3 - As atividades de avaliação conta com o envolvimento dos responsáveis pelos processos e recursos de negócio?

4 - É desenvolvido um plano estratégico para determinar a abordagem mais abrangente a ser adotada para a continuidade do negócio?

5 - O plano é validado pela direção?

9.1.3 DOCUMENTANDO E IMPLEMENTANDO PLANOS DE CONTINUIDADE

1 - A organização desenvolve planos para manutenção ou recuperação das operações do negócio?

2 - São levantadas todas as responsabilidades e procedimentos de emergência?

3 - Os procedimentos de emergência são implantados para que a recuperação ocorra dentro dos prazos?

4 - Os processos são documentados e acordados?

5 - O pessoal é treinado para os procedimentos e processo de emergência levantada e o gerenciamento da crise?

6 - Os planos são testados e atualizados?

7 - O planejamento está focado para os objetivos do negócio?

8 - Todos os serviços e recursos estão previstos para a recuperação?

9.1.4 ESTRUTURA DO PLANO DE CONTINUIDADE DO NEGÓCIO

1 - É mantida uma estrutura básica de plano de continuidade do negócio?

2 - Os planos de continuidade possuem claramente identificados às condições de sua ativação?

3 - Quando existe a identificação de novos requisitos os procedimentos de emergência são ajustados de forma apropriada?

4 - Nos procedimentos de emergência estão descritos as ações a serem tomadas em caso de risco das operações do negócio e/ou vidas humanas?

5 - Nos procedimentos de recuperação estão descritas as ações necessárias para transferir as atividades essenciais para localidade alternativas?

6 - Nos procedimentos de recuperação estão descritos as ações para o restabelecimento das operações?

7 - Existe uma programação de manutenção dos planos?

8 - Existe o desenvolvimento de atividades educativas para assegurar a continuidade dos processos?

9 - São designados responsabilidades e suplentes pela execução dos itens do plano?

9.1.5 TESTES, MANUTENÇÃO E REAVALIAÇÃO DOS PLANOS DE CONTINUIDADE DO NEGÓCIO

9.1.5.1 Teste dos planos

1 - Os planos são testado regularmente?

2 - É assegurado que nos teste os membros da equipe saibam da importância dos planos?

3 - O plano de continuidade indica como e quando cada item deve ser testado?

4 - Componentes isolados dos planos são testado freqüentemente?

5 - São utilizados teste de mesa com diferentes cenários?

6 - São feitas simulações?

7 - São feitos testes de recuperação técnica?

8 - São feitos teste em locais alternativos?

9 - São feitos testes dos recursos, serviços e instalações dos fornecedores?

10 - É feito um ensaio geral da equipe?

9.1.5.2 Manutenção e reavaliação dos planos

1 - Os planos de continuidade passam por analises críticas regulares a atualizações?

2 - São incluídos procedimentos de gerenciamento de mudanças da organização?

3 - A responsabilidade pela analise crítica periódica de cada parte do plano está definida e estabelecida?

4 - Na identificação de mudanças, o plano de continuidade de negócio passa por uma atualização?

10 CONFORMIDADE

10.1 CONFORMIDADE COM REQUISITOS LEGAIS

10.1.1 IDENTIFICAÇÃO DA LEGISLAÇÃO VIGENTE

1 - A organização possui explicitamente definidos para cada sistema de informação os estatutos, regulamentações ou cláusulas contratuais?

2 - A organização possui documentados para cada sistema de informação os estatutos, regulamentações ou cláusulas contratuais?

3 - Os controles e as responsabilidades referente à legislação vigente estão definidos e documentados?

10.1.2 DIREITOS DE PROPRIEDADE INTELECTUAL

10.1.2.1 Direitos autorais

1 - São implementados procedimentos para garantir a conformidade com os direitos autorais?

10.1.2.2 Direitos autorais de *software*

1 - É divulgada uma política de conformidade de direito autoral de *software*?

2 - São emitidos padrões para procedimentos de aquisição de produtos de *software*?

3 - Existe uma política de aquisição e de direitos autorais de *software* e ações para quem viola essas políticas?

4 - Os registros são mantidos adequadamente?

5 - São mantidos evidências de propriedade?

6 - Os controles asseguram que o número de usuários não vai ultrapassar o número de licenças?

7 - São verificados que somente *software* licenciados serão instalados?

8 - É estabelecida uma política para manutenção de licenças?

9 - É estabelecida uma política para disposição ou transferência para outros?

10 - São utilizadas ferramentas de auditoria apropriadas?

10.1.3 SALVAGUARDA DE REGISTROS ORGANIZACIONAIS

1 - Os registros importantes da organização são protegidos contra perda, destruição e falsificação?

2 - Os registros são categorizados em tipo de registro?

3 - As chaves criptográficas relacionadas com arquivos citados ou assinaturas digitais são mantidas de forma segura e disponibilizadas somente ao pessoal autorizado?

4 - Procedimentos de armazenamento e tratamento de mídias são implementados conforme a recomendação dos fabricantes?

5 - O acesso a mídias eletrônicas armazenadas possuem procedimentos que garantam acesso aos seus dados na mudança da tecnologia?

6 - O armazenamento dos dados é feita de tal maneira que possa ser recuperado de forma aceitável pelo tribunal de justiça?

7 - Os registros são claramente identificados com seus períodos?

8 - É permitida a destruição dos registros logo após o sue período de armazenamento?

10.1.4 PREVENÇÃO CONTRA USO DE RECURSOS DE PROCESSAMENTO DA INFORMAÇÃO

1 - O uso dos recursos de processamento da informação para propósito não profissional ou não autorizado, é considerado como uso impróprio?

2 - As atividades de uso impróprio quando descobertas são levados ao gestor responsável e ações cabíveis são tomadas?

3 - Os funcionários de uma organização estão cientes que nenhum acesso é permitido, com exceção daqueles que foram autorizados?

4 - No momento da conexão inicial no sistema é apresentada uma mensagem referente ao acesso privado e exige a aprovação do usuário?

10.1.5 REGULAMENTAÇÃO DE CONTROLES DE CRIPTOGRAFIA

1 - É obtida assessoria jurídica para garantir a conformidade com a legislação nacional vigente?

2 - É obtida assessoria jurídica para transferir informações para outros países?

10.1.6 COLETA DE EVIDÊNCIAS

10.1.6.1 Regras para evidências

1 - Se existir a necessidade de apoiar um processo jurídico são colhidas evidências para tal?

2 - As evidencias são verificadas perante sua admissibilidade?

3 - As evidencias são verificadas perante sua importância?

4 - As evidencias são verificadas se estavam operando correta e consistentemente?

10.1.6.2 Qualidade e inteireza da evidência

1 - Os documentos em papel são mantidos de forma segura, com registro de que encontro, onde foi encontrado, quando e quem testemunhou?

2 - As investigações garantem os originais contra adulteração?

3 - São obtidas cópias de mídia para garantir a disponibilidade?

4 - É mantido registro e acompanhamento de todo o processo?

5 - É feita uma cópia e mantida em segurança?

6 - Tão logo que seja constatado a possibilidade de processo jurídico, a polícia ou advogado é consultado?

10.2 ANÁLISE CRÍTICA DA POLÍTICA DE SEGURANÇA E DA CONFORMIDADE TÉCNICA

10.2.1 CONFORMIDADE COM A POLÍTICA DE SEGURANÇA

1 - Os procedimentos de segurança são avaliados pelos gestores para garantir que estão sendo executados corretamente?

2 - Todos as áreas na organização passam por análise crítica periódica?

3 - Análises críticas são apoiados pelos proprietários dos sistemas de informação?

10.2.2 VERIFICAÇÃO DA CONFORMIDADE TÉCNICA

1 - Os sistemas de informação são periodicamente verificados em sua conformidade com as normas de segurança implementados?

2 - Esta verificação é feita por engenheiro de sistemas experiente o por funções de *software* que gerem relatório técnico?

3 - Cuidados são tomados em teste de invasão para que não comprometa a segurança dos sistemas?

4 - As verificações são executadas por pessoas competentes e autorizadas?

10.3 CONSIDERAÇÕES QUANTO À AUDITORIA DE SISTEMAS

10.3.1 CONTROLES DE AUDITORIA DE SISTEMA

1 - Os requisitos de auditorias são acordados com o nível apropriado da direção?

2 - O escopo da verificação é acordado e controlado?

3 - A verificação se limita somente à leitura de *software* de dados?

4 - Os recursos de tecnologia estão identificados e disponíveis?

5 - Requisitos para processamento adicional ou especial são identificados e acordados?

6 - O acesso é monitorado e registrado para produzir uma trilha de referência?

7 - Os procedimentos, requerimentos e responsabilidades são documentadas?

10.3.2 PROTEÇÃO DAS FERRAMENTAS DE AUDITORIA DE SISTEMAS

1 - As ferramentas de auditoria de sistemas são protegidas contra qualquer possibilidade de uso impróprio ou comprometimentos?

2 - Estas ferramentas estão separadas de sistemas em desenvolvimento e em operação, como não são mantidos em fitas de bibliotecas ou áreas de usuários?

ANEXO B: PARTE DO CÓDIGO FONTE DA CLASSE DE REFERÊNCIAS

Como descrito nos capítulos anteriores, o objetivo deste anexo é trazer a implementação de uma classe desenvolvida para o protótipo. Foi selecionada a classe de referências por ser uma classe padrão de desenvolvimento para as outras classes. O quadro 6.1 mostra a classe com seus atributos e métodos.

Quadro 6.1 – Classe com seus atributos e métodos

```
   TReferencias = class
   private
      Codigo : Longint;
      Descricao : String;
      URL : String;
      Observacao : String;
      TabReferencias : TTable;
   public
      constructor Create;
      destructor Destroy; override;

      function Verificar_Referencia(pCodigo:Longint):Boolean;

      procedure Gravar_Referencia(pDescricao : String;
                                  pURL : String;
                                  pObservacao : String);
   end;
```

Nesta classe verificamos os atributos e também seus métodos. O acesso físico a tabela de referências é feito através da variável `TabReferencias` que é do tipo `TTable`, padrão do Delphi, sendo que esta variável, como os seus atributos estão sendo declarados como privados, o que significa dizer, que a interface que instanciar esta classe não terá acesso direto a estas informações, e sim se precisar, através da criação de métodos, que terão que ser colocados no publico. No Quadro 6.2 são mostrados trechos da implementação desta classe.

Quadro 6.2 – Implementação dos métodos

```
resourcestring
  STR_CODIGO = 'CODIGO';
  STR_DESCRICAO = 'DESCRICAO';
  STR_URL = 'URL';
  STR_OBSERVACAO = 'OBSERVACAO';

{ TReferencias }

//metodo de criacao da classe de referências
constructor TReferencias.Create;
begin
  inherited Create;

  TabReferencias := TTable.Create(TabReferencias);
  TabReferencias.DatabaseName := 'TCC';
  TabReferencias.TableName    := 'REFERENCIAS';
```

```
  TabReferencias.Active       := True;
end;

//método de liberação da classe de referência
destructor TReferencias.Destroy;
begin
  TabReferencias.Active := False;
  TabReferencias.Free;

  inherited Destroy;
end;

//método para gravar uma referência
procedure TReferencias.Gravar_Referencia(pDescricao : String;
                                         pURL : String;
                                         pObservacao : String);

  procedure Carrega_Classe_Tabela;
  begin
    //código é autoincrement
    TabReferencias.FieldByName(STR_DESCRICAO).AsString  := pDescricao;
    TabReferencias.FieldByName(STR_URL).AsString        := pURL;
    TabReferencias.FieldByName(STR_OBSERVACAO).AsString := pObservacao;
  end;

begin
  If  Self.Verificar_Referencia(Self.Codigo) Then
      Begin
        TabReferencias.Edit;
        Carrega_Classe_Tabela;
        TabReferencias.Post;
        ShowMessage('Referência alterada com sucesso !');
      End
  Else
      Begin
        TabReferencias.Insert;
        TabReferencias.FieldByName(STR_CODIGO).AsInteger := 0;
        Carrega_Classe_Tabela;
        TabReferencias.Post;
        ShowMessage('Referência cadastrada com sucesso !');
      End;
end;

//verifica se o codigo da referencia existe
function TReferencias.Verificar_Referencia(pCodigo:Integer): Boolean;
begin
  Result := TabReferencias.FindKey([pCodigo]);
  if   Result then
       Self.CarregarCampos;
end;
```

No quadro 6.2, verifica-se a utilização de `resourcestring` que são constantes utilizadas para definir os nomes dos campos da tabela. Estes campos são utilizados juntamente com a variável `TabReferencias`, que faz todos acessos ao Banco de Dados, para gravar e verificar.